Στον πατέρα μου και τη μάνα μου,
για τις σπουδές που δεν μπόρεσαν να κάνουν

… Κι από την ανάποδη

φοριέται η φαντασία

και σ' όλα τα μεγέθη της

Οδυσσέας Ελύτης, «Απόκριες»

ΕΥΧΑΡΙΣΤΙΕΣ

Η εκπόνηση διδακτορικής διατριβής είναι μια μάχη με τον εαυτό σου. Με είχαν προειδοποιήσει για αυτό αρκετοί καλοί μου φίλοι, οι οποίοι είχαν περάσει πριν από εμένα αυτήν την διαδικασία. Και σε μια μάχη κανείς δεν μπορεί να είναι μόνος...

Και, βεβαίως, δεν ήμουν μόνος. Είμαι πολύ τυχερός γιατί στάθηκαν δίπλα μου σε αυτή τη μάχη πολλοί και σημαντικοί άνθρωποι – τόσοι πολλοί που, τώρα που γράφω αυτές τις γραμμές, φοβάμαι ότι θα ξεχάσω αρκετούς. Φέρνοντας στο μυαλό μου ένα-ένα πολλά χαμογελαστά πρόσωπα βλέπω ότι όλοι αυτοί έχουν πολλές διαφορές μεταξύ τους αλλά ένα κοινό χαρακτηριστικό. Ξέρουν να αγαπούν...

Ο Καθηγητής μου Νέστωρ Κουράκης, επιβλέπων αυτής της διδακτορικής διατριβής, έδωσε με τα σοφά λόγια του τη δύναμη στις σκέψεις μου να βγουν στο χαρτί. Με ενθάρρυνε, με «μάλωσε», μα πάνω απ' όλα με εμπιστεύθηκε. Ας μου επιτρέπει να τον νιώθω «πνευματικό μου πατέρα».

Οι αγαπημένοι μου Καθηγητές Μαρία Κρανιδιώτη και Δημήτρης Κιούπης είχαν πάντοτε ορθάνοιχτη την πόρτα τους για να μου λύσουν απορίες ή να ακούσουν τους προβληματισμούς μου.

Κατά τη συγγραφή αυτού του πονήματος ήρθαν στο μυαλό μου όλοι οι Καθηγητές μου στον Τομέα Ποινικών Επιστημών της Νομικής Αθηνών, καθώς σε ανύποπτες στιγμές θυμόμουν διδαχές και συμβουλές τους...

Ο Καθηγητής στο ΑΤΕΙ Μεσολογγίου Χρήστος Τσουραμάνης ήταν αυτός που με «μύησε» στο ηλεκτρονικό έγκλημα όταν μου χάρισε το βιβλίο του «Ψηφιακή παραβατικότητα», το πρώτο σχετικό βιβλίο που διάβασα... Μετά μου χάρισε και πολλά άλλα βιβλία, τα οποία χρησιμοποίησα στη βιβλιογραφία!

Ο Δικηγόρος (LL.M.) και υπ. Δρ. Νομικής Αθηνών Απόστολος Γιαννακούλιας με υποδέχθηκε για μία εβδομάδα στο μικρό του δωμάτιο στην εστία του New York University στην Νέα Υόρκη και με βοήθησε στην αναζήτηση βιβλιογραφίας, την περίοδο που η εργασία αυτή βρισκόταν ακόμη στα σπάργανα. Κάποια χρόνια μετά,

όταν η διατριβή πλησίαζε στην ολοκλήρωσή της, ήταν ο ίδιος που με τα «μαγικά του χέρια» επιμελήθηκε λέξη-λέξη και με περισσή φροντίδα το κείμενο και τη μορφοποίησή του. Ένα «ευχαριστώ» είναι λίγο...

Ο Δρ. ρομποτικής Στέφανος Δολτσίνης και ο Συμβολαιογράφος (LL.M.) Παύλος Γανιάρης μου υπέδειξαν την προκήρυξη της υποτροφίας του προγράμματος «ΗΡΑΚΛΕΙΤΟΣ ΙΙ» ένα βράδυ εξόδου μου από τον στρατό.

Η Δικηγόρος Πέγκυ Προβατάρη μαζί με τη Δικηγόρο (LL.M.) Μαριέττα Βαρβέρη κράτησαν «όρθιο» το δικηγορικό μου γραφείο παλεύοντας καθημερινά στα δικαστήρια ενώ εγώ ήμουν απών προκειμένου να εκπονήσω τη διατριβή αυτή.

Η ερευνητική μου ομάδα που συγκροτήθηκε από μέλη του Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών (Διευθυντής: Καθηγητής Νέστωρ Κουράκης) και του Σπουδαστηρίου Κοινωνικών Μελετών του ΑΤΕΙ Δυτικής Ελλάδος (Διευθυντής: Καθηγητής Χρήστος Τσουραμάνης) και στην οποία συμμετείχαν οι εξής: Ευαγγελία Ανδρουλάκη (δικηγόρος – υπ. ΜΔΕ Εγκληματολογίας Παντείου Πανεπιστημίου), Καλλιόπη Πιτερού (δικηγόρος – ποινικολόγος – ΜΔΕ Παντείου Πανεπιστημίου), Φώτης Δασκαλάκης (τεχνικός ασφαλείας δικτύων – διαχειριστής ηλεκτρονικών δεδομένων), Ιωάννα Καρναχωρίτη (φοιτήτρια Νομικής Αθηνών) και ο Ηλίας Πολυχρονιάδης [επιστήμονας πληροφορικής, τεχνικός ασφαλείας δικτύων (MSc) και πρώην συνεργάτης του CERN – εκεί που «γεννήθηκε» το διαδίκτυο - ως ειδικός επιστημονικός σύμβουλος της έρευνας σε θέματα τεχνολογίας και ασφάλειας ηλεκτρονικών δεδομένων και συστημάτων πληροφοριών]. Χωρίς τη συμμετοχή έστω και ενός εξ αυτών η έρευνα αυτή θα ήταν πολύ κατώτερη...

Φίλοι μου επιστήμονες που θαυμάζω (όπως ο Δρ. Πολιτικής Δικονομίας του Πανεπιστημίου της Κολωνίας Μιχάλης Μαρκουλάκης, ο Δρ. Ψυχιατρικής Παιδιών και Εφήβων Κωνσταντίνος Σιώμος, η υπ. Δρ. LSE Ιωάννα Γουσέτη, ο υπ. Δρ. τμήματος Νομικής Πανεπιστημίου Αθηνών Διονύσης Χιόνης, ο υπ. Δρ. τμήματος διεθνών και ευρωπαϊκών σπουδών Πανεπιστημίου Πειραιώς Κώστας Μπαλωμένος, ο υπ. Δρ. Παντείου Πανεπιστημίου Βαγγέλης Χαϊνάς και πολλοί άλλοι) άκουσαν με υπομονή όλα αυτά τα χρόνια τις ανασφάλειές μου και μου έδωσαν δύναμη να συνεχίσω...

Ένα εντυπωσιακό σύνολο 310 ανθρώπων διέθεσαν τον χρόνο τους για να συμμετάσχουν στο δείγμα της έρευνας. Θέλω ιδιαιτέρως να σταθώ στην Ελληνική Χάκινγκ Σκηνή, για την εμπιστοσύνη που μου επέδειξαν τα μέλη της.

Στα 25 χρόνια μου στα βιβλία και τα θρανία γνώρισα πολλούς δασκάλους. Όλοι αυτοί έχουν βάλει με τον τρόπο τους ένα λιθαράκι στο οικοδόμημα αυτής της διατριβής. Ιδιαίτερη μνεία θεωρώ ότι οφείλω στον δάσκαλο που μου δίδαξε αισθητική, τον μουσικό Σπύρο Χολέβα.

Άφησα για το τέλος την οικογένειά μου. Τον πατέρα μου Μπάμπη, τη μητέρα μου Γιάννα και την αδερφή μου Σοφία, οι οποίοι εδώ και τριάντα ένα συναπτά έτη προσπαθούν να διαχειριστούν τις «ανησυχίες» μου με μοναδικό τους στόχο να είμαι χαρούμενος.

Τα χρόνια αυτά δεν ήταν εύκολα. Προέκυψαν δυσκολίες: οικογενειακές, προσωπικές, επαγγελματικές. Η παρουσία, όμως, όλων αυτών των «συμπολεμιστών» δίπλα μου στον αγώνα όχι μόνο της διατριβής αλλά και της ζωής δεν άφησε περιθώρια εγκατάλειψης – παρουσία ανιδιοτελής, με μόνο κίνητρο την αγάπη. Τους ευχαριστώ όλους χιλιάδες φορές...

Βύρωνας, καλοκαίρι 2014

Φ.Σ.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Ελληνικό αλφάβητο

ά.	άρθρο
αγγλ.	αγγλικά
ΑΔΑΕ	Αρχή Διαφύλαξης Απορρήτου Επικοινωνιών
αδημ.	αδημοσίευτη δικαστική απόφαση
Α.Ε.Ι.	Ανώτατο Εκπαιδευτικό Ίδρυμα
ΑΠ	Άρειος Πάγος
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
απόφ.	Απόφαση
αρ.	αριθμός
Αρμεν.	Αρμενόπουλος (επιστημονικό περιοδικό – εκδ. Δικηγορικού Συλλόγου Θεσσαλονίκης)
ΑΣΟΕΕ	Ανώτατη Σχολή Οικονομικών και Εμπορικών Επιστημών (Οικονομικό Πανεπιστήμιο Αθηνών)
Α.Τ.Ε.Ι.	Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα
βλ.	βλέπε
γαλλ.	γαλλικά
ΓΕΕΘΑ	Γενικό Επιτελείο Εθνικής Άμυνας
γεν. εποπτ.	γενική εποπτεία
γερμ.	γερμανικά

Δ.Ε.Υ.	Διεύθυνση Εσωτερικών Υποθέσεων
δηλ.	δηλαδή
ΔιΜΕΕ	Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (επιστημονικό περιοδικό – εκδ. Νομική Βιβλιοθήκη)
ΔΠΘ	Δημοκρίτειο Πανεπιστήμιο Θράκης
Δρ.	Διδάκτωρ
δρχ.	δραχμή / -ές
ΔΣΑ	Δικηγορικός Σύλλογος Αθηνών
ΔΣΑΠΔ	Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα
ΕΒΕΑ	Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών
εδ.	εδάφιο
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΔΔΔ	Επιθεώρηση Δημοσίου Δικαίου και Διοικητικού Δικαίου (επιστημονικό περιοδικό – ιδιοκτήτης: Παναγιώτης Μετζελόπουλος)
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΚ	Ευρωπαϊκό Κοινοβούλιο
εκδ.	έκδοση / εκδόσεις
εκδ. επιμ.	εκδοτική επιμέλεια
ΕΚΠΑ	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
ΕΛ.ΑΣ.	Ελληνική Αστυνομία
Ε.Ο.Κ.	Ευρωπαϊκή Οικονομική Κοινότητα
επ.	επόμενα / επόμενες / επόμενοι

επιμ.	επιμέλεια
επισ.	επισυνάπτεται
επιστ.	επιστημονικός –ή – ό
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΕΣΣΔ	Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών
εφημ.	εφημερίδα
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
Η/Υ	ηλεκτρονικός υπολογιστής
Ι.Ε.Κ.	Ινστιτούτο Επαγγελματικής Κατάρτισης
κ.ά.	και άλλα / και άλλοι / και άλλες
Κ.Α.Π.Η.	Κέντρο Ανοιχτής Προστασίας Ηλικιωμένων
κ.λπ.	και λοιπά
ΚΝοΒ	Κώδικας Νομικού Βήματος (νομικό περιοδικό – εκδ. ΔΣΑ)
κ.ο.κ.	και ούτω καθεξής
ΚΠΔ	Κώδικας Ποινικής Δικονομίας
λατ.	λατινικά
λ.χ.	λόγου χάρη, λόγου χάριν
Μ.Δ.Ε.	Μεταπτυχιακό Δίπλωμα Ειδίκευσης
Μ.Μ.Ε.	Μέσα Μαζικής Ενημέρωσης
ν.	νόμος
Ναυτ. Πειρ.	Ναυτοδικείο Πειραιά
ΝοΒ	Νομικό Βήμα (επιστημονικό περιοδικό – έκδ. ΔΣΑ)
Ν.Π.Δ.Δ.	Νομικό Πρόσωπο Δημοσίου Δικαίου
Ν.Π.Ι.Δ.	Νομικό Πρόσωπο Ιδιωτικού Δικαίου

Ο.Η.Ε.	Οργανισμός Ηνωμένων Εθνών
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
όπ. π.	όπως παραπάνω
Ο.Τ.Α.	Οργανισμός Τοπικής Αυτοδιοίκησης
παρ.	παράγραφος
Π.Δ.	Προεδρικό Διάταγμα
περίπτ.	περίπτωση
ΠΕΙΡΝ	Πειραϊκή Νομολογία (επιστημονικό περιοδικό – εκδ. Νομική Βιβλιοθήκη σε συνεργασία με τον Δικηγορικό Σύλλογο Πειραιώς)
ΠΚ	Ποινικός Κώδικας
ΠοινΔικ	Ποινική Δικαιοσύνη (επιστημονικό περιοδικό - εκδ. Νομική Βιβλιοθήκη)
ΠοινΛόγος	Ποινικός Λόγος (επιστημονικό περιοδικό – εκδ. Αντ. Ν. Σάκκουλα)
ΠοινΧρ	Ποινικά Χρονικά (επιστημονικό περιοδικό – εκδ. Π. Ν. Σάκκουλα)
πρβλ.	παράβαλε
π.χ.	παραδείγματος χάριν / -η
Σ	Σύνταγμα
ΣΛΕΕ	Συνθήκη Λειτουργίας Ευρωπαϊκής Ένωσης
σ.σ.	σημείωση συντάκτη / συγγραφέα
στ.	στίχοι
σελ.	σελίδα / σελίδες
συν.	συνεργάτες
Τ.Ε.Ι.	Τεχνολογικό Εκπαιδευτικό Ίδρυμα

τεύχ. ή τ.	τεύχος
τομ.	τόμος
υπ.	υποψήφιος / υποψήφια
υπ’ αρ.	υπ’ αριθμόν
Υπερ.	Υπεράσπιση (επιστημονικό περιοδικό – εκδ. Αντ. Ν. Σάκκουλα)
υποσ.	υποσημείωση
ΦΕΚ	Φύλλο Εφημερίδας της Κυβέρνησης

Λατινικό αλφάβητο

apps (αγγλ.)	Applications Software / applications
ATM (αγγλ.)	Automated Teller Machine
CA (αγγλ.)	California
CEPOL (γαλλ.)	College Européen de Police
CERN (γαλλ.)	Organisation Européenne pour la Recherche Nucléaire
CERT (αγγλ.)	Computer Emergency Response Team
CFAA (αγγλ.)	Computer Fraud and Abuse Act
COM (αγγλ.)	Component Object Model
CPU (αγγλ.)	Central Processing Unit
CRC (αγγλ.)	Cyclic redundancy check
DC (αγγλ.)	District of Columbia
DDoS (αγγλ.)	Distributed Denial of Service

Dec. (αγγλ.)	December
DNA (αγγλ.)	Deoxyribonucleic acid
DNS (αγγλ.)	Domain Name System
DSL (αγγλ.)	Digital Subscriber Line
ed. (αγγλ.)	edition or editor
eds. (αγγλ.)	editors
EDV (γερμ.)	Elektronische Datenverarbeitung
ENISA (αγγλ.)	European Network and Information Security Agency
f. (αγγλ.)	and the following
fb. (αγγλ.)	facebook
FBI (αγγλ.)	Federal Bureau of Investigation
G8 (αγγλ.)	Group 8
GHS (αγγλ.)	Greek Hacking Scene
High Tech. L. (αγγλ.)	High Technology Law
ID (αγγλ.)	Identity Document
IMEI(αγγλ.)	International Mobile Station Equipment Identity
IMSI (αγγλ.)	International Mobile Subscriber Identity
Inc. (αγγλ.)	Incorporation or include / -ed / -ing
ISO (αγγλ.)	International Standards Organisation
Inst. (αγγλ.)	Institute
IQ (αγγλ.)	Intelligence Quotient
ISSN (αγγλ.)	International Standard Serial Number
IP (αγγλ.)	Internet Protocol
IRC (αγγλ.)	Internet Relay Chat
IT (αγγλ.)	Information Technology

LL. M. (λατ.)	Legum Magister (Master of Laws)
LSE (αγγλ.)	London School of Economics
M.Ed. (αγγλ.)	Master of Education
MIT (αγγλ.)	Massachusetts Institute of Technology
MSc (αγγλ.)	Master of Science
MS – DOS (αγγλ.)	Microsoft – Disc Operating System
NATO (αγγλ.)	North Atlantic Treaty Organization
NC or N. Carolina (αγγλ.)	North Carolina
No. or n. (αγγλ.)	number
Nos. (αγγλ.)	numbers
NSA (αγγλ.)	National Security Agency
NSFNet (αγγλ.)	National Science Foundation Network
NY (αγγλ.)	New York
NYU (αγγλ.)	New York University
p. (αγγλ.)	page
pp. (αγγλ.)	pages
PA (αγγλ.)	Panama
pdf (αγγλ.)	Portable Document Format
PhD (αγγλ.)	Doctor of Philosophy Degree
PHP (αγγλ.)	Hypertext Preprocessor
PIN (αγγλ.)	Personal Identification Number
pub. (αγγλ.)	publisher or publications
RAND (αγγλ.)	Research And Development
REV. (αγγλ.)	Review
SoPol apps	Social and Political applications

SQL (αγγλ.)	Structured Query Language
StGB (αγγλ.)	Strafgesetzbuch
TCP/IP (αγγλ.)	Transmission Control Protocol / Internet Protocol
TSR (αγγλ.)	Terminate and Stay Resident Program
UN (αγγλ.)	United Nations
url (αγγλ.)	Uniform Resource Locator
U.S.A. (αγγλ.)	United States of America
U.S. (αγγλ.)	United States
Vol. (αγγλ.)	Volume
vs. (αγγλ.)	versus
Wi – Fi (αγγλ.)	Wireless Fidelity
Winsock (αγγλ.)	Windows Sockets API

1. ΕΙΣΑΓΩΓΗ

1.1 Διαδίκτυο και ηλεκτρονικές πληροφορίες στον 21ο αιώνα

Είναι προφανής και αδιαμφισβήτητη η ευρεία εξάπλωση της χρήσης ηλεκτρονικών υπολογιστών τα τελευταία τριάντα περίπου χρόνια. Οι ηλεκτρονικές συσκευές επεξεργασίας και αποθήκευσης πληροφοριών γενικότερα και ο υπολογιστής ειδικότερα αποτελούν σήμερα τη βάση λειτουργίας της σύγχρονης κοινωνικής, οικονομικής, πολιτιστικής και κάθε είδους οργάνωσης. Η σύγχρονη κοινωνία εκ του τρόπου λειτουργίας της καλείται «ψηφιακή»[1]. Παράλληλα, όμως, έχουν αναπτυχθεί στο πεδίο αυτό συμπεριφορές που σχετίζονται με τους ηλεκτρονικούς υπολογιστές και έχουν χαρακτηριστεί εγκληματικές[2] [3].

---

[1] Βλ. την ανάπτυξη του Τσουραμάνη για την «ψηφιακή κοινωνία» [*Χρ. Τσουραμάνης,* Ψηφιακή εγκληματικότητα – Η (αν)ασφαλής όψη του διαδικτύου, εκδ. Κατσαρού, Αθήνα, 2005, σελ. 1, κεφάλαιο «1. Ψηφιακή κοινωνία, Διαδίκτυο (Internet) και ασφάλεια πληροφοριακών συστημάτων»].

[2] Βλ. *Χρ. Τσουραμάνη*, Ψηφιακή εγκληματικότητα, όπ. π., Αθήνα, 2005, σελ. 10 επ. όπου αναλύονται κατηγοριοποιήσεις ψηφιακών εγκλημάτων σύμφωνα με αρκετούς θεωρητικούς – στις κατηγοριοποιήσεις αυτές είναι εμφανής η ανάλυση συμπεριφορών και εγκλημάτων που τελούνται μόνο με τη χρήση υπολογιστών ακόμη και χωρίς τη χρήση διαδικτύου.

[3] Ο Ιωάννης Αγγελής διακρίνει τα ηλεκτρονικά εγκλήματα ως εξής:

α) **εγκλήματα που διαπράττονται τόσο σε κοινό περιβάλλον όσο και στο διαδίκτυο** (internet), π.χ. η συκοφαντική δυσφήμηση, η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρο 66 ν. 2121/1993) ή ενός προγράμματος ηλεκτρονικού υπολογιστή, η πορνογραφία ανηλίκων κ.λπ. Όταν το έγκλημα αυτό τελεστεί σε περιβάλλον internet, τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με τη βοήθεια του κυβερνοχώρου (internet related crime).

β) **εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών** (εννοείται χωρίς τη χρήση του διαδικτύου), π.χ. τα εγκλήματα που προβλέπονται από το άρθρο 370Γ παρ. 1 ΠΚ, όπως η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM ή σε ηλεκτρονικό υπολογιστή.

γ) **γνήσια εγκλήματα κυβερνοχώρου ή δικτύου** με την έννοια της ποινικοποίησης συμπεριφοράς που έχει σχέση αποκλειστικά με τον κυβερνοχώρο, π.χ. η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking).

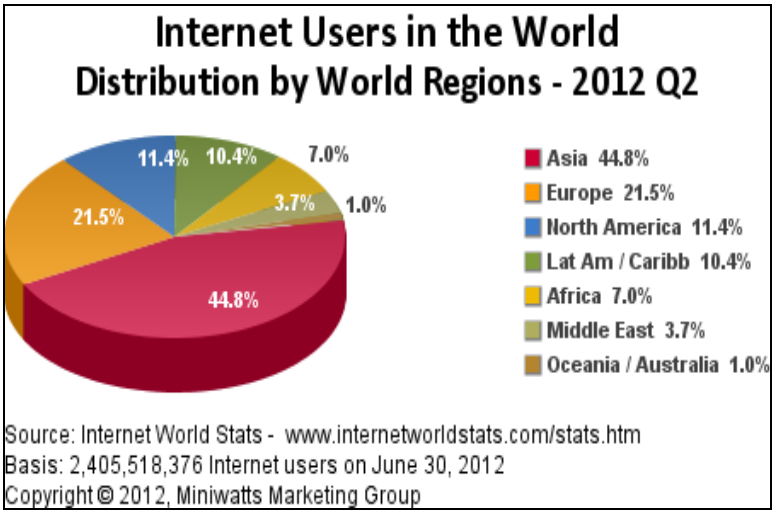
(έτσι *Ιωάν. Αγγελής*, Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη, Νομική Επιθεώρηση, τεύχος 30, http://www.eofn.gr/attachments/084_aggelis.pdf).

Αντίστοιχη, βεβαίως, τα τελευταία είκοσι περίπου χρόνια είναι και η ευρεία εξάπλωση και συνεχής ανάπτυξη των δικτύων ηλεκτρονικών συσκευών (intranets) αλλά κυρίως του διαδικτύου (του δικτύου διασύνδεσης, δηλαδή, τοπικώς απομακρυσμένων ηλεκτρονικών συσκευών - internet) ως του μεγαλύτερου συστήματος πληροφοριών. Οι χρήστες του διαδικτύου ανέρχονται σε περίπου 2,5 δισεκατομμύρια[4] και είναι προφανές από τα διδάγματα της κοινής πείρας ότι οι τάσεις είναι αυξητικές[5] με δεδομένο και ότι οι νεότερες γενιές χρησιμοποιούν το διαδίκτυο («ιθαγενείς» της ψηφιακής κοινωνίας) περισσότερο από τις παλαιότερες γενιές («μετανάστες» στον κόσμο της ψηφιακής κοινωνίας) καθώς και ότι η χρήση της τεχνολογίας διαδίδεται όλο και περισσότερο σε μέχρι πρότινος όχι τόσο ανεπτυγμένες χώρες[6].

Στην Ελλάδα η χρήση του διαδικτύου είναι πλέον ευρέως διαδεδομένη[7], τόσο που πλέον μιλούμε ακόμη και για διαδικτυακό αναλφαβητισμό[8] όσων δεν γνωρίζουν να

Βλ. και σχετικές αναπτύξεις του *David S. Wall*, The Internet as a Conduit for Criminals, pp. 77-98 in Pattavina, A. (ed.) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage (ISBN: 0761930191), 2005.

[4] Ενδεικτικά τα ποσοστά αναφορικά με τη χρήση του διαδικτύου ανά ήπειρο, όπως φαίνονται στον παρακάτω πίνακα:



[5] Συμφωνα με την Ευρωπαϊκή Επιτροπή και τα δελτία τύπου που αφορούν στο «Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο», σήμερα οι χρήστες του διαδικτύου ανέρχονται σε 2,5 δισεκατομμύρια παγκοσμίως (όπως και στην προηγούμενη υποσημείωση) και προβλέπεται ότι εντός των επομένων τεσσάρων ετών θα αυξηθούν κατά 1,5 δισεκατομμύριο επιπλέον (url: http://europa.eu/rapid/press-release_IP-14-129_el.htm).

[6] Βλ. χαρακτηριστικά την εξέλιξη και αυξανόμενη διάδοση της χρήσης του διαδικτύου στην αφρικανική ήπειρο [λήμμα "Internet in Africa" της ηλεκτρονικής εγκυκλοπαίδειας "wikipedia" (url: http://en.wikipedia.org/wiki/Internet_in_Africa#cite_ref-Livraghi2008_12-0) όπου και αναλυτικά στατιστικά στοιχεία].

[7] Βλ. χαρακτηριστικά αναφορικά με τα ποσοστά χρήσης του διαδικτύου στην Ελλάδα, τους λόγους πρόσβασης στο διαδίκτυο και άλλα ενδιαφέροντα ευρήματα την έρευνα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας με τίτλο «Η χρήση του διαδικτύου από τους Έλληνες» (url: http://www.observatory.gr/files/meletes/A100526_%CE%A0%CF%81%CE%BF%CF%86%CE%AF

«σερφάρουν» στα «κύματα» της διασυνδεδεμένης εποχής. Μάλιστα, σε κάποιες περιπτώσεις η χρήση του διαδικτύου γίνεται αρκετά έντονη και προκαλεί εξάρτηση – η κατάσταση αυτή έχει οδηγήσει την επιστημονική κοινότητα να αναφέρεται πλέον ακόμη και στον «εθισμό στο διαδίκτυο»[9] ως ψυχική διαταραχή, η οποία υποστηρίζεται ότι πολλές φορές συνδέεται με τα ελκυστικά πλεονεκτήματα του διαδικτύου, όπως είναι η ανωνυμία ή η δυνατότητα να εμφανίζεται κανείς ως κάποιος άλλος (π.χ. το «παιχνίδι με τις μάσκες»[10])[11].

Η ιδιαίτερη σημασία των ηλεκτρονικών δεδομένων και πληροφοριών και η προσπάθεια για επίτευξη ταχύτητας στην επεξεργασία, αποστολή, αποθήκευση και κάθε άλλης σχετική λειτουργία είναι τα στοιχεία που απετέλεσαν τον καταλύτη της ανάπτυξης των δικτύων υπολογιστών και - του μεγαλύτερου αυτών - του διαδικτύου. Χαρακτηριστικά, τον Δεκέμβριο του 2011 υπήρχαν στο διαδίκτυο περίπου 583.000.000 διαδικτυακοί τόποι (websites), τον Δεκέμβριο του 2012 υπήρχαν περίπου 634.000.000 διαδικτυακοί τόποι (51.000.000 διαδικτυακοί τόποι περισσότεροι σε σχέση με τον Δεκέμβριο του 2011)[12] και τον Δεκέμβριο του 2013 οι

%CE%BB%20%CF%87%CF%81%CE%B7%CF%83%CF%84%CF%8E%CE%BD%20internet%202010.pdf).

[8] Βλ. χαρακτηριστικά την έρευνα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας με θέμα: «Διαδικτυακός Αλφαβητισμός στην Ελλάδα και στην ΕΕ των 27 (2007 – 2010)» (url: http://www.observatory.gr/files/meletes/INCL_%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CF%8C%CF%82_%CE%91%CE%BB%CF%86%CE%B1%CE%B2%CE%B7%CF%84%CE%B9%CF%83%CE%BC%CF%8C%CF%82_%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1_%CE%95%CE%95%202010.pdf) στην οποία τα κύρια ευρήματα καταδεικνύουν περιληπτικά ότι: (α) μόλις το 22% των Ελλήνων πολιτών διαθέτουν ικανοποιητικές δεξιότητες στη χρήση του διαδικτύου, συγκριτικά με το 40% που αντιστοιχεί στο μέσο όρο των χωρών της Ευρωπαϊκής Ένωσης των 27 κρατών μελών, (β) οι μισοί περίπου Έλληνες χρήστες του διαδικτύου διαθέτουν μη ικανοποιητικές δεξιότητες στη χρήση αυτού και (γ) παρουσιάζεται βελτίωση των ψηφιακών δεξιοτήτων των Ελλήνων πολιτών το χρονικό διάστημα 2007-2010, που υστερεί όμως σε σύγκριση με την αντίστοιχη για τους πολίτες της Ευρωπαϊκής Ένωσης των 27 κρατών μελών.

[9] Για τον εθισμό στο διαδίκτυο βλ. *Ν. Κουράκη*, Εθισμός στο διαδίκτυο, ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών, τ. 16, Νοέμβριος 2010 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1289401434). Επίσης, βλ. την εκτεταμένη δράση και τις σχετικές έρευνες της «Ελληνικής Εταιρείας Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο» (url: http://www.hasiad.gr), την οποία ίδρυσε ο Παιδοψυχίατρος Δρ. Κωνσταντίνος Σιώμος – ενδεικτικά: *Κ. Σιώμος, Γ. Φλώρος και συν.* (εκδ. επιμ.), Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου, εκδ. Λιβάνης, 2012.

[10] Ο Παπάνης παραπέμπει στους Gajjala (2008), Ktotoski (2006) και Steinkuehler (2007) κατά τους οποίους οι ίδιοι οι συμμετέχοντες μέσω των προσωπείων τους απεικονίζουν τον εαυτό τους και υποδύονται ρόλους που ίσως «κρύβουν» στην πραγματικότητα γιατί οι συνθήκες δεν τους το επιτρέπουν (έτσι *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 46).

[11] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 67.

[12] Βλ. το άρθρο με τίτλο "Internet 2012 in numbers" (url: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers).

διαδικτυακές ιστοσελίδες ανήρχοντο σε 861.023.217![13] Αυτή η ραγδαία αύξηση των ιστοσελίδων στο διαδίκτυο συνεπάγεται εξίσου ραγδαία αύξηση των δεδομένων που υπάρχουν πλέον διαθέσιμα στο διαδίκτυο. Τούτο είναι λογικό καθώς το διαδίκτυο αποτελεί σήμερα το κυρίαρχο μέσο επικοινωνίας, ανταλλαγής πληροφοριών και μηνυμάτων, διενέργειας εμπορικών συναλλαγών, εκπαιδευτικών προγραμμάτων, τραπεζικών υπηρεσιών και ακόμη και υπηρεσιών διακυβέρνησης[14].

Επίσης, το διαδίκτυο αλλά και η ψηφιακή τεχνολογία εν γένει δύνανται να χρησιμοποιηθούν για τη δημιουργία «χώρων», «κοινοτητων» κ.ά., όπου παύουν να υφίστανται οι κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο. Η επικοινωνία μέσω του διαδικτύου καθίσταται άμεση και αμφίδρομη. Δίνεται η δυνατότητα σε κάθε χρήστη ηλεκτρονικής συσκευής (π.χ. ηλεκτρονικού υπολογιστή) συνδεδεμένης στο διαδίκτυο να πληροφορηθεί αλλά και να πληροφορήσει, ανταλλάσσοντας απόψεις μέσω ενός πιο συμμετοχικού και λιγότερο ελεγχομένου διαύλου επικοινωνίας [βλ. τις δυνατότητες του συμμετοχικού διαδικτύου (web 2.0) από το 2004 και έπειτα[15]]. Οι χρήστες αποκτούν, επίσης, ολοένα και περισσότερο την ιδιότητα του παγκόσμιου πολίτη.

Δυνάμει των ανωτέρω, το διαδίκτυο, ήδη από την αρχή της εμφάνισής του, θεωρείται ένα άκρως δημοκρατικό μέσο μαζικής επικοινωνίας (δεδομένου ότι πρόσβαση σε υπολογιστή και κατ' επέκταση στο διαδίκτυο δεν έχουμε πλέον αποκλειστικά όταν βρισκόμαστε στο σπίτι ή στο χώρο εργασίας μας, αλλά οπουδήποτε και ανά πάσα στιγμή π.χ. μέσω ενός smart phone), το οποίο καθιστά ισχυρότερο τον μέσο άνθρωπο καθώς δίνει στον τελευταίο δυνατότητες πρόσβασης σε μεγάλο όγκο πληροφοριών συγκεντρωμένων σε έναν «χώρο», προσωπικής επιλογής των πληροφοριών αυτών[16] αλλά και (εύκολης) ανάρτησης πληροφοριών και απόψεων με τη χρήση των μέσων

---

[13] Βλ. την ιστοσελίδα http://news.netcraft.com/archives/category/web-server-survey όπου και οι σχετικές πληροφορίες καθώς και αναλυτικά στοιχεία ανά μήνα ιδίως αναφορικά με την συνεχή αύξηση του αριθμού των ιστοσελίδων.

[14] Βλ. για τις δραστηριότητες στον κυβερνοχώρο το ομώνυμο κεφάλαιο στο πόνημα του *Νίκου Λέανδρου*, Το Διαδίκτυο – Ανάπτυξη και αλλαγή, εκδ. Καστανιώτη, Αθήνα, 2004, σελ. 106 επ.

[15] Για τον ορισμό του συμμετοχικού διαδικτύου (web 2.0) βλ. url: http://www.techterms.com/definition/web20.

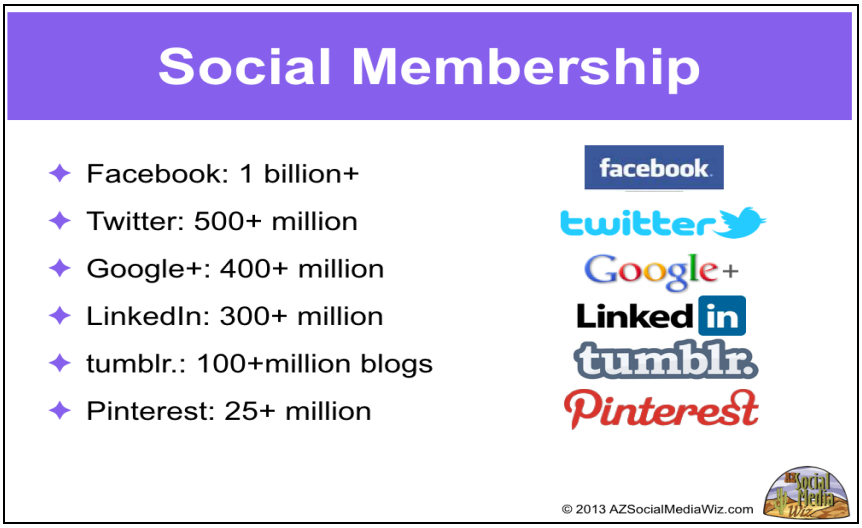
[16] Πρβλ. ενδεικτικά για τις ως άνω απόψεις *Ευστράτιου Παπάνη,* Δημοκρατία και διαδίκτυο, url: http://www.emprosnet.gr/emprosnet-archive/371b9acc-32b2-4af8-8a0d-da7162151531 και http://my.aegean.gr/web/article2985.html καθώς και το κεφάλαιο 5.6 με τίτλο «Δημοκρατία και διαδίκτυο» στο πόνημά του Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 117 επ.

κοινωνικής δικτύωσης[17]. Για όλα τα ανωτέρω, πιστεύω πως στο μέλλον θα αναφερόμαστε σε εποχή προ και μετά τη δημιουργία και τη χρήση του διαδικτύου[18].

Παράλληλα, έχει γίνει πλέον πρόδηλη η μεγάλη σημασία των ηλεκτρονικών δεδομένων και πληροφοριών που δημιουργούνται, διακινούνται, γίνονται αντικείμενο επεξεργασίας και αποθηκεύονται σε υπολογιστές ή σε σχετικές ηλεκτρονικές συσκευές και σε συστήματα πληροφοριών. Πολλά από αυτά τα δεδομένα και πληροφορίες αφορούν καθέναν από εμάς ξεχωριστά - γι' αυτό και μιλούμε σήμερα ακόμη και για τον «ψηφιακό άνθρωπο»[19].

Επομένως, η εξέλιξη των τεχνολογιών της πληροφορικής έχει αλλάξει ριζικά τις σύγχρονες κοινωνίες. Στις πιο αναπτυγμένες τεχνολογικά χώρες η διείσδυση των πληροφορικών συστημάτων σε όλους σχεδόν τους τομείς κρατικής, κοινωνικής, οικονομικής[20] αλλά και ατομικής δραστηριότητας παρουσιάζει τέτοιο βάθος και έκταση, που έχει συμπροσδιορίσει με τρόπο καθοριστικό τα χαρακτηριστικά τους. Οι «κοινωνίες της πληροφορίας»[21] διαχειρίζονται σήμερα με τη βοήθεια των

[17] Αναφορικά με τη χρήση των κοινωνικών δικτύων:



[18] Ο *Αργυρόπουλος* παραπέμπει στον *Sieber* αναφερόμενος σε δεύτερη βιομηχανική επανάσταση και στην μετατόπιση της ανθρώπινης νόησης στις μηχανές (έτσι *Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, σειρά Εγκληματο-λογικά, αρ. 19, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2001, σελ. 17, υποσ. 2-3). Ωστόσο, πρέπει να ληφθεί υπόψιν ότι σήμερα πλέον με τις απεριόριστες δυνατότητες του συμμετοχικού διαδικτύου (web 2.0) αλλά και με το πλήθος συσκευών που συνδέονται πλέον στο διαδίκτυο και των πληροφοριών που ανταλλάσσουν μιλάμε ίσως για την συγκλονιστικότερη τεχνολογική δημιουργία στην ιστορία της ανθρωπότητας.

[19] Πρβλ. σχετικά και ενδεικτικά το πόνημα του *Daniel J. Solove*, The digital person – Technology and Privacy in the Information age, New York University Press, 2004.

[20] Βλ. αναπτύξεις αναφορικά με την αγορά του διαδικτύου και τις διαδικτυακές επιχειρήσεις στο πονημα του *Νίκου Λέανδρου*, Το Διαδίκτυο – Ανάπτυξη και αλλαγή, εκδ. Καστανιώτη, Αθήνα, 2004.

[21] Κοινώς αποδεκτός ορισμός της κοινωνίας της πληροφορίας δεν φαίνεται να υφίσταται. Σύμφωνα με τον Κοφίνη «*κοινωνία της πληροφορίας είναι μία μορφή κοινωνικής και οικονομικής ανάπτυξης, όπου η απόκτηση, αποθήκευση, επεξεργασία, αποτίμηση, μεταβίβαση και διάχυση πληροφοριών οδηγεί στη*

τεχνολογιών της πληροφορικής την κυβέρνηση, τη στρατιωτική άμυνα των κρατών, την επικοινωνία, τις μεταφορές, το σύστημα υγείας, την εκπαίδευση και πολλούς άλλους τομείς κρατικών και κοινωνικών δραστηριοτήτων[22] [23]. Αυτές οι άνευ προηγουμένου οικονομικές και κοινωνικές αλλαγές ανέδειξαν με τη σειρά τους τα συστήματα πληροφοριών και τα δεδομένα που αυτά διακινούν σε στοιχεία χρήζοντα προστασίας.

Η προστασία αυτή φαίνεται απαραίτητη καθώς σε περιβάλλον ηλεκτρονικών υπολογιστών που δεν είναι διασυνδεδεμένοι[24] [25] και στο διαδίκτυο έχουν αναπτυχθεί συμπεριφορές επιβλαβείς για τα συστήματα πληροφοριών και τις ηλεκτρονικές πληροφορίες˙ κάποιες, μάλιστα, από αυτές έχουν χαρακτηριστεί εγκληματικές[26] με σκοπό την προστασία των συστημάτων πληροφοριών. Σύμφωνα με την ανακοίνωση της Ευρωπαϊκής Επιτροπής της 22.11.2010 για τη «Στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη» [COM(2010) 673 τελικό] «*Η ραγδαία ανάπτυξη και εφαρμογή νέων τεχνολογιών πληροφόρησης είχε επίσης ως αποτέλεσμα την εμφάνιση νέων μορφών εγκληματικών δραστηριοτήτων*»[27]. Τα ηλεκτρονικά δεδομένα είναι πλέον δυνητικός στόχος

δημιουργία γνώσης και στην ικανοποίηση αναγκών ατόμων και επιχειρήσεων παίζοντας έτσι κεντρικό ρόλο στην οικονομική δραστηριότητα, την παραγωγή πλούτου και τη διαμόρφωση της ποιότητας της ζωής των πολιτών» [*Στ. Κοφίνης*, Η συμμετοχή στην κοινωνία της πληροφορίας ως ένα νέο συνταγματικό δικαίωμα (ά. 5Α παρ. 2 Σ), ΔίΜΜΕ 2007, σελ. 515-516]. Επίσης, βλ. *Απ. Παπακωνσταντίνου*, Το συνταγματικό δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας, ΕΔΔΔΔ, 2006, σελ. 234.

[22] Βλ. *Steven Furnell*, Κυβερνοέγκλημα - Καταστρέφοντας την κοινωνία της πληροφορίας, Εκδόσεις Παπαζήση 2006, σελ. 1 επ.

[23] Βλ. το εξαιρετικά ενδιαφέρον άρθρο του δικηγόρου και blogger *Θ. Αλάμπαση*, iPhone vs Police. Η ψηφιοποίηση των στοιχείων που συνθέτουν την αντικειμενική υπόσταση του εγκλήματος. "Body-tracking wristbands", "tap n pay", "tap n vote" και "Wearable Democracy". Η επερχόμενη έκρηξη των κοινωνικοπολιτικών apps (SoPol apps), (url: http://alampasis.blogspot.gr/2014/05/iphone-vs-police-body-tracking.html) στο οποίο υποστηρίζει ότι η εξέλιξη των εφαρμογών, τεχνολογικών πρακτικών και συσκευών **wearable democracy** στις οποίες αναφέρεται «*θα σηματοδοτήσει τη μετάβαση από τις αναλογικές πρωτόγονες σημερινές κοινωνίες του Μεταβιομηχανικού Κοινωνικού Μεσαίωνα, στις προηγμένες ανώτερες κοινωνίες, πάνω στις οποίες θα χτιστούν οι Τέλειες Δημοκρατίες του μέλλοντος*».

[24] Βλ. σχετικά ανωτέρω υποσημειώσεις 2 και 3.

[25] Για την ηλεκτρονική εγκληματικότητα και τις μορφές της καθώς και για την διάκριση ηλεκτρονικού εγκλήματος και εγκλήματος στον κυβερνοχώρο βλ. την εμπεριστατωμένη προσέγγιση και ανάλυση του *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 405 επ.

[26] Βλ. *Αναστασία Ζάννη*, Το διαδικτυακό έγκλημα, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2005, σελ. 128 και *Αγ. Τσήτσουρα*, Εγκληματικότητα και αντεγκληματική πολιτική στην εποχή της παγκοσμιοποίησης, εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. ΙΙ, σελ. 1413.

[27] Βλ. το πλήρες κείμενο της εν λόγω ανακοίνωσης στο url: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0673_/com_com(2010)0673_el.pdf.

αξιόποινων πράξεων[28]. Κατά τον Φαρσεδάκη, οι άνθρωποι περνούν ευκολότερα σε μια εγκληματική δραστηριότητα στο διαδίκτυο σε σχέση με τον φυσικό κόσμο[29]. Ο Κιούπης εύστοχα σημειώνει ότι «... *η επέκταση του διαδικτύου με την ραγδαία αύξηση των χρηστών του, την διόγκωση του περιεχομένου του και την συχνότητα της χρήσης του*[30] *μειώνει συνεχώς τον αριθμό των ηλεκτρονικών εγκλημάτων που δεν είναι ταυτοχρόνως και διαδικτυακά εγκλήματα ή εγκλήματα κυβερνοχώρου*»[31]. Όπως επισημαίνει και η Ζαραφωνίτου (παραπέμποντας στον Alshalan, 2005) «*Το διαδίκτυο αποτελεί ένα νέο μέσο θυματοποίησης όπου λόγω της αύξησης των διαδικτυακών χρηστών αναμένεται να αυξηθεί και ο αριθμός των διαδικτυακών θυμάτων*»[32]. Σύμφωνα με τον δημιουργό του παγκόσμιου ιστού (world wide web – WWW) Τιμ Μπέρνερς-Λι, η δημοκρατική φύση που έως τώρα χαρακτήριζε το διαδίκτυο, κινδυνεύει από «*ένα ογκούμενο κύμα παρακολουθήσεων και λογοκρισίας*»[33] [34]. Επομένως, μπορεί βάσιμα να υποστηριχθεί ότι όποιος ελέγχει τα ηλεκτρονικά δεδομένα στο διαδίκτυο ενδεχομένως να είναι ο νέος κυρίαρχος του κόσμου! Το hacking (κυρίως ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, όπως θα αναλυθεί κατωτέρω[35]) είναι το φαινόμενο που αναφέρεται ουσιαστικά στις προσβολές της ασφάλειας των ηλεκτρονικών δεδομένων (κυρίως στη διάσταση της ιδιωτικότητας και του απορρήτου των πληροφοριών) αλλά και, ίσως, ο πυρήνας των

---

[28] Βλ. *Α. Αργυρόπουλο*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 18.

[29] *Ιακ. Φαρσεδάκης,* Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, Πάντειο Πανεπιστήμιο, 19/05/2009 (url: http://criminology.panteion.gr/attachments/article/386/j%20farsedakis%20%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BFs.pdf). Σε αυτό σίγουρα διευκολύνουν και τα ιδιαίτερα χαρακτηριστικά του κυβερνοεγκλήματος όπως η ανωνυμία, η ταχύτητα κ.λπ. (βλ. σχετικά *Χρ. Τσουραμάνη*, Ψηφιακή εγκληματικότητα, όπ. π., σελ. 7-8 καθώς και *του γράφοντος*, «Digital και cyber bullying και αθέμιτη χρήση ηλεκτρονικών πληροφοριών ως το "bullying" του μέλλοντος – Γνώση και πρόληψη», πρακτικά 2ου συνεδρίου Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος ΕΛ.ΑΣ., 2013, σελ. 62 επ.).

[30] ... όπως καταδείχθηκε και στο παρόν πόνημα σε ανωτέρω αναπτύξεις.

[31] Έτσι *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 407-408. Στο ίδιο ακριβώς πνεύμα και η ανάπτυξη του Παπαθεοδώρου (*Θ. Παπαθεοδώρου,* Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 205).

[32] Έτσι *Χρ. Ζαραφωνίτου και συν*., Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο, url: http://criminology.panteion.gr/attachments/article/407/e-life%20ppt.pdf, σελ. 2.

[33] Βλ. σχετικό δημοσίευμα «Η δημοκρατία του διαδικτύου κινδυνεύει - Σήμα κινδύνου από τον δημιουργό του, Τιμ Μπέρνερς-Λι» (url: http://www.newsbeast.gr/technology/arthro/611783/i-dimokratia-tou-diadiktuou-kinduneuei-/).

[34] Βλ. *Jonathan Zittrain* and *Benjamin Edelman*, Empirical Analysis of Internet Filtering in China, Berkman Center for Internet & Society, Harvard Law School, url: http://cyber.law.harvard.edu/filtering/china/ και το άρθρο «Λογοκρισία και διαδίκτυο», url: http://www.euro2day.gr/news/highlights/article-news/1167473/logokrisia-sto-diadiktyo.html.

[35] Στο κεφάλαιο 2 του παρόντος πονήματος.

συμπεριφορών για τις οποίες μπορεί να πει κανείς ότι επιδιώκεται λογοκρισία[36] (ως περιορισμός στην πρόσβαση στην πληροφορία)[37].

Η χρήση των πληροφορικών συστημάτων στο πεδίο του εγκλήματος είναι ίσως η σημαντικότερη πρόκληση με την οποία ήρθαν αντιμέτωπες οι κοινωνίες της πληροφορίας. Το στοιχείο αυτό έγινε, λοιπόν, σχετικά γρήγορα κατανοητό στην ιστορική εξέλιξη των εφαρμογών της πληροφορικής τεχνολογίας με συνέπεια πολλές έννομες τάξεις, ήδη από τη δεκαετία του 1980, να προβούν σε μία προσπάθεια αναγωγής των συστημάτων πληροφοριών και των δεδομένων που αυτά διακινούν, σε έννομα αγαθά, και σε ποινικοποίηση των σχετικών συμπεριφορών προσβολής τους[38].

Στη σημερινή εποχή, δηλαδή, η διάδοση της χρήσης των ηλεκτρονικών υπολογιστών, η ανάπτυξη του διαδικτύου και η έκρηξη της νέας ψηφιακής οικονομίας, όπως ανωτέρω αναλύθηκε, και, γενικότερα, η πλήρης εξάρτηση από τα ψηφιακά συστήματα[39] επέφεραν ραγδαία αύξηση της λεγόμενης ψηφιακής εγκληματικότητας (digital criminality)[40]. Οι ηλεκτρονικοί υπολογιστές αλλά και ποικίλες άλλες ηλεκτρονικές συσκευές με δυνατότητα διασύνδεσης [«έξυπνα» τηλέφωνα (smart phones)[41], «έξυπνες» τηλεοράσεις (smart tv), tablets κ.α] συχνά καθίστανται είτε στόχοι, είτε εργαλεία εγκλήματος[42], καθώς μεταδίδουν πληροφορίες ή τις καθιστούν προσβάσιμες. Και οι τεχνολογικές εξελίξεις προβλέπονται αλματώδεις: ήδη αναπτύσσεται το «διαδίκτυο των πραγμάτων» ("Internet of things")[43], με «πεδίο δόξης λαμπρό»[44] για τους επίδοξους hackers![45]

---

[36] Για την ελευθερία του λόγου στο διαδίκτυο πρβλ. το πολύ ενδιαφέρον άρθρο του *Πάσχου Μανδραβέλη*, «Ελευθερολογία πριν και μετά το Διαδίκτυο», εφημερίδα «Καθημερινή», 17 Δεκεμβρίου 2010, url: http://www.medium.gr/internet-/3715-1659.html και http://www.kathimerini.gr/723205/opinion/epikairothta/arxeio-monimes-sthles/eley8erologia-prin-kai-meta-to-diadiktyo.

[37] Η θέση των hackers για πλήρη ελευθερία της πληροφορίας στο διαδίκτυο και η αυτή αιτιολόγηση/δικαιολόγηση των δράσεών τους, όπως αναλύεται κατωτέρω, αυτομάτως θέτει το hacking απέναντι από κάθε λογοκρισία αλλά και τις δράσεις τους αυτές αντικείμενο λογοκρισίας.

[38] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, Αρμεν. 2007, σελ. 1059.

[39] Έτσι ο *Peter Grabosky*, Security in the 21st Century, Security Journal (2007) 20, 9 – 11.

[40] Βλ. *Θεόδωρος Σιδηρόπουλος*, Το Δίκαιο του διαδικτύου, β' Έκδοση, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2008, σελ. 33.

[41] Για ενέργειες hacking σε έξυπνα τηλέφωνα βλ. το χαρακτηριστικό άρθρο της *Christina Scelsi*, The i-phone hacking and cracking and copyright, Entertainment and Sports Lawyer, Fall, 2008, lexisnexis database.

[42] *Rob D' Ovidio*, The Evolution of Computers and Crime: Complicating Security Practice, Criminal Justice Program, Drexel University, Philadelphia PA, U.S.A., Security Journal (2007) 20, p. 47.

[43] Για τον ορισμό του "Internet of things" βλ. url: http://www.techopedia.com/definition/28247/internet-of-things-iot καθώς και *Kevin Ashton*, That

1.2 Ιστορία του διαδικτύου και της ηλεκτρονικής πληροφορίας – οι πρωτοπόροι του διαδικτύου

Σήμερα σχεδόν όλες οι ψηφιακές συσκευές πληροφορικής είναι διασυνδεδεμένες στο διαδίκτυο[46] (εκτός από κάποιες οι οποίες λειτουργούν αποκλειστικά σε κλειστά δίκτυα – intranets – όπως συστήματα τραπεζών κ.ά.). Η διασύνδεσή τους αυτή τις καθιστά αναπόφευκτα πιο ευάλωτες σε «επιθέσεις»[47] χωρίς δικαίωμα εισβολής στο σύστημα πληροφοριών που αντιπροσωπεύουν. Για αυτό έχει ιδιαίτερη σημασία η μελέτη της ιστορίας και της φύσης του διαδικτύου και, κατ' επέκταση, του τρόπου λειτουργίας του,[48] προκειμένου να κατανοηθεί καλύτερα το πρόβλημα της εγκληματικότητας που αναπτύσσεται σε αυτό το περιβάλλον.

Το διαδίκτυο (αγγλ.: internet) είναι ένα επικοινωνιακό δίκτυο που επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου υπολογιστή ή συσκευής. Η τεχνολογία του είναι κυρίως βασισμένη στη διασύνδεση επιμέρους

"Internet of Things" thing, RFiD Journal, 22 Ιουνίου 2009, url: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf. Επίσης, βλ. το αναλυτικό πόνημα των *Rolf H. Weber & Romana Weber*, Internet of Things - Legal Perspectives, Springer Heidelberg Dordrecht London New York, Zurich – Basel – Geneva 2010.

[44] Βλ. το άρθρο «Χάκερς απειλούν…ψυγεία και οδοντόβουρτσες», εφημερίδα larissanet.gr, 15 Ιανουαρίου 2014, url: http://www.larissanet.gr/2014/01/15/hackers-apeiloun-psygeia-kai-odontovourtses/ καθώς και το άρθρο του *Ben Feinstein*, "Smart Shoe Takes on Wearable Technology Field", 28/07/2014 (url: http://www.biznob.com/smart-shoe-takes-wearable-technology-field/3320#), το οποίο αναφέρεται σε παπούτσια που διασυνδέονται στο διαδίκτυο ή σε δίκτυο με άλλες «έξυπνες» συσκευές.

[45] Σύμφωνα και με το ΓΕΕΘΑ «*η εξάρτηση της κρατικής ή ιδιωτικής υποδομής στα μέσα της πληροφορικής τις καθιστά δυνητικούς στόχους του κυβερνοπολέμου*». [Έτσι στο άρθρο "ΓΕΕΘΑ: Ο κυβερνοπόλεμος είναι το νέο στρατηγικό όπλο" (url: http://www.onalert.gr/default.php?pname=Article&catid=20&art_id=1673)].

[46] Πρβλ. *Β. Σωτηρόπουλο*, Δωρεάν ασύρματη πρόσβαση πολιτών στο Διαδίκτυο, νομικό ιστολόγιο "e-lawyer", url: http://elawyer.blogspot.gr/2014/03/blog-post_7.html για την πρόσφατη θεσμοθέτηση δυνατότητας ασύρματης πρόσβασης πολιτών στο διαδίκτυο η οποία πρέπει να παρέχεται από τους Δήμους.

[47] Βλ. την χαρακτηριστική ανάπτυξη του *Ulrich Sieber* με τίτλο "Vulnerability of the Information society" στο βασικό αναφορικά με το ποινικό δίκαιο του διαδικτύου πόνημά του Legal aspects of computer-related crime in the Information society, January 1998, prepared for the European Commission.

[48] Για τη δημιουργία και τον τρόπο λειτουργίας του διαδικτύου βλ. το αναλυτικό πόνημα των *Romualdo Pastor-Satorras & Alessandro Vespignani*, Evolution and Structure of the Internet – A statistical physics approach, Cambridge University Press, 2004.

δικτύων ανά τον κόσμο[49]. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη μορφή του, με τον όρο διαδίκτυο, περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και ψηφιακών συσκευών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του[50].

Χαρακτηριστικό είναι το γεγονός ότι το διαδίκτυο (όπως και πολλές άλλες τεχνολογικές και επιστημονικές εξελίξεις) δημιουργήθηκε και χρησιμοποιήθηκε καταρχάς και στην πιλοτική του μορφή στον στρατό[51]. Οι ίδιες οι καταβολές του διαδικτύου καταδεικνύουν την άμεση σχέση διαδικτύου και πληροφοριών με στρατηγική σημασία.

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Προκειμένου να ενισχυθεί η προστασία από μια πιθανή πυρηνική επίθεση εκ μέρους της ΕΣΣΔ, οι ΗΠΑ δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ARPA (Advanced Research Project Agency) γνωστή και ως DARPA (Defense Advanced Research Projects Agency)[52]. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας, το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση.

Το αρχικό θεωρητικό υπόβαθρο είχε δοθεί από τον J. C. R. Licklider, ο οποίος ανέπτυξε τη θεωρία του αναφορικά με το λεγόμενο «γαλαξιακό δίκτυο» (“galactic network”)[53]. Η θεωρία του Licklider περιέγραφε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Η αναγκαία

[49] Στην ελληνική νομοθεσία δεν υπάρχει ορισμός του διαδικτύου. Στις ΗΠΑ περιέχεται ορισμός του διαδικτύου στον νόμο περί εξαίρεσης του διαδικτύου από την φορολόγηση (“Internet Tax Freedom Act”). Βλ. ειδικότερα *Εμμ. Μεταξάκη*, Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου, ΠοινΧρ ΞΔ/ 2014, σελ. 12, υποσ. 53.

[50] Για μια συνοπτική και περιεκτική προσέγγιση της ιστορίας του διαδικτύου και μάλιστα ανά σημαντική χρονολογία βλ. το άρθρο της ενημερωτικής ιστοσελίδας www.tvxs.gr με τίτλο «Η ιστορία του διαδικτύου», url: http://tvxs.gr/news/internet-mme/i-istoria-toy-diadiktyoy.

[51] Βλ. αναλυτικότερα για τη δημιουργία του διαδικτύου *Anthony Giddens*, Κοινωνιολογία, εκδ. Gutenberg, μετάφραση-επιμέλεια Δημήτρη Τσαούση, σελ. 520 επ.

[52] Βλ. αναλυτικά για την ιστορία του διαδικτύου url:http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet καθώς και το κεφάλαιο με τίτλο «Από το Arpanet στο διαδίκτυο» στο πόνημα του *Νίκου Λέανδρου*, Το Διαδίκτυο – Ανάπτυξη και αλλαγή, εκδ. Καστανιώτη, Αθήνα, 2004, σελ. 27 επ.

[53] Βλ. σχετικά url: http://www.ibiblio.org/pioneers/licklider.html καθώς και το άρθρο του *J. C. R. Licklider*, Man – Computer Symbiosis, url: http://groups.csail.mit.edu/medg/people/psz/Licklider.html.

«αποκεντρωτική» λειτουργία αυτού του δικτύου, έτσι ώστε ακόμα κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές, αναπτύχθηκε από τον Πολ Μπάραν (Paul Baran)[54] με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής «πακέτων» του Λέοναρντ Κλάινροκ (Leonard Kleinrock)[55], σύμφωνα με την οποία πακέτα πληροφοριών, που θα περιείχαν ως στοιχείο και την προέλευση και τον προορισμό τους, μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο.

Στηριζόμενο, λοιπόν, σε αυτές τις τρεις θεωρίες και τρόπους λειτουργίας δημιουργήθηκε το διασυνδεμένο δίκτυο υπολογιστών, γνωστό ως ARPANET το 1969[56].

Το 1974 δημοσιεύτηκε η μελέτη των Βιντ Σερφ (Vint Cerf) και Μπομπ Κάαν (Bob Kahn)[57] από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol). Αργότερα, κατά το έτος 1978, το πρωτόκολλο αυτό μετετράπη στο TCP/IP - προσετέθη δηλαδή το Internet Protocol (IP). Το 1983 το TCP/IP έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET[58].

Ο όρος διαδίκτυο (internet) ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το ARPANET με το δίκτυο NSFNet[59]. "Internet", ουσιαστικά, σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε το πρωτόκολλο TCP/IP. Η μεγάλη ανάπτυξη

---

[54] Βλ. σχετικά url: http://www.ibiblio.org/pioneers/baran.html.

[55] Για τον Leonard Kleinrock βλ. url: http://www.lk.cs.ucla.edu/index.html.

[56] Για το Arpanet βλ. url: http://www.columbia.edu/~hauben/CS/arpanet-encyc.txt.

[57] Βλ. ενδεικτικά για τη ζωή και το έργο των έργο των Cerf και Kahn το url: http://georgewbush-whitehouse.archives.gov/government/cerf-kahn-bio.html.

[58] «*Το Internet είναι μια παγκόσμια συνένωση από ανεξάρτητα μεταξύ τους δίκτυα και υπολογιστές, τα οποία μπορούν να ανταλλάσσουν στοιχεία και πληροφορίες βάσει του σύνθετου πρωτοκόλλου TCP/IP (Transmission Control Protocol/ Internet Protocol)*» (έτσι *Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 27). Ο Αργυρόπουλος περιγράφει, επίσης, αναλυτικά τον τρόπο λειτουργίας και τις υπηρεσίες που παρείχε το διαδίκτυο κατά το έτος 2001 (*Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 28-34). Βέβαια, πλέον πρέπει να λάβουμε υπόψιν μας τις συνδέσεις DSL, τις δυνατότητες του συμμετοχικού διαδικτύου (web 2.0) (όπως ανωτέρω), τα κοινωνικά δίκτυα, τις «έξυπνες» συσκευές οι οποίες συνδέονται πλέον στο διαδίκτυο κ.ά. αλλά και τη συνεχή εξέλιξη της τεχνολογίας ακόμη σε πειραματικό επίπεδο [π.χ. παροχή ασύρματης σύνδεσης οπουδήποτε υπάρχει τεχνητό φως μέσω του φωτός – βλ. παρουσίαση έρευνας της Ελληνικής Εταιρείας Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο στις 14/01/2014 με θέμα «Ασφαλής πλοήγηση και κοινωνική δικτύωση στον Ελληνικό Στρατό» και επιστ. υπεύθυνο τον Δρ. Κωνσταντίνο Σιώμο (αδημ.)].

[59] Το NSFNet ήταν δίκτυο υπολογιστών για ανταλλαγή πληροφοριών το οποίο αναπτύχθηκε στις ΗΠΑ μεταξύ ακαδημαϊκών και ερευνητικών Ιδρυμάτων από το 1985 και έπειτα. Για ειδικότερες πληροφορίες βλ. url: http://www.nsfnet-legacy.org/about.php.

του διαδικτύου, όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού (World Wide Web – WWW)[60] από τον Τιμ Μπέρνερς-Λι (Tim Berners-Lee)[61] στο ερευνητικό ίδρυμα CERN το 1989[62], «πλατφόρμα» η οποία έκανε εύκολη την πρόσβαση στο διαδίκτυο πλέον ακόμη και για ιδιώτες και στη μορφή που είναι γνωστό σήμερα[63].

Αυτή η τεχνολογία του διαδικτύου και του παγκόσμιου ιστού (world wide web – www) διεύρυνε απεριόριστα τις δυνατότητες διακίνησης πληροφοριών και επικοινωνίας καθώς και τη λειτουργία θεμελιωδών υποδομών ζωτικής σημασίας[64] [65] [66]. Σύμφωνα με τον ΟΟΣΑ, «... *η ηλεκτρονική διακυβέρνηση και η προστασία των*

---

[60] Πρβλ. το άρθρο της ενημερωτικής ιστοσελίδας www.tvxs.gr με τίτλο «Το Internet γίνεται 25 ετών» (url: http://tvxs.gr/news/internet-mme/internet-ginetai-25-eton).

[61] Για τον Τιμ Μπέρνερς – Λι βλ. url: http://www.w3.org/People/Berners-Lee/.

[62] Για την γέννηση του διαδικτύου στο CERN βλ. url: http://home.web.cern.ch/topics/birth-web.

[63] Πρβλ. το άρθρο του *Κ. Δεληγιάννη*, «Τα 25α γενέθλιά του "γιορτάζει" σήμερα το World Wide Web», εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 12 Μαρτίου 2014, url: http://www.kathimerini.gr/757719/article/texnologia/diadiktyo/ta-25a-gene8lia-toy-giortazei-shmera-to-world-wide-web όπου και πολύ ενδιαφέρουσες οι παρατηρήσεις του ίδιου του Τιμ Μπέρνερς-Λι για το μέλλον του διαδικτύου και την κατοχύρωση των δικαιωμάτων στο διαδίκτυο.

[64] Είναι επιβεβλημένη η μελέτη αυτής της αθέμιτης χρήσης του διαδικτύου καθώς, στο σύγχρονο τοπίο, οι επιθέσεις κατά συστημάτων πληροφοριών μπορεί να στρέφονται κατά των **θεμελιωδών υποδομών ζωτικής σημασίας (ΥΖΣ)** και να έχουν επιπτώσεις στα υφιστάμενα συστήματα έγκαιρης προειδοποίησης σε πολλούς τομείς, με ενδεχόμενες καταστροφικές συνέπειες για το κοινωνικό σύνολο. Οι Υποδομές Ζωτικής Σημασίας (ΥΖΣ) περιλαμβάνουν τις **τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ)** που παρέχουν την πλατφόρμα πληροφοριών και επικοινωνιών η οποία αποτελεί τη βάση για την προσφορά σημαντικών αγαθών και υπηρεσιών, συμπεριλαμβανομένων ζωτικών κοινωνικών λειτουργιών όπως η **ηλεκτροδότηση, η υδροδότηση, οι μεταφορές, ο τραπεζικός τομέας, οι υγειονομικές υπηρεσίες έκτακτης ανάγκης, τα σώματα ασφαλείας, το σύστημα διαχείρισης κυκλοφορίας, το χρηματιστήριο κ.λπ**.

Με βάση την **Οδηγία 2008/114/ΕΚ** της 08/12/08 «***σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την αξιολόγηση της ανάγκης βελτίωσής της προστασίας τους***» ως ΥΠΟΔΟΜΕΣ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ νοούνται «*τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών*». (url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EL:PDF).

[65] Έτσι και *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking underground, 2004, url: http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf, σελ. 27, όπου και αναφέρει συγκεκριμένα παραδείγματα για τον καίριο ρόλο του διαδικτύου στη διοίκηση στις ΗΠΑ.

[66] Πρβλ. *Aunshul Rege-Patwardhan*, Cybercrimes against critical infrastructures: a study of online criminal organization and techniques, Rutgers School of Criminal Justice, Criminal Justice Studies, Vol. 22, No. 3, Routledge, September 2009, 261–271 όπου εξηγούνται οι υποδομές ζωτικής σημασίας (μεταφορές, τηλεπικοινωνίες, ύδρευση) και αναφέρονται παραδείγματα επιθέσεων σε τέτοιες υποδομές και τυπολογία και μέθοδοι των επιτιθέμενων κυβερνοεγκληματιών καθώς και *Misha Glenny*, Cyberthieves, Cybercops and You, Alfred A. Knopf ed., New York, 2011 όπου αναλύονται περιστατικά επιθέσεων στο διαδίκτυο και στον πρόλογο του εν λόγω πονήματος γίνεται ειδική αναφορά στην στήριξη των υποδομών ζωτικής σημασίας ως critical national infrastructure (cni) στα συστήματα ηλεκτρονικών υπολογιστών στο βραχύ διάστημα της τελευταίας εικοσαετίας.

εθνικών υποδομών πληροφοριών φαίνεται να είναι δύο κύριοι μοχλοί για την ανάπτυξη μιας αντίληψης για την ασφάλεια σε εθνικό επίπεδο»[67]. Όπως εύστοχα επισημαίνει ο Αργυρόπουλος, η ηλεκτρονική επεξεργασία στοιχείων έχει καταφέρει να κατακτήσει κάθε σφαίρα της ανθρώπινης δραστηριότητας αλλά και η δραστηριότητά μας αυτή συνάμα εξαρτάται από την εν λόγω επεξεργασία[68].

Αντιστοίχως, όμως, μέσα από αυτή την υπέρμετρη ανάπτυξη της χρήσης και των δυνατοτήτων του «κυβερνοχώρου» ("cyberspace"[69]) -όπως ονομάστηκε ο «κόσμος» του διαδικτύου-, το σύστημα αυτό κατέστη αναπόφευκτα πιο ευάλωτο σε προσβολές και σε διαρροές των στοιχείων του (όπως αναφέρθηκε ήδη) καθώς και σε αθέμιτη χρήση του[70]. Η επικινδυνότητα της αθέμιτης χρήσης μεγιστοποιείται από το γεγονός ότι η ηλεκτρονική πληροφορία αυτή καθεαυτή έχει σήμερα τεράστια οικονομική αξία[71] (ιστοσελίδες στις οποίες διενεργείται ηλεκτρονικό εμπόριο[7273], τραπεζικές

---

[67] *Organisation for Economic Co-operation and Development, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, Working Party on Information Security and Privacy*, "THE PROMOTION OF A CULTURE OF SECURITY FOR INFORMATION SYSTEMS AND NETWORKS IN OECD COUNTRIES", December 16th, 2005, p. 3.

[68] Έτσι *Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 17.

[69] Τον όρο "cyberspace" εμπνεύστηκε ο συγγραφέας *William Gibson* στο μυθιστόρημα επιστημονικής φαντασίας «Νευρομάντης» ("Neuromancer"), το οποίο εκδόθηκε το 1984. Αργότερα, ο *Gibson* όρισε τον «κυβερνοχώρο» με τη φράση «εκεί δεν υπάρχει εκεί – there's no there, there» (βλ. *Michael Bachmann*, όπ. π., σελ. 31). Ο συγγραφέας υπήρξε πρωτοπόρος του είδους της επιστημονικής λογοτεχνίας του «κυβερνοπάνκ» ("cyberpunk") και το βιβλίο του "Neuromancer" («Νευρομάντης») είναι αυτό που θεμελίωσε το ως άνω είδος τέχνης, του οποίου το ιδιαίτερο γνώρισμα ήταν η σχέση της ζωής με την υψηλή τεχνολογία ("high tech – low life"). Η υπόθεση εξελίσσεται σε ένα παγκόσμιο δίκτυο υπολογιστών που συνενώνει ανθρώπους και πληροφορία, μηχανές, προγράμματα και δεδομένα, σχηματίζοντας το υλικό υπόβαθρο μέσα στο οποίο πραγματοποιείται η κίνηση (πλοήγηση) σε έναν αλληλεπιδραστικό δυνητικό κοινωνικό χώρο (βλ. σχετικά και *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-Zavrsnik.pdf, p. 6 καθώς και *Ευστράτιο Παπάνη*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ.172 για τον ορισμό του όρου "cyberpunk").

[70] Βλ. χαρακτηριστικά το άρθρο «Διάτρητα τα συστήματα IT κυβερνητικών και αμυντικών οργανισμών, λέει η Kaspersky», url: http://tech.in.gr/analysis/article/?aid=1231263192

[71] «*Το πληροφορικό έγκλημα αποτέλεσε ειδικό ζήτημα όταν συνειδητοποιήθηκε ότι ένα νέο πεδίο πλούτου (η πληροφορία και η γνώση) είχε αναδειχθεί, ένα πεδίο μέχρι πρότινος άγνωστο ως προς τις δυνατότητες που προσέφερε για οικονομικό πλουτισμό. "Αρχικά", ο πληροφορικός-γνωστικός πλούτος αυτός ήταν δημόσιος και ελεύθερος για όλους. ... Ο απέραντος πλούτος της κοινωνικής γνώσης- ενός κατ' εξοχήν κοινωνιακού αγαθού έπρεπε να αλλοτριωθεί και να μορφοποιηθεί σε ατομική ιδιοκτησία που αποσκοπεί πρωτ' απ' όλα στο οικονομικό κέρδος. ... το πληροφορικό έγκλημα αποτελεί έναν από τους τρόπους διαχείρισης και διευθέτησης του τρόπου με τον οποίο ο κοινωνικός πλούτος μετατρέπεται σε ατομική ιδιοκτησία. ... το πληροφορικό έγκλημα αποδεικνύεται ιδιαίτερα λειτουργικό στη μορφοποίηση του αγαθού "γνώση" σε εμπόρευμα ...* », έτσι *Γ. Λάζος*, Πληροφορική και έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα 2001, σελ. 239.

[72] Το ηλεκτρονικό εμπόριο έχει απασχολήσει νομοθετικά και την Ευρωπαϊκή Ένωση. Βλ. χαρακτηριστικά την Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 08.06.2000 (ΕΕ L178 της 17.07.2000, σελ. 1-16), η οποία έχει ενσωματωθεί στο ελληνικό δίκαιο με το

συναλλαγές κ.ά.)[74]. Εξάλλου, σημαντική θεωρείται και η οικονομική αξία των σύγχρονων ηλεκτρονικών προγραμμάτων λογισμικού[75]. Η ηλεκτρονική αυτή πληροφορία, η οποία θα μπορεί να έλθει σε γνώση ή κατοχή μετά από χωρίς δικαίωμα πρόσβαση, μπορεί να αποτελέσει ακόμη και αντικείμενο εκβίασης[76]. Για τους λόγους αυτούς έχει λεχθεί ότι τα οικονομικά εγκλήματα συνιστούν τον πυρήνα των ηλεκτρονικών εγκλημάτων[77]. Τέλος, αυτή η συστηματική αποθήκευση πληροφοριών σε διασυνδεδεμένες συσκευές καθιστά κάθε πρόσωπο ή επιχείρηση ευάλωτο σε έλεγχο[78], ο οποίος πολλές φορές δύναται να λαμβάνει χώρα χωρίς δικαίωμα.

1.3 Η έννοια της ασφάλειας

Π.Δ. 131/2003 (βλ. και *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013, σελ. 4 και κυρίως σελ. 103 επ.).

[73] Αναλυτικό για τους κινδύνους στο ηλεκτρονικό εμπόριο το ρεπορτάζ της εφημερίδας «Καθημερινή» στις 25/01/2014 με τίτλο «Στόχος ηλεκτρονικών επιθέσεων αμερικανικές εμπορικές αλυσίδες» (url: http://www.kathimerini.gr/553853/article/oikonomia/die8nhs-oikonomia/stoxos-hlektronikwn-epi8esewn-amerikanikes-emporikes-alysides).

[74] Βλ. το χαρακτηριστικό παράδειγμα, το οποίο αναφέρεται από τον Κουράκη, της επίθεσης που υπέστησαν στις 7 και 8 Φεβρουαρίου 2000 γνωστές εμπορικές ιστοσελίδες και η οποία τους προκάλεσε ζημία και διαφυγόντα κέρδη χιλιάδων δολαρίων μέσα σε μόνο λίγες ώρες. Επίσης, ο Κουράκης αναφέρεται σε θέματα επιχειρηματικών μυστικών και βιομηχανικής κατασκοπείας (*Ν. Κουράκης*, Εγκληματολογικοί ορίζοντες, τομ. Β': Πραγματολογική προσέγγιση και επιμέρους ζητήματα, ε,δ Αντ. Ν. Σάκκουλα, 2η εκδ., Αθήνα – Κομοτηνή, 2005, σελ. 184). Επίσης, για την οικονομική αξία και εμπορευματοποίηση της πληροφορίας βλ. *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf, p. 24.

[75] Πρβλ. *Α. Αργυρόπουλο*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ 36.

[76] Βλ. δημοσίευμα της ενημερωτικής ιστοσελίδας tvxs.gr στις 16/06/2014 με τίτλο «Χάκερ ζητούν λύτρα από την Dominos κρατώντας «όμηρους» τους πελάτες» (url: http://tvxs.gr/news/internet-mme/xaker-zitoyn-lytra-apo-tin-dominos-kratontas-%C2%ABomiroys%C2%BB-toys-pelates) σύμφωνα με το οποίο hackers οι οποίοι διαχειρίζονταν προφίλ στον ιστότοπο κοινωνικής δικτύωσης twitter με όνομα Rex Mundi υπέκλεψαν τα στοιχεία περισσότερων από 600.000 πελατών της εταιρείας διανομής πίτσας Dominos Pizza Inc στη Γαλλία και στο Βέλγιο και ζητούσαν 30.000 € λύτρα από την εταιρεία προκειμένου να μην τα δημοσιεύσουν.

[77] *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 409, όπως παραπέμπει στον Sieber.

[78] Βλ. έτσι *Αν. Χάιδου*, Σύγχρονη τεχνολογία και κοινωνικός έλεγχος, Εγκληματολογικά κείμενα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, σελ. 99 όπως παραπέμπει στον S. Cohen ο οποίος ήδη από το 1985 αναφερόταν σε «*φυλακή πληροφοριών*» και πρβλ. ενδεικτικά *Gary T. Marx*, The Engineering of Social Control: The Search for the Silver Bullet, published in *J. Hagan and R. Peterson*, Crime and Inequality, 1995, Stanford University Press.

Στο πλαίσιο του κινδύνου[79] τον οποίο διατρέχουν ηλεκτρονικές πληροφορίες και δεδομένα, πολύς λόγος έχει γίνει για την ασφάλεια στο διαδίκτυο[80].

Η οριοθέτηση της ασφάλειας[81] αποτελεί δυσεπίλυτο εννοιολογικό πρόβλημα[82]. Ο γενικός ορισμός προφανώς ποικίλλει ανάλογα με τον χώρο και τον τρόπο που χρησιμοποείται η εν λόγω έννοια[83]. Δύναται, ενδεχομένως, να λάβει διαφορετικό κάθε φορά περιεχόμενο ανάλογα με την κοσμοθεωρία αυτού που ερμηνεύει τον όρο, τις συνθήκες ασκήσεως του επαγγέλματός του κ.λπ.[84] Ακόμη και σε συγκεκριμένα επιστημονικά πεδία (π.χ. εννοιολόγηση της «δημόσιας ασφάλειας» σε συνταγματικό επίπεδο) δεν υπάρχει κοινώς αποδεκτός ορισμός της ασφάλειας[85].

Στην καθομιλουμένη γλώσσα, ασφάλεια φέρεται να είναι η κατάσταση εκείνη στην οποία δεν εντοπίζεται καμία περίπτωση (απειλή ή κίνδυνος) επέλευσης επιβλαβών συνεπειών και κατά την οποία δεν αισθάνεται κανένας ότι απειλείται. Σε μια γενική προσέγγιση, δηλαδή, ως ασφάλεια φαίνεται να εννοείται η κατάσταση εκείνη κατά

---

[79] Αναφορικά με την έννοια του κινδύνου στο εγκληματικό φαινόμενο πρβλ. ενδεικτικά το κεφάλαιο με τίτλο «Το πρόβλημα της αποτίμησης του κινδύνου τέλεσης νέων εγκληματικών πράξεων» στο πόνημα του *Α. Μαγγανά*, Το εγκληματικό φαινόμενο στην πράξη, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 67 επ.

[80] Πρβλ. ενδεικτικά για την ασφάλεια στο διαδίκτυο σε δραστηριότητες ανηλίκων την ιστοσελίδα http://internet-safety.sch.gr/.

[81] Πρβλ. και *Αν. Μαγγανά*, Η ιδιωτική ασφάλεια. Προβληματισμοί και επισημάνσεις, ΠοινΔικ, 2001, σελ. 274-284.

[82] Πρβλ. *Μαίρη Μπόση*, Ζητήματα ασφάλειας στη νέα τάξη πραγμάτων, εκδ. Παπαζήση, Αθήνα, 1999 και κυρίως κεφάλαιο 1 και 2.

[83] Πρβλ. για την έννοια της ασφάλειας σύμφωνα με τη νομολογία του ΕΔΔΑ *Μαρίας Γαλανού*, Ζητήματα ερμηνείας του δικαιώματος στην προσωπική ελευθερία και ασφάλεια στο κείμενο της ΕΣΔΑ, εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 140.

[84] Έτσι ο *Ιωάννης Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 12/2001, 1293 επ. Σύμφωνα με το παράδειγμα του Αγγελή, π.χ. για κάποιον στρατιωτικό ο όρος «ασφάλεια» έχει διαφορετικό περιεχόμενο απ' ό,τι για κάποιον αστυνομικό, ο οποίος επίσης αντιλαμβάνεται την «ασφάλεια» εντελώς διαφορετικά από κάποιον εργαζόμενο σε οικοδομικές εργασίες κ.ο.κ. Μπορεί, όμως, ακόμη και στον ίδιο ευρύτερο επαγγελματικό κλάδο η «ασφάλεια» να έχει διαφορετικό περιεχόμενο (π.χ. για τον στρατιωτικό που ασχολείται με τα όπλα η έννοια της ασφάλειας δεν ταυτίζεται με αυτή που αντιλαμβάνεται ο στρατιωτικός ο οποίος ασχολείται με τους ηλεκτρονικούς υπολογιστές και τα ηλεκτρονικά συστήματα πληροφοριών – πρβλ. ενδεικτικά για το πώς παρουσιάζεται η έννοια της ασφάλειας των συστημάτων ηλεκτρονικών πληροφοριών στον στρατό *Ευάγγελου Βαρλάμου*, Ασφάλεια Δεδομένων Ηλεκτρονικών Υπολογιστών, Στρατιωτική Επιθεώρηση, Σεπτέμβριος – Οκτώβριος 2006, σελ. 116 επ.).

[85] Βλ. *Ιωάννη Δρόσο*, Δημόσια τάξη και δημόσια ασφάλεια, Επιθεώρησις Δημοσίου Δικαίου και Διοικητικού Δικαίου, τομ. 35, τ. Απρίλιος – Ιούνιος 1991, Αθήνα, σελ. 198 ο οποίος, μάλιστα, αναφέρει ότι «*Δεν αποτελεί ελληνική ιδιοτυπία η απουσία συνταγματικού ή νομοθετικού ορισμού της δημόσιας ασφάλειας…*». Για τη «δημόσια ασφάλεια» και την «εθνική ασφάλεια» βλ. και *Ν. Κουράκη*, Ασφάλεια και ελευθερία – Τα μεταξύ τους στατικά και δυναμικά όρια, εις: *Χ. Ζαραφωνίτου, (επιμ.)*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, σειρά Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών αρ. 7, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2007, σελ. 20.

την οποία δεν υπάρχει για τους εμπλεκομένους κανένας κίνδυνος[86] ή απειλή προς αποτροπή με αποτέλεσμα να αισθάνονται βέβαιοι και σίγουροι να συνεχίσουν απρόσκοπτα την όποια δραστηριότητά τους[87].

Ο Κουράκης έχει προβεί σε ετυμολογική ανάλυση της έννοιας «ασφάλεια» μέσω της οποίας καταδεικνύει πως «*ασφάλεια υπάρχει όταν κάποιος δεν εκτίθεται σε κίνδυνο, όταν δηλ. απουσιάζει η πιθανότητα επέλευσης ενός κακού*»[88]. Κατά τον Παπαθεοδώρου, «*με τον όρο ασφάλεια περιγράφεται εννοιολογικά η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, η κατάσταση στην οποία αισθάνται κανείς ότι δεν απειλείται. ... Η ασφάλεια ως έννοια, αλλά και ως προσλαμβανόμενη αίσθηση προϋποθέτει μια συγκεκριμένη τάξη πραγμάτων στον κόσμο που μας περιβάλλει, ενώ συνιστά ταυτόχρονα το αποτέλεσμα μιας θετικής συστοιχίας δράσεων και αντιδράσεων μεταξύ του υποκειμένου και των διαφόρων καταστάσεων που το επηρεάζουν*»[89].

1.3.1 Ασφάλεια - ανασφάλεια στο διαδίκτυο και φόβος του εγκλήματος

Σε επίπεδο συστημάτων πληροφοριών ο ν. 3979/2011 στο ά. 3 ορίζει την ασφάλεια πληροφορικών συστημάτων ως εξής: «*Ασφάλεια Πληροφοριακών Συστημάτων: ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος (εφεξής ΠΣ), αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή*». Ο συγκεκριμένος ορισμός αναφέρεται σε σειρά στοιχείων τα οποία μπορούν να συνδράμουν στην αξιοπιστία και την ομαλή λειτουργία των συστημάτων

[86] Πρβλ. *Αν. Μαγγανά*, Το πρόβλημα της αποτίμησης του κινδύνου τέλεσης νέων εγκληματικών πράξεων, ΠοινΔικ, 1999, σελ. 1008-1016.

[87] Στο «Τεγόπουλος – Φυτράκης, Μικρό ελληνικό λεξικό» (1996) η λέξη «ασφάλεια» ορίζεται ως «***έλλειψη κινδύνου, σιγουριά***» και ως αντίθετή της καταγράφεται η λέξη «ανασφάλεια». Άλλες ερμηνείες της είναι: α) προφύλαξη από σφάλμα, ολίσθημα ή κίνδυνο, β) μέσο που αποτρέπει κίνδυνο (ασφάλεια όπλου, ηλεκτρική ασφάλεια) και γ) σύμβαση (μεταξύ ασφαλιστή και ασφαλιζόμενου με τηνοποία προβλέπεται αποζημίωση σε περίπτωση φθορών, καταστροφών ή άλλων ατυχημάτων.

[88] *Ν. Κουράκης*, Ασφάλεια και ελευθερία – Τα μεταξύ τους στατικά και δυναμικά όρια, εις: *Χ. Ζαραφωνίτου, (επιμ.)*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 7.

[89] Βλ. *Θ. Παπαθεοδώρου*, Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, όπου και εξαιρετική φιλοσοφική, θεωρητική και νομική προσέγγιση της έννοιας της ασφάλειας.

πληροφοριών. Είναι, όμως, γεγονός ότι έννοιες όπως «αντιλήψεις», «διαδικασίες» κ.ά., είναι αρκετά γενικές προκειμένου να μπορέσει ο νομοθέτης να τις επικαλεστεί αποτελεσματικά. Δεύτερο στοιχείο άξιο προσοχής, είναι το γεγονός ότι ο νομοθέτης αναφέρεται και σε τυχαία γεγονότα τα οποία μπορούν να συνιστούν απειλή για ένα σύστημα πληροφοριών, επεκτείνοντας με αυτόν τον τρόπο την έννοια του κινδύνου και ενδεχομένως τις τυχόν αποδιδόμενες ευθύνες.

Ο Κουράκης υποστηρίζει εύστοχα ότι «*...η ασφάλεια αποτελεί αυτονόητη προϋπόθεση για την ακώλυτη άσκηση και απόλαυση όλων των Δικαιωμάτων του Ανθρώπου ...*» και συνεχίζει λέγοντας ότι «*...η ασφάλεια αποτελεί τον τελικό σκοπό χάριν του οποίου οι άνθρωποι εγκαταλείπουν την επικίνδυνη κατάσταση του status naturalis και πειθαρχούν στην κρατική εξουσία του status civilis, θυσιάζοντας μέρος των ελευθεριών τους...*»[90]. Είναι προφανές ότι η διάσταση αυτή της ασφάλειας (safety / security)[91] τυγχάνει άμεσης εφαρμογής και στον ψηφιακό κόσμο και στο διαδίκτυο[92], καθώς τα δίκτυα και τα συστήματα πληροφοριών και ο κυβερνοχώρος αποτελούν πεδία ανάπτυξης, άσκησης και απόλαυσης δικαιωμάτων[93] [94]. Εξάλλου, και ο Παπαθεοδώρου υποστηρίζει ότι «*Η δημόσια ασφάλεια συνιστά, σε μια δημοκρατικά οργανωμένη κοινωνία, ένα προϊόν της ορθής λειτουργίας των θεσμών και μια προϋπόθεση της εγγύησης των δικαιωμάτων των πολιτών*»[95].

Στην εγκληματολογία, στην έννοια της «ανασφάλειας»[96] μπορούν να αναφέρονται πολλοί από εκείνους που απαντούν στις σχετικές έρευνες και δημοσκοπήσεις πως

---

[90] Βλ. *Ν. Κουράκη*, Το δικαίωμα του πολίτη στην ασφάλειά του, εις: Εγκληματολογικοί Ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, 2η εκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2005, σελ. 160.

[91] Πρβλ. την εννοιολογική διάκριση μεταξύ των λέξεων safety και security όπως καταγράφεται από τη *Χ. Ζαραφωνίτου* στον πρόλογο του τόμου επιμέλειάς της με τίτλο (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 7-9.

[92] Για διαδικτυακούς τόπους οι οποίοι αναφέρονται στην ασφάλεια στο διαδίκτυο βλ. *Χρ. Τσουραμάνη*, Internet και Ποινική Δικαιοσύνη – Προστασία της πνευματικής ιδιοκτησίας στο Internet, ΠοινΔικ 11/2002, σελ. 1177.

[93] Όλως ενδεικτικώς βλ. ά. 5, 5Α και 9Α του Συντάγματος, ά. 8 και 10 της ΕΣΔΑ, ά. 6 και 11 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ά. 10 Σύμβασης για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (Ρώμη, 4 Νοεμβρίου 1950), ά. 19 Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα κ.ά.

[94] Πρβλ. ενδεικτικά *Δ. Αναστασόπουλο*, Η προστασία της ιδιωτικότητας κατά το άρθρο 8 της ΕΣΔΑ στο ψηφιακό περιβάλλον, ΔιΜΜΕ 3/2012, σελ. 330, κατά τον οποίο «*το άρθρο 8 της ΕΣΔΑ δύναται να τύχει εφαρμογής σε κάθε δραστηριότητα που λαμβάνει χώρα στο σύγχρονο ψηφιακό περιβάλλον...*».

[95] *Θ. Παπαθεοδώρου*, Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 27.

[96] Πρβλ. σχετικώς *Έφης Λαμπροπούλου*, Κοινωνίες σε «κίνδυνο» και αίσθημα ανασφάλειας, ΠοινΔικ 5/2002, σελ. 556 επ. Βλ. επίσης και την κριτική προσέγγιση του *Γ. Πανούση*, Ανασφάλεια – Το "σκιάχτρο" της παγκοσμιοποίησης, ΠοινΔικ 10/2004, σελ. 1153 επ.

φοβούνται ότι θα θυματοποιηθούν[97]. Το αίσθημα της ανασφάλειας είναι η εντύπωση πως το έγκλημα αποτελεί πραγματική και σοβαρή απειλή, ώστε να επηρεάζει τη διαχείριση της καθημερινότητας σε ατομικό επίπεδο[98]. Το αίσθημα ασφάλειας (ή ανασφάλειας) στη χρήση συστημάτων ηλεκτρονικών πληροφοριών πρέπει να ιδωθεί και υπό το πρίσμα της «ψηφιακής κοινωνίας της διακινδύνευσης»[99], λαμβανομένου, μάλιστα, υπόψιν ότι δεν υπάρχει σύστημα ψηφιακά διασυνδεδεμένων συσκευών απολύτως ασφαλές[100]. Στο «ηλεκτρονικό περιβάλλον» οι συνθήκες είναι κατάλληλες για πλήρη ανάπτυξη φόβου θυματοποίησης. Ειδικότερα, ο φόβος του εγκλήματος[101] εκδηλώνεται όταν ο κίνδυνος εμφάνισης ενός δυσάρεστου περιστατικού δεν είναι αμελητέος, οι δυνατότητες άμυνας ή προστασίας φαίνονται ανεπαρκείς για την αντιμετώπισή του και οι προβλεπόμενες συνέπειες είναι πολύ δυσάρεστες και υπάρχει αδυναμία αποτροπής τους[102] - όλες οι ανωτέρω περιστάσεις φαίνεται να συντρέχουν στους χρήστες ηλεκτρονικών υπολογιστών και του διαδικτύου. Εξάλλου, σημαντικός παράγοντας έντασης της ανασφάλειας είναι η αντίληψη περί «ευπάθειας» / «ευάλωτου» (vulnerability)[103] των υποκειμένων[104] - το, δε, «ευάλωτο» των

---

[97] Έτσι *Χ. Ζαραφωνίτου*, Όψεις και διαστάσεις του κοινωνικού φαινομένου της ανασφάλειας, εις: *Χ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 37.

[98] Έτσι *Χρ. Ζαραφωνίτου*, Μελέτες Ευρωπαϊκής Νομικής Επιστήμης, Ο φόβος του εγκλήματος, Εγκληματολογικές προσεγγίσεις και προβληματισμοί με βάση την εμπειρική διερεύνηση του φαινομένου στο εσωτερικό της Αθήνας, Αθήνα-Κομοτηνή, Εκδόσεις Αντ. Ν. Σάκκουλα, 2002, σελ. 15 επ.

[99] Βλ. σχετικώς την εμπεριστατωμένη προσέγγιση των *Jonathan Jackson, Nick Allum and George Gaskell*, Perceptions of risk in cyberspace, London School of Economics and Politics, Cyber Trust & Crime Prevention Project, 04/06/2004, όπου και αναφέρονται στην έννοια της διακινδύνευσης κατά τον Beck και στην εμπειρική προσέγγιση της διακινδύνευσης σε συνδυασμό με το συναίσθημα σε ό,τι αφορά τον κυβερνοχώρο, καθώς το αίσθημα αυτό «*χρωματίζει τις αντιλήψεις και τις ερμηνείες τους*».

[100] *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, p. 19.

[101] «*...ο φόβος του εγκλήματος ορίζεται ως "μια λογική ή παράλογη κατάσταση συναγερμού ή ανησυχίας που προκαλείται από την πεποίθηση πως κάποιος κινδυνεύει να γίνει θύμα εγκλήματος" (McLaughlin, 2006)*» (έτσι *Χρ. Ζαραφωνίτου και συν.*, Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο, url: http://criminology.panteion.gr/attachments/article/407/e-life%20ppt.pdf, σελ. 4).

[102] *M. Killias*, Precis de criminology, Staempfli Editions SA Berne, 2001, p. 411.

[103] Οι Skogan & Maxfield (1981) εισήγαγαν πρώτοι την έννοια του ευάλωτου (βλ. *M. Killias & C. Clerici*, Different Measures of Vulnerability in their Relation to Different Dimensions of Fear of Crime, British Journal of Criminology, vol. 40 (3), 2000, p. 437-450 καθώς και *Wesley Skogan*, Fear of crime and neighborhood change, url: http://www.skogan.org/files/Fear.of.Crime.and.Neighborhood.Change.1986.pdf) στην εγκληματολογία και στον ρόλο που μπορεί να διαδραματίσει στο αίσθημα (αν)ασφάλειας και, άρα, στην επιστήμη της εγκληματολογίας. Η Perloff ορίζει το "ευάλωτο" ως «*...την αίσθηση ότι κάποιος είναι ευαίσθητος στα αρνητικά μελλοντικά αποτελέσματα και απροστάτευτος από τον κίνδυνο ή κάποια ατυχία (misfortune)...*» (βλ. *J. Jackson*, A psychological perspective on Vulnerability in the Fear of Crime, Psychology, Crime & Law, vol. 15(4), 2009, p. 369). Η έννοια του ευάλωτου συνδέεται, επομένως, άμεσα με τα αισθήματα άγχους και φόβου και ο Hale υποστήριξε ότι οποιοδήποτε μοντέλο επιχειρήσει να εξηγήσει τον φόβο του εγκλήματος είναι σημαντικό να συμπεριλάβει την έννοια του ευάλωτου. Ο πρώτος που

συστημάτων υπολογιστών[105] μπορούμε να υποστηρίξουμε ότι είναι συστατικό στοιχείο της λειτουργίας τους (χαρακτηριστικό παράδειγμα η χρήση "backdoors"[106] στα προγράμματα ηλεκτρονικών υπολογιστών: οι «πίσω πόρτες» ("backdoors") είναι σημεία τα οποία έχουν αφεθεί «ανοικτά» επίτηδες από τους δημιουργούς του προγράμματος του υπολογιστή για πρόσβαση στο πρόγραμμα, προκειμένου να μπορεί αυτός να εισέλθει για να διορθώσει τυχόν πρόβλημα – τα "backdoors" αποτελούν δυνητική «πύλη» χωρίς δικαίωμα πρόσβασης στα συστατικά στοιχεία του ηλεκτρονικού προγράμματος).

1.3.2 Η τεχνική διάσταση του όρου ασφάλεια στα συστήματα ηλεκτρονικών πληροφοριών και στο διαδίκτυο

Από τεχνική άποψη, ασφάλεια (security) είναι η προστασία ενός συστήματος πληροφοριών, υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη και αποτροπή της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα.

παρουσίασε ένα θεωρητικό μοντέλο για το ρόλο του «ευάλωτου» στην εκδήλωση ανασφάλειας και φόβου του εγκλήματος είναι ο Martin Killias κατά το έτος 1990. Το μοντέλο αυτό διακρίνει μεταξύ προσωπικών, κοινωνικών και περιστασιακών όψεων του «ευάλωτου» (φύλο, ηλικία, περιοχή κατοικίας κ.λπ.) και διαστάσεων των απειλών (πιθανότητα εγκλήματος, σοβαρότητα των ανεπιθύμητων συνεπειών και αίσθηση περί αδυναμίας ελέγχου των καταστάσεων αυτών) – (βλ. *Χρ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, Αθήνα-Κομοτηνή, Εκδόσεις Αντ. Ν. Σάκκουλα, 2007, σελ. 39).

[104] *Χρ. Ζαραφωνίτου*, Ανασφάλεια και επέκταση του κοινωνικού ελέγχου: Ποινικοποίηση των «αντικοινωνικοτήτων» και της «αταξίας», Ποινικός Λόγος, τεύχος 4, 2004 (ΕΤΟΣ 4ο), σελ. 2050.

[105] Για τις έννοιες του κινδύνου, της απειλής και της ευπάθειας στα συστήματα ηλεκτρονικών υπολογιστών βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 7 καθώς και *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, σελ. 22 επ. Επίσης, ο Φαρσεδάκης αναφέρεται αναλυτικά στα στοιχεία που καθιστούν ευάλωτους τους υπολογιστές και τα συστήματα πληροφοριών (βλ. *Ιακ. Φαρσεδάκης,* Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π., παρ. Ι).

[106] Αναφορικά με τα "backdoors" βλ. σχετικό λήμμα της ηλεκτρονικής εγκυκλοπαίδειας για θέματα υπολογιστών webopedia (url: http://www.webopedia.com/TERM/B/backdoor.html).

Ειδικότερα, η ασφάλεια των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να καλύπτει τις ειδικότερες εκφάνσεις της και, συγκεκριμένα, την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων[107]:

Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος.

Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας.

Διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος[108].

1.3.3 Η έννοια της ασφάλειας στον ελληνικό ΠΚ

Η έννοια της «ασφάλειας» δεν είναι άγνωστη στο ποινικό δίκαιο[109]. Στο 14ο κεφάλαιο του Ποινικού Κώδικα (άρθρα 290 επ.)[110], ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών και των κοινωφελών εγκαταστάσεων. Διαφορετική είναι η έννοια της «ασφάλειας» στο άρθρο 388 ΠΚ το οποίο ρυθμίζει την απάτη την σχετική με τις ασφάλειες[111]. Επίσης, η έννοια της «ασφάλειας» δεν έχει σχέση με τις ανωτέρω διατάξεις όπως χρησιμοποιείται στα άρθρα 69 επ. ΠΚ, τα

[107] Έτσι η ανάλυση και οι στόχοι της έννοιας της ασφάλειας στο πεδίο των δικτύων υπολογιστών περιγράφονται στο εγχειρίδιο εκπαίδευσης ασφαλείας υπολογιστικών συστημάτων της Microsoft (Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, p.5). Βλ. και *Ιωάννης Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 12/2001 (Έτος 4ο) σελ. 1295.

[108] Βλ. για περαιτέρω ανάλυση των εννοιών αυτών *Steven Furnell*, όπ. π., σελ. 21 επ. καθώς και παράγραφο 5.1.2 του παρόντος πονήματος.

[109] Βλ. και *Ιωάν. Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 12/2001, 1294.

[110] Βλ. αναλύσεις των άρθρων 290-298 ΠΚ ενδεικτικά στο πόνημα του *Μιχαήλ Μαργαρίτη*, Ποινικός Κώδικας (Ερμηνεία – εφαρμογή), εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2003, σελ. 752 επ.

[111] Βλ. ενδεικτικά *Μιχαήλ Μαργαρίτη*, Ποινικός Κώδικας, όπ. π., σελ. 1177 επ.

οποία αναφέρονται στα μέτρα ασφαλείας[112] ως μέρος της επιβολής ή εκτέλεσης των ποινών.

Η χρήση της ίδιας της έννοιας της ασφάλειας ως αυτοτελές προστατευόμενο δικαίωμα είναι βασίμως αμφισβητήσιμη[113]. Ωστόσο, η εξειδίκευση της ασφάλειας στο διαδίκτυο, όπως ανωτέρω (σε τεχνικό επίπεδο) αναλύεται, μπορεί ενδεχομένως να αποτελέσει αυτή καθεαυτή προστατευτέο έννομο αγαθό[114], λαμβανομένης υπόψιν της τεχνικής συγκεκριμενοποίησης των στοιχείων της, όπως προσδιορίστηκαν αμέσως ανωτέρω. Ο ποινικός κώδικας, πάντως, δεν αναφέρεται σε κανένα σημείο στην έννοια της ασφάλειας στο διαδίκτυο – τούτο, θεωρώ, διότι η ανάπτυξη των προστατευόμενων έννομων αγαθών, όπως θα αναλυθεί κατωτέρω, καταλαμβανόταν κυρίως από την έννοια του απορρήτου[115]. Οι ως άνω εκφάνσεις της ασφάλειας στον κυβερνοχώρο σε συνδυασμό με τον τρόπο δράσης των δραστών και των αποτελεσμάτων που επιφέρουν στα ηλεκτρονικά δεδομένα (π.χ. αποκλεισμός της πρόσβασης χωρίς να θιγεί το «απόρρητο» των δεδομένων) θεωρώ ότι επιβάλλουν την επαναθεώρηση της ποινικής προσέγγισης των ζητημάτων της ηλεκτρονικής ασφάλειας πληροφοριών σε θεωρητικό και ερευνητικό επίπεδο.

1.4 Αντικείμενο του παρόντος πονήματος

[112] Αναφορικά με τα μέτρα ασφαλείας βλ. αναλύσεις των ά. 69-76 ΠΚ ενδεικτικά *Μιχαήλ Μαργαρίτη,* Ποινικός Κώδικας, όπ. π., σελ. 177 επ. καθώς και *Ν. Κουράκη*, Εισαγωγή στη θεωρία της ποινής, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 46 επ. Πρβλ. ιδίως για την ιστορική τους βάση *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 74 επ.

[113] Πρβλ. *Μ. Καϊάφα – Γκμπάντι*, Ευρωπαϊκό ποινικό δίκαιο και Συνθήκη της Λισσαβώνας, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2011, σελ. 8-9, όπου και σχετικές παραπομπές. Πρβλ. και σχετικές αναπτύξεις των *Ν. Κουράκη*, Το δικαίωμα του πολίτη στην ασφάλειά του, εις: *Ν. Κουράκη*, Εγκληματολογικοί Ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π., σελ. 159 επ., *Ν. Λίβου*, Το πρόβλημα της ασφάλειας και η ασφάλεια ως πρόβλημα: Το παράδειγμα του ποινικού δικαίου, εις: Τιμητικός Τόμος για τον Ιωάννη Μανωλεδάκη, εκδ. Π. Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2005, σελ. 185-207 και συγκεκριμένα σελ. 189 υποσ. 11 και 12, *Κ. Χρυσόγονου*, Το θεμελιώδες δικαίωμα στην ασφάλεια, εις: *Χ. Ανθόπουλου, Ξ. Κοντιάδη και Θ. Παπαθεοδώρου (επιμ.)*, Ασφάλεια και δικαιώματα στην κοινωνία της διακινδύνευσης, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, σελ. 137-154 και *Θ. Παπαθεοδώρου*, Κυβερνητική της ασφάλειας και αντεγκληματική πολιτική: Η ποινική διαχείριση των δικαιωμάτων, εις: *Χ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 59 επ.

[114] Βλ. κατωτέρω παράγραφο 5.1.2 του παρόντος πονήματος.

[115] Βλ. σχετικές αναπτύξεις στα κεφάλαια 4 και 5 του παρόντος πονήματος.

Οι συμπεριφορές που αναπτύσσονται σε ηλεκτρονικό περιβάλλον, στα συστήματα πληροφοριών και στο διαδίκτυο απασχολούν πλέον ένα μεγάλο τμήμα της επιστημονικής κοινότητας. Τούτο διότι σε αρκετές περιπτώσεις ακόμη ελλείπουν – ή μάλλον είναι ακόμη υπό διαμόρφωση – οι ανεπίσημες νόρμες (απορρέουσες από δημοφιλή πεποίθηση) οι οποίες θα αποτελέσουν κάθε φορά τη «λυδία λίθο» για τον χαρακτηρισμό μιας συμπεριφοράς στο διαδίκτυο κατ' αρχάς ως παρεκκλίνουσας και εν συνεχεία ως ποινικώς κολάσιμης[116]. Αυτή ακριβώς είναι και η πρόκληση για νομικούς και εγκληματολόγους που καλούνται να σχεδιάσουν σήμερα αντεγκληματική πολιτική[117] αναφορικά με διαδικτυακές συμπεριφορές.

Συγκεκριμένα, στο πόνημα αυτό φιλοδοξείται να καταδειχθούν οι συνθήκες υπό τις οποίες μπορεί να αναπτυχθεί μια εγκληματοπροληπτική πολιτική η οποία θα συνδράμει στην ενίσχυση της ασφάλειας των ηλεκτρονικών πληροφοριών. Η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα εντάσσεται στο πλαίσιο συμπεριφορών που περιγράφονται με τον όρο hacking[118] και θέτει τουλάχιστον υπό αμφισβήτηση την ασφάλεια των ηλεκτρονικών πληροφοριών[119]. Στην ανά χείρας διατριβή προβαίνουμε σε επισκόπηση της έννοιας και των πρακτικών του hacking και στη συσχέτιση αυτών με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Καταγράφονται, επίσης, οι διακρίσεις και η διαστρωμάτωση των hackers, η εξέλιξή τους, η ηθική, η ιδεολογία και η (υπο)κουλτούρα τους και οι μέθοδοι και τεχνικές της δράσης τους.

Στη συνέχεια, στο κεφάλαιο 3 της διατριβής παρουσιάζονται εγκληματολογικές θεωρίες, οι οποίες δύνανται να ερμηνεύσουν και να εξηγήσουν τη χωρίς δικαίωμα

---

[116] Βλ. *του γράφοντος*, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

Επίσης, βλ. αντίστοιχα για τις διαφορετικές προσεγγίσεις – οι οποίες αταλάντευτα συνδέονται με τα (υπό διαμόρφωση) διαδικτυακά ήθη – αναφορικά με τη νομική αντιμετώπιση του πληροφορικού εγκλήματος *Γ. Λάζου*, Πληροφορική και Έγκλημα, όπ. π., σελ. 83 επ. Προς αυτήν την κατεύθυνση και ο Παπάνης κατά τον οποίο «*Στο Διαδίκτυο οι ανθρώπινες αξίες είναι ρευστές εξαιτίας της απεριόριστης ελευθερίας που παρέχει*» (έτσι *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 42).

[117] Για μια σύγχρονη θεώρηση της αντεγκληματικής πολιτικής πρβλ. ενδεικτικά *Σοφίας Βιδάλη*, Αντεγκληματική πολιτική: από τη μικροεγκληματικότητα έως το οργανωμένο έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013.

[118] Βλ. κατωτέρω αναλυτικά το κεφάλαιο 2 της διατριβής.

[119] Βλ. ανωτέρω την παράγραφο 1.3.3 αναφορικά με την τεχνική έννοια της ασφάλειας των ηλεκτρονικών δεδομένων.

πρόσβαση σε ηλεκτρονικά δεδομένα ειδικότερα, και το hacking γενικότερα, καθώς και να προτείνουν προσεγγίσεις πρόληψης.

Ιδιαίτερο βάρος δίνεται στη de lege lata προσέγγιση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking. Το hacking στο ποινικό δίκαιο, η παρουσίαση των διατάξεων διαφόρων χωρών αλλά και η ανάλυση των ελληνικών ποινικών διατάξων θα «φωτίσουν» τις έννοιες και θα δείξουν το «μονοπάτι», το οποίο έχει ήδη χαραχθεί από τον νομοθέτη και την ποινική θεωρία, προκειμένου να εξελίξουμε την νομική αντιμετώπιση του φαινομένου. Σημαντικό ρόλο διαδραματίζουν και οι νομοθετικές πρωτοβουλίες που έχουν αναληφθεί σε ευρωπαϊκό και διεθνές επίπεδο – γι' αυτόν τον λόγο στο κεφάλαιο 6 της παρούσας παρουσιάζονται και οι σύγχρονες ρυθμίσεις σε διακρατικό επίπεδο.

Στη συνέχεια εκτίθενται αποτελέσματα διερευνητικής/ περιγραφικής/ επεξηγητικής και αξιολογητικής έρευνας με ποσοτική και ποιοτική ανάλυση σε δείγμα νομικών, επιστημόνων πληροφορικής και hackers. Στόχος της έρευνας η διασαφήνιση του όρου hacking, η ανίχνευση του αν υπερέχει η ιδεολογία ή το οικονομικό όφελος ως κίνητρο του hacking, η αξιολόγηση της αποτελεσματικότητας της ισχύουσας ποινικής νομοθεσίας και οι προτάσεις εγκληματοπροληπτικών πρακτικών. Στο κεφάλαιο 7 παρουσιάζονται αναλυτικά τα αποτελέσματα της έρευνας επί των τριών ως άνω δειγμάτων καθώς και συγκρίσεις μεταξύ τους. Επ' αυτών των στόχων στο κεφάλαιο 8 αξιολογούνται τα αποτελέσματα της έρευνας και στο κεφάλαιο 9 διατυπώνονται σύγχρονες τάσεις και απόψεις για την ενίσχυση της ασφάλειας των συστημάτων πληροφοριών.

Η εργασία αυτή δεν (δύναται να) συμπεριλαμβάνει όλες τις παρεκκλίνουσες ή εγκληματικές συμπεριφορές στο διαδίκτυο[120] ή συμπεριφορές και πράξεις εκτός διαδικτύου, οι οποίες, όμως, έχουν ως αφετηρία τους τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα ειδικότερα[121] ή/και τη χρήση του διαδικτύου γενικότερα[122].

---

[120] Π.χ. ενδεικτικά την απάτη με ηλεκτρονικό υπολογιστή. Πρβλ. σχετικώς *Γ. Νούσκαλη*, Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκής Ένωση, ΠοινΔικ 2/2003, σελ. 178 επ.

[121] Π.χ. και όλως ενδεικτικώς τη δημοσίευση μιας φωτογραφίας σε κάποιο ηλεκτρονικό μέσο, η οποία έχει αποκτηθεί χωρίς δικαίωμα από τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό λογαριασμό.

[122] Είναι γεγονός ότι ως ηλεκτρονική εγκληματικότητα ή ως έγκλημα στο διαδίκτυο γίνεται πολλές φορές αντιληπτό και οποιοδήποτε έγκλημα μπορεί να έχει οποιαδήποτε σχέση (ακόμη και ως απλή «γενεσιουργό» αιτία) μια συμπεριφορά στο διαδίκτυο (βλ. ενδεικτικά τα δημοσιεύματα «Σοκ με την

17χρονη που δολοφονήθηκε από γνωριμία στο Facebook: Της χορήγησαν δια της βίας ηρωίνη», url: http://www.koolnews.gr/crime/sok-me-thn-17xronh-pou-dolofonithike-apo-gnwrimia-sto-facebook-ths-xorhghsan-dia-ths-vias-hrwinh/, *Β. Λαμπρόπουλου*, «Ειρωνείες προς το θύμα στο Facebook μετά τη δολοφονία - Νέα στοιχεία για τη δολοφονία που έγινε για ένα like», εφημερίδα «Το Βήμα», url: http://www.tovima.gr/society/article/?aid=405499 κ.ά.).

2. ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ (UNAUTHORIZED ACCESS TO ELECTRONIC DATA) ΚΑΙ HACKING

2.1 Ορισμός της έννοιας "hacking"

Η έννοια του "hacking"[123] αναφέρεται παραδοσιακά στη μη εξουσιοδοτημένη πρόσβαση (διείσδυση) σε σύστημα πληροφοριών ή σε στοιχεία εισηχθέντα σε υπολογιστή ή σύστημα υπολογιστών ή σε στοιχεία που μεταδίδονται με συστήματα υπολογιστών[124] [125]. Η πράξη αυτή, καταρχήν, δεν λαμβάνει χώρα με σκοπό

[123] Υποστηρίζεται ότι η λέξη "hacker" πρωτοεμφανίστηκε στην γερμανοεβραϊκή διάλεκτο Yiddish, όπου και σήμαινε κάποιον ανίκανο να φτιάξει έπιπλα με τσεκούρι. Η λέξη άλλαξε σημασίες μέσα στον χρόνο (εργαλείο κοπής ξύλου γύρω στα 1480, βίαιος κλέφτης έπειτα, κακός χρήστης της γλώσσας στα 1618 σύμφωνα με τον Thomas Cartwright κ.ά.). Τον 17ο αιώνα η διττή χρήση της λέξης προκαλεί εντύπωση (σε συνάρτηση και με το σημερινό της νόημα): από τη μια αναφέρεται σε κάποιον που δρα εκτός νόμου, από την άλλη, όμως, δύναται να περιγράφει και κάποιον εξαιρετικό επαγγελματία στο νόμιμο επάγγελμά του. Ο όρος πέφτει σε αχρησία μέχρι το 1960 οπότε και επανεισάγεται ως νεολογισμός με θετική έννοια για ιδιαιτέρως ικανούς και αποτελεσματικούς τεχνικούς ηλεκτρονικών υπολογιστών και προγραμματιστές.

Για την έννοια και την προέλευση της λέξης "hack" βλ. το αναλυτικό πόνημα του *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, url: http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf καθώς και το ενδιαφέρον άρθρο της *Aemilia Phillips*, In And Around Language: "Hack", The Harvard Crimson, url: http://www.thecrimson.com/article/2013/10/24/in-and-around-language-hack/.

Επίσης, για τον ορισμό του hacking βλ. ενδεικτικά urls: http://www.iss.net/security_center/advice/Underground/Hacking/default.htm http://www.urbandictionary.com/define.php?term=hacking, την ιστοσελίδα http://whatishacking.org/ καθώς και το αναλυτικό περιεχόμενο του κεφαλαίου "The meaning of 'hack' " (url: http://www.catb.org/jargon/html/meaning-of-hack.html).

[124] Για τη χωρίς δικαίωμα ή άδεια πρόσβαση σε ηλεκτρονικά δεδομένα βλ. την περιεκτική περιγραφή από την *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal Theory, Working Paper No. 249030, url: http://papers.ssrn.com/paper.taf?abstract_id=249030, p. 19 f.

[125] Σε ό,τι αφορά τον ορισμό του λήμματος hacker σε λεξικά: ενδεικτικά, το *21st Century Dictionary of Computer Terms* στο λήμμα hacker σημειώνει ότι «*..είναι μία λέξη της αγγλικής αργκό που αναφέρεται σε κάποιον που δεν έχει εκπαιδευτεί στη χρήση των ηλεκτρονικών υπολογιστών, για τους οποίους όμως επιδεικνύει πολύ μεγάλο ενδιαφέρον. Το άτομο αυτό μαθαίνει πειραματιζόμενο με τους ηλεκτρονικούς υπολογιστές, κάτι που συνεπάγεται συχνά το ότι αποπειράται να μπει σε βάσεις δεδομένων ή συστήματα ηλεκτρονικών υπολογοστών χωρίς να έχει σχετική εξουσιοδότηση από τον ιδιοκτήτη τους. Ένας hacker μπορεί ή δεν μπορεί να ενδιαφέρεται να αποκτήσει πληροφορίες στις οποίες δεν έχει νόμιμη*

υποκλοπής ή καταστροφής δεδομένων ή αρνητικής επενέργειας στις ηλεκτρονικές πληροφορίες αλλά κυρίως με σκοπό την ικανοποίηση του hacker για το γεγονός ότι πέτυχε να παρακάμψει το εκάστοτε σύστημα ασφαλείας που του απαγόρευε την εν λόγω πρόσβαση[126] [127]. Επίσης, hackers χαρακτηρίζονται και γενικότερα όσοι πλήττουν την ασφάλεια των συστημάτων πληροφοριών (σε οποιαδήποτε από τις εκφάνσεις της, π.χ. στη διαθεσιμότητα των πληροφοριών[128]) ακόμη και αν δεν αποκτούν χωρίς δικαίωμα πρόσβαση (π.χ. με DoS attack[129]) (άποψη για την οποία, βέβαια, υπάρχει αντίλογος από μερίδα των hackers[130])[131].

Ο όρος hacker απέκτησε αρνητική χροιά στη δεκαετία του 1980, όταν άρχισαν οι πρώτες επιθέσεις κατά ηλεκτρονικών δεδομένων. Στον hacker («παραβιαστή» κατά την Ακαδημία Αθηνών)[132] συχνά αποδίδονται και πράξεις επέμβασης πάνω στα στοιχεία στα οποία έχει αποκτηθεί η πρόσβαση όπως η τροποποίηση, η αλλοίωση[133], η υποκλοπή τους, ο ηλεκτρονικός βανδαλισμός κ.λπ.[134] [135] Οι επιθέσεις αυτές έγιναν η αφορμή για τη δημιουργία ως αντίθετου διευκρινιστικού όρου της λέξης cracker[136]

πρόσβαση...». Στο *The New Oxford Dictionary of English, 1998*, ως «hacker» ορίζεται το πρόσωπο που χρησιμοποιεί υπολογιστές προκειμένου να αποκτήσει πρόσβαση δίχως άδεια σε δεδομένα. Στο *Cambridge International Dictionary of English, 1995*, «hacker» είναι ένα πρόσωπο που διεισδύει σε υπολογιστικά συστήματα άλλων ανθρώπων.

[126] *Ulrich Sieber*, Legal aspects of computer-related crime in the Information society, January 1998, prepared for the European Commission, p. 41.

[127] Έτσι και *Α. Αργυρόπουλος*, Ηλεκτρονική Εγκληματικότητα, όπ. π., σελ. 34-35.

[128] Βλ. ανωτέρω παράγραφο 1.3.2.

[129] Βλ. κατωτέρω παράγραφο 2.11.2.2.2.

[130] Βλ. κατωτέρω και ιδίως στο Παράρτημα ΙΙΙ της παρούσας τις απαντήσεις των hackers στην ερώτηση 13 και συγκεκριμένα στα ερωτηματολόγια υπ' αρ. 7, 11, 14, 17 στα οποία υποστηρίζεται ότι οι "Anonymous" δεν είναι hackers γιατί προβαίνουν σε επιθέσεις Denial of Service (Dos), οι οποίες ουσιαστικά δεν είναι hacking!

[131] Βλ. και παράγραφο 7.8.4.2 κατωτέρω σχετικά με τις απαντήσεις των hackers και την ανάλυση σχετικά με τη sticto και lato sensu θεώρηση της έννοιας του hacking.

[132] Έτσι ο *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες. Β΄: Πραγματολογική προσέγγιση και επιμέρους ζητήματα, Δεύτερη Ανανεωμένη Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ. 183.

[133] Για την αλλοίωση δεδομένων βλ. την αναλυτική προσέγγιση του *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 422-423.

[134] *Tim Jordan*, Hacking and power: Social and technological determinism in the digital age, Journal "first Monday", vol. 14, n. 7, 6/7/2009, url: http://firstmonday.org/ojs/index.php/fm/article/view/2417/2240.

[135] Προς αυτήν την κατεύθυνση μάλλον ο Κιούπης αποδίδει στο πόνημά του τον όρο hacking ως «παρέμβαση» (έτσι *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 409 και 414 επ.).

[136] *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 13.

(όπως αναλύεται κατωτέρω[137]). Ωστόσο, αυτές οι συμπεριφορές δεν πρέπει να συγχέονται μεταξύ τους και ιδίως με την απλώς αποκτηθείσα πρόσβαση στα στοιχεία. Η διευκρίνιση αυτή είναι καίρια καθώς το hacking με τη μορφή της χωρίς εξουσιοδότησης πρόσβαση σε ηλεκτρονικές πληροφορίες αποτελεί τις περισσότερες φορές το πρώτο απαραίτητο βήμα[138] για την αλλοίωση ή καταστροφή ή οποιαδήποτε άλλη κακόβουλη και καταστροφική επενέργεια επί ηλεκτρονικών πληροφοριών[139], όπως η χρησιμοποίησή τους για ηλεκτρονικές απάτες[140] κ.ά. Μονάχα η πρόσβαση, ωστόσο, δεν προκαλεί (συνήθως) καταστροφή των ηλεκτρονικών πληροφοριών. Συνεπεία αυτών, πάντως, υποστηρίζεται ότι σήμερα ο όρος hacker είναι αμφιλεγόμενος[141].

Ο Jordan στον σύγχρονο ορισμό του για το hacking αναφέρεται σε υλικές πρακτικές (στο πλαίσιο χρησιμοποίησης υλικών μέσων - π.χ. ηλεκτρονικών υπολογιστών) που περιλαμβάνουν την προσπάθεια για διαφοροποίηση στον τομέα των τεχνολογιών πληροφορικής, επικοινωνιών και δικτύων, οι οποίες μπορούν να είναι παράνομες αλλά απολαμβάνουν τεχνικά κριτήρια αριστείας και μέσω αυτών έρχονται σε διαπραγμάτευση οι σχέσεις με την κοινότητα και την κοινωνία[142]. Η προσέγγιση αυτή πραγματοποιείται από τον Jordan συνδυαζόμενη και με απόψεις τεχνολογικού ντετερμινισμού[143] καθώς υποστηρίζει ότι η έννοια του hacking (έτσι όπως εξελίσσεται πάντα αντίστοιχα με την τεχνολογία) διαπραγματεύεται και αναδιαπραγματεύεται συνεχώς τη σχέση τεχνολογίας και κοινωνίας[144].

---

[137] Βλ. παράγραφο 2.3.1 του παρόντος πονήματος.

[138] Ως «βασικό έγκλημα» αναφέρει το hacking –με παραπομπή στον Sieber - ο *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 409.

[139] Έτσι και *Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 36.

[140] Πρβλ. ενδεικτικώς για τις σύγχρονες διαστάσεις τις οποίες λαμβάνει η απάτη μέσω συστημάτων ηλεκτρονικών πληροφοριών *Kristy Holtfreter, Shanna Van Slyke & Thomas G. Blomberg*, Sociolegal change in consumer fraud: From victim-offender interactions to global networks, Crime, Law & Social Change (2005) 44: 251–275.

[141] *Soumyo D. Moitra*, Developing Policies for Cybercrime - Some Empirical Issues, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13/3, 2005, pp. 435-464.

[142] *Tim Jordan*, Hacking and power: Social and technological determinism in the digital age, Journal "first Monday", vol. 14, n. 7, 6/7/2009, url: http://firstmonday.org/ojs/index.php/fm/article/view/2417/2240.

[143] Πρβλ. ενδεικτικά *Lynn Jr. White*, Medieval technology and Social Change, Oxford: University Press, 1962, *Peter Large*, The Micro Revolution, Fontana, 1980.

[144] Αξίζει να σημειωθεί στο παρόν σημείο ότι, σύμφωνα με ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή πρόβλεψης και πρόληψης εγκλήματος (Foresight Crime Prevention Panel), διαπιστώθηκε ότι το έτος 2020 οι hackers θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα μπορούν να ξεπερνούν

Ο ίδιος όρος (hacking) χρησιμοποιείται και για τις περιπτώσεις παραβίασης των τρόπων προστασίας και άλλων ηλεκτρονικών συσκευών ή διαδικασιών – χαρακτηριστικό παλαιότερο παράδειγμα ο χειρισμός τηλεφωνικών κυκλωμάτων με σκοπό τις δωρεάν κλήσεις σε όλο τον κόσμο (phone-hacking / phreaking)[145] – αλλά και γενικότερα για καινοτόμες δράσεις και πρακτικές, οι οποίες δεν έχουν απαραίτητα σχέση με υπολογιστικά συστήματα και πληροφορική (π.χ. biohacking και neurohacking)[146].

2.2 Ιστορία του hacking

οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμη δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού (Βλ. Εφημερίδα Έθνος της 6/4/2000, Ένθετο New Gen, σελ. 4).

[145] *Α. Αργυρόπουλος*, Ηλεκτρονική Εγκληματικότητα, Εγκληματο-Λογικά, σελ. 34-35.

[146] Χαρακτηριστικά παραδείγματα hacking που δεν έχουν να κάνουν με υπολογιστικά συστήματα είναι το ***biohacking*** και το ***neurohacking***.

Ειδικότερα, biohacking καλείται η πρακτική του συνδυασμού της βιολογίας με την ηθική των hackers. Το «biohacking» καλύπτει ένα ευρύ φάσμα των πρακτικών και κινημάτων, όπως το κίνημα «Grinders» («Μύλοι»), το οποίο σχεδιάζει και εγκαθιστά DIY (Do It Yourself) σωματικές βελτιώσεις, όπως τα μαγνητικά εμφυτεύματα. Επίσης, το biohacking έχει αναδειχθεί σε μια αυξανόμενη τάση «εξωθεσμικής» τεχνολογικής ανάπτυξης και μπορεί να παραπέμπει στη διαχείριση της βιολογίας ενός ατόμου, χρησιμοποιώντας ένα συνδυασμό της ιατρικής, διατροφής και των ηλεκτρονικών τεχνικών. Αυτό μπορεί να περιλαμβάνει τη χρήση «nootropics» και / ή «cybernetic» συσκευών για την καταγραφή των βιομετρικών δεδομένων. (βλ. αναλυτικότερα urls: http://en.wikipedia.org/wiki/Biohacking και http://en.wikipedia.org/wiki/Do_it_yourself).

Χαρακτηριστική ομάδα biohacking είναι η "DIYbio". Συγκεκριμένα, το δίκτυο "DIYbio" ιδρύθηκε το 2005 από τους Mackenzie Cowell και Jason Bobe και είναι ένα δίκτυο ατόμων από όλο τον κόσμο που έχει ως στόχο να προωθήσει τη βιολογία ως μια αξιόλογη επιστήμη για τους επιστήμονες, τους πολίτες, τους "biohackers", τους ερασιτέχνες βιολόγους, των οποίων κοινές αρχές είναι η διαφάνεια και η ασφάλεια. Οι συμμετέχοντες στα δίκτυα αυτά αυτοαποκαλούνται "biohackers" – οι hackers αυτοί δεν έχουν σχέση με υπολογιστικά συστήματα, με δίκτυα υπολογιστών και με ηλεκτρονικές πληροφορίες αλλά αναφέρονται περισσότερο στην αρχική σημασία της έννοιας, δηλαδή της τοποθέτησης με καλύτερο τρόπο ξεχωριστών πραγμάτων σε ενιαίο σύνολο (βλ. αναλυτικότερα url: http://en.wikipedia.org/wiki/DIYbio).

Το neurohacking είναι μορφή biohacking, η οποία εστιάζει στον εγκέφαλο και το κεντρικό νευρικό σύστημα. Ειδικότερα, ως neurohacking περιγράφεται οποιαδήποτε μέθοδος χειρισμού ή παρέμβασης της δομής ή / και της λειτουργίας των νευρώνων για τη βελτίωση και την αποκατάστασή τους. Κύριος στόχος του neurohacking είναι η βέλτιστη ψυχική υγεία του ατόμου. Άλλοι στόχοι περιλαμβάνουν την αποκατάσταση των βλαβών, την προσομοιωμένη πραγματικότητα, την πρόληψη των ασθενειών και την αύξηση των ικανοτήτων ή της νοημοσύνης. Επίσης, στο neurohacking χρησιμοποιείται τεχνολογία της πληροφορίας και κυρίως από τους τομείς της επιγενετικής, της βιο/νευροανάδρασης, της ψυχοφαρμακολογίας, της βιολογικής ψυχολογίας και της λειτουργικής ανάλυσης. Πολλοί χρησιμοποιούν και τη σωματική άσκηση, διατροφικές οδηγίες, βιταμίνες και συμπληρώματα, τον διαλογισμό ή / και την αυτο-ύπνωση. Η ηθική βάση του neurohacking για την υγεία είναι ότι θα πρέπει να εφαρμόζεται αυστηρά με τη συναίνεση του ατόμου (βλ. αναλυτικότερα url: http://en.wikipedia.org/wiki/Neurohacking).

Το hacking ως νοοτροπία και πρακτική υπάρχει ήδη από τη δεκαετία του 1950[147] (πολύ πριν από την εμφάνιση των δικτύων και των συστημάτων υπολογιστών και πληροφοριών). Ως «hack-ίστικη» (δηλαδή καινοτόμος) ιδέα ορίσθηκε αυτή που αναδιέτασσε τα μέχρι τότε δεδομένα στη χρήση της τεχνολογίας και της γνώσης γενικότερα (θα λέγαμε «τάραζε τα λιμνάζοντα νερά!»). Hacker, δηλαδή, αρχικώς θεωρήθηκε αυτός ο οποίος έβρισκε λύσεις σε προβλήματα, χρησιμοποιώντας μεθόδους πέρα από τις συμβατικές που στην εκάστοτε περίπτωση επικρατούν. Επίσης, κατά τον Levy, ο χαρακτηρισμός hacker αποδίδεται στις δεκαετίες του 1950 και του 1960 στους «γκουρού» της πληροφορικής (σε αυτούς, δηλαδή, οι οποίοι έχοντας εξαιρετικές δυνατότητες στην πληροφορική, ήταν ικανοί να βρίσκουν προχωρημένες λύσεις σε πολύπλοκα τεχνικά προβλήματα, καθώς οι λεπτομέρειες της τεχνολογίας των ηλεκτρονικών υπολογιστών ασκούν πάνω τους μια «παράξενη γοητεία»)[148].

Συγκεκριμένα, κατά τη δεκαετία του 1960 οι υπολογιστές τότε ήταν μηχανήματα κλειδωμένα σε δωμάτια με ελεγχόμενη θερμοκρασία και τεράστιο κόστος λειτουργίας και, συνεπώς, στους ερευνητές παρεχόταν περιορισμένος χρόνος εργασίας. Εκμεταλλευόμενοι τις τεχνικές γνώσεις τους, κάποιοι από αυτούς δημιούργησαν τα πρώτα "hacks", προγράμματα, δηλαδή, τα οποία βοηθούσαν στη γρηγορότερη εκτέλεση υπολογισμών. Αρκετές φορές τα προγράμματα αυτά (hacks) ήταν καλύτερα από τα αρχικά. Χαρακτηριστικό παράδειγμα ενός από τα πλέον γνωστά hacks είναι αυτό της δημιουργίας ενός προγράμματος hack για την αύξηση της ταχύτητας των ηλεκτρονικών υπολογιστών το 1969, το οποίο ονομάστηκε UNIX και σήμερα αποτελεί ένα ευρέως γνωστό λειτουργικό σύστημα[149].

Στα τέλη της δεκαετίας του 1960 στις Ηνωμένες Πολιτείες Αμερικής αντίστοιχες πρακτικές ακολουθήθηκαν από τους νεαρούς Αμερικανούς «phone phreaks», οι οποίοι προσπαθούσαν να «ξεγελάσουν» ηλεκτρονικά τα συστήματα της αμερικανικής τηλεφωνικής εταιρείας AT&T με σκοπό να κάνουν μακράς διάρκειας υπεραστικά τηλεφωνήματα χωρίς να πληρώνουν. Κατά τον Lapsley, είναι τότε που οι hackers θέτουν ως στόχο την περιπλάνηση σε απαγορευμένες ζώνες πληροφοριών, ώστε να

[147] Βλ. αναλυτικά για την ιστορία του hacking το άρθρο "A history of hacking" της εφημερίδας St. Petersburg Times online (url: http://www.sptimes.com/Hackers/history.hacking.html).

[148] *Steven Levy*, Hackers – Heroes of the Computer Revolution, ed. O'reilly.

[149] *Bruce Sterling*, The hacker crackdown: Law and Disorder on the Electronic Frontier, Bantam Books, 1992.

αποδείξουν την αδυναμία των συστημάτων ασφαλείας να τους σταματήσουν αλλά και αντίστοιχα τη δική τους ικανότητα διείσδυσης.[150]

Η διερεύνηση των ηλεκτρονικών συστημάτων υπήρξε, λοιπόν, ο σκοπός των πρώτων hackers. Οι πρώτοι αυτοί hackers αρκούνταν να εισέρχονται και να επεμβαίνουν σε συστήματα απλώς για να νιώθουν τη χαρά και την ικανοποίηση που τους προσέφερε, παραδείγματος χάριν, η εξεύρεση λύσης σε ένα πρόβλημα, όπως το σπάσιμο ενός κωδικού. Έτσι, το hacking θεωρήθηκε αρχικά μία ενδιαφέρουσα «περιπέτεια» χωρίς απώτερα οικονομικά συμφέροντα[151].

Άρα, αρχικά το «hacking» είχε την έννοια της καινοτομίας! Κάποια από τα χαρακτηριστικά, λοιπόν, του "πρώτου" hacker θα μπορούσε κάποιος να υποστηρίξει ότι είναι η πραγματιστική αντιμετώπιση του περιβάλλοντός του σε συνδυασμό με περιέργεια και «παιχνιδιάρικη» ευφυΐα. Σύμφωνα με τον Taylor[152], hacking θεωρείται η χρήση της τεχνολογίας με τρόπο που κανένας δεν είχε σκεφτεί ότι μπορεί να χρησιμοποιηθεί.[153]

Ωστόσο, με την ανάπτυξη των δικτύων ηλεκτρονικών πληροφοριών και της γιγάντωσης της σημασίας και αξίας των πληροφοριών αυτών[154], το hacking άρχισε να προσλαμβάνει σοβαρότερη μορφή, έχοντας ενίοτε ωφελιμιστικό χαρακτήρα και συνέπειες σε περιουσιακά αγαθά ή δεδομένα ατόμων ή φορέων του ιδιωτικού ή του κρατικού τομέα[155]. Οι δραστηριότητες των hackers έρχονται πλέον αντιμέτωπες με

---

[150] Για τους "phone phreaks" πρβλ. *Phil Lapsley*, Exploding the phone, 2013.

[151] Βλ. *Χρήστος Ε.Τσουραμάνης*, «Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου», όπ. π. σελ. 105.

[152] *P. Taylor*, Hackers: Crime in the digital sublime. London: Routledge, 1999.

[153] Ο γνωστός hacker Kevin Poulsen εξέτισε ποινή φυλάκισης για πράξεις hacking και φέρεται να δήλωσε: «*Έχω μάθει πολλά από τους νέους μου γείτονες... Τώρα γνωρίζω πώς μπορώ να ανάψω ένα τσιγάρο από μια πρίζα και πως μπορώ να φτιάξω μεταμφεταμίνη από έναν κύβο κότας»!* (Αναφορικά με τον Kevin Poulsen βλ. url: http://kingpin.cc/about/ και το σχετικό λήμμα "Kevin Poulsen" της ηλεκτρονικής εγκυκλοπαίδειας Wikipedia (url: http://en.wikipedia.org/wiki/Kevin_Poulsen).

[154] Βλ. ανωτέρω παράγραφο 1.2 του παρόντος πονήματος.

[155] Βλ. ενδεικτικά δημοσιεύματα α) "Γαλλία: «Εισβολή» χάκερς στο υπουργείο Οικονομικών με στόχο έγγραφα της G20" – url: http://tvxs.gr/news/%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5%CF%84-%CE%BC%CE%BC%CE%B5/%CE%B3%CE%B1%CE%BB%CE%BB%CE%AF%CE%B1-%C2%AB%CE%B5%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%C2%BB-%CF%87%CE%AC%CE%BA%CE%B5%CF%81%CF%82-%CF%83%CF%84%CE%BF-%CF%85%CF%80%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF%CE%BF-%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8E%CE%BD-%CE%BC%CE%B5-%CF%83%CF%84%CF%8C%CF%87%CE%BF-%CE%AD%CE%B3%CE%B3%CF%81%CE%B1%CF%86%CE%B1-%CF%84%CE%B7%CF%82-g20, β) «Οι χάκερς "Anonymous" χτύπησαν το NATO» – url: http://tvxs.gr/news/%CF%87%CE%AC%CE%BA%CE%B5%CF%81%CF%82/%CE%BF%CE%B9-

ζητήματα εθνικής ασφάλειας, προστασίας ανηλίκων, προστασίας της ανθρώπινης αξιοπρέπειας, προστασίας της ιδιωτικής ζωής, φθοράς ξένης ιδιοκτησίας, προστασία της καλής φήμης και της υπόληψης, πνευματικής ιδιοκτησίας[156], βιομηχανικής κατασκοπείας, ηλεκτρονικής κλοπής κωδικών πιστωτικών καρτών (carding[157]) και τραπεζικών κωδικών και ηλεκτρονικής απάτης σε χρηματιστηριακές συναλλαγές[158]. Απειλείται, δηλαδή, η ασφάλεια της ροής των πληροφοριών και δημιουργείται συγχρόνως κίνδυνος για σημαντικότατες βλάβες περιουσιακών αγαθών[159]. Η έτερη διάσταση του hacking, όμως, στην «ψηφιακή κοινωνία» την οποία δημιούργησαν τα ηλεκτρονικά συστήματα πληροφοριών, είναι αυτή της σημαντικής συμβολής στην ενίσχυση του δικαιώματος για ελεύθερη πρόσβαση στην πληροφόρηση[160] και τη γνώση[161].

%CF%87%CE%AC%CE%BA%CE%B5%CF%81%CF%82-anonymous-%CF%87%CF%84%CF%8D%CF%80%CE%B7%CF%83%CE%B1%CE%BD-%CF%84%CE%BF-%CE%BD%CE%B1%CF%84%CE%BF, γ) «επίθεση του Έλληνα hacker [PAOK] σε αξιωματικούς διωκτικών αρχών!» - url: http://thesspress.gr/index.php/texnologia/item/13591-epithesi-tou-ellina-hacker-paok-se-aksiomatouxous-dioktikon-arxon.html

[156] Για την πνευματική ιδιοκτησία στο διαδίκτυο βλ. *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 426-427 και για την προστασία την πευματικής ιδιοκτησίας όπως παρουσιάζεται σε ιστοσελίδες στο διαδίκτυο βλ. *Χρ. Τσουραμάνη*, Internet και Ποινική Δικαιοσύνη – Προστασία της πνευματικής ιδιοκτησίας στο Internet, ΠοινΔικ 11/2002, σελ. 1177.

[157] *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 129.

[158] Βλ. *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες, τομ. Β΄: Πραγματολογική προσέγγιση και επιμέρους ζητήματα, Δεύτερη Ανανεωμένη Έκδοση, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ. 185, 186 και 187.

[159] Βλ. *Ειρήνη Βασιλάκη*, Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής τους καταστολής: Προετοιμάζοντας το Ποινικό Δίκαιο του 21ου αιώνα;, εις: *Ν. Κουράκη (εκδ. επιμ.)*, Αντεγκληματική πολιτική, τομ. ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2000, σελ. 26 επ.

[160] Πρβλ. τη συνταγματική κατοχύρωση του εν λόγω δικαιώματος (ά. 5Α Σ και ιδίως την παρ. 2). Ωστόσο, υποστηρίζεται η άποψη ότι ήδη υπάρχουσες διατάξεις του Σ (ά. 5 παρ. 1, ά. 10 παρ. 1 ΕΣΔΑ και ά. 19 παρ. 2 ΔΣΑΠΔ) αρκούσαν για την προστασία των εν λόγω δικαιωμάτων (έτσι *Π. Δαγτόγλου*, Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα, τομ. Α' και Β', εκδ, Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, 2002, σελ. 524 και *Α. Τάκη*, Κοινωνία της Πληροφορίας και Σύνταγμα – μια πρώτη προσέγγιση, ΝοΒ 2002, σελ. 44).

[161] Χαρακτηριστικό παράδειγμα της απόλυτης διαφάνειας στο διαδίκτυο αλλά και του ηλεκτρονικού «πολέμου» και της τεράστιας σημασίας της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα (hacking) αποτελεί η περίπτωση της πολύκροτης υπόθεσης «wikileaks».

Η φημισμένη ιστοσελίδα ιδρύθηκε το 2006 και σύμφωνα με τον αρχισυντάκτη της Τζούλιαν Ασάνζ (ιδρυτής της και υπεύθυνος αυτής κατ' άλλους – ο ίδιος, ωστόσο, δεν το έχει ποτέ παραδεχθεί), αποτελεί «*αναμφίβολα την πιο αξιόπιστη πηγή πληροφοριών που υπάρχει, επειδή δημοσιεύουμε υλικό από πρωτογενείς πηγές*». Έχει προκαλέσει πονοκέφαλο σε αρκετές κυβερνήσεις, δημόσιες υπηρεσίες και ιδιωτικές εταιρείες, εξαιτίας της δημοσιοποίησης χιλιάδων απόρρητων εγγράφων που έφτασαν με άγνωστους τρόπους στην κατοχή της. (βλ. δημοσίευμα «Τζούλιαν Ασάνζ: από το χάκινγκ στα... βουλευτικά έδρανα;», url: http://gr.euronews.com/2013/01/30/assange-wikileaks-elections-senate-australia-ekloges-ypopsifiotita/). Ενδεικτικά για το περιεχόμενο των δημοσιευθέντων εγγράφων βλ. το δημοσίευμα «WikiLeaks: Η 11η Σεπτεμβρίου της διπλωματίας» - url:

Άρα, η δυναμική ανάπτυξη της τεχνολογίας και μετέπειτα η εμφάνιση του διαδικτύου συνετέλεσε στην αλλαγή των ποιοτικών χαρακτηριστικών του hacking[162], καθώς το

http://tvxs.gr/news/%CE%BA%CF%8C%CF%83%CE%BC%CE%BF%CF%82/wikileaks-%CE%B7-11%CE%B7-%CF%83%CE%B5%CF%80%CF%84%CE%B5%CE%BC%CE%B2%CF%81%CE%AF%CE%BF%CF%85-%CF%84%CE%B7%CF%82-%CE%B4%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%AF%CE%B1%CF%82.

Ο Τζούλιαν Ασάνζ υπήρξε hacker από την εφηβεία του στην Αυστραλία με το ψευδώνυμο Mendax, μέλος της ομάδας "International Subversives". Το 1991 καταδικάστηκε για 24 αδικήματα - αφέθηκε ελεύθερος πληρώνοντας εγγύηση 2.400 δολαρίων Αυστραλίας. Το 1994 αποφάσισε να δουλέψει ως προγραμματιστής ελεύθερου λογισμικού και το 1999 καταχώρησε το domain leaks.org. Μεταξύ 2003 και 2006 σπούδασε στο Πανεπιστήμιο της Μελβούρνης φυσική και μαθηματικά, αλλά δεν κατάφερε να πάρει πτυχίο (βλ. *Ειρήνη Μητροπούλου*, «"Διαρρέω", άρα υπάρχω!», εφημερίδα «ΤΟ ΒΗΜΑ», 24 Δεκεμβρίου 2010, url: http://www.tovima.gr/society/article/?aid=374595).

Η ιστοσελίδα wikileaks.org φαίνεται να ακολουθεί και αυτή πρακτικές hacking προκειμένου να αποκτήσει πρόσβαση σε πληροφορίες (βλ. *Michael Riley*, "Is WikiLeaks Hacking for Secrets?", Bloomberg Business Week Magazine, 3 Φεβρουαρίου 2011, url: http://www.businessweek.com/magazine/content/11_07/b4215046290051.htm. Ωστόσο, η ίδια η σελίδα η οποία έχει επικεφαλής της έναν (πρώην;) hacker(!) καταγγέλλει ότι γίνεται και αυτή θύμα επίθεσης hacking με τη μορφή DoS attack εν όψει δημοσιοποίησης απόρρητων εγγράφων των ΗΠΑ τον Νοέμβριο του 2010 (βλ. «Πώς δόθηκαν στη δημοσιότητα οι αποκαλύψεις του WikiLeaks», 29 Νοεμβρίου 2010, url: http://tvxs.gr/news/%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5%CF%84-%CE%BC%CE%BC%CE%B5/%CF%80%CF%8E%CF%82-%CE%B4%CF%8C%CE%B8%CE%B7%CE%BA%CE%B1%CE%BD-%CF%83%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%BF%CF%83%CE%B9%CF%8C%CF%84%CE%B7%CF%84%CE%B1-%CE%BF%CE%B9-%CE%B1%CF%80%CE%BF%CE%BA%CE%B1%CE%BB%CF%8D%CF%88%CE%B5%CE%B9%CF%82-%CF%84%CE%BF%CF%85-wikileaks).

Πέραν των ανωτέρω, η κολεκτίβα των hackers την με την επωνυμία "Anonymous" όχι μόνο στήριζαν την δράση του wikileaks, παρέχοντας στην ιστοσελίδα έγγραφα και πληροφορίες τα οποία έχουν αποκτήσει μέσω hacking, αλλά και όταν εταιρείες όπως το Amazon και το Paypal διέκοψαν την χρηματοδότηση της ιστοσελίδας wikileaks τον Δεκέμβριο του 2010 αυτές κατέστησαν θύματα επιθέσεων των "Anonymous" (βλ. άρθρο «13 Anonymous Hackers Plead Guilty To 2010 PayPal Attack», url: http://www.redorbit.com/news/technology/1113023408/anonymous-hackers-plead-guilty-to-paypal-attack-120913/#7Uvfvofcvlbgmfds.99) – για τη σχέση "Anonymous" και wikileaks βλ. το άρθρο «Anonymous and WikiLeaks: Is it really a breakup?», url: http://rt.com/news/anonymous-wikileaks-assange-paywall-572/).

Είναι προφανές ότι η διπλωματική κατασκοπεία αλλά και η στρατηγική επίδειξης ισχύος έχει πλέον ως βασικό της παράγοντα την ικανότητα απόκτησης χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα.

[162] Γενικότερα, η ευρύτατη διάδοση της χρήσης του διαδικτύου μετέβαλλε σταδιακά την παραδοσιακή ηλεκτρονική εγκληματικότητα. Από τη φαινομενολογία της εγκληματικότητας αυτής γίνεται λόγος για μία μετα-ηλεκτρονική εγκληματικότητα, σκοπός της οποίας φαίνεται να μην είναι τόσο η απόκτηση περιουσιακού οφέλους αλλά η αθέμιτη χρήση τεχνικών πληροφορικής, ενώ η παράνομη επεξεργασία πληροφοριών και ηλεκτρονικών στοιχείων κατευθύνεται σε διαφορετικό στόχο (βλ. *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, όπ. π. σελ. 191). Πρόσθετα γνωρίσματα αυτής της μετα-ηλεκτρονικής εγκληματικότητας είναι η αδυναμία εξατομίκευσης του θύματος, η χρήση του διαδικτύου, η τοπική απόσταση του δράστη από το θύμα κ.λπ.

διαδίκτυο, ως κατεξοχήν χώρος διασύνδεσης δικτύων και αρχείων, αποτελεί τον πλέον προνομιακό χώρο για τους επίδοξους hackers[163].

Χαρακτηριστικό της εξέλιξης του hacking είναι ότι, πέραν της επιδιωκόμενης ελευθερίας της πληροφορίας, οι γνώσεις και τεχνικές των hackers χρησιμοποιούνται πλέον και για κυβερνοεπιθέσεις, οι οποίες λαμβάνουν χώρα με τη χρήση κακόβουλων λογισμικών – ιών – σκουληκιών – ειδικών προγραμμάτων ("malware") καθώς και με τη χρήση παράνομου δικτύου προγραμμάτων ρομπότ (BOTNET)[164]. Οι ίδιες οι πρακτικές hacking έχουν λάβει πλέον τέτοια διάσταση ώστε ακόμη και νέα «επαγγέλματα» εχουν προκύψει όπως π.χ. ο "botnet herder"[165]: ο "βοσκός botnet" ("botnet herder") είναι αυτός που διαχειρίζεται ένα μεγάλο σύνολο υπολογιστών zombies (ένα «botnet») και το εκμισθώνει σε όσους επιθυμούν να στείλουν spam μηνύματα[166] ή να το χρησιμοποιήσουν κακόβουλα (π.χ. DDoS attacks ή εκβίαση με την απειλή DDoS attacks κ.λπ.).

Με βάση την κατηγοριοποίηση των ψηφιακών εγκλημάτων[167] σε γνήσια και παραδοσιακά, το hacking θεωρείται γνήσιο ψηφιακό έγκλημα, με την έννοια ότι

---

[163] Βλ. *Ιωάννης Κ. Καράκωστας*, Δίκαιο και Internet. Νομικά ζητήματα του Διαδικτύου, 3η έκδοση, Εκδόσεις Δίκαιο & Οικονομία Π. Ν. Σάκκουλας, Αθήνα 2009, σελ. 160.

[164] Ο όρος «BOTNET» υποδηλώνει ένα δίκτυο υπολογιστών που έχουν προσβληθεί από κακόβουλο λογισμικό (π.χ. ιούς). Ένα τέτοιο δίκτυο υπονομευμένων υπολογιστών, τον έλεγχο των οποίων έχουν απολέσει οι νόμιμοι χρήστες καθίσταται "ZOMBIE", χρησιμοποιείται εν αγνοία των νόμιμων χρηστών προκειμένου να επιτεθούν σε συστήματα πληροφοριών. Τα BOTNETS που χρησιμοποιούνται για επιθέσεις μεγάλης κλίμακας που αγγίζουν μέχρι και τις 100.000 συνδέσεις.

Τα BOTNETS χρησιμοποιούνται, επίσης, για να προκαλέσουν DoS Attacks (Denial of Service Attacks – «Άρνηση Υπηρεσίας») αλλά και για την αποστολή spam e-mails (ενοχλητικό ηλεκτρονικό ταχυδρομείο). Βλ. αναφορικά με τους υπολογιστές-zombies *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker*, Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series No 78, Australian Institute of Criminology, pp. 56 f και το ενδιαφέρον πόνημα του *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-Zavrsnik.pdf, p. 3.

[165] *Tyler Moore, Richard Clayton, and Ross Anderson*, The Economics of Online Crime, Journal of Economic Perspectives—Volume 23, Number 3—Summer 2009 — p. 5.

[166] Αναφορικά με τα μηνύματα spam και τον ρόλο τους στο διαδίκτυο πρβλ. *David S. Wall*, Digital Realism and the Governance of Spam as Cybercrime, European Journal on Criminal Policy and Research, 10(4): 309 – 335 και *Michael Kunz & Patrick Wilson*, Computer Crime and Computer Fraud, Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004, url: http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf, p. 17 και στην ελληνική βιβλιογραφία για το φαινόμενο του spamming βλ. *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 430 επ.

[167] Για την κατηγοριοποίηση των ψηφιακών εγκλημάτων από τον Αγγελή βλ. χαρακτηριστικά ανωτέρω και την υποσημείωση υπ' αρ. 3.

τελείται και εξιχνιάζεται αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας[168].

2.3 Κατηγοριοποιήσεις των "hackers"

2.3.1 Hackers και crackers

Η μετάλλαξη του hacking από εκδήλωση περιέργειας σε εγκληματική δραστηριότητα δημιούργησε την ανάγκη στις κοινότητες των hackers για «απομόνωση» όσων προβαίνουν σε επιβλαβείς ενέργειες. Βασική, λοιπόν, διάκριση αποτελεί ο διαχωρισμός των ηλεκτρονικών παραβιαστών σε hackers και crackers[169]. Με τον όρο cracker[170] περιγράφεται αυτός που αρέσκεται σε επιβλαβείς πράξεις στα συστήματα στα οποία εισχωρεί, όπως ενδεικτικά η καταστροφή αρχείων, η διαγραφή ή τροποποίηση δεδομένων, η κατάρρευση συστημάτων και η υποκλοπή πληροφοριών. Η λέξη "cracker" φέρεται να επινοήθηκε το 1985 από τους ίδιους τους hackers (προφανώς προέρχεται από μια ευρηματική ένωση των λέξεων "criminal" + "hacker" = cracker ή από το ρήμα "crack" το οποίο σημαίνει «σπάζω»[171]) προκειμένου να διαχωριστούν οι ίδιοι από όσους, παραβιάζοντας την ασφάλεια συστημάτων, παρεμποδίζουν τη λειτουργία τους ή προκαλούν βλάβες σε αυτά[172]. Έτσι, ενώ οι

---

[168] Βλ. *Χρήστος Ε.Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, όπ. π. σελ. 12.

[169] Ο Αργυρόπουλος αναφέρει ως τρίτη κατηγορία τους *crashers*, η πρακτική των οποίων, όμως, δεν διαφέρει από αυτήν των crackers. Ωστόσο, ο Αργυρόπουλος επισημαίνει ότι οι crackers είναι πιο επικίνδυνοι (έτσι *Α. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 41).

[170] Σύμφωνα με το *Λεξικό διαδικτύου και δικτύων της Microsoft* ο "cracker" είναι «*...διαρρήκτης, σπάστης... Κάποιος που παρακάμπτει τα μέτρα ασφαλείας ενός συστήματος υπολογιστή και αποκτά μη εξουσιοδοτημένη πρόσβαση…*». Βλ. και *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 54.

[171] ... ή από έξυπνο συνδυασμό και των δύο αυτών απόψεων!

[172] *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 9 (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

crackers συχνά αυτοαποκαλούνται hackers, οι hackers που δεν προβαίνουν σε επιζήμιες ενέργειες θεωρούν τους crackers ξεχωριστή και υποδεέστερη κατηγορία[173].

Ως hackers, δηλαδή, συμπληρωματικά σε όσα ειπώθηκαν παραπάνω, εννοούνται όσοι «εισβάλλουν» στα ξένα συστήματα κυρίως από ευχαρίστηση ή περιέργεια και από αγάπη για την πρόκληση, χωρίς να επιδιώκουν εμφανώς (αρχικώς τουλάχιστον) να αντλήσουν οικονομικό όφελος ή να προκαλέσουν οικονομική ζημία[174]. Αντίθετα, στην έννοια του cracker εντάσσονται όσοι βλάπτουν τα αρχεία του ξένου συστήματος, στο οποίο απέκτησαν παράνομη πρόσβαση, αποσκοπώντας κυρίως σε οικονομικό όφελος ή ζημία[175]. Βέβαια, οι συμπεριφορές που περιγράφονται από αμφότερους τους παραπάνω όρους σε αρκετές νομοθεσίες θεωρούνται αξιόποινες, ανεξάρτητα από το κίνητρο το οποίο ώθησε στη διάπραξή τους[176].

2.3.2 Διαχωρισμός των hackers ανάλογα με τον σκοπό και το αποτέλεσμα της δράσης τους

Ένας επιπλέον διαχωρισμός των hackers είναι εκείνος μεταξύ των όρων «hacker με μαύρο καπέλο», «hacker με άσπρο καπέλο» και «hacker με γκρι καπέλο»[177] [178] [179]. Η έμπνευση για τον ευφάνταστο αυτό διαχωρισμό φαίνεται να προέρχεται από τις παλιές ταινίες «γουέστερν», στις οποίες οι «κακοί» φορούσαν μαύρα καπέλα ενώ οι «ήρωες» άσπρα καπέλα![180] [181] Ο τύπος «hacker με μαύρο καπέλο» (“black hat

---

[173] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, Μετάφραση: Φωτεινή Α. Μηλιώνη, εκδ. Παπαζήση, Αθήνα, 2006, σελ. 51-52.

[174] Βλ. *Ιωάννης Εμμ. Αγγελής*, Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο, ΠοινΧρ Ν/2000, σελ. 677.

[175] Βλ. *Donn B. Parker*, Fighting Computer Crime, Εκδόσεις Wiley, New York 1998, σελ. 15.

[176] Βλ. *Χρήστος Ε. Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, Εκδόσεις Βασ. Ν. Κατσαρού, Αθήνα 2005, σελ. 101.

[177] *Larisa April Long*, Profiling hackers, January 2012, url: http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864, p. 4 f.

[178] Αναφορικά με τους «hackers με λευκά καπέλα», «μάυρα καπέλα» και «γκρι καπέλα» και τη «διαμάχη» μεταξύ τους βλ. το δημοσίευμα «Οι φυλές των χάκερ – Ένας άτυπος πόλεμος βρίσκεται σε εξέλιξη μεταξύ καλών και κακών», εφημερίδα «ΤΑ ΝΕΑ», Τετάρτη 10 Ιουλίου 2013, σελ. 30.

[179] Βλ. σχετικές αναλύσεις στο πόνημα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 46 f. και στο κεφάλαιο με τον ευφάνταστο τίτλο “The Colors of the Underground”.

[180] Βλ. url: http://searchsecurity.techtarget.com/definition/black-hat.

hackers") αναφέρεται στους hackers που προσπαθούν να αποκτήσουν πρόσβαση σε συστήματα ή δεδομένα χωρίς άδεια συνήθως, με σκοπό το οικονομικό όφελος ή την περαιτέρω επιβλαβή δράση (π.χ. καταστροφή ιστοσελίδας κ.ά.). Ουσιαστικά, θεωρώ πως όσοι κατατάσσονται στην κατηγορία των "black hat hackers" συμπίπτουν σε μεγάλο βαθμό με όσους θεωρούνται crackers, σύμφωνα με όσα αναπτύχθηκαν προηγουμένως[182]. Οι "hackers του λευκού καπέλου" ("white hat hackers"), αντίθετα, είναι αυτοί οι οποίοι δρουν με γνώμονα το καλό των συστημάτων ασφαλείας καθώς προσπαθούν να ανακαλύψουν τις «κερκόπορτες» - τα αδύνατα σημεία των συστημάτων, να τα επισημάνουν και να τα διορθώσουν, προκειμένου να αποφευχθούν οι ως άνω πράξεις των παραβιαστών με μαύρο καπέλο.[183]

Περαιτέρω, ο όρος «χάκερ με γκρίζο καπέλο» ("gray/ grey hat hackers")[184] χρησιμοποιείται για όσους βρίσκονται ανάμεσα στις δύο ως άνω κατηγορίες και των οποίων τα κίνητρα είναι αδιευκρίνιστα ή έχουν την τάση να αλλάζουν, όπως κατά τον Furnell είναι οι κυβερνοτρομοκράτες, οι κυβερνοπολεμιστές, οι «χακτιβιστές», οι δημιουργοί επιβλαβών προγραμμάτων, οι φρίκερ, οι σαμουράι, οι κλέφτες προγραμμάτων, οι Warez d00dz κ.α[185]. Σύμφωνα με άλλον ορισμό, οι "grey hat hackers" διαφέρουν από τους "white hat hackers" αναφορικά με το ότι οι "white hat" δεν δημοσιοποιούν τα κενά ασφαλείας που εντοπίζουν ενώ οι "grey hat" τα δημοσιοποιούν, δίνοντας έτσι ευκαιρία σε "black hat hackers" να τα εκμεταλλευτούν.[186]

---

[181] Για τις «ομοιότητες» του διαδικτύου με την "άγρια δύση" (sic), παρομοίωση η οποία χρησιμοποιείται αρκετά και δίνει ουσιαστικά την αφορμή για την χρησιμοποίηση των εν λόγω παραδειγμάτων και κατηγοριοποιήσεων βλ. το άρθρο "Geek Rants: Why the Internet is Like the Wild West" – url: http://www.howtogeek.com/62135/geek-rants-why-the-internet-is-like-the-wild-west/.

[182] Βλ. ενδεικτικά το άρθρο του *Paul Gil (contributing writer, John "r3d h4tt3r" Anonymous)*, "What is a 'Hacker'? Is that the same as a 'hax0r'?", url: http://netforbeginners.about.com/od/h/f/haxor.htm στο οποίο ως "black hat hackers" ορίζονται αυτοί οι οποίοι παραβαίνουν τον νόμο και ως "white hat hackers" ορίζονται οι ειδικοί στην προώθηση της ασφάλειας των ηλεκτρονικών δεδομένων.

[183] Για τον ορισμό των "black hat hackers" και τη διάκριση από τους "white hat hackers" βλ. url: http://www.techopedia.com/definition/26342/black-hat-hacker.

[184] Ο όρος «χάκερ με γκρίζο καπέλο» (gray/ grey hat hackers) επινοήθηκε από μια από τις παλαιότερες ομάδες hackers με όνομα "L0pht" (*Cynthia Fitch*, Crime and Punishment: The Psychology of Hacking in the New Millennium, url: http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795, όπου και ορισμοί για "white hat hackers", "black hat hackers" και "gray hat hackers").

[185] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 55.

[186] Έτσι για τους "gray/ grey hat hackers" ο ορισμός που δίνεται στο url: http://searchsecurity.techtarget.com/definition/gray-hat

2.3.3 Διαστρωμάτωση («τάξεις») των hackers

Στη βιβλιογραφία έχουν καταγραφεί ειδικότερες κατηγοριοποιήσεις του ετερογενούς συνόλου των hackers με βασικό κριτήριο το πλαίσιο των γνώσεων και δεξιοτήτων αλλά και των δράσεών τους[187]. Οι συχνότερα αναφερόμενες «τάξεις»[188] των hackers είναι οι εξής[189]:

Elite[190]: Στην «τάξη» αυτή (την «ελίτ») συμμετέχουν οι hackers που έχουν γνώσεις και δεξιότητες του υψηλότερου επίπεδου[191], εμπειρία, ηθική και ακεραιότητα. Φαίνεται ότι η κατηγορία αυτή είναι η σπανιότερη και περιλαμβάνει τους λιγότερους hackers. Οι elite hackers συνήθως κατατάσσονται στους white hat hackers καθώς δεν προβαίνουν σε κακόβουλες ενέργειες αλλά ανακαλύπτουν κενά ασφαλείας και άλλα προβλήματα κωδικοποίησης σε ηλεκτρονικά προγράμματα. Οι περισσότεροι elite hackers κρούουν τον κώδωνα του κινδύνου στους διαχειριστές συστημάτων αναφορικά με θέματα ασφαλείας ενημερώνοντάς τους για τα τρωτά σημεία των δεδομενων τους και δεν δημοσιεύουν τα κενά ασφαλείας των συστημάτων. Η είσοδος στην elite τάξη των hackers μπορεί επίσης να λάβει χώρα χάριν ενός περίφημου κατορθώματος hacking ή μετά από διαρκή σημαντική παρουσία στο πεδίο του hacking.

---

[187] Για μια διαφορετική από την παρούσα «ταξινόμηση» των hackers βλ. *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, url: http://bscw.cs.ncl.ac.uk/pub/bscw.cgi/d48026/Arief%20and%20Besnard%20-%20Technical%20and%20Human%20Issues%20in%20Computer-Based%20Systems%20Security.pdf, σελ. 12.

[188] Βλ. *Cynthia Fitch*, M.Ed., Crime and Punishment: The Psychology of Hacking in the New Millennium, url: http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795, pp. 6-7.

[189] Η εν λόγω παρουσίαση της διαστρωμάτωσης των hackers αποτελεί συνδυασμό άλλων «ταξινομήσεων» κατ' επιλογήν του γράφοντος.

[190] Βλ. ιστοσελίδα για τους elite hackers στο οικείο url: http://www.elite-hackers.com/

[191] Αναφορικά με τις εξαιρετικές ικανότητες των elite hackers βλ. το ρεπορτάζ του *Russell Brandom*, The NSA's elite hackers can hijack your Wi-Fi from 8 miles away, 30 Δεκεμβρίου 2013, url: http://www.theverge.com/2013/12/30/5256636/nsa-tailored-access-jacob-appelbaum-speech-30c3.

Script kiddies[192] [193]: Οι hackers της «τάξης» αυτής αποτελούν μια αρκετά ευρεία[194], αλλά περιφρονημένη υποομάδα εντός της ευρύτερης κοινότητας των hackers, λόγω του ότι σε αυτήν κατατάσσονται οι νεώτεροι [σε εμπειρία αλλά και κάποιες φορές και ηλικιακά (ανήλικοι)] και λιγότερο ικανοί hackers. Οι hackers αυτοί χρησιμοποιούν «εργαλεία» που δημιουργούνται από την τάξη των elite hackers[195] επειδή οι ίδιοι δεν έχουν τις γνώσεις για να τα δημιουργήσουν[196]. Είναι αρκετά επικίνδυνοι, όμως, και συνήθως κατατάσσονται στους black hat hackers[197]. Οι script kiddies δεν υποκινούνται από κανέναν συγκεκριμένο παράγοντα και μάλλον αναζητούν εύκολους στόχους. Χαρακτηρίζονται, επίσης, ανώριμοι και φυγόπονοι και, συνεπώς, δεν απολαμβάνουν αναγνώριση[198] και σεβασμό. Ωστόσο, η αναφορά σε αυτούς είναι σημαντική γιατί η δημόσια αντίληψη για το hacking σε μεγάλο βαθμό φαίνεται να διαμορφώνεται από τις ενέργειες αυτής της κατηγορίας.

Novices (αρχάριοι)[199]: Οι αρχάριοι ("novices") είναι έφηβοι[200] οι οποίοι φιλοδοξούν να γίνουν hackers αλλά δεν έχουν τις τεχνικές ικανότητες. Οι επιθέσεις τους δεν είναι τόσο επικίνδυνες αλλά κάποιοι από αυτούς είναι εξελίξιμοι[201].

---

[192] Αναφορικά με τους ***"script kiddies"*** ή ***"skiddies"*** ή ***"script bunnies"*** ή ***"script kitties"*** ή ***"script-running juveniles (SRJ)"*** και τα χαρακτηριστικά τους βλ. το ενδιαφέρον άρθρο στην ιστοσελίδα του Πανεπιστημίου Princeton στο url: https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Script_kiddie.html καθώς και *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 53.

[193] ... ή "***Script Weenies***" σύμφωνα με την *Suelette Dreyfus*, Computer hackers: Juvenile Deliquents or International Saboteurs?, εισήγηση η οποία παρουσιάστηκε στο συνέδριο "Internet Crime" το οποίο έλαβε χώρα στη Μελβούρνη της Αυστραλίας στις 16-17 Φεβρουαρίου 1998 και διοργανώθηκε από το Australian Institute of Criminology.

[194] Βλ. λήμμα με τίτλο script kiddies, url: http://www.iss.net/security_center/advice/Underground/Hacking/Script-Kiddies/default.htm.

[195] Βλ. άρθρο με τίτλο "What are script kiddies", url: http://www.wisegeek.com/what-are-script-kiddies.htm.

[196] Βλ. λήμμα με τίτλο script kiddie, url: http://www.techopedia.com/definition/4090/script-kiddie.

[197] Βλ. άρθρο με τίτλο "What is a script kiddie?", url: http://www.pctools.com/security-news/script-kiddie/.

[198] Βλ. άρθρο με τίτλο "How to avoid becoming a script kiddie", url: http://www.wikihow.com/Avoid-Becoming-a-Script-Kiddie.

[199] Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 17.

[200] Βλ. σχετικά url: http://labrinth.wordpress.com/2007/06/01/a-guide-to-hacking/.

[201] Βλ. το κλασικό εγχειρίδιο αρχαρίων A Novice's Guide to Hacking - 1989 edition (url: http://www.ussrback.com/docs/novice_hacking.txt), το οποίο γράφτηκε από τον hacker με το ψευδώνυμο Mentor το 1989. Ο hacker Mentor είναι και ο συγγραφέας του κλασικού κειμένου «Το Μανιφέστο του hacker", όπως αναλύεται κατωτέρω.

Cyber-terrorists (κυβερνοτρομοκράτες): Οι διαδικτυακοί τρομοκράτες[202] [203] χρησιμοποιούν τις τεχνικές hacking προκειμένου να ανακαλύψουν ή να αποκρύψουν πληροφορίες και να κάνουν επιθέσεις, οι οποίες συνδέονται με τρομοκρατική δράση[204] [205] [206]. Υποστηρίζεται ότι ο κυβερνοπόλεμος[207] αποτελεί πολλαπλασιαστή ισχύος[208], καθώς ο υπολογιστής μπορεί να είναι «όπλο» με μικρό σχετικά κόστος

[202] Ο ορισμός της τρομοκρατίας αποτελεί τεράστιο ζήτημα, το μέγεθος του οποίου δείχνει ο Schmid, ο οποίος παραθέτει 109 διαφορετικούς ορισμούς για την τρομοκρατία [Schmid, «Political Terrorism: A research guide to concepts, theories, data bases and literature», 1983 (όπως παραθέτει σε αυτόν ο *Van Krieken* στο έργο του «Terrorism and the International legal order», The Hague 2002, σελ. 14)].

[203] Πρβλ. και *Ευστράτιο Παπάνη*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, ιδίως το κεφάλαιο με τίτλο «Η έρευνα για την τρομοκρατία στο διαδίκτυο», σελ. 123 επ.

[204] Για τον ορισμό της κυβερνοτρομοκρατίας και αναφορικά με το πώς η τεχνολογία μπορεί να υποβοηθήσει την τρομοκρατία πρβλ. ενδεικτικά *Peter Grabosky*, Requirements of prosecution services to deal with cyber crime, Crime Law Soc Change (2007) 47, p. 204 f.

[205] Γνωστό παράδειγμα επίθεσης κυβερνοτρομοκρατίας είναι η μαζική ηλεκτρονική επίθεση η οποία καταγράφηκε τον Μάιο του 2007 στην Εσθονία και έπληξε τα ψηφιακά συστήματα κυβερνητικών υπηρεσιών, κομμάτων, ΜΜΕ και του τραπεζικού συστήματος της χώρας (βλ. σχετικά το άρθρο «Ο Α' Παγκόσμιος Κυβερνοπόλεμος!», περιοδικό "Focus", Τρίτη 10 Φεβρουαρίου 2009, url: http://www.focusmag.gr/articles/view-article.rx?oid=410433). Η περίπτωση αυτή αποτελεί την πρώτη κυβερνοεπίθεση εναντίον ενός κράτους, η οποία, μάλιστα, διήρκεσε τρεις εβδομάδες. Βασική αιτία θεωρήθηκε η απομάκρυνση του «Χάλκινου Στρατιώτη», μνημείου υπέρ των πεσόντων σοβιετικών στο Β' Παγκόσμιο πόλεμο, από το κέντρο της εσθονικής πρωτεύουσας. Η επίθεση συνίστατο σε βομβαρδισμό συστημάτων με πληροφορίες προκειμένου να δημιουργηθεί ως αποτέλεσμα υπερφόρτωση του δικτύου και κατάρρευση της λειτουργίας του (DoS – Denial of Service Attack). Από την επίθεση αυτή προσβλήθηκαν όλα σχεδόν τα δίκτυα των Υπουργείων της Εσθονίας και τέθηκαν εκτός λειτουργίας τα δίκτυα δύο μεγάλων εσθονικών τραπεζών. Επιπλέον, στην ιστοσελίδα του πολιτικού κόμματος του Πρωθυπουργού της Εσθονίας κατά την περίοδο εκείνη κ. Andrus Ansip αναρτήθηκε μια ψεύτικη επιστολή συγγνώμης δήθεν από τον ίδιο τον Πρωθυπουργό για την απομάκρυνση του μνημείου. Παρά τις εικασίες ότι η επίθεση είχε συντονιστεί από τη ρωσική κυβέρνηση, ο Υπουργός Άμυνας της Εσθονίας δήλωσε ότι δεν υπήρχε κανένα αποδεικτικό στοιχείο που να συνδέει αυτές τις επιθέσεις στον κυβερνοχώρο με τις ρωσικές αρχές. Από την άλλη, οι ρωσικές αρχές χαρακτήρισαν τις κατηγορίες αναφορικά με συμμετοχή της «αβάσιμες» – ούτε οι ειδικευμένοι επιστήμονες του NATO ή της Ευρωπαϊκής Επιτροπής κατάφεραν να βρουν αναμφισβήτητες αποδείξεις για συμμετοχή της ρωσικής κυβέρνησης. Εν τέλει, τον Ιανουάριο του 2008, ένας νεαρός φοιτητής ρωσικής καταγωγής καταδικάστηκε από εσθονικό δικαστήριο ως υπαίτιος για τις ως άνω πράξεις.

[206] Περισσότερες περιπτώσεις κυβερνοεπιθέσεων αναφέρονται στα κάτωθι άρθρα και ρεπορτάζ εφημερίδων και ενημερωτικών ιστοσελίδων: «Κυβερνοπόλεμος ακτιβιστών κατά της βιομηχανίας μουσικής και κινηματογράφου» (url: http://news.in.gr/science-technology/article/?aid=1231059839), «Κυβερνο-πόλεμος ΗΠΑ-Κίνας» (url: http://www.ethnos.gr/article.asp?catid=11381&subid=2&pubid=42240951), «Κυβερνοτρομοκρατία» (url: http://www.eeei.gr/interbiz/articles/sarin.htm) (το άρθρο αναφέρεται σε περιπτώσεις στην Ιαπωνία), «Μαίνεται ο κυβερνοπόλεμος για τον Ασάνζ» (url: http://www.tanea.gr/default.asp?pid=2&ct=2&artid=4608980).

[207] Βλ. τις αναπτύξεις του Furnell αναφορικά με τον κυβερνοπόλεμο και την κυβερνοτρομοκρατία (*Steven Furnell*, όπ. π., σελ. 316 επ.).

[208] Κατά την ανάλυση του Mearsheimer για τις διεθνείς σχέσεις αναφερόμενος στα κράτη υποστηρίζει ότι η ισχύς εδράζεται σε συγκεκριμένες υλικές ικανότητες, εκ των οποίων και η τεχνολογία (έτσι *John J. Mearsheimer*, Η τραγωδία της πολιτικής των μεγάλων δυνάμεων, Μετάφραση: *Κωνσταντίνος Κολιόπουλος*, Επιστ. επιμέλεια: *Π. Ήφαιστος – Ηλ. Κουσκουβέλης*, εκδ. Ποιότητα, 5η εκδ., Αθήνα, 2009, σελ. 127). Βλ. και την ανάλυση του *Bert-Jaap Koops*, Law, Technology, and Shifting Power Relations, TILT Law & Technology Working Paper No. 014/2009, September 2009, Version: 1.0 &

αλλά με συγκριτικά πολύ μεγάλα αποτελέσματα[209]. Η σχέση με το hacking είναι προφανής, λαμβανομένου υπόψιν ότι στην άσκηση κυβερνοπολέμου πρωτεύοντα ρόλο παίζει η εφευρετικότητα και η πρωτοτυπία![210] Οι hackers αυτοί χρησιμοποιούν τις δεξιότητές τους[211] (συμμετέχοντας σε ομάδες ή μεμονωμένα)[212] για την οργάνωση και την εκτέλεση επιθέσεων κατά δικτύων, συστημάτων ηλεκτρονικών υπολογιστών και τηλεπικοινωνιακών υποδομών ή για την ανταλλαγή πληροφοριών ή την πραγματοποίηση απειλών ηλεκτρονικά, συχνά προκειμένου να απενεργοποιηθούν ηλεκτρονικές και φυσικές υποδομές ζωτικής σημασίας[213] ή να επηρεαστεί επί τα χείρω η λειτουργία τους. Με αυτόν τον τρόπο πλήττουν βασικούς στόχους ή κατακτούν τον έλεγχο συστημάτων πληροφοριών (π.χ. ηλεκτρονικά οπλικά συστήματα κ.λπ.)[214] προβαίνοντας, έτσι, και σε δράσεις τύπου nation-state hacking, σε πόλεμο πληροφοριών και κυβερνητική κατασκοπεία (υπέρ ή εναντίον κυβερνητικών οργανισμών)[215].

Tilburg University Legal Studies Working Paper No. 014/2009, url: http://ssrn.com/abstract=1479819 αναφορικά με τις άνισες σχέσεις ισχύος (ιδίως μεταξύ κράτους-πολίτη, εργοδότη-εργαζομένου και επιχειρήσεων-καταναλωτών) όπως καταγράφονται από τις αλλαγές που σχετίζονται με την τεχνολογία.

[209] Βλ. ενδεικτικά το κεφάλαιο «Ηλεκτρονική Τρομοκρατία και Εγκλήματα Υψηλής Τεχνολογίας» εις *Μ. Μπόση,* Ζητήματα Ασφάλειας στη Νέα Τάξη Πραγμάτων, εκδ. Παπαζήση, Αθήνα, 1999, σελ. 229 επ. όπου και αναφέρεται: «*Η μεταψυχροπολεμική εποχή βασίζεται και στηρίζεται στην Πληροφορική και στη δυνατότητα αξιοποίησης των νέων μορφών τεχνολογίας προς όφελός της. Ενδιαφέρον παρουσιάζουν τα σενάρια πολέμου, ενός ιδιότυπου ανορθόδοξου πολέμου, που ... αφορά τη χρήση της Πληροφορικής. ... οι Mollander, Riddile and Wilson, σε μελέτη τους για το θέμα, αναφέρονται στη "στρατηγική χρήση του πολέμου της πληροφορικής"*».

[210] Έτσι στο άρθρο "ΓΕΕΘΑ: Ο κυβερνοπόλεμος είναι το νέο στρατηγικό όπλο" (url: http://www.onalert.gr/default.php?pname=Article&catid=20&art_id=1673).

[211] Για τη διάκριση «καλών» hackers και κυβερνοτρομοκρατών βλ. ενδεικτικά το δημοσίευμα με τίτλο "Good" hackers vs. Cyber-terrorists, url: http://www.cyberspacers.com/news/hackers4usa/

[212] Αναφορικά με την κυβερνοτρομοκρατία και τη συνάρτηση με το οργανωμένο έγκλημα βλ. *Louise I. Shelley*, Organized Crime, Terrorism and Cybercrime, Security Sector Reform: Institutions, Society and Good Governance, Alan Bryden/Philipp Fluri (eds.), 2003, pp. 303-312.

[213] Βλ. αναφορικά με τις υποδομές ζωτικής σημασίας σχετική υποσημείωση ανωτέρω.

[214] Για την κυβερνοτρομοκρατία βλ. και *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-Zavrsnik.pdf, p. 3.

[215] Βλ. τον ορισμό που υιοθετεί το FBI για την κυβερνοτρομοκρατία - περαιτέρω ανάλυση στο άρθρο του *William L. Tafoya*, Cyber terror, url: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror - βλ. επίσης *Bruce Schneier*, Beyond Fear: Thinking Sensibly about Security in an Uncertain World (New York: Copernicus Book 2003), *Joshua Green*, The Myth of Cyberterrorism, Washington Monthly, November 2002, url: http://www.washingtonmonthly.com/features/2001/0211.green.html, *Andrew Donoghue*, Cyberterror:

Clear and present danger or phantom menace?, ZDNet, 2004, url: http://insight.zdnet.co.uk/specials/networksecurity/0,39025061,39118365-2,00.htm, *James Lewis*, Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington, DC: Center or Strategic and International Studies, December 2002, url: http://www.csis.org/ tech/0211_lewis.pdf και *Dorothy Denning*, Is Cyber Terror Next? In Understanding September 11, edited by C. Calhoun, P. Price, and A. Timmer (2001), url: http://www.ssrc.org/sept11/ essays/denning.htm.

Disgruntled (ex) employees [Δυσαρεστημένοι (πρώην) εργαζόμενοι]: Η «τάξη» αυτή είναι από τις λιγότερο γνωστές αλλά χαρακτηρίζεται ως μία από τις πιο επικίνδυνες[216]. Οι (πρώην) συνεργάτες εταιρειών ή οργανισμών ή τέως έχοντες οποιαδήποτε σχέση με το απειλούμενο σύστημα πληροφοριών, γνωρίζουν συγκεκριμένες πληροφορίες σχετικά με τις πρακτικές και τις πολιτικές ηλεκτρονικής ασφάλειας μιας εταιρείας ή ενός οργανισμού ή σε κάθε περίπτωση του διαχειριστή του συστήματος[217]. Είναι, επομένως, ευκολότερο για αυτούς να παρακάμψουν τις δικλείδες ασφαλείας και να αποκτήσουν χωρίς δικαίωμα πρόσβαση[218]. Πέραν τούτου, έχουν οι ίδιοι τρόπο να αφήσουν εφόσον και όποτε το επιθυμήσουν (π.χ. μόλις μάθουν ότι απολύονται) κάποια «τρύπα» στο σύστημα, προκειμένου να εισχωρήσουν σε αυτό αργότερα. Η κατηγορία αυτη φαίνεται ότι χαρακτηρίζεται από την ψευδαίσθηση της συνέχειας της κατοχής δικαιωμάτων ή από τον ναρκισσισμό των προσωπικοτήτων που συμμετέχουν σε αυτήν. Επίσης, σε κάποιες περιπτώσεις φαίνεται να πιστεύουν ότι τους οφείλεται ειδική αναγνώριση και ενίοτε λειτουργούν εκδικητικά για αυτόν τον λόγο[219].

2.3.4 Διάκριση των hackers με κριτήριο τη δημιουργική τους ικανότητα

Μια επιπλέον διάκριση μεταξύ των hackers είναι αυτή σε "makecrafters" και "techcrafters". Ως "makecrafters" ορίζονται οι επιδέξιοι hackers, οι οποίοι

---

[216] Κατά τον Zavrsnik το 80% των κυβερνοεγκλημάτων διαπράττεται από τους υπαλλήλους των θυμάτων – τα θύματα στις περισσότερες περιπτώσεις κυβερνοεγκλημάτων είναι εταιρείες και κρατικοί οργανισμοί (*Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-Zavrsnik.pdf, p. 13).

[217] Ο Furnell τους προσδιορίζει ως «έκπτωτους» (Βλ. *Steven Furnell*, όπ. π., σελ.31).

[218] Έτσι και *Ν. Κουράκης*, Εγκληματολογικοί ορίζοντες, όπ. π., σελ. 183.

[219] Βλ. για αντίστοιχα περιστατικά όλως ενδεικτικώς τα δημοσιεύματα της *Mary Shell*, Fired employee admits to hacking Gucci, 18 Ιουλίου 2012, url: http://www.workforce.com/articles/fired-employee-admits-to-hacking-gucci, του *Gerry Smith*, Matthew Keys Case Shows Rogue Employees Can Be Just As Dangerous As Hackers, 19 Μαρτίου 2013, url: http://www.huffingtonpost.com/2013/03/19/matthew-keys-rogue-employee-hackers_n_2903021.html και της *Elaine Silvestrini*, Ex-employee agrees to plead guilty in hacking of Tampa firm, 3 Απριλίου 2014, url: http://tbo.com/news/crime/ex-employee-guilty-of-hacking-tampa-firm-20140403/.

κατασκευάζουν και παράγουν νέα εργαλεία που μπορούν να χρησιμοποιηθούν για hacking. Από την άλλη, ως "techcrafters" ορίζονται οι χρήστες των ως άνω εργαλείων hacking[220].

2.4 Η εξέλιξη των hackers και τα χαρακτηριστικά τους από την εμφάνιση των ηλεκτρονικών πληροφοριών μέχρι σήμερα[221]

Υποστηρίζεται ότι οι hackers έχουν δράσει σε τέσσερις διαδοχικές «γενιές»[222]:

Η *πρώτη γενιά* hackers αποτελείται από τους επιστήμονες που είχαν συμμετοχή στην ανάπτυξη των πρώτων μεθόδων προγραμματισμού υπολογιστών. Κλεισμένοι στα εργαστήρια κατά τις δεκαετίες του 1950 και του 1960, είχαν ιδιαίτερο ενδιαφέρον στο να εξερευνούν τις λεπτομέρειες συστημάτων και προγραμμάτων και να αναπτύσσουν τις ικανότητές τους σε αυτά τα συστήματα, σε αντίθεση με τους περισσότερους χρήστες που απλώς επιλέγουν να μάθουν και να γνωρίζουν μόνο όσα είναι αναγκαία προκειμένου να εξυπηρετήσουν τις ανάγκες τους[223].

Ακολούθως, η *δεύτερη γενιά* περιλαμβάνει τους κυρίως επιχειρηματικά προσανατολισμένους επιστήμονες, οι οποίοι έθεσαν ως σκοπό τους τη μετάδοση της χρήσης της πληροφορικής τεχνολογίας στον ευρύτερο πληθυσμό. Επιπλέον, η

---

[220] Η λέξη "craft" όπως χρησιμοποιείται σε αυτήν την περίπτωση περιγράφει τον ειδικό τρόπο με τον οποίο «κατέχουν» οι hackers τη γνώση της τεχνολογίας. Βλ. *Thomas Holt & Bernadette Schell*, Hackers and hacking: a reference handbook, Contemporary World Issues – Science, Technology and Medicine, 2013, url: http://books.google.gr/books?id=FZVfAQAAQBAJ&pg=PA149&lpg=PA149&dq=bossler+and+burruss&source=bl&ots=lL57-n6LHz&sig=0nOIvybIGJTRRSWsOEJWMxfHe3A&hl=el&sa=X&ei=OvsAU6TZI-O7ygO_noLgCQ&ved=0CEwQ6AEwAw#v=onepage&q=subculture&f=false, σελ. 21-22.

[221] Για την εξέλιξη του όρου hacker βλ. την ενδιαφέρουσα ανάλυση σε πίνακα στο πόνημα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 36.

[222] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, pp. 41 f. Έτσι και *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, url: http://bscw.cs.ncl.ac.uk/pub/bscw.cgi/d48026/Arief%20and%20Besnard%20-%20Technical%20and%20Human%20Issues%20in%20Computer-Based%20Systems%20Security.pdf, σελ. 10, όπως παραπέμπουν στον Rogers.

[223] Βλ. *Μιχάλης Σφακιανάκης*, Εισαγωγή στην Πληροφορική σκέψη, Εκδόσεις Κλειδάριθμος, 2003, σελ. 291, ο οποίος παραπέμει στο λεξικό "Jargon"για τον ορισμό του hacker της «πρώτης γενιάς».

δεύτερη γενιά ασχολήθηκε συστηματικά με τη μελέτη και τον πειραματισμό πάνω στους τρόπους βελτίωσης της επικοινωνίας μέσω της ανάπτυξης της χρήσης των υπολογιστών, πειραματιζόμενοι βέβαια και με αποκκλίνουσες συμπεριφορές όπως η δωρεάν διενέργεια τηλεφωνικών κλήσεων ("phone – phreaking")[224].

Η *τρίτη γενιά* αποτελείται από τους προγραμματιστές που σχεδίασαν τις πρώτες αρχιτεκτονικές πάνω στις οποίες θα αναπτύσσονταν στο άμεσο μέλλον τα ηλεκτρονικά παιχνίδια. Είναι, δε, φανερό ότι η τρίτη γενιά είναι σαφώς προσανατολισμένη σε μία δημιουργημένη αγορά πληροφορικής τεχνολογίας γύρω από τον προσωπικό υπολογιστή[225] και προσπαθεί να ανταποκριθεί στη ζήτηση ή να δημιουργήσει μία ζήτηση βάσει πιθανών δυναμικών αναγκώ

Οι πρώτες γενιές των hackers δεν έχουν ιδιαίτερη σχέση με το πληροφορικό έγκλημα αλλά κυρίως με την ανάπτυξη των ηλεκτρονικών προγραμμάτων. Προϊόντος του χρόνου, η *τέταρτη γενιά* προσεγγίζει την έννοια του hacking περισσότερο ως παρεκκλίνουσα/εγκληματική συμπεριφορά, όπως έχει αυτή περιγραφεί σε νομικά και εγκληματολογικά κείμενα[226]. Η γενιά αυτή είναι σαφώς πολυπληθέστερη, έχει γεννηθεί και ενσωματωθεί ήδη σε ένα υπάρχον πληροφορικό περιβάλλον και αποτελείται από άτομα που ζουν σε διαφορετικές συνθήκες και έχουν διαφορετικούς στόχους και σκοπούς από τις προηγούμενες. Μεγάλο μέρος των δραστηριοτήτων που αναπτύσσονται στα εργαστήρια λαμβάνουν ουσιαστικά έναν διαφορετικό χαρακτήρα όταν μεταφέρονται στην ευρύτερη κοινωνία μέσω του κυβερνοχώρου. Στο νέο αυτό πλαίσιο, η πρόσβαση δεν θεωρείται πλέον αμέσως ελεύθερη και συνήθως απαιτείται εξουσιοδότηση. Ευνόητο είναι ότι η χωρίς εξουσιοδότηση πρόσβαση σε έναν

---

[224] Χαρακτηριστικό παράδειγμα οι ιδρυτές της πρωτοπόρου εταιρείας υπολογιστών "Apple" **Steve Wozniak** και **Steve Jobs,** οι οποίοι υπήρξαν "phone phreakers" (βλ. ανωτέρω) και διενεργούσαν τηλεφωνικές κλήσεις χωρίς να πληρώνουν (βλ. δημοσίευμα της ενημερωτικής ιστοσελίδας bloomberg του *Jordan Robertson*, "Famous Hackers: Then and Now", 19 Απριλίου 2012, url: http://www.bloomberg.com/slideshow/2012-04-18/famous-hackers-then-and-now.html#slide10).

[225] Έχει λεχθεί ότι θα μπορούσε ακόμη και να υποτεθεί ότι ο προσωπικός υπολογιστής να μην είχε υπάρξει χωρίς τη συμβολή και την κουλτούρα των hackers (Chandler, 1996, σελ. 229). Έτσι η *Orly Turgeman-Goldschmidt*, Identity construction among hackers, εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf, pp. 32-34.

[226] Βλ. ιδίως κεφάλαια 4, 5 και 6 του παρόντος πονήματος. Βέβαια, υπάρχουν (ομάδες) hackers με τα χαρακτηριστικά της τέταρτης αυτής γενιάς οι οποίοι αντιμετωπίζουν το hacking ως πειραματισμό χωρίς απαραίτητα να έχουν ως σκοπό την παράβαση του νόμου (βλ. π.χ. την ομάδα hackerspace.gr όπως παρουσιάζεται κατωτέρω στην παράγραφο 7.5.5.5 του παρόντος πονήματος).

υπολογιστή αρχίζει να γίνεται αντιληπτή ως παραβίαση, η οποία μπορεί να αξιολογείται ως ανήθικη και εγκληματική[227].

Ο hacker της τέταρτης γενιάς (ο σύγχρονος hacker) φέρει χαρακτηριστικά τα οποία συνίστανται στα εξής:

(α) εξειδικευμένη τεχνική επιδεξιότητα[228].

(β) άρτια γνώση πληροφορικής και του διαδικτύου καθώς και του επιμέρους ηλεκτρονικού «περιβάλλοντος» και των μυστικών του χώρου που επιθυμεί να παραβιάσει[229].

(γ) δυνατότητα προμήθειας ή κατοχή των κατάλληλων τεχνικών μέσων (π.χ. ηλεκτρονικό υπολογιστή και τεχνικό εξοπλισμό, συνδρομή σε παροχέα πρόσβασης, ειδικά λογισμικά κ.λπ.) χωρίς τα οποία το «πέρασμα στην πράξη» ("passage à l'acte") είναι αδύνατο[230].

Ωστόσο, η σύγχρονη γενιά των hackers φαίνεται ότι δεν ενστερνίζεται τόσο τις αξίες των hackers των προηγούμενων γενιών, αφού οι σύγχρονοι hackers δεν ασχολούνται τόσο πολύ με τη συγγραφή κώδικα (λόγω και της δυνατότητας προμήθειας έτοιμων των τεχνικών μέσων, όπως αναφέρεται ανωτέρω στο υπό γ' στοιχείο), πολλές φορές δεν ακολουθούν τη δεοντολογία των παλαιοτέρων σε ό,τι αφορά τα συστήματα πληροφοριών τα οποία πλήττουν (π.χ. έχουν λάβει χώρα επιθέσεις σε συστήματα νοσοκομείων) καθώς και δεν μοιράζονται τόσο απλόχερα τη γνώση[231].

Η πνευματική «υπεροχή» των hackers θεωρείται από πολλούς βασικό γνώρισμα της προσωπικότητάς τους[232]. Οι hackers, δηλαδή, εκλαμβάνονται ως πνευματικά "προικισμένοι", σκεπτόμενοι, ικανοί να λύσουν σημαντικής δυσκολίας προβλήματα

---

[227] Βλ. *Μιχάλης Σφακιανάκης*, «Εισαγωγή στην Πληροφορική σκέψη», όπ. π. σελ. 291-292.

[228] Βλ. *Donn B. Parker*, Fighting Computer Crime, όπ. π., σελ. 136.

[229] Πρβλ. κατωτέρω πρακτικές συλλογής πληροφοριών για το σύστημα στην παράγραφο 2.11.2.1.1 του παρόντος πονήματος.

[230] Βλ. *Ιωάννης Εμμ. Αγγελής*, Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο, όπ. π. σελ. 677. Βλ. και εδώ τον ορισμό του hacking από τον Jordan αναφορικά με την υλική διάσταση των πράξεων hacking, όπως αναφέρεται ανωτέρω στην παράγραφο 2.1.

[231] Βλ. το ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy.

[232] Σχετικά με τις συνήθειες, τα ενδιαφέροντα και γενικότερα το προφίλ των hackers βλ. *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, pp. 11-16 (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

και ιδιαιτέρως ευφυείς.[233] Η βαθειά γνώση της τεχνολογίας των υπολογιστών και τα επιτεύγματά τους που στηρίζονται σε αυτή δίνουν αναφορικά με τους hackers μία έντονη αίσθηση υπεροχής και ένα αίσθημα ανωτερότητας έναντι των υπόλοιπων ανθρώπων. Εξάλλου, αν παρατηρήσουμε την εξέλιξη των γενεών των hackers, όπως αναλύθηκε ανωτέρω, διαπιστώνουμε ότι η «αφρόκρεμα» επιστημόνων ασχολήθηκε με το hacking. Ωστόσο, σήμερα η επιλογή κάποιου να γίνει «hacker» δεν του προσδίδει αυτομάτως τα παραπάνω χαρακτηριστικά. Πολλοί hackers επιτυγχάνουν χάριν της ιδιαίτερης επιμονής τους, της αποφασιστικότητάς τους και σε εξαιρετικές περιπτώσεις της προσπάθειάς τους να εκμεταλλευτούν «δημιουργικά» τον χρόνο τους (δεν πρέπει να παραβλεφθεί το γεγονός ότι μία επιτυχημένη προσπάθεια hacking μπορεί να οφείλεται στη συνεχόμενη εφαρμογή της ίδιας τεχνικής σε διάφορα συστήματα έως ότου βρεθεί κάποια αδυναμία στο σύστημα ασφαλείας)[234]. Τέλος, καταδεικνύεται ερευνητικά ότι οι hackers σήμερα αυτοπροσδιορίζονται ως «ειδικοί των υπολογιστών» (και γι' αυτό δεν αισθάνονται βέβαια ντροπή για τις πράξεις τους)[235], ετικέτα που σε κάθε περίπτωση δεν θεωρείται «αποκλίνουσα» (αλλά μπορεί βεβαίως να θεωρηθεί «τεχνική ηθικής ουδετεροποίησης»[236]).

2.5 Τα κίνητρα των hackers

Τα κίνητρα του hacking ποικίλλουν[237] και για την ανίχνευση αυτών μπορούν να χρησιμοποιηθούν έρευνες (όπως αυτή η οποία ακολουθεί) και, βεβαίως, κείμενα των ίδιων των hackers – όπως το κείμενο «*Η συνείδηση ενός hacker*» - "*The conscience of*

[233] Υπάρχουν σχετικά «αφιερώματα» στους πλέον έξυπνους hackers π.χ. το δημοσίευμα "Top 10 smartest hackers of all times", url: http://thetoptenlisting.blogspot.gr/2013/11/top-10-smartest-hackers-of-all-times.html.

[234] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 76.

[235] Έτσι, *Orly Turgeman-Goldschmidt*, Identity construction among hackers, εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf, pp. 47-48.

[236] Βλ. κατωτέρω στο κεφάλαιο 3 την παράγραφο 3.5 για τις «τεχνικές ηθικής ουδετεροποίησης» την εγκληματολογική θεωρία των Matza και Sykes.

[237] Βλ. πίνακα ο οποίος αναφέρει αναλυτικά κίνητρα παραβιαστών στο πόνημα των *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, p. 49 καθώς και αναλυτική λίστα με αναφερόμενα κίνητρα στο πόνημα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 145-146.

a hacker" γνωστό και ως «Μανιφέστο του hacker»[238] [239] [240]. Πολλές φορές, βέβαια, οι hackers επικαλούνται «ψευδοκίνητρα» για να δικαιολογήσουν τις πράξεις τους[241] (π.χ. υποστηρίζεται ότι οι πιο κοινές μορφές επίθεσης των hackers μέσω διαδικτύου δικαιολογούνται από τους δράστες με το επιχείρημα ότι οι πράξεις τους έχουν ιδεολογικό υπόβαθρο[242]). Όπως επισημαίνουν οι Grabosky και Smith, οι λόγοι που προβάλλονται από τους hackers ως αιτία για τις πράξεις τους είναι πιθανό να είναι ιδιοτελείς και, συνεπώς, πρέπει να αντιμετωπίζονται με σκεπτικισμό[243].

Άρα, προκειμένου να κατανοήσουμε τις ενέργειες των hackers και να αξιολογήσουμε τις εξηγήσεις τους, πρέπει να ληφθεί υπόψιν το πλήρες φάσμα των κινήτρων που διέπουν τις συμπεριφορές αυτές[244] [245]. Υπάρχει η εικόνα των hackers ως «σκαπανείς εξερευνητές», κατά την οποία οι hackers απλώς εξερευνούν το διαδίκτυο συμβάλλοντας στην επίτευξη ενός αξιόλογου σκοπού μέσω των δραστηριοτήτων τους[246]. Ωστόσο, ο hacker της σύγχρονης εποχής δεν είναι απαραίτητο ότι έχει ένα

---

[238] Το «Μανιφεστο του hacker» γράφτηκε από τον hacker Mentor (το κανονικό του όνομα είναι Loyd Blankenship – βλ. url: https://web.archive.org/web/20050414161009/http://www.h2k2.net/display_grid.khtml?who=3) μετά τη σύλληψή του για πράξεις σχετικές με το hacking. Ο Mentor ήταν μέλος μιας μεγάλης ομάδας hackers, της "Legion of Doom". Το κείμενο αυτό δημοσιεύτηκε για πρώτη φορά στο (περιθωριακό) περιοδικό hacker Phrack στο Volume One, Τεύχος 7, Phile 3 από 10 στις 8 Ιανουαρίου 1986 και θεωρείται ο ακρογωνιαίος λίθος της κουλτούρας των hackers καθώς σε αυτό αναπτύσσονται και περιγράφονται θέσεις και απόψεις, δίνονταιι στοιχεία σχετικά με την ψυχολογία των πρώτων hackers και αντίστοιχα έχει διαμορφώσει την ταυτότητα των hackers και τα κίνητρά τους. Στο Μανιφέστο αναφέρεται ότι οι hackers προβαίνουν σε αυτές τις ενέργειες προκειμένου να έρθουν σε επαφή με τη γνώση, επειδή συχνά απογοητεύονται και πλήττουν λόγω των περιορισμών αλλά και προκειμένου να ελέγξουν («τεστάρουν») τις γνώσεις τους.

[239] Το πλήρες κείμενο «Η συνείδηση ενός hacker» - "The conscience of a hacker" (Hacker manifesto) βρίσκεται δημοσιευμένο στην ηλεκτρονική διεύθυνση http://www.phrack.org/archives/issues/7/3.txt και μεταφρασμένο στα ελληνικά εις *Steven Furnell*, όπ. π., σελ. 73.

[240] Πρβλ. συνέντευξη του hacker με το ψευδώνυμο "Mentor" (συγγραφέα του εν λόγω κειμένου – βλ. αμέσως προηγούμενη υποσημείωση) με ημερομηνία 31/07/2000 στο url: http://www.elfqrin.com/docs/hakref/interviews/eq-i-mentor.html.

[241] Βλ. και τη θεωρία της ηθικής ουδετεροποίησης του Matza & Sykes και όπως αναλύονται κατωτέρω στην παράγραφο 3.5 (πρβλ. *Στ. Αλεξιάδη*, Εγκληματολογία, εκδ. Σάκκουλα, 4η εκδ. Θεσσαλονίκη, 2004, σελ. 68 επ. καθώς και το κεφάλαιο "ο Matza και ο Sykes – οι τεχνικές ή θεωρία της «εξουδετέρωσης»" εις *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, 2η εκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, σελ. 268 επ.)

[242] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π. σελ. 68.

[243] *P. Grabosky & R. Smith*, Crime in the digital age, Sydney: Federation Press, 1998, pp. 52-53.

[244] *P. Grabosky & R. Smith*, Crime in the digital age, Sydney: Federation Press, 1998, pp. 52-53.

[245] Για σύγχρονη ανάλυση των κινήτρων των hackers βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 44 f.

[246] Οι *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., διαχωρίζουν τα κίνητρα των hackers σε κοινωνιολογικά/ψυχολογικά και τεχνικά – βλ. σελ. 12-13 για περαιτέρω αναπτύξεις.

μόνο συγκεκριμένο κίνητρο. Το hacking χρησιμοποιείται συχνά ως μέσο για να επιτευχθούν διαφορετικοί μεταξύ τους στόχοι όπως η αποκόμιση κερδών[247], η εκδίκηση, η ικανοποίηση του «εγώ» κ.ά. Παρατηρείται, επίσης, ότι κάποια κίνητρα αφορούν διαφορετικές υποομάδες hacking[248] όπως, για παράδειγμα, το κίνητρο του χρήματος εντοπίζεται, συνήθως, στους φρίκερ, τους warez d00dz[249] και τους δημιουργούς βλαπτικών προγραμμάτων (malware)[250].

Ειδικότερα, βασικό κίνητρο των hackers είναι η έμπρακτη εκδήλωση «*…της πίστης τους ότι στον κυβερνοχώρο η πληροφορία πρέπει να είναι ελεύθερη, προσβάσιμη σε όλους, και ότι δεν μπορούν να υπάρχουν στεγανά, λογοκρισία, ιδιοκτήτες ή πνευματικά δικαιώματα*»[251]. Περαιτέρω, για αρκετούς hackers το κίνητρο είναι απλώς η διασκέδαση[252] (ακόμη και φάρσες[253])[254] στο πλαίσιο «νεανικής επιπολαιότητας»[255]

[247] Αναφορικά με την αποκόμιση κερδών βλ. κατωτέρω τις αναπτύξεις στην παρούσα παράγραφο αλλά και στη δεύτερη υπόθεση έρευνας (παράγραφοι 7.2.2 και 8.2) και την αναφορά σε τρόπους αποκόμισης κερδών με αντίστοιχες παραπομπές. Επίσης, βλ. χαρακτηριστικά άρθρο του περιοδικού "FOCUS" με τίτλο «Ο Α' Παγκόσμιος Κυβερνοπόλεμος!», Τρίτη 10 Φεβρουαρίου 2009, url: http://www.focusmag.gr/articles/view-article.rx?oid=410433 σύμφωνα με το οποίο hackers ή crackers που έχουν δυνατότητες προσβολής ιστοσελίδων και διεξαγωγής κυβερνοεπιθέσεων είναι σχεδόν όλοι «μισθοφόροι». Στο ίδιο άρθρο προσδιορίζεται ότι **στην αγορά των «υπηρεσιών κυβερνοεγκλήματος» η τιμή για μια DDoS επίθεση μπορεί να φτάσει τα 20 δολάρια για την επίθεση μιας ώρας και τα 200 δολάρια για μια ημερήσια επίθεση**.

[248] Μια αναλυτική παρουσίαση των πιο γνωστών ομάδων hackers βρίσκεται στο πόνημα του *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 86 επ.

[249] Οι warez d00dz ασχολούνται με την αντιγραφή προγραμμάτων, κατά παράβαση των κανόνων προστασίας της πνευματικής ιδιοκτησίας. Για αναλυτικότερο ορισμό βλ. url: http://dictionary.reference.com/browse/warez+d00dz.

[250] Βλ. κατωτέρω την παράγραφο 2.11 του παρόντος πονήματος.

[251] Έτσι ο *Ν. Κουράκης*, Εγκληματολογικοί ορίζοντες, όπ. π., σελ. 183.

[252] Κατά την όμορφη έκφραση του Κουράκη «*χάριν παιδιάς ή / και αυτοδιαφήμισης*»! (έτσι *Ν. Κουράκης*, Εγκληματολογικοί ορίζοντες, όπ. π., σελ. 183). Αντίστοιχα και *Γ. Πανούσης*, Εγκληματολογία, εγκληματολογική έρευνα και ΜΜΕ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1999, σελ. 75).

[253] Για φάρσες των hackers στην Ελλάδα βλ. το εμπεριστατωμένο ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy, στο οποίο και παρουσιάζεται η ιστορία του hacking στην Ελλάδα.

[254] Η διασκέδαση μπορεί να συνίσταται ακόμη και σε συγγραφή κώδικα. Οι Grabosky και Smith (1998) αναφέρουν τη δημιουργία του ιού Morris, ο οποίος εν μέρει απενεργοποίησε το διαδίκτυο, ως παράδειγμα περιέργειας που οδήγησε σε απροσδόκητες συνέπειες (έτσι *Tony Krone*, Hacking Motives, January 2005, url: http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb006.html).

[255] Βλ. κατωτέρω αναπτύξεις για το «νεανικό πρόβλημα» στο hacking (κεφάλαιο 3 της παρούσας) καθώς και τα αποτελέσματα της έρευνας στο κεφάλαιο 7 της παρούσας σύμφωνα με την οποία αρκετοί hackers φαίνεται ότι είναι έφηβοι ή στην αμέσως μετεφηβική ηλικία.

και η ικανοποίηση που αντλούν μέσα από την πρόκληση που προσφέρει το «παιχνίδι» της παραβίασης του ξένου συστήματος[256].

Σύμφωνα με το «Μανιφέστο του hacker», hacker είναι αυτός ο οποίος αναζητεί συνεχώς νέες προκλήσεις[257]. Ο Tony Krone αναφέρει ότι κίνητρο για hackers δύναται να αποτελεί και η πνευματική πρόκληση του hacking σε ασφαλείς ή υψηλού προφίλ ιστοσελίδες, χωρίς να ενδιαφέρονται κατ' ανάγκην για αναγνώριση. Εάν κανείς καταφέρει να υποτάξει την πολυπλοκότητα και να υπερνικήσει τις τεχνικές δυσκολίες της παραβίασης της ασφάλειας ενός συστήματος, τότε ικανοποιείται από την επιτυχία και η αίσθηση του κατορθώματος είναι μεγάλη[258]. Η πνευματική πρόκληση είναι συχνά και το κίνητρο εκείνων που δημιουργούν ιούς και «σκουλήκια» και με τον τρόπο αυτό, οι hackers παρέχουν ουσιαστικά εργαλεία σε άλλους hackers για κακόβουλη χρήση και ενέργειες[259].

Ένα επιπλέον κίνητρο για τους hackers έχει υποστηριχθεί ότι είναι η αίσθηση του να ανήκουν σε μια κοινότητα (γενικώς στην κοινότητα του hacking ή ειδικότερα σε υποομάδα hackers, καθώς οι hackers δρουν σε υποομάδες[260]), σε αντίθεση με την στερεότυπη εικόνα του hacker ως μοναχικού «υπερ-χρήστη» υπολογιστών. Η αίσθηση αυτή μπορεί να εκπληρώνεται με την ανταλλαγή εμπειριών με άλλους hackers, τη συνεργασία σε χτυπήματα ή ακόμη και στην απλή επαφή με την hacking κοινότητα[261]. Οι online κοινότητες μπορούν να παρέχουν την αναγνώριση στους hackers[262] αλλά και τα εργαλεία hacking μέσω της ανταλλαγής γνώσεων, δεξιοτήτων,

---

[256] Βλ. Συνέντευξη του θρυλικού hacker Κέβιν Μίτνικ στο Θανάση Λάλα, ΒΗΜAgazino της 28ης Νοεμβρίου 2004, σελ. 60.

[257] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38.

[258] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π. σελ. 66.

[259] Βλ. *Tony Krone*, Hacking motives, όπ. π.

[260] Βλ. *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 21 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) και *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 41-42 και 164 για την εσωτερική οργάνωση των ομάδων αυτών και *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 11.

[261] Βλ. αναφορικά με τις υποομάδες των hackers σχετικές αναπτύξεις και υποσημειώσεις στις παραγράφους 2.6, 2.7 και 2.8 της παρούσας.

[262] Σχετικά ερευνητικά αποτελέσματα στην παράγραφο 7.8.4.1 – ερώτηση υπ' αρ. 15.

τεχνικών και εν γένει τεχνολογίας[263]. Μερικές φορές υπάρχει ανταγωνισμός μεταξύ υποομάδων των hackers και, έτσι, το hacking ως δραστηριότητα γίνεται το πεδίο της προσπάθειάς τους για υπεροχή[264].

Κίνητρο σε πολλές περιπτώσεις συνιστά η εκτόνωση της περιέργειάς τους[265] και η απόκτηση γνώσης πληροφοριών, οι οποίες είναι απρόσιτες στο ευρύ κοινό. Εξάλλου, μία από τις βασικές αρχές της δράσης των hackers είναι η «*κοινωνία της γνώσης*», όπως αυτή αναφέρεται στο «Μανιφέστο του hacker» του 1986[266]. Ειδικότερα, για αρκετούς hackers το κίνητρο της γνώσης μυστικών πληροφοριών δεν είναι παρά η απλή περιέργεια, χωρίς να διακατέχονται από υστερόβουλες προθέσεις. Ο γνωστός hacker Κέβιν Μίτνικ[267] με την προσωπική του εμπειρία τονίζει ότι το πρωταρχικό κίνητρο των «hackers – κοινωνικών μηχανικών», οι οποίοι δεν επιδιώκουν τον παράνομο πλουτισμό, την εξαπάτηση ή την πρόκληση καταστροφών, είναι η

---

[263] Βλ. και παράγραφο 3.9 αναφορικά με τη θεωρία της διαφοροποιούσας συναναστροφής του Edwin Sutherland και τη συσχέτισή της με τις υποομάδες των hackers.

[264] Έτσι *Tony Krone*, Hacking motives, όπ. π.

[265] Χαρακτηριστικό το παράδειγμα hacker ο οποίος χρησιμοποίησε έναν «δούρειο ίππο» προκειμένου να αποκτήσει χωρίς δικαίωμα πρόσβαση στους υπολογιστές της Bloomsbury Publishing και να ανακαλύψει το κείμενο του τελευταίου βιβλίου του Χάρι Πότερ πριν από τη δημοσίευσή του (βλ. γενικότερα *Orly Turgeman-Goldschmidt*, Identity construction among hackers, εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf, pp. 47-48).

[266] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 73 – βλ. επίσης και ανωτέρω υποσημειώσεις ανφορικά με το «Μανιφέστο του hacking».

[267] Ο Κέβιν Μίτνικ (Kevin Mitnick) ξεκίνησε τη δραστηριότητα του με την κατάχρηση του συστήματος καρτών των λεωφορείων του Los Angeles από το οποίο εκτύπωνε πλαστές κάρτες για δωρεάν διαδρομές. Στη συνέχεια το ενδιαφέρον του στράφηκε στην κινητή τηλεφωνία – απέκτησε χωρίς δικαίωμα πρόσβαση στο σύστημα της Digital Equipment Corporation και αντέγραψε πολύτιμο software. Έπειτα και για δυόμιση περίπου έτη απέκτησε πρόσβαση χωρίς δικαίωμα σε υπολογιστές, δίκτυα τηλεφώνων, κυβερνητικά έγγραφα και δημόσια συστήματα (βλ. για τον Μίτνικ καθώς και για άλλους γνωστούς hackers δημοσίευμα με τίτλο «Οι 5 μεγαλύτεροι παράνομοι hackers όλων των εποχών», 22 Ιουνίου 2011, url: http://archive.today/20121127063559/hackingexperience.blogspot.com/2011/06/5-hackers.html). Συνελήφθη στη Νότια Καρολίνα και δικάστηκε στις 09.08.1999 στο Λος Άντζελες. Καταδικάστηκε σε συνολική ποινή 68 μηνών φυλάκισης ενώ ως παρεπόμενη ποινή του επεβλήθη απαγόρευση να έρθει σε επαφή με ηλεκτρονική συσκευή πληροφορικής μετά την αποφυλάκισή του. Βλ. *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 193. Επίσης, βλ. συνέντευξη του Κέβιν Μίτνικ στον δημοσιογράφο Θανάση Λάλα όπως εμπεριέχεται στο εγχειρίδιο του *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, όπ. π. Τέλος, βλ. το σχετικό λήμμα της ηλεκτρονικής εγκυκλοπαίδειας «Βικιπαιδεία» για τον Κέβιν Μίτνικ στο url: http://el.wikipedia.org/wiki/%CE%9A%CE%AD%CE%B2%CE%B9%CE%BD_%CE%9C%CE%AF%CF%84%CE%BD%CE%B9%CE%BA.

περιέργεια και η θέληση για την απόκτηση της πληροφορίας ως υπέρτατης μορφής δύναμης[268].

Υπάρχουν, επίσης, περιπτώσεις κινήτρων hackers που λειτουργούν κάποιες φορές ως δικαιολογίες – όπως είδαμε ανωτέρω – με προσπάθεια να υποβαθμίσουν την όποια βλάβη και αναφέρονται είτε στον έλεγχο ασφαλείας των συστημάτων, είτε στην αμφισβήτηση του δικαιώματος πρόσβασης σε πληροφορίες, είτε στην ανάληψη του ελέγχου για παράνομες πράξεις[269].

Ένα άλλο κίνητρο που αναφέρεται στο ως άνω Μανιφέστο είναι το να καταστεί ελεύθερη η χρήση των υπηρεσιών διαδικτύου ή τουλάχιστον να γίνουν φθηνότερες οι υπηρεσίες αυτές, ειδικά σε περιπτώσεις μονοπωλίου[270].

Επίσης, συχνά οι hackers, μετά από μία επιτυχημένη επίθεσή τους, υποδεικνύουν τα τρωτά σημεία των συστημάτων[271], ζητώντας κάποιες φορές χρήματα για να δώσουν αυτήν την πληροφορία ή κλέβουν εμπιστευτικά στοιχεία, τα οποία και χρησιμοποιούν[272].

Επομένως, υπάρχει σε αρκετές περιπτώσεις σύνδεση και με οικονομικά οφέλη στα κίνητρα των hackers[273]. Οι τρόποι με τους οποίους μπορούν να κερδηθούν χρήματα περιλαμβάνουν ενδεικτικά μεταφορά κεφαλαίων με ηλεκτρονικά μέσα (skimming πιστωτικής κάρτας, υποκλοπή κωδικών κ.ά.), «κλοπή» ή πρόσβαση σε πολύτιμα δεδομένα (λίστες πελατών, λίστες ηλεκτρονικού ταχυδρομείου, πληροφορίες σε περιπτώσεις π.χ. βιομηχανικής κατασκοπείας κ.ά.), χρήση υπηρεσιών χωρίς καταβολή του τιμήματος (π.χ. δυνατοτήτων επικοινωνίας ή δυνατότητα για την αποθήκευση των δεδομένων όπως χρήση νεφελοειδών συστημάτων αποθήκευσης

---

[268] Βλ. *Κέβιν Μίτνικ και Ουίλιαμ Σίμονς*, Η τέχνη της απάτης, σε μετάφραση Λ. Καρατζά, εκδ. Ωκεανίδα, 2003.

[269] Έτσι *Tony Krone*, Hacking motives, όπ. π.

[270] Γίνεται λόγος για ιδιοτέλεια και «λαίμαργον κέρδος»!

[271] Π.χ. το παράδειγμα του Adrian Lamo, ο οποίος παραβίασε ηλεκτρονικά συστήματα γνωστών επιχειρήσεων και μετά προσφέρθηκε να επιδιορθώσει τα συστήματα αυτά δωρεάν (έτσι *Tony Krone*, Hacking motives, όπ. π.).

[272] Βλ. *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ 2/2003, σελ. 192.

[273] Πέρα από τις ανωτέρω αναπτύξεις βλ. και την ανάλυση του *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 405 επ. και ιδίως σελ. 409 όπου αναφέρει ότι το hacking έχει αναχθεί σε ένα είδος «βασικού εγκλήματος» προκειμένου να τελεσθεί κάποιο οικονομικό έγκλημα.

παρακάμπτοντας την υποχρέωση προς πληρωμή), παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας («πειρατεία»), "botnet herder"[274] κ.ά.[275]

Αναφορικά, πάντως, με τις συμπεριφορές των hackers, τα κίνητρά τους και τελικά το «πέρασμα στην πράξη» ("passage à l' acte") ενδιαφέρουσα είναι η θέση ότι, με δεδομένη και την «πλαστικότητα» του εγκεφάλου, σύμφωνα με τη νευροβιολόγο Susan Greenfield, «*η συνεχής επαφή με το ίντερνετ μπορεί να επιφέρει κάποιες θετικές αλλαγές,* ***όπως ένα υψηλότερο IQ και τη δυνατότητα επεξεργασίας πολύπλοκων πληροφοριών σε γρήγορο χρόνο****, αλλά οδηγεί το άτομο στο να συμπεριφέρεται σαν ένα κομπιούτερ και να αναπτύσσει μια ποικιλία αντιδράσεων απέναντι στην ποικιλία ερεθισμάτων που δέχεται. Έτσι, όμως, το άτομο κάνει αυτό που κάνει και ο υπολογιστής: δεν κατανοεί τί συμβαίνει»*[276]. Άρα, διαπιστώνεται ότι από τη μια η συστηματική έως έντονη επαφή με τον υπολογιστή και το διαδίκτυο[277] «δημιουργεί» μάλλον πιο έξυπνους εγκεφάλους[278] στους χρήστες, οι οποίοι όμως από την άλλη στερούνται ενσυναίσθησης (empathy)[279] σχετικά και με την ανάπτυξη της κοινωνικής συνοχής ακόμη και σε διαδραστικό επίπεδο. Τούτο είναι εξάλλου λογικό και από την ίδια τη φύση της ηλεκτρονικής επικοινωνίας, η οποία δεν προσφέρει τη δυνατότητα ανάλυσης της ματιάς, του τόνου της φωνής ή ακόμη και της γλώσσας του σώματός

---

[274] Για τον "botnet herder" βλ. παρ. 2.2 του παρόντος πονήματος.

[275] Έτσι *Tony Krone*, Hacking motives, όπ. π.

[276] Βλ. τη συνέντευξη της Susan Greenfield στο περιοδικό «Ε (έψιλον)» της εφημερίδας «Κυριακάτικη Ελευθεροτυπία», τ. 1037, 27.02.2011 στον δημοσιογράφο Σπύρο Χατζηγιάννη.

[277] Έχει υποστηριχθεί ότι σε παιδιά και εφήβους που καταφεύγουν σε υπερβολική χρήση του διαδικτύου εντοπίζονται, μεταξύ άλλων βιοψυχολογικών επιπτώσεων, μεταβολές στα επίπεδα ορμονών [Έτσι *Γιάννης Α. Δελημάρης & Στ. Πιπεράκης*, Βιολογική θεώρηση της υπερβολικής χρήσης του διαδικτύου σε παιδιά και εφήβους, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 220]. Αναφορικά με τη σχολική βία πρβλ. *Ν. Κουράκη,* Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της, ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr (τεύχος 11) (url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1247152434) και ΠοινΧρ ΝΘ/2009, σελ. 865-871, όπου και αναφέρει ότι έχει καταγραφεί πως η έλλειψη κορτιζόλης ευθύνεται για «συναισθηματική ψυχρότητα» των ανηλίκων θυτών, η οποία τους οδηγεί σε πράξεις βίας.

[278] Βλ. χαρακτηριστικά *Γενοβέφας Χρίστου*, Οι θετικές επιδράσεις των MMORPGs, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 82 επ., όπου και ως θετικές επιδράσεις στους χρήστες – «παίκτες» αναφέρονται και αναλύονται η ανάπτυξη των αισθήσεων και των οπτικοκινητικών λειτουργιών, η ανάπτυξη ψυχοκοινωνικών δεξιοτήτων (σε επίπεδο βέβαια κοινωνικοποίησης μέσα από τα παιχνίδια και όχι ανάπτυξης απομονωτικής διάθεσης) καθώς και η χρήση των παιχνιδιών αυτών ως υποστηρικτικό και ψυχοθεραπευτικό μέσο.

[279] Βλ. χαρακτηριστικά *Ηλία Κορομηλά*, Sensibilis modus operandi (?) – Οπτικός πολιτισμός και σύγχρονη εγκληματικότητα, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τομ. Ι, σελ. 362, υποσ. 9 όπου και αναλύεται η έκφραση των συναισθηματικών καταστάσεων σε σχέση με την νευροφυσιολογία του εγκεφάλου.

του συνομιλητή[280], δεν εμπλέκει, επομένως, συναίσθημα[281]. Αυτή η «έλλειψη κοινωνικοποίησης» επιτείνει το δίχως άλλο το πρόβλημα της κατάχρησης της τεχνολογίας. Εξάλλου, όπως χαρακτηριστικά αναφέρει ο Λάζος για το hacking « ... *το hacking φαίνεται να περιλαμβάνει μιαν ισχυρή κοινωνικοσυναισθηματική συνιστώσα, χωρίς την οποία οι υπόλοιπες συνιστώσες του θα παρέμεναν ανενεργές ή θα οδηγούνταν προς άλλες εμφάσεις και εστιάσεις. Πρόκειται για μία μόνιμη δυσφορία του ατόμου απέναντι στον τρόπο που ο γνωστός του κοινωνικός κόσμος είναι οργανωμένος και λειτουργεί.*»[282].

2.6 Η ηθική των hackers

Διατυπώνεται η άποψη ότι δεν υπάρχει ένας συγκεκριμένος ηθικός κώδικας, στον οποίο υπακούουν όλοι οι hackers. Αυτό συμβαίνει λόγω του ότι οι hackers δρουν είτε μεμονωμένα είτε σε πολλές υποομάδες[283] αλλά κυρίως διότι η ίδια η δυναμική εξέλιξη της τεχνολογίας διαμορφώνει συνεχώς νέες συνθήκες, οι οποίες χρήζουν κάθε φορά διαφορετικής αντιμετώπισης. Άρα, γράφεται ότι το όποιο αντίστοιχο «ηθικό υπόβαθρο» ανανεώνεται και αυτό συνεχώς[284].

Σε κάθε περίπτωση, στα «κλασικά» κείμενα που αναφέρονται στους hackers –όπως το «Μανιφέστο του hacker» - ανευρίσκονται κατευθυντήριες γραμμές της ηθικής βάσης της δραστηριότητας των hackers. Ειδικότερα, το περιεχόμενο του κειμένου «Μανιφέστο του hacker» στο βαθμό που αποτυπώνει την «ηθική των hackers» προέκυψε αρχικά χάρη στους πρώτους hackers των δεκαετιών του ’50 και ’60 στα

[280] Βλ. ενδεικτικά την ενότητα «Η επίπτωση της προβληματικής χρήσης του διαδικτύου στις σταθερές σχέσεις» στο πόνημα του *Γ. Φλώρου*, Η σκοτεινή πλευρά του διαδικτύου – ο ρόλος της πρόληψης, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 104.

[281] *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, p. 49.

[282] *Γρ. Λάζος*, Πληροφορική και Έγκλημα, όπ. π., σελ. 98.

[283] Για τις υποομάδες των hackers βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 41 και 42 και για την εσωτερική οργάνωση αυτών p. 164 καθώς και αναπτύξεις στην παράγραφο 2.5 του παρόντος πονήματος.

[284] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 39-40.

Πανεπιστήμια του MIT και του Stanford. Χαρακτηριστικό είναι το ότι ο συντάκτης του «Μανιφέστου» δεν χρησιμοποιεί τον όρο «hacker» για να περιγράψει τους «γκουρού» των συστημάτων πληροφοριών και των κωδικών, αλλά παρουσιάζει τους hackers ως περίεργους εξερευνητές που κυνηγούν την γνώση και τις πνευματικές προκλήσεις.

Συγκεκριμένα, η ηθική των hackers φαίνεται να συνοψίζεται στο κείμενο «Μανιφέστο» σε έξι βασικές αρχές. Η πρώτη αρχή συνίσταται στο ότι η πρόσβαση στους υπολογιστές πρέπει να είναι απεριόριστη και συνολική. Σύμφωνα με τη δεύτερη αρχή, όλες *οι πληροφορίες πρέπει να είναι ελεύθερες και προσβάσιμες σε όλους*, χωρίς να υπάρχουν στεγανά, λογοκρισία, ιδιοκτήτες ή πνευματικά δικαιώματα[285]. Ως τρίτη αρχή προβάλλεται η έλλειψη εμπιστοσύνης στην εξουσία σε συνδυασμό με την ταυτόχρονη προώθηση της αποκέντρωσης και την πάταξη της γραφειοκρατίας. Τέταρτον, οι hackers πρέπει να κρίνονται και να αξιολογούνται με βάση τις επιδόσεις τους και όχι βάσει κριτηρίων, όπως είναι τα πτυχία, οι βαθμοί, η ηλικία, το γένος ή η θέση τους. Τέλος, οι δύο τελευταίες αρχές αναφέρονται στη χρησιμότητα του ηλεκτρονικού υπολογιστή: πέμπτον, ως μέσο δημιουργίας τέχνης και ομορφιάς και έκτον, ως μέσο αλλαγής της ζωής του χρήστη προς το καλύτερο[286].

Εάν οι ως άνω αρχές ληφθούν υπόψη μεμονωμένα, χωρίς να υπολογίζεται το κείμενο από το οποίο προέρχονται ή ο σκοπός τους, τότε είναι εύκολο να θεωρηθεί ότι κατά ένα μέρος αφορούν διακήρυξη για εισβολή σε υπολογιστές. Πλην όμως, είναι σημαντικό να αναγνωριστεί ότι οι αρχές αυτές προέρχονται όχι από κυβερνοεγκληματίες αλλά από hackers, οι οποίοι ανταποκρίνονται στο περιεχόμενο και τη σημειολογία που είχε ο όρος τις δεκαετίες του ’50 και ’60[287]. Χαρακτηριστικά, σύμφωνα με την ηθική των hackers αποδοκιμάζονται δράσεις όπως π.χ. η εισβολή σε σύστημα νοσοκομείων κ.λπ.[288]

---

[285] Βλ. και *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες, τομ. β’, όπ. π., σελ. 183.

[286] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 79 και *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker’s mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 8 (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

[287] Βλ. ανωτέρω αναφορικά με την πρώτη γενιά των hackers την παράγραφο 2.4 του παρόντος πονήματος.

[288] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 11.

Η εμπορευματοποίηση της πληροφορίας[289] και η ανακάλυψη των διαφόρων ιών (viruses) των ηλεκτρονικών υπολογιστών[290] δεν άργησε να σημάνει το τέλος της "ρομαντικής" εποχής των πρώτων hackers. Γύρω στις αρχές του 1980 οι hackers ξεκινούν τις εισβολές σε κυβερνητικές υπηρεσίες διαφόρων κρατών –κυρίως στις ΗΠΑ– με σκοπό να αποδείξουν την ανεπάρκεια των συστημάτων ασφαλείας τους. Στη συνέχεια, η δράση των hackers κατά τη δεκαετία του '90 ήταν τέτοια, ώστε ο αναρχικός υπόκοσμος των hackers να θεωρείται ότι έχει σταδιακά διαβρωθεί από τους επαγγελματίες hackers.

Ωστόσο, δραστηριότητες όπως η πρόσβαση χωρίς εξουσιοδότηση, το «σπάσιμο» κωδικών και η πειρατεία λογισμικού θεωρούνται αρκετές φορές –τουλάχιστον από τους ίδιους τους hackers– μέσα περιφρούρησης των ελευθεριών τους. Σε πολλές, δέ, περιπτώσεις, η παραβίαση της ασφάλειας εξακολουθεί επίσης να θεωρείται μία συμβολική κίνηση ενάντια σε οργανισμούς που αρνούνται την πρόσβαση σε πληροφορίες ή αποκομίζουν οικονομικό κέρδος από τη χρήση αυτών των πληροφοριών.

Αν ο ορισμός που αποδοθεί στον hacker διατυπωθεί stricto sensu και, συνεπώς, εξαιρεθούν οι crackers και οι "black hat hackers", τότε μπορεί να θεωρηθεί ότι αρχές του ως άνω ηθικού κώδικα υφίστανται ακόμα. Τούτο προκύπτει και από το γεγονός ότι η δράση των crackers ή άλλων κατηγοριών θεωρείται κατώτερη ή απορρίπτεται από την κοινότητα των hackers. Την ίδια στιγμή, όμως, διαπιστώνεται ότι, κατά μια lato sensu θεώρηση, οι ως άνω ηθικοί κώδικες δεν εκφράζουν το σύνολο των ψηφιακών «παραβιαστών» και, άρα, ελλείπει ένας ευρύτερα αποδεκτός κώδικας ηθικής. Οι ανωτέρω προβληματισμοί σίγουρα επιτείνονται και από το γεγονός ότι, όπως ήδη αναφέρθηκε[291], γενικότερα στο διαδίκτυο φαίνεται να «*ελλείπει –ή είναι, μάλλον, υπό διαμόρφωση– αυτή η ανεπίσημη νόρμα που απορρέει από μια δημοφιλή πεποίθηση η οποία θα αποτελέσει την «λυδία λίθο» για τον χαρακτηρισμό μιας συμπεριφοράς στο διαδίκτυο ως παρεκκλίνουσας*»[292] [293]. Επομένως, τα θολά νερά της

[289] Βλ. ανωτέρω παράγραφο 1.2 του παρόντος πονήματος.

[290] Αναφορικά με τους ιούς των ηλεκτρονικών υπολογιστών πρβλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 17.

[291] Στην παράγραφο 1.4 του παρόντος πονήματος.

[292] Βλ. *του γράφοντος*, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

οργάνωσης στο διαδίκτυο είναι αυτά τα οποία επιτρέπουν στους hackers να επικαλούνται και να υιοθετούν θέσεις και στάσεις οι οποίες δυνητικά μπορεί είτε να υποστηριχθούν είτε να απορριφθούν.

Έχει διατυπωθεί η άποψη ότι πολλοί που θα συσχέτιζαν τον εαυτό τους με το μοντέρνο ορισμό του όρου «hacker» είναι ευχαριστημένοι με το να βλέπουν και να αποδέχονται την ηθική των hackers ως περιγραφή της συμπεριφοράς τους (μάλλον καθότι αυτή λειτουργεί όχι μόνο ως τεχνική ηθικής ουδετεροποίησης και δικαιολόγησης της συμπεριφοράς τους αλλά ακόμη και ως επιβράβευση). Το γεγονός αυτό έχει οδηγήσει κάποιους στο να διατυπώσουν την απορία εάν στην πραγματικότητα ο σύγχρονος hacker υπακούει, τελικά, σε ένα συγκεκριμένο ηθικό κώδικα[294]. Σύμφωνα με την άποψη του Mckenzie Wark[295] οι αρχές της νέας ηθικής των σύγχρονων hackers συνοψίζονται σε συνθήματα όπως: «*Τα ταξικά συμφέροντα των hackers δεν είναι η ιδιοκτησία αλλά η χειραφέτηση της πληροφορίας από τα υλικά της δεσμά*», «*Η μεγαλύτερη κλοπή είναι η ατομική ιδιοκτησία», «Ο χάκερ κατακτά την ελευθερία της γνώσης για να χαρίσει σε όλη την κοινωνία τη γνώση της ελευθερίας», «Το hacking είναι μία παλαιά πρακτική που αναφέρεται στη δημιουργική απαλλοτρίωση και ελεύθερη χρήση όλου του πλούτου*» κ.ά. Πάντως, η τελική εκτίμηση του Furnell είναι ότι, από τη μια, είναι αδύνατον να διαπιστωθεί και να υποστηριχθεί ξεκάθαρα ότι όλοι οι hackers ενστερνίζονται έναν (ενιαίο) ηθικό κώδικα, αλλά, από την άλλη, φαίνεται να υπάρχει μία «αίσθηση του καλού και του κακού»[296] η οποία οδηγεί τα πράγματα[297].

Επίσης, βλ. αντίστοιχα για τις διαφορετικές προσεγγίσεις –οι οποίες αταλάντευτα συνδέονται με τα (υπό διαμόρφωση) διαδικτυακά ήθη– αναφορικά με τη νομική αντιμετώπιση του πληροφορικού εγκλήματος *Γ. Λάζου*, Πληροφορική και Έγκλημα, όπ. π., σελ. 83 επ.

[293] Αναφορικά με την παρεκκλίνουσα συμπεριφορά πρβλ. *Alex Thio*, Παρεκκλίνουσα συμπεριφορά (επιμ. Χρήστος Τσουραμάνης), ίων, εκδ. έλλην, 2008.

[294] Βλ. *Steven Mizrach*, Is there a Hacker Ethic for 90s Hackers?, url: http://www2.fiu.edu/~mizrachs/hackethic.html.

[295] Βλ. *Χρήστος Ε.Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του διαδικτύου, όπ. π. σελ. 107.

[296] … με δεδομένο ότι η τεχνολογία δεν είναι ποτέ ουδέτερη, σύμφωνα με την άποψη του *Bert-Jaap Koops*, Criteria for Normative Technology - An essay on the acceptability of 'code as law' in light of democratic and constitutional values, TILT Law & Technology Working Paper No. 005/2007 Version 0.4 & Tilburg University Legal Studies Working Paper No. 007/2007, 7 December 2007, url: http://ssrn.com/abstract=1071745 (πρβλ. σχετικά *Αν. Χάιδου*, Σύγχρονη τεχνολογία και κοινωνικός έλεγχος, όπ. π., σελ. 97 όπου και αναφέρεται στον Gary Marx σύμφωνα με τον οποίο «*η αντίληψη σχετικά με την "τεχνική ουδετερότητα", σύμφωνα με την οποία η τεχνολογία είναι ηθικά και εθιμικά ουδέτερη ... στην πραγματικότητα εμποδίζει την κριτική σκέψη*»).

[297] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π. σελ. 81.

2.7 Η ιδεολογία των hackers

Η ιδεολογία[298] των hackers επηρεάζεται άμεσα και από στοιχεία της ηθικής των hackers[299]. Τα στοιχεία της ηθικής θέσης και άποψής τους συνιστούν τους ιδεολογικούς πυλώνες βάσει των οποίων οι hackers δρουν και αυτοπροσδιορίζουν τον ρόλο τους στο κοινωνικό γίγνεσθαι και στον κυβερνοχώρο. Οι αναπτύξεις και θέσεις π.χ. για ελευθερία της πληροφορίας (και σύμφωνα με τον Wark) προσδιορίζουν ηθικό υπόβαθρο με ιδεολογικές απολήξεις. Ιδιαιτέρως, επισημαίνεται η ανησυχία που επιδεικνύουν οι hackers αναφορικά με την αυξανόμενη ποσότητα των πληροφοριών που είναι αποθηκευμένες σε μεγάλες τράπεζες δεδομένων και τον περιορισμό της πρόσβασης για χρήση των πληροφοριών αυτών από ιδιώτες, αναφέροντας ότι είναι κοινωνική τους ευθύνη η εξασφάλιση της δυνατότητας

---

[298] Στην έννοια της ιδεολογίας έχουν δοθεί αρκετοί ορισμοί. Κατωτέρω παρατίθενται ορισμοί του Eagleton αναφορικά με το τι (διαζευκτικά ή παραπληρωματικά) έχει θεωρηθεί «ιδεολογία» κατά τις τελευταίες δεκαετίες [*Terry Eagleton*, Ideology: An Introduction (London: Verso, 1991), pp. 1-2]:

α) διαδικασία παραγωγής νοημάτων, σημείων και αξιών στην κοινωνική ζωή

β) σώμα ιδεών χαρακτηριστικό μιας συγκεκριμένης κοινωνικής ομάδας ή τάξης

γ) ιδέες που συνδράμουν στην νομιμοποίηση μιας κυρίαρχης πολιτικής δύναμης

δ) λανθασμένες ιδέες που συνδράμουν στην νομιμοποίηση μιας κυρίαρχης πολιτικής δύναμης

ε) συστηματική στρέβλωση επικοινωνίας

στ) ό,τι παρέχει θέση για ένα θέμα

ζ) μορφές σκέψης υποκινούμενες από κοινωνικά συμφέροντα

η) τρόπος σκέψης με κοινή ταυτότητα

θ) κοινωνικώς αναγκαία ψευδαίσθηση

ι) η σύζευξη λόγου και εξουσίας

ια) η συνισταμένη στην οποία συνειδητοί κοινωνικοί φορείς κατανοούν τον κόσμο τους

ιβ) προσανατολισμένα σε δράση σύνολα πεποιθήσεων

ιγ) σύγχυση γλωσσικής και φαινομενικής πραγματικότητας

ιδ) συμπέρασμα σημείων

ιε) το απαραίτητο μέσο στο οποίο βιώνουν τα άτομα τη σχέση τους με μια κοινωνική δομή

ιστ) η διαδικασία κατά την οποία λέγεται ότι η ζωή μετατρέπεται σε μία φυσική πραγματικότητα.

Είναι προφανές πως σε ό,τι αφορά την ιδεολογία των hackers δεν μπορούμε να ορίσουμε την ιδεολογία τους π.χ. κατά την ως άνω υπό γ' προσέγγιση – κάποιοι, όμως, από τους ανωτέρω ορισμούς, και ειδικά ο υπό η', μπορούμε να πούμε ότι καλύπτουν την περίπτωση των hackers, σύμφωνα με τη δράση τους σε υποομάδες και την ανάπτυξη κοινών στοιχείων (υπο)κουλτούρας (βλ. κατωτέρω αναπτύξεις για την υποκουλτούρα των hackers στην παράγραφο 2.8 του παρόντος πονήματος).

[299] Πρβλ. κριτική προσέγγιση ηθικής και ιδεολογίας κατά την μαρξιστική θεώρηση *David Marjoribanks*, Ideology and Morality, University of Kent, 2010 (url: http://www.academia.edu/306649/Ideology_and_Morality).

ανταλλαγής πληροφοριών[300]. Άρα, οι ως άνω αναπτύξεις για την ηθική των hackers σε κάθε περίπτωση δίνουν σαφή εικόνα αναφορικά και με την ιδεολογία τους.

Ειδικότερα, το «Μανιφέστο του hacker», όπως αναλύθηκε ανωτέρω, συνιστά ίσως το σημαντικότερο και το πιο δημοφιλές κείμενο από το οποίο εκπορεύεται και η ιδεολογία των hackers, ιδίως αναφορικά με την χρήση της τεχνολογίας και τον ρόλο τους στην κοινωνία. Συγκεκριμένα, σε ό,τι αφορά στη χωρίς άδεια/δικαίωμα πρόσβαση σε ξένο σύστημα, αυτή δεν είναι κατακριτέα, εφόσον δεν προξενεί ζημία ή βλάβη[301]. Οι έξι βασικές αρχές της ηθικής του hacker, σύμφωνα με το «Μανιφέστο», όπως παρουσιαστηκαν στην οικεία παράγραφο, αποτελούν ουσιαστικά και τον πυρήνα της ιδεολογία του hacker (με τη μορφή π.χ. ενός τρόπου σκέψης με κοινή ταυτότητα) καθώς η ελευθερία της πληροφορίας μπορεί να θεωρηθεί ότι αποτελεί το κυρίαρχο ιδεολογικό υπόβαθρο των πράξεων hacking.

Επιπρόσθετα, το «Μανιφέστο» φέρνει στο προσκήνιο μηνύματα αντιπολεμικά και κατά του ρατσισμού και στρέφεται εναντίον «της κοινωνίας της απάτης και του ψεύδους», με την παρατήρηση ότι τέτοιου είδους πρακτικές είναι αντίθετες με το ήθος των hackers (αγνοώντας, ωστόσο, το γεγονός ότι κάποιες από τις μεθόδους που χρησιμοποιούν οι hackers για να αποκτήσουν παράνομη πρόσβαση σε ένα σύστημα έχουν ως βάση την εξαπάτηση των κατόχων των δεδομένων - βλ. κατωτέρω την ανάλυση των πρακτικών των hackers[302]).

Περαιτέρω, η ιδεολογία του σύγχρονου hacker απεικονίζεται και στο κείμενο του προγραμματιστή και συγγραφέα Eric Steven Raymond με τον τίτλο «Πώς να γίνεις Hacker»[303], όπου τονίζεται ότι για να γίνει κάποιος αποδεκτός ως hacker, πρέπει να συμπεριφέρεται ως εμφορούμενος από την ιδεολογία του hacker και χωρίς μοναδικό σκοπό να γίνει αναγνωρίσιμος ως hacker.

Συγκεκριμένα, σύμφωνα με τον Raymond, η ιδεολογία του hacker συνοψίζεται σε πέντε παραδοχές – αρχές:

---

[300] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 11.

[301] Κατά τον Furnell, βέβαια, ορθώς κάποιες πληροφορίες είναι απρόσιτες στο ευρύ κοινό, διότι κάτι τέτοιο έρχεται σε σύγκρουση με την έννοια και τους στόχους της κοινωνίας της γνώσης (Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π. σελ. 75).

[302] Παράγραφος 2.11 του παρόντος πονήματος.

[303] Βλ. *Eric Steven Raymond*, Πώς να γίνεις Χάκερ, Μετάφραση Αριστοτέλης Μικρόπουλος, 2001, url: http://earthlab.uoi.gr/indy/hacker-howto-gr/.

(α) υπάρχουν πάρα πολλά διασκεδαστικά προβλήματα προς λύση

(β) κανένα πρόβλημα δεν πρέπει να λύνεται δύο φορές

(γ) η πλήξη και η αγγαρεία είναι «διαβολικές»

(δ) η ελευθερία είναι «αγαθή» και

(ε) η ιδεολογία δεν υποκαθιστά την ικανότητα.

Ειδικότερα, για να γίνει και να θεωρηθεί κάποιος hacker πρέπει να έχει ως κίνητρο τον ενθουσιασμό για να λύνει προβλήματα και να εξασκεί συνεχώς τις ικανότητες και την ευφυΐα του. Ακολούθως, οι hackers δεν πρέπει να σπαταλούν τον πολύτιμο χρόνο τους και έχουν ηθικό καθήκον να μοιράζονται τις πληροφορίες και τις λύσεις των προβλημάτων μεταξύ τους. Εξάλλου, οι hackers πιστεύουν στην ελευθερία και στην εθελοντική αμοιβαία βοήθεια. Επίσης, οι hackers δεν πρέπει ποτέ να πλήττουν και να εξαναγκάζονται να κάνουν δουλειά ρουτίνας, καθώς φαίνεται ανεπίτρεπτο και επιβλαβές για τους ίδιους και την κοινωνία να σπαταλούν τον χρόνο τους. Αυτό που δεν πρέπει να παραβλεφθεί είναι το γεγονός ότι συνήθως οι hackers διακατέχονται από μία ενστικτώδη αντιπάθεια για κάθε λογοκρισία. Τέλος, εμφαίνεται ότι με το να ασπαστεί κανείς απλώς μία ιδεολογία δεν γίνεται αυτομάτως hacker. Ο hacker αναγνωρίζεται από τις δυνατότητες και τις ενέργειές του, οι οποίες, βέβαια, υπακούουν στην ως άνω ιδεολογική προσέγγιση.

Ο Himanen υποστηρίζει ότι οι σύγχρονοι hackers λειτουργούν με βάση έναν νέο τρόπο εργασίας κατάλληλα προσαρμοσμένο στον 21ο αιώνα, ο οποίος μπορεί να αποτυπωθεί σε επτά αξίες: πάθος, ελευθερία, κοινωνική αξία, διαφάνεια, δράση, φροντίδα και (η σημαντικότερη όλων) δημιουργικότητα[304]. Σε μια θεώρηση από διαφορετική ίσως αφετηρία, ο Wark βλέπει στους hackers την επαναστατική τάξη του εικοστού πρώτου αιώνα: «*Το να "χακάρεις" σημαίνει να διαφέρεις.... Οι hackers δημιουργούν τη δυνατότητα εισδοχής νέων πραγμάτων στον κόσμο. Όχι πάντα σπουδαία πράγματα, ή ακόμη και καλά πράγματα, αλλά νέα πράγματα. Στην τέχνη, στην επιστήμη, στη φιλοσοφία και τον πολιτισμό, σε κάθε παραγωγή της γνώσης, οπουδήποτε*

[304] *P. Himanen*, The hacker ethic: A radical approach to the philosophy of business. New York: Random House, 2001, p. 141.

δεδομένα μπορούν να συγκεντρωθούν, οπουδήποτε πληροφορία μπορεί να εξαχθεί, ... υπάρχουν οι hackers που χακάρουν (σ.σ. ξεχωρίζουν) *το νέο από το παλιό*»[305].

Οι δύο ως άνω προσεγγίσεις διαφέρουν ως προς το ότι ο Himanen θεωρεί τους hackers συμμάχους των επιχειρήσεων ενώ ο Wark επαναστάτες. Επομένως, αποδίδουν στους hackers διαφορετικές ιδεολογικές προσλαμβάνουσες. Ωστόσο, έχουν ως κοινό σημείο την δημιουργικότητα των hackers και την πεποίθηση ότι είναι αυτοί που μπορούν να κάνουν τη διαφορά. Η πιο σύγχρονη, δηλαδή, προσέγγιση της ιδεολογίας του hacking είναι αυτή της δημιουργίας.

2.8 Η (υπο)κουλτούρα του hacking

Υποστηρίζεται ότι η (υπο)κουλτούρα[306] του hacking[307] είναι μία από τις λίγες αποκλίνουσες υποκουλτούρες που μπορούμε να παρατηρήσουμε από τους προσωπικούς μας υπολογιστές[308]. Οι hackers φαίνονται να είναι οργανωμένοι και να δρουν σε υποομάδες[309] - άρα, η υποκουλτούρα των hackers είναι στην πραγματικότητα μια χαλαρά δικτυωμένη συλλογή από υποκουλτούρες (διαφορετική για κάθε υποομάδα με κοινά χαρακτηριστικά πολλά από όσα αναφέρθηκαν ανωτέρω[310]) στις οποίες εκφράζονται κοινές εμπειρίες, κοινές ρίζες και κοινές

[305] *M. Wark*, A hacker manifesto. Cambridge, Mass.: Harvard University Press, 2004.

[306] Για την έννοια κουλτούρας και της υποκουλτούρας και τη συμβολή της στην παρεκκλίνουσα / εγκληματική συμπεριφορά βλ. *Αν. Χάιδου*, Θετικιστική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996, σελ. 160 επ.

[307] Βλ. σχετικά και τον ορισμό της έννοιας «Κυβερνοκουλτούρα» εις: *Ευστρατίου Παπάνη*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 171, στον οποίο ανευρίσκονται σε μεγάλο βαθμό στοιχεία της ηθικής και της ιδεολογίας του hacking (παράγραφοι 2.6 και 2.7 αντίστοιχα ως ανωτέρω) όπως η περισσότερη ελευθερία κ.ο.κ.

[308] Βλ. Digital Crime: Hackers, Part 2, LETN (Law Enforcement Training Network), pp. 4-5, url: http://www.twlk.com/law/tests/LETN1520009ct.pdf

[309] *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 21 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) καθώς και *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 11 – οι τελευταίοι θεωρούν αυτήν τη δράση σε υποομάδες ως ιδιαίτερο μέρος του προβλήματος.

[310] Βλ. παραγράφους 2.5, 2.6 και 2.7 του παρόντος πονήματος.

αξίες[311]. Επίσης, η υποκουλτούρα αυτή εδράζεται και στην ηθική και την ιδεολογία των hackers, όπως αυτές αναλύθηκαν ανωτέρω, και παραμένει σημείο αναφοράς – με δεδομένο ότι έχει και «ιστορικές ρίζες»[312]- ως ομαδική απάντηση στην διαμάχη που υπάρχει με την κυρίαρχη αντίθετη κουλτούρα, αυτήν της θέσης ορίων στο διαδίκτυο[313] (στο πλαίσιο ενός αντικομφορμισμού[314]), όπως η τελευταία αποτυπώνεται από την ποινικοποίηση των συμπεριφορών hacking σε αρκετές έννομες τάξεις[315]. Στην υποκουλτούρα, δηλαδή, του hacking ανιχνεύεται ένα σύνολο αξιών και κανόνων (όπως περιεγράφησαν ανωτέρω με τις εκάστοτε διαφοροποιήσεις – π.χ. black hat hackers και white hat hackers) που έρχονται σε αντίθεση με την κυρίαρχη κουλτούρα[316].

Μολονότι οι hackers δεν αποτελούν ομοιογενή ομάδα ή κοινότητα, η παγκόσμια υποκουλτούρα του hacking ("computer underground")[317] υποστηρίζεται ότι καθοδηγεί τη συμπεριφορά των hackers με βάση τρεις νόρμες[318]:

(α) Παρουσία της τεχνολογίας και στενή σχέση με αυτήν, έτσι ώστε να διευκολύνεται η δυνατότητά τους να κάνουν hacking[319]

(β) Μυστικότητα προκειμένου να αποφευχθεί η ανεπιθύμητη προσοχή από τους μηχανισμούς εφαρμογής του νόμου, συνδυασμένη, ωστόσο, με

---

[311] Βλ. αναλυτικά για την υποκουλτούρα των hackers και για τα γλωσσικά τους ιδιώματα την ιστοσελίδα με τίτλο "Hacker slang and hacker culture", url: http://www.catb.org/jargon/html/introduction.html.

[312] Βλ. την παράγραφο "Origins of hacker culture" στο άρθρο με τίτλο "Hacker culture", url: http://subcultureslist.com/hacker-culture/, όπου και αναλύεται πως η κουλτούρα του hacking αναπτύχθηκε ουσιαστικά μαζί με το hacking και τα δίκτυα υπολογιστών στα εργαστήρια των πανεπιστημίων της ανατολικής ακτής των ΗΠΑ στις δεκαετίες του '50 και του '60.

[313] Δεν πρέπει βέβαια να παροράται η περίπτωση επιθέσεων hacking στο πλαίσιο οργανωμένου εγκλήματος – βλ. σχετικά *Rob McCusker*, Transnational organised cyber crime: distinguishing threat from reality, Crime Law Soc Change (2006) 46:257–273.

[314] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38 όπου καταγράφεται η αντίθεση των hackers κατά του status quo.

[315] Βλ. νομοθετικές ρυθμίσεις σε έννομες τάξεις ανά την υφήλιο όπως παρουσιάζονται αναλυτικά και ανά χώρα στην ιστοσελίδα http://www.cybercrimelaw.net/Cybercrimelaw.html και ανά πολιτεία στις ΗΠΑ στην ιστοσελίδα http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[316] Βλ. *Αν. Χάιδου*, Θετικιστική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996, σελ. 161.

[317] *Orly Turgeman-Goldschmidt*, Identity construction among hackers, εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf, pp. 31.

[318] Έτσι *Thomas Holt & Bernadette Schell*, Hackers and hacking: a reference handbook, όπ. π., σελ. 24.

[319] Βλ. και ανωτέρω τον ορισμό του Jordan για το hacking και την σύνδεσή του με τα υλικά στοιχεία.

την επιθυμία για κομπορρημοσύνη και για μετάδοση της συσσωρευμένης γνώσης

(γ) «Μαεστρία» ή αλλιώς συνεχής εκμάθηση νέων δυνατοτήτων αναφορικά με το φυσικό και κοινωνικό περιβάλλον

Οι νόρμες αυτές εξηγούν τις συμπεριφορές των hackers[320]. Ειδικότερα, στοιχεία αυτής της υποκουλτούρας είναι το ότι οι hackers επιζητούν την αναγνώριση και την ενίσχυσή τους σε περιπτώσεις επιτυχημένων επιθέσεων[321]. Επίσης, έρευνες δείχνουν ότι οι hackers δεν αισθάνονται καμία ντροπή για τη δράση τους (ανεξαρτήτως αν ανήκουν στην κατηγορία "good" ή "bad hackers")[322] Περαιτέρω, υποστηρίζεται ότι ασπάζονται αξίες υποστήριξης μη ηθικών χρήσεων της τεχνολογίας[323], ότι υπάρχει μεταξύ τους ιεραρχία[324] (βλ. π.χ. "elite hackers", "makecrafters" και "techcrafters"[325]). Τέλος, υιοθετούν κοινά ιδιαίτερα γλωσσικά ιδιώματα[326] [327] [328].

---

[320] Υποστηρίζεται ότι η ετικέτα του "hacker" χρησιμοποιείται γενικότερα για την υποκουλτούρα της χρήσης υπολογιστών (έτσι *Orly Turgeman-Goldschmidt*, όπ. π., σελ. 31-32).

[321] Έτσι *Thomas Holt & Bernadette Schell*, Hackers and hacking: a reference handbook, όπ. π., σελ. 150.

[322] Βλ. *Orly Turgeman-Goldschmidt*, Identity construction among hackers, όπ. π., σελ. 47.

[323] Έτσι *Thomas Holt & Bernadette Schell*, Hackers and hacking: a reference handbook, όπ. π., σελ. 151.

[324] *Orly Turgeman-Goldschmidt*, όπ. π., σελ. 31.

[325] Βλ. ανωτέρω παράγραφο 2.3 του παρόντος πονήματος.

[326] *Orly Turgeman-Goldschmidt*, όπ. π., σελ. 31.

[327] Κατά τη Χάιδου, το ιδιαίτερο λεξιλόγιο σχετικό με τις δράσεις της ομάδας το οποίο τη διαφοροποιεί από το ευρύτερο κοινωνικό περιβάλλον αποτελεί χαρακτηριστικό υποκουλτούρας (βλ. *Αν. Χάιδου*, Θετικιστική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996, σελ. 161). Η γλώσσα βοηθά να ισχυροποιηθούν τα όρια μεταξύ των hackers και όσων δεν είναι hackers, καθώς και μεταξύ hackers και crackers. Οι hackers, λοιπόν, έχουν αναπτύξει τη δική τους γλώσσα. Πέρα από ορολογίες της πληροφορικής, οι οποίες δεν είναι γνωστές σε όσους δεν έχουν εξειδίκευση στην πληροφορική (π.χ. TCP, IP, Winsock, Linux κ.λπ.), μερικοί hackers έχουν τροποποιήσει την αγγλική γλώσσα αντικαθιστώντας το γράμμα f με το δίφθογγο ph (πιθανόν αντικατάσταση αυτή έχει τις ρίζες της στους "phreaks", οι οποίοι έδειχναν ιδιαίτερο ενδιαφέρον για τα τηλέφωνα - phones) καθώς και το γράμμα s με το γράμμα z [ιδίως όταν το γράμα s είναι τελικό – π.χ. filmz – έτσι ο *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 416, υποσ. 27]. Επίσης, οι hackers χρησιμοποιούν αριθμούς στη θέση γραμμάτων, όπως π.χ. τον αριθμό 1 στη θέση του i ή l, τον αριθμό 3 στη θέση του E, τον αριθμό 4 στη θέση του a και τον αριθμό 7 στη θέση του t. Επιπρόσθετα, σημαντικό ρόλο παίζει η τυχαία χρήση κεφαλαίων γραμμάτων (π.χ. caPitAlizaTioN), συντομογραφιών, λέξεων της αργκό, τονισμός των λέξεων με την τοποθέτηση του προθέματος k- πριν από αυτές (π.χ. "k-rad") κ.λπ. (βλ. "Hackers language", url: http://www.campusactivism.org/html-resource/hackers/section8.html καθώς και "Hacker slang and hacker culture", url: http://www.catb.org/jargon/html/introduction.html).

[328] Βλ. ως χαρακτηριστικό παράδειγμα το κείμενο το οποίο εστάλη από την ελληνική χάκινγκ σκηνή (greek hacking scene – ghs) στον γράφοντα ως παρουσίαση της δράσης και της ιδεολογίας της ελληνικής χάκινγκ σκηνής (παράρτημα IV). Στο συγκεκριμένο κείμενο βλέπουμε π.χ. να χρησιμοποιείται από την GHS το ελληνικό γράμμα «ω» ως το αγγλικό γράμμα "w" και το ελληνικό γράμμα «ε» ως το αγγλικό γράμμα "e", ως ειδικό γλωσσικό μόρφωμα.

Ο Taylor[329] προχωράει την ανάλυσή του πέρα από την αντιμετώπιση του hacking μόνο ως τεχνική δραστηριότητα και εντάσσει τη δραστηριότητα αυτή στο κοινωνικό πλαίσιο διαμάχης μεταξύ κοινωνικών ομάδων[330]. Ειδικότερα, αναφέρεται σε διαμάχη ανάμεσα στην υποκουλτούρα των χρηστών υπολογιστών (εκεί δηλαδή όπου αναπτύσσονται οι πρακτικές hacking) και την βιομηχανία ασφαλείας των υπολογιστικών συστημάτων[331].

2.9 Ειδικές εκφάνσεις του hacking

2.9.1 Ηθικό hacking ("Ethical hacking")

Η κατηγορία των ηθικών hackers ("ethical hackers") αποτελείται από αυτούς που χρησιμοποιούν τις τεχνικές τους και τις δεξιότητές τους όχι για να βλάψουν αλλά για να ενισχύσουν την ασφάλεια συστημάτων και πληροφοριών, αναζητώντας τα «ευαίσθητα» σημεία και τα κενά ασφαλείας των ηλεκτρονικών συστημάτων[332]. Αρκετές φορές, μάλιστα, δρουν κατά παραγγελία του διαχειριστή του δικτύου ή/και των ηλεκτρονικών δεδομένων/πληροφοριών[333]. Αυτή η δραστηριότητα καλείται ειδικότερα και "ethical hacking" ("ηθικό hacking")[334].

---

[329] *Paul A. Taylor*, Hackers: Crime in the Digital Sublime, Routledge, 1999, όπ. π., pp. vii.

[330] Βλ. για την κουλτούρα του hacking και τις αναπτύξεις του *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf όπως παραπέμπει και στον Taylor.

[331] Ωστόσο, ο ίδιος ο Taylor επισημαίνει ότι (τουλάχιστον κατά τον χρόνο σύνταξης του πονήματός του) οι δύο κατ' αυτόν «αντιμέτωπες» ομάδες στερούνται συνοχής (*Paul A. Taylor*, Hackers: Crime in the Digital Sublime, όπ π., σελ. vii).

[332] Βλ. αναλυτικά *Marilyn Leathers*, A Closer Look at Ethical Hacking and Hackers, East Carolina University, url: http://www.infosecwriters.com/text_resources/pdf/MLeathers_Ethical_Hackers.pdf.

[333] Αντίθετη άποψη από τους *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 55 σύμφωνα με τους οποίους οι "ηθικοί hackers" δεν προβαίνουν σε αυτή τη δραστηριότητα για χρήματα ή για φήμη.

[334] Αναλυτικά για το "ethical hacking" βλ. το εμπεριστατωμένο άρθρο του *C. C. Palmer*, Ethical hacking, url: http://pdf.textfiles.com/security/palmer.pdf καθώς και *Brian A. Pashel*, Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level, Kennesaw State University, url: http://cs.potsdam.edu/faculty/laddbc/Teaching/Ethics/StudentPapers/2006Pashel-TeachingStudentsToHack.pdf.

Ειδικότερα, οι ηθικοί hackers επιτίθενται σε ένα δίκτυο υπολογιστών για λογαριασμό των ιδιοκτητών του, αναζητώντας τρωτά σημεία τα οποία ένας κακόβουλος hacker θα μπορούσε να εκμεταλλευτεί. Οι ηθικοί hackers χρησιμοποιούν τις ίδιες μεθόδους με τους κακόβουλους hackers αλλά αναφέρουν τα προβλήματα που εντοπίζουν αντί να επωφεληθούν από αυτά. Οι ομάδες που αποτελούνται από ηθικούς hackers καλούνται και «κόκκινες ομάδες» (red teams)[335]. «Κόκκινες ομάδες» ηθικών hackers χρησιμοποίησε ήδη από τη δεκαετία του 1970 η κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής προκειμένου να ελέγξει την ασφάλεια των συστημάτων ηλεκτρονικών υπολογιστών που είχαν αρχίσει τότε να αναπτύσσονται[336].

Για να ενταχθεί μια ενέργεια στο φάσμα του ηθικού hacking πρέπει να υπακούει στους εξής κανόνες[337]:

- Ο hacker πρέπει να έχει τη συγκατάθεση του υποκειμένου και διαχειριστή των δεδομένων (αρκετές φορές μάλιστα με τη μορφή γραπτής άδειας)[338] να «εξετάσει» το δίκτυο ή τον ιστότοπο και να προσπαθήσει να εντοπίσει πιθανούς κινδύνους ασφαλείας.

- Η δραστηριότητα του ηθικού παραβιαστή πρέπει να ασκείται με γνώμονα τον σεβασμό της ιδιωτικής ζωής του ατόμου ή της εταιρείας, και να συμπεριλάβει μόνο δεδομένα τα οποία είναι απαραίτητα για τον έλεγχο ασφαλείας των ηλεκτρονικών συστημάτων.

- Ο ηθικός hacker πρέπει να αναφέρει όλες τις ευπάθειες ασφαλείας που ανιχνεύει στο σύστημα και να ενημερώσει σχετικώς και αναφορικά με τα κενά ασφαλείας τον προγραμματιστή λογισμικού ή τον κατασκευαστή του υλικού, προκειμένου να γνωρίζουν οι τελευταίοι τα τρωτά σημεία της ασφάλειας που εντοπίζει στο λογισμικό ή στο υλικό τους.

---

[335] Υπάρχουν ακόμη και σεμινάρια αλλά και πιστοποιήσεις «ηθικού» hacker αναφορικά με την ικανότητά τους σε έλεγχο ικανότητας διείσδυσης (penetration testing) – βλ. σχετικά urls: http://en.wikipedia.org/wiki/Certified_Ethical_Hacker, http://www.ethicalhacking.com,

[336] Έτσι *Marilyn Leathers,* A Closer Look at Ethical Hacking and Hackers, όπ. π. Βλ. σχετικά και url: http://searchsecurity.techtarget.com/definition/ethical-hacker.

[337] Βλ. σχετικά url: http://www.computerhope.com/jargon/e/ethihack.htm.

[338] Με γραπτή άδεια δηλώνει ότι πράττει και ο hacker – ελεγκτής ασφαλείας συστημάτων με το όνομα «Γιώργος», όπως αναφέρεται στο ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy.

Ο όρος «ηθικό hacking» έχει λάβει επικρίσεις κατά καιρούς, ιδίως από όσους θεωρούν το hacking έγκλημα κατά την τυπική ή/και ουσιαστική έννοια. Ωστόσο, είναι αλήθεια ότι οι ηθικοί hackers έχουν συμβάλλει στη βελτίωση της ασφάλειας των συστημάτων ηλεκτρονικών πληροφοριών και, άρα, το hacking φαίνεται να μπορεί να έχει και μια ηθική διάσταση[339].

2.9.2 "Hacktivism" («ΧΑΚτιβισμός» - παραβιαστές με ακτιβιστική δράση)

Σε εφαρμογή των ως άνω αρχών της ηθικής και ιδεολογίας των hackers και σε συνδυασμό με την δράση σε πολιτικούς και κοινωνικούς χώρους[340] και την αντίθεσή τους στην καθεστηκυία τάξη[341], αναπτύχθηκε στο διαδίκτυο το κίνημα του «χακτιβισμού» ("hactivism" = hacking + activism), το οποίο αποτελεί μία μεταφορά του ακτιβισμού της πραγματικής ζωής σε ένα ψηφιακό επίπεδο έκφρασης. Η άποψη πως οι hackers διαπνέονται από το σύνδρομο του «Ρομπέν των Δασών» φαίνεται να περιγράφει ειδικότερα τα κίνητρα των χακτιβιστών. Συγκεκριμένα, σύμφωνα με την ανωτέρω οπτική, οι χακτιβιστές hackers φαίνεται να πιστεύουν πως η πρόκληση βλάβης σε ατομικά αγαθά αποτελεί ανήθικη πράξη. Αντιθέτως, θεωρούν αποδεκτή συμπεριφορά την επίθεσή τους στο σύστημα μιας επιχείρησης ή ενός (κυβερνητικού) οργανισμού, που κατά τη γνώμη τους δρα καταπιεστικά έναντι στο κοινωνικό σύνολο – σε αυτόν, δέ, τον σκοπό τους είναι πλήρως αφοσιωμένοι [342].

Η αρχική έκφανση του «χακτιβισμού» συνίσταται στην ανάδειξη των τρωτών σημείων των δικτύων ηλεκτρονικών δεδομένων και του διαδικτύου και την απαλλαγή

---

[339] *Marilyn Leathers*, A Closer Look at Ethical Hacking and Hackers, East Carolina University, url: http://www.infosecwriters.com/text_resources/pdf/MLeathers_Ethical_Hackers.pdf.

[340] Πρβλ. αναφορικά με την εμπιστευτικότητα πληροφοριών σε συνάρτηση με πολιτικές θεωρίες και δράσεις *Charles Raab*, Beyond activism: Research perspectives on privacy, The University of Edinburgh & Tilburg University, TILT Law & Technology Working Paper No. 007/2008, 22 February 2008, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 004/2008, url: http://ssrn.com/abstract=1096562.

[341] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38 όπου καταγράφεται η αντίθεση των hackers κατά του status quo.

[342] Βλ. *Cynthia Fitch*, M.Ed., Crime and Punishment: The Psychology of Hacking in the New Millennium, url: http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795, pp. 6-7.

τους από οποιοδήποτε επιβλαβές ηλεκτρονικό στοιχείο, ηλεκτρονικό κώδικα και ελαττωματικό πρόγραμμα. Η διάκριση μεταξύ ethical hacking και χακτιβιστών είναι ότι οι χακτιβιστές αναζητούν και αποκαλύπτουν κενά ασφαλείας και για λόγους κοινωνικού ακτιβισμού και θέλησης να κάνουν τα ηλεκτρονικά προγράμματα ασφαλέστερα. Είναι, βέβαια, γεγονός ότι στις περισσότερες περιπτώσεις πρόκειται για τους ίδιους white hat hackers[343], οι οποίοι μπορούν να θεωρηθούν χακτιβιστές ή ηθικοί hackers ανάλογα με την περίσταση.

Η δεύτερη – και πιο ενδιαφέρουσα ίσως – έκφανση του χακτιβισμού είναι η μεταχείριση των ειδικών γνώσεων και τεχνικών των hackers για την προώθηση στο διαδίκτυο πολιτικών απόψεων και κοινωνικών αιτημάτων και διεκδικήσεων[344] καθώς και την χρησιμοποίηση του διαδικτύου ως μέσου διαμαρτυρίας[345]. Οι χακτιβιστές θεωρούνται μια από τις πιο γρήγορα αναπτυσσόμενες υποομάδες hackers. Χαρακτηριστικά παραδείγματα «χακτιβιστών» είναι οι υποστηρικτές των «Ζαπατίστας» με έδρα τη Νέα Υόρκη και οι "Electrohippies"[346], οι οποίοι διαμαρτύρονται για τα γενετικώς τροποποιημένα προϊόντα. Επίσης, δράσεις "χακτιβισμού" έχουν λάβει χώρα για την ελευθερία διάθεσης καλλιτεχνικών έργων στο διαδίκτυο (π.χ. μουσική).

2.10 Ο «σκοτεινός αριθμός» των περιστατικών hacking (αφανής εγκληματικότητα)

[343] Ο Furnell κατατάσσει τους χακτιβιστές στους grey hat hackers (βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 55), αλλά, μάλλον, όχι λόγω των συμπεριφορών τους αναφορικά με τα κενά ασφαλείας αλλά λόγω των λοιπών δραστηριοτήτων τους.

[344] Πρβλ. το άρθρο του *Michael Stohl*, Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?, Crime Law Soc Change (2006) 46:223–238, κατά τον οποίο η θεωρία δεν έχει ακόμη επιτύχει να οριοθετήσει επακριβώς τον χακτιβισμό σε σχέση με την κυβερνοτρομοκρατία.

[345] Αναφορικά με τη σχέση ή τη διάσταση των όρων «χακτιβιστής» και «κυβερνοτρομοκράτης» βλ. το αναλυτικό άρθρο του *Sandor Vegh*, Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking, url: http://firstmonday.org/ojs/index.php/fm/article/view/998/919.

[346] Βλ. ενδεικτικά το λήμμα "Electrohippies collective" url: http://searchsecurity.techtarget.com/definition/Electrohippies-Collective.

Η δραστηριότητα του hacking εντάσσεται στη λεγόμενη αφανή εγκληματικότητα[347] [348]. Τα περιστατικά τα οποία έρχονται είτε στη δημοσιότητα, είτε σε γνώση της αστυνομίας ή οποιουδήποτε άλλου επίσημου φορέα, με οποιονδήποτε τρόπο, και καταγράφονται, αποτελούν μάλλον την «κορυφή του παγόβουνου»[349] του hacking και, άρα, τα περισσότερα περιστατικά hacking αποτελούν «σκοτεινό αριθμό»[350].

Τούτο διότι τα θύματα (συνήθως εταιρείες) – ιδίως σε περιπτώσεις που εξυπηρετούν διαδικτυακά οικονομικά συμφέροντα ή διαχειρίζονται δεδομένα[351], των οποίων η ασφάλεια είναι sine qua non στοιχείο για την εμπιστοσύνη του κοινού – ουδέποτε θα παραδεχθούν ή θα δώσουν αφορμή να κοινοποιηθεί με οποιονδήποτε τρόπο ότι το ηλεκτρονικό τους σύστημα έχει πληγεί από μια ηλεκτρονική επίθεση[352], καθώς με αυτόν τον τρόπο θα χάσουν την αξιοπιστία τους και θα πλήξουν τη δημόσια εικόνα και τη φήμη τους[353] [354].

Το πρόβλημα της αφανούς εγκληματικότητας, όπως εξηγεί η Σπινέλλη, είναι αρκετά σημαντικό. Αφενός, δημιουργείται αβεβαιότητα από την άγνοια του πραγματικού μεγέθους του φαινομένου – αυτή, δε, η κατ' ουσίαν άγνοια των ποιοτικών και ποσοτικών διαστάσεων του hacking έχει ως αποτέλεσμα την δυσκολία στην χάραξη

---

[347] Αναφορικά με την αφανή ή σκοτεινή περιοχή της εγκληματικότητας πρβλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 138 επ. καθώς και *Ιακ. Φαρσεδάκη*, Στοιχεία εγκληματολογίας, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2005, σελ. 46.

[348] Η Ζαραφωνίτου παραπέμπει στον Φαρσεδάκη, ο οποίος αναφέρει ότι σε περιπτώσεις εγκλημάτων στο διαδίκτυο το ποσοστό καταγγελιών είναι μικρό και, συνεπώς, αντιστρόφως αναλογα μεγάλος ο «σκοτεινός αριθμός» (έτσι *Χρ. Ζαραφωνίτου και συν.*, Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο, όπ. π., σελ. 5). Συγκεκριμένα, ο Φαρσεδάκης αναφέρεται ότι μόλις το 15% των εγκλημάτων στο διαδίκτυο αναφέρεται στις αρχές (έτσι *Ιακ. Φαρσεδάκης,* Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π.). Για «σκοτεινό αριθμό» μιλάει και ο Τσουραμάνης (*Χρ. Τσουραμάνης,* Ψηφιακή εγκληματικότητα, όπ. π., σελ. 8).

[349] Βλ. χαρακτηριστικά στοιχεία που παρατίθενται από τους *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, p. 43 σύμφωνα με τους οποίους κατά την περίοδο συγγραφής του πονήματός τους 1% των εγκλημάτων που αφορούν ηλεκτρονικούς υπολογιστές ανιχνεύονταν και μόλις το 7% αυτού του 1% καταγγέλονταν στις αρχές!

[350] Αναφορικά με τον «σκοτεινό αριθμό» της εγκληματικότητας βλ. αναλυτικά *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, κεφάλαιο 5, παρ. 2, σελ. 128 επ.

[351] ...οι οποίες αποτελούν την πλειοψηφία των θυμάτων κυβερνοεγκλήματος (βλ. *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-Zavrsnik.pdf, p. 13).

[352] Αναφορικά με τους παράγοντες μη καταγγελίας των αξιόποινων πράξεων από τα θύματα πρβλ. *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 265 επ.

[353] Έτσι η *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, url: http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf, όπως παραπέμπει στους Randazzo, Keeney, Kowalski, Cappelli, & Moore, σελ. 8.

[354] «*... τα "θύματα-εταιρείες" συνήθως προτιμούν έναν διακριτικό συμβιβασμό από ένα σκάνδαλο που θα έβλαπτε την επιχείρηση*» (έτσι *Γ. Πανούσης*, Εγκληματολογία, εγκληματολογική έρευνα και ΜΜΕ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1999, σελ. 75).

ορθολογικής και συνάμα αποτελεσματικής αντεγκληματικής ή εγκληματοπροληπτικής πολιτικής. Αφετέρου, για την πληρέστερη κατανόηση του φαινομένου, απαιτείται η γνώση όλων των περιπτώσεων, προκειμένου να αποφευχθούν γενικεύσεις που θα προέρχονται μοναχά από την εμφανή εγκληματικότητα[355] [356], θα καταλαμβάνουν, όμως, και τις περιπτώσεις της αθέατης εγκληματικότητας.

2.11 Μέθοδοι και τεχνικές (modi operandi) των hackers για την απόκτηση χωρίς δικαίωμα πρόσβασης

Η πρόσβαση ενός hacker στο σύστημα πληροφοριών του υποψήφιου θύματος προϋποθέτει δύο στάδια: ένα προπαρασκευαστικό και ένα κύριο. Στο πρώτο στάδιο ο παραβιαστής κάνει όλες εκείνες τις ενέργειες, οι οποίες του είναι απαραίτητες, για να αποκτήσει πρόσβαση στο σύστημα που τον ενδιαφέρει. Στο δεύτερο στάδιο έρχεται σε επαφή ή συλλέγει τις πληροφορίες που αναζητούσε και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη της εισβολής του και έπειτα να διατηρήσει το δικαίωμα της επανεισόδου του. Αναφορικά, επομένως, με τις μεθόδους και τεχνικές που δύναται να χρησιμοποιήσει ο hacker, σκόπιμη είναι η διάκρισή τους σε "insiders" (αυτοί που μπορούν να έχουν πληροφόρηση «εκ των έσω» για ένα σύστημα ερχόμενοι σε επαφή με τους διαχειριστές του, με τις διαδικασίες λειτουργίας του κ.λπ.[357]) και "outsiders" (αυτοί που προσπαθούν να προσεγγίσουν και να παραβιάσουν το σύστημα χωρίς να έχουν – αρχικώς τουλάχιστον ή εκ κάποιας ιδιότητός τους – εσωτερική πληροφόρηση)[358].

---

[355] Έτσι *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 139.

[356] Η έρευνα που ακολουθεί έχει συμπεριλάβει και έρευνα αυτοομολογούμενης παραβατικότητας σε hackers αλλά και προσέγγιση του φαινομένου του hacking μέσα από τεχνικούς ηλεκτρονικών υπολογιστών οι οποίοι έχουν αντιμετωπίσει περιστατικά hacking, σύμφωνα και με τις πρακτικές αντιμετώπισης του προβλήματος της σκοτεινής περιοχής, όπως αυτές προτείνονται από τη Σπινέλλη (*Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 139-140).

[357] Βλ. σχετικά και *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, όπ. π., σελ. 183 για την περίπτωση που αναφέρει ότι «*Οι δράστες προέρχονται τις περισσότερες φορές μέσα από τους κόλπους των επιχειρήσεων…*». Βλ. επίσης ανωτέρω παράγραφο 2.3.3 αναφορικά με την κατηγορία «Disgruntled (ex) employees [Δυσαρεστημένοι (πρώην) εργαζόμενοι]».

[358] Αναφορικά με τη διάκριση "insiders" και "outsiders" και γενικότερα για την χωρίς άδεια πρόσβαση βλ. *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker*, Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series No 78, Australian Institute of Criminology,

Σε γενικές γραμμές, υπάρχουν τρεις βασικοί τρόποι για να απόκτηση χωρίς δικαίωμα πρόσβασης («εισβολή» / "intrusion") από "outsiders" σε ένα σύστημα[359]:

• «Φυσική εισβολή» ("Physical intrusion") καλείται η περίπτωση κατά την οποία ο εισβολέας έχει φυσική πρόσβαση στη συσκευή, η οποία αποτελεί στόχο του. Υπάρχει σε αυτήν την περίπτωση η δυνατότητα αυτός που απέκτησε χωρίς δικαίωμα πρόσβαση να ελέγξει όλο το σύστημα και να αντιγράψει ηλεκτρονικά δεδομένα άμεσα σε δικό του σύστημα πληροφοριών (ακόμη και με μόνη τη χρήση ενός καλωδίου).

• «Εισβολή μέσω του συστήματος» ("System intrusion"). Στην περίπτωση αυτή ο εισβολέας έχει ήδη προνόμια χαμηλού επιπέδου για την είσοδό του στο σύστημα πληροφοριών και εκμεταλλευόμενος τρωτά σημεία ασφάλειας προσπαθεί να αναβαθμίσει τη δυνατότητα αυθεντικοποίησής του (authentication) προκειμένου να αποκτήσει πρόσβαση σε δεδομένα από τα οποία είναι αποκλεισμένος.

• «Απομακρυσμένη εισβολή» ("Remote intrusion") έχουμε στην περίπτωση κατά την οποία ο εισβολέας προσπαθεί να μπει στο σύστημα εξ αποστάσεως μέσω δικτύου στο οποίο είναι συνδεδεμένο το σύστημα πληροφοριών. Είναι ο πλεόν κοινός τρόπος χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα.

2.11.1 Η ανακάλυψη της ταυτότητας του χρήστη – η «κλοπή ταυτότητας» (identity theft)

Η μέθοδος που χρησιμοποιείται περισσότερο για την πιστοποίηση ενός χρήστη, ιδίως αναφορικά με την χορήγηση πρόσβασης, είναι αυτή που στηρίζεται στο όνομά του (user's ID) σε συνδυασμό με ένα συνθηματικό/κωδικό εισόδου (password). Αυτά τα στοιχεία πρέπει να δώσει ο χρήστης προκειμένου να του επιτραπεί η είσοδος στο

pp. 51 f. και *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker,* The future of technology-enabled crime in Australia, TRENDS & ISSUES in crime and criminal justice, Australian Institute of Criminology, No 341, July 2007, p. 3 καθώς και *Steven Furnell*, όπ. π., σελ.31.

[359] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 2.

σύστημα[360]. Συνιστούν, δηλαδή, την «ηλεκτρονική ταυτότητα» του χρήστη και, άρα, είναι λογικό ότι τις περισσότερες φορές αποτελούν στόχο των hackers[361]. Για αυτόν τον λόγο αναφερόμαστε εν προκειμένω σε identity theft («κλοπή ταυτότητας»)[362] ή/και password theft[363] [364].

Η επιλογή των passwords έχει πολύ μεγάλη σημασία για την ασφάλεια ενός συστήματος. Ασφαλές password είναι εκείνο που θα υποκλαπεί/ παραβιαστεί/ αποκαλυφθεί όσον το δυνατόν δυσκολότερα από έναν hacker. Ωστόσο, ακόμα και οι πιο δύσκολοι κωδικοί και τα προστατευόμενα με τον ασφαλέστερο τρόπο αρχεία στοιχείων ταυτότητας και αυθεντικοποίησης ενός συστήματος δεν είναι δυνατό να μην αποκαλυφθούν στον hacker που έχει καταφέρει π.χ. να εγκαταστήσει σε αυτό ένα πρόγραμμα sniffer (π.χ. key logger[365]), με το οποίο θα έχει τη δυνατότητα να καταγράφει όλα τα χτυπήματα στα πλήκτρα του πληκτρολογίου του χρήστη. Ο hacker χρησιμοποιώντας, επίσης, ειδικά προγράμματα που περιέχουν καταλόγους με λέξεις (wordlists)[366] αυξάνει σημαντικά τις πιθανότητες να ανακαλύψει τον κωδικό

---

[360] Τα στοιχεία αυτά βρίσκονται συνήθως αποθηκευμένα στο αρχείο «passwd» που υπάρχει στο σύστημα, εφόσον αυτό χρησιμοποιεί το λειτουργικό σύστημα Unix, κάτι που ισχύει για τους εξυπηρετητές (servers) των περισσότερων συστημάτων που υπάρχουν στο διαδίκτυο (Internet). Προκειμένου ο hacker να μάθει τα δύο ως άνω στοιχεία τα οποία προσδιορίζουν την ταυτότητα του χρήστη, να την «κλέψει» (identity theft) και συνεπώς να αποκτήσει πρόσβαση στις ηλεκτρονικές πληροφορίες, μπορεί είτε να διερευνήσει συστηματικά το αρχείο «passwd» με ειδικά προγράμματα για την αποκάλυψη κωδικών (special password guessing programs), είτε να αναλύσει τα πρωτόκολλα επικοινωνίας με ειδικά προγράμματα διερεύνησης δικτύων, είτε να απομονώσει τους κωδικούς με τη χρήση προγραμμάτων που μένουν στη μνήμη (TSR) του συστήματος ή «Δούρειων Ίππων» είτε τέλος να χρησιμοποιήσει εξωπρογραμματιστικές πρακτικές (π.χ. κοινωνική μηχανική, dumpster diving κ.ά., όπως περιγράφονται κατωτέρω).

[361] Βλ. για την απειλή της «κλοπής ταυτότητας» από hackers το άρθρο των *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, pp. 2 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

[362] Πρβλ. *Εμμ. Μεταξάκη*, Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου, ΠοινΧρ ΞΔ/ 2014, σελ. 10, παρ. 1.4 αναφορικά με υπόθεση κατά την οποία ο κατηγορούμενος αντιμετώπισε και την κατηγορία της «κλοπής ταυτότητας».

[363] Βλ. αναφορικά με "identity theft" *Chuck Easttom and Det. Jeff Taylor*, Computer Crime, Investigation and the Law, Course Technology PTR, A part of Cengage Learning, 2011, pp. 171 f. καθώς και *Kristan T. Cheng*, Identity Theft and the Case for a National Credit Report Freeze Law, North Carolina Banking Institute, 12 N.C. Banking Inst. 239, March, 2008, lexisnexis database.

[364] Αναφορικά με το password theft βλ. *Ιακ. Φαρσεδάκης*, Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π., σελ. 3 καθώς και urls: http://www.softstack.com/security/password-theft.html και http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Password_theft/default.htm.

[365] Βλ. κατωτέρω παράγραφο 2.11.2.2.11.

[366] Για την ανακάλυψη κωδικών υπάρχουν λίστες λέξεων στο διαδίκτυο οι οποίες διατίθενται ελεύθερα στους επίδοξους hackers (βλ. χαρακτηριστικά url: http://www.hackreports.com/2013/05/biggest-password-cracking-wordlist-with.html).

και το όνομα χρήστη, τα οποία θα του επιτρέψουν να εισέλθει και να κινηθεί μέσα σε ένα σύστημα πληροφοριών κατέχοντας όλα τα δικαιώματα ενός νόμιμου χρήστη του.

2.11.2 Η πρόσβαση στο σύστημα

Όπως είδαμε ανωτέρω, ο hacker, καταρχάς, συγκεντρώνει πληροφορίες (information gathering) για το σύστημα στο οποίο επιθυμεί να εισέλθει και, κατά δεύτερον, προσπαθεί να αποκτήσει πρόσβαση σε αυτό ανακαλύπτοντας ή «σπάζοντας» τους κωδικούς εισόδου (password cracking), αποκτώντας έτσι τα δικαιώματα (privileges) ενός νόμιμου χρήστη του συστήματος[367]. Η προσπάθεια αυτή μπορεί να λάβει χώρα είτε με τεχνικά μέσα [ειδικά προγράμματα τα οποία προορίζονται για την δημιουργία προβλημάτων στο σύστημα και για να επιφέρουν βλαπτικές συνέπειες και τα οποία καλούνται "*malicious software*" (επιβλαβές πρόγραμμα υπολογιστή) και για συντομία "*malware*"[368]] – για τη χρήση των οποίων εισφέρεται στην παρούσα εργασία ο όρος «***πρακτικές hacking με χρήση ηλεκτρονικών προγραμμάτων (software)*» (άλλως *«γνήσιες πρακτικές hacking»*[369])** – είτε με πρακτικές ενημέρωσης των hackers για το σύστημα και προσπάθειας εξαπάτησης του χρήστη (δημιουργίας πλάνης στο νοητικό του θύματος[370]) για την αποκάλυψη των στοιχείων που θα επιτρέψουν τη χωρίς δικαίωμα είσοδο στο σύστημα («***εξωπρογραμματιστικές πρακτικές hacking***»). Βασική διαφορά μεταξύ των πρακτικών των δύο αυτών ομαδοποιήσεων είναι ότι στη χρήση ηλεκτρονικών προγραμμάτων απαιτείται είτε η γνώση προγραμματισμού είτε η κατοχή και γνώση χρήσης εργαλείων hacking (hacking tools), ενώ στις

---

[367] Βλ. «The Modus Operandi of Hacking», url: http://www.drtomoconnor.com/3100/3100lect04.htm.

[368] Αναφορικά με την ανάπτυξη επιβλαβών προγραμμάτων βλ. *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker*, Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series No 78, Australian Institute of Criminology, pp. 55 f. και *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker*, The future of technology-enabled crime in Australia, TRENDS & ISSUES in crime and criminal justice, Australian Institute of Criminology, No 341, July 2007, p. 3.

[369] Το επίθετο «γνήσια» σε αναλογία και αντιστοιχία με την κατηγοριοποίηση του Τσουραμάνη για τα ψηφιακά εγκλήματα (έτσι όπως τα «γνήσια» ψηφιακά εγκλήματα τελούνται αποκλειστικά και μόνο με την χρήση της ψηφιακής τεχνολογία, οι εν λόγω πρακτικές hacking λαμβάνουν χώρα μόνο με χρήση ηλεκτρονικών προγραμμάτων και όχι με παραδοσιακές μεθόδους ανεύρεσης κωδικών κ.λπ.). Βλ. *Χ. Τσουραμάνη*, Ψηφιακή εγκληματικότητα, όπ. π. σελ. 12.

[370] Με την έκφραση αυτή ο Κιούπης συνδέει το "phising" με το social engineering κάνοντας σαφές το κοινό χαρακτηριστικό τους και, άρα, «σφραγίζοντας» την συμπερίληψη και των δύο αυτών πρακτικών στις εξωπρογραμματιστικές πρακτικές hacking σύμφωνα με το παρόν πόνημα [βλ. *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 416, υποσ. 30].

εξωπρογραμματιστικές πρακτικές hacking συνήθως δεν απαιτούνται διόλου ειδικές γνώσεις, αλλά μπορεί να τις ασκήσει ακόμη και ο απλός χρήστης ηλεκτρονικών συσκευών πληροφορικής.

Σημειώνεται ότι οι hackers προκειμένου να φτάσουν στον στόχο τους δύνανται να χρησιμοποιήσουν και να συνδυάσουν διάφορες πρακτικές, οι οποίες μπορούν να καταταγούν και στις δύο αυτές ομαδοποιήσεις. Επιπρόσθετα, είναι προφανές ότι η κατωτέρω αναφορά πρακτικών και εργαλείων hacking δεν μπορεί παρά να είναι ενδεικτική καθώς οι τεχνικές του hacking καθημερινώς εξελίσσονται παράλληλα με τα ηλεκτρονικά συστήματα και, κυρίως, εναπόκεινται στην φαντασία του hacker.

2.11.2.1 Εξωπρογραμματιστικές πρακτικές hacking

2.11.2.1.1 Συλλογή πληροφοριών για το σύστημα (information gathering)

Το αγαπημένο ρητό των hackers «*Η γνώση αποτελεί δύναμη*» (*"scientia potential est"* - αποδίδεται στον άγγλο φιλόσοφο και πολιτικό του 17ου αιώνα *Francis Bacon*)[371] εκφράζει με τον καλύτερο τρόπο τις αντιλήψεις τους (όπως και ανωτέρω επισημάνθηκε σχετικά με την περιέργειά τους και την αγάπη τους για γνώση[372]) και, συνεπώς, την χρήση της γνώσης ως δύναμη. Η «αγάπη» αυτή για τη γνώση καταδεικνύεται και από πρακτικές που χρησιμοποιούν οι hackers προκειμένου να έλθουν σε επαφή με τη γνώση ή με στοιχεία απαραίτητα για να αποκτήσουν περισσότερες γνώσεις διά της δράσης τους. Τέτοιες πρακτικές είναι ενδεικτικά η λεγόμενη «κοινωνική μηχανική» ("social engineering")[373] – η απόσπαση πληροφοριών στο πλαίσιο κοινωνικής επαφής με αποσπασματικές ερωτήσεις και παρελκυστικές ενέργειες (π.χ. φιλίες σε δίκτυα κοινωνικής δικτύωσης όπου ο hacker κερδίζει την εμπιστοσύνη του θύματος και αποσπά απ' αυτόν πληροφορίες - λ.χ.

[371] Βλ. url: http://en.wikipedia.org/wiki/Scientia_potentia_est. Επισημαίνεται ότι η ακριβής φράση "scientia potential est" βρίσκεται για πρώτη φορά σε γραπτό κείμενο στο έργο «Λεβιάθαν» του Thomas Hobbes, ο οποίος νεότερος είχε υπάρξει γραμματέας του Francis Bacon.

[372] Βλ. ανωτέρω παράγραφοι 2.5, 2.6 και 2.7 του παρόντος πονήματος.

[373] Ακόμη και σεμινάρια «κοινωνικής μηχανικής» προσφέρονται στο διαδίκτυο! Ειδικότερα για τον ορισμό και της λεπτομέρειες της «κοινωνικής μηχανικής» βλ. url: http://www.social-engineer.org/.

ημερομηνία γέννησης – οι οποίες μπορεί να τον οδηγήσουν στο να ανακαλύψει κάποιον κωδικό) – καθώς και η αναζήτηση στα (ηλεκτρονικά) «σκουπίδια» του «στόχου» ("dumpster diving")[374] σε περιπτώσεις κατά τις οποίες ο hacker ενδεχομένως αναζητεί ακόμη και διαγεγραμμένα αρχεία ή ηλεκτρονικά στοιχεία προκειμένου να φτάσει στον στόχο του.

Κατωτέρω ακολουθεί παρουσίαση και ανάλυση πρακτικών συλλογής πληροφοριών για τα συστήματα πληροφοριών, οι οποίες χρησιμοποιούνται από τους hackers. Η συλλογή των αναγκαίων πληροφοριών για το σύστημα[375] αποτελεί ίσως το βασικότερο σκαλοπάτι στην κλίμακα ενός επιτυχημένου hacking. Κι αυτό διότι, όσα περισσότερα γνωρίζει ένας hacker για ένα σύστημα, τόσο περισσότερο αυξάνονται οι πιθανότητές του να εισβάλλει σε αυτό χωρίς να γίνει αντιληπτός. Έτσι, η γνώση του hacker αναφορικά τόσο με το ανθρώπινο δυναμικό (διαχειριστές, μηχανικούς, χειριστές, χρήστες) του συστήματος όσο και με το ίδιο το σύστημα (hardware, λειτουργικό, ενδεχόμενες ιδιομορφίες του κ.λπ.) αποδεικνύεται σημαντική. Τις ως άνω πληροφορίες ο hacker μπορεί να τις αποκτήσει από το ίδιο το σύστημα, από την επιχείρηση στην οποία αυτό ανήκει, από ειδικούς τεχνικούς επιστήμονες των ηλεκτρονικών υπολογιστών και από άλλους συναδέλφους του hackers[376]. Ακόμη και το ίδιο το διαδίκτυο μπορεί να προσφέρει πολύτιμες πληροφορίες για τις πρακτικές ασφάλειας που ακολουθούνται σε συστήματα πληροφοριών – «στόχους» από τους διαχειριστές τους[377].

[374] Για το dumpster diving πρβλ. url: http://theeconomiccollapseblog.com/archives/dumpster-diving.

[375] Οι *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., αναφέρονται αναλυτικά σε πρακτικές απου ακολουθούν οι hackers για την απόκτηση χωρίς δικαίωμα πρόσβασης.

[376] Βλ. «Τρόποι και κόλπα των hackers!», url: http://projecthackers-hacking.blogspot.gr/2012/10/blog-post_11.html

[377] Οι hackers μπορούν να ψάχνουν και να αλιεύουν πληροφορίες στο διαδίκτυο, στην ιστοσελίδα εταιρειών των οποίων τα συστήματα αποτελούν στόχους, σε ειδήσεις, σε δελτία τύπου κ.λπ. (βλ. *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 2).

2.11.2.1.1.1 «Κοινωνική μηχανική» ("Social engineering[378]")[379]

Ο Jordan υποστηρίζει ότι η κοινωνική μηχανική είναι παραβίαση υπολογιστών χωρίς υπολογιστές![380] (δικαιολογώντας, πιστεύω, με αυτόν τον τρόπο τη συμπερίληψη της κοινωνικής μηχανικής στις εξωπρογραματιστικές πρακτικές hacking). Έχει επανειλημμένα αποδειχθεί ότι είναι πιο εύκολο να αποκτήσει κανείς μία πληροφορία εκμεταλλευόμενος τις γνώσεις ή «γνωριμίες» που ήδη έχει, παρά προσπαθώντας να την «κλέψει». Γιατί λοιπόν ένας hacker να προσπαθήσει να «κλέψει» μία πληροφορία που τον ενδιαφέρει για το σύστημα και να μην την αποκτήσει δημιουργώντας απλά το κατάλληλο («φιλικό») περιβάλλον με το πρόσωπο εκείνο που πιθανότατα την κατέχει; Ο εντοπισμός του κατάλληλου προσώπου από τον hacker και η στο πλαίσιο μιας κοινωνικής επαφής απόκτηση της εμπιστοσύνης του είναι γνωστά στη γλώσσα των hacker ως *κοινωνική μηχανική (social engineering)*[381].

Ο Κέβιν Μίτνικ προσδιορίζει την έννοια της «κοινωνικής μηχανικής» ως «*την τέχνη της απόσπασης, με ποικίλες μεθόδους, καίριων πληροφοριών από ανθρώπους και της άνομης χρησιμοποίησής τους*».[382] [383]. Έτσι, ακόμη και μέσω παιχνιδιών, τα οποία ζητούν τους κωδικούς από το νόμιμο χρήστη, ο hacker που «παίζει» π.χ. με τον υπάλληλο της επιχείρησης μπορεί να πάρει μία ιδέα και για τους κωδικούς που ενδεχομένως χρησιμοποιούνται στην εργασία του τελευταίου. Επίσης, γνώση

---

[378] ... ή human engineering ή gagging (Βλ. σχετική ανάλυση και παράδειγμα στο πόνημα του Steven Furnell, όπ. π., σελ. 174 επ.) καθώς και *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 133.

[379] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 18.

[380] *Tim Jordan*, Hacking and power: Social and technological determinism in the digital age, Journal "first Monday", vol. 14, n. 7, 6/7/2009, url: http://firstmonday.org/ojs/index.php/fm/article/view/2417/2240.

[381] Για τον ορισμό του "social engineering" βλ. *Thomas Holt & Bernadette Schell*, Hackers and hacking: a reference handbook, Contemporary World Issues – Science, Technology and Medicine, 2013, url: http://books.google.gr/books?id=FZVfAQAAQBAJ&pg=PA149&lpg=PA149&dq=bossler+and+burruss&source=bl&ots=lL57-n6LHz&sig=0nOIvybIGJTRRSWsOEJWMxfHe3A&hl=el&sa=X&ei=OvsAU6TZI-O7ygO_noLgCQ&ved=0CEwQ6AEwAw#v=onepage&q=subculture&f=false, σελ. 25.

[382] Αναφορικά με εργαλεία «κοινωνικής μηχανικής» βλ. url: http://hellinikogenos.blogspot.gr/2013/11/blog-post_10.html.

[383] Βλ. *Κέβιν Μίτνικ και Ουίλιαμ Σίμονς*, Η τέχνη της απάτης, σε μετάφραση Λ. Καρατζά, εκδ. Ωκεανίδα, 2003.

τεχνικών χαρακτηριστικών του συστήματος οι hackers μπορούν να αποκτήσουν και μετά από υποβολή ψευδών και παραπειστικών ερωτήσεων[384].

2.11.2.1.1.2 «Κατάδυση στα σκουπίδια» ("Dumpster diving")[385]

Είναι σύνηθες φαινόμενο πολλές πληροφορίες να «πετιούνται στα σκουπίδια» με τη μορφή άχρηστων σημειωμάτων, που περιέχουν μισοσβησμένους κωδικούς, ή αντιγράφων αναφορών για διάφορα εμπιστευτικά ζητήματα που έχουν τυπωθεί σε εκτυπωτή κ.λπ. Οι πληροφορίες που περιλαμβάνονται σε όλα τα παραπάνω είναι πολύ πιθανό να αναφέρονται σε χαρακτηριστικά του συστήματος, σε κωδικούς καθώς και σε κάθε είδους ζητήματα λειτουργίας των διαφόρων μηχανημάτων ενώ η αξία τους για τους hackers μπορεί να θεωρηθεί ανυπολόγιστη, όπως μπορεί να είναι και η ζημία που ίσως προκληθεί στις ηλεκτρονικές πληροφορίες οι οποίες ουσιαστικά κατέστησαν προσβάσιμες εξαιτίας της ανεύρεσης αυτών των πληροφοριών[386]. Άρα, ο hacker μπορεί να βρει σημαντικές πληροφορίες για κάθε στόχο ψάχνοντας επισταμένως τα «σκουπίδια» του στόχου (dumpster diving). Πολύτιμα για τους hackers μπορούν να φανούν ακόμη και τα «ηλεκτρονικά σκουπίδια» (π.χ. διαγεγραμμένα αρχεία τα οποία μπορούν, όμως, να ανακτηθούν (restore) από κάποιον «ηλεκτρονικό κάδο ανακύκλωσης» κ.λπ.). Επίσης, οι hackers μπορούν να συγκεντρώσουν εκτενείς πληροφορίες για το σύστημα και τα «αδύνατα σημεία» του μέσα από δημόσιες πηγές και τράπεζες πληροφοριών, οι οποίες ίσως αρχικώς φαντάζουν άχρηστες.

2.11.2.1.1.3 «Ιχνηλάτηση» ("Footprinting")

Ο όρος footprinting χρησιμοποιείται στη μελέτη του DNA. Σε επίπεδο συστημάτων ηλεκτρονικών πληροφοριών, ως footprinting καλείται η διαδικασία συγκέντρωσης

[384] Βλ. *Νικόλαος Δ. Φαραντούρης*, όπ. π., σελ. 192, υπ' αρ. 10 παραπομπή σε Clauss F./ Krone K., «Computerrecht I», FU- Berlin, 2001, σελ. 21.

[385] Βλ. *Steven Furnell*, όπ. π., σελ. 177 επ.

[386] Βλ. *Χρήστος Ε. Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, όπ. π., σελ. 121.

και σώρευσης δεδομένων που αφορούν ένα συγκεκριμένο περιβάλλον δικτύου (μιας εταιρίας), συνήθως με σκοπό την εξεύρεση τρόπων για εισχώρηση και επίθεση στο περιβάλλον και, ουσιαστικά, είναι το πρώτο βήμα για την αξιολόγηση της ασφάλειας ενός συστήματος πριν την επίθεση. Ο σκοπός αυτής της δραστηριότητας είναι να αποκτηθεί μια πλήρης εικόνα της τεχνολογίας και των πρακτικών ασφαλείας που χρησιμοποιεί ο στόχος[387]. Με την τεχνική του "footprinting" είναι δυνατό να αποκαλυφθούν τα τρωτά σημεία του συστήματος και να εξελιχθεί ο τρόπος και η δυνατότητα εκμετάλλευσής τους.

Το "footprinting" ξεκινά με τον καθορισμό της θέσης και του στόχου για μια επερχόμενη εισβολή και έπειτα συγκεντρώνονται συγκεκριμένες πληροφορίες για το σύστημα με τη χρήση μη παρεμβατικών μεθόδων[388]. Για παράδειγμα, η ιστοσελίδα μιας εταιρίας μπορεί να παρέχει χρήσιμες πληροφορίες όπως ονόματα, διευθύνσεις e-mail, βιογραφικά σημειώματα κ.λπ. Ακόμη και οι μηχανές αναζήτησης παρέχουν πληροφορίες στους επίδοξους hackers ειδικά αν πρόκειται για εταιρία που λειτουργεί στο διαδίκτυο[389]. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν από τους hackers σε συνδυασμό και με άλλες τεχνικές (π.χ. social engineering) προκειμένου να αποκτηθεί πρόσβαση ή/και να παραβιαστεί το σύστημα.

2.11.2.1.1.4 Shoulder surfing («κρυφοκοίταγμα»)

Το shoulder surfing («κρυφοκοίταγμα» - «κοίταγμα πάνω από τον ώμο») αποτελεί, ίσως, την πλέον παραδοσιακή μέθοδο «κλοπής» κωδικών, η οποία χρησιμοποιεί τεχνικές άμεσης παρατήρησης για να αποσπάσει πληροφορίες. Η μέθοδος αυτή δεν στηρίζεται σε τεχνικές γνώσεις ή μέσα αλλά σε «κόλπα» που μπορούν να αποκαλύψουν διάφορους κωδικούς πρόσβασης.[390] Π.χ. αν κάποιος δει, χωρίς το θύμα να το αντιληφθεί, το username και το password, τότε μπορεί να αποκτήσει χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικούς λογαριασμούς του θύματος. Είναι αποτελεσματική κυρίως σε πολυσύχναστα μέρη (βιβλιοθήκες, internet cafés, ATM

[387] Αναλυτικά για το footprinting και τα βήματα τα οποία ακολουθούνται βλ. *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 3-4.

[388] Για το footprinting βλ. url: http://searchsecurity.techtarget.com/definition/footprinting.

[389] Βλ. σχετικώς url: http://techtips.gr/how-to-tricks-tips/2015/i-texniki-tou-footprinting.

[390] Βλ. για το shoulder surfing στο url: http://searchsecurity.techtarget.com/definition/shoulder-surfing.

τράπεζας[391]) και συνήθως χρησιμοποιείται για να αποσπασθούν κωδικοί ασφαλείας (PIN) και άλλα παρόμοια δεδομένα.

2.11.2.1.2 Phishing

"Phishing" ονομάζεται η πρακτική των hackers κατά την οποία ο hacker εμφανίζεται ως ένα φαινομενικά έμπιστο πρόσωπο (με e-mail ή κάποιο άλλο στιγμιαίο μήνυμα) και προσπαθεί να παραπλανήσει το θύμα προκειμένου να αποσπάσει τα στοιχεία ηλεκτρονικής ταυτότητας του θύματος (όνομα χρήστη, κωδικό πρόσβασης και άλλα στοιχεία ταυτότητας)[392]. Η έκφραση "phishing" φέρεται να προέρχεται από την συνήθεια των hackers να χαρακτηρίζουν τους ηλεκτρονικούς τόπους στους οποίους έχουν πρόσβαση "phish"[393] [394].

Ειδικότερα, "phishing" λέγεται η αποστολή ηλεκτρονικών μηνυμάτων (e-mails) που σκοπό έχουν να προκαλέσουν την κλοπή εμπιστευτικών στοιχείων που ανήκουν στον παραλήπτη του ηλεκτρονικού μηνύματος[395]. Τα ηλεκτρονικά αυτά μηνύματα δίνουν αρκετές φορές την εντύπωση πως προέρχονται από κάποια τράπεζα είτε από ιστοσελίδα που έχει κερδίσει την εμπιστοσύνη των χρηστών του διαδικτύου και ζητούν από τον παραλήπτη την αποκάλυψη δεδομένων, όπως τον αριθμό τραπεζικού

---

[391] Για το shoulder surfing σε περίπτωση ΑΤΜ τράπεζας αλλά και για άλλες αντίστοιχες μεθόδους περιέλευσης σε γνώση κωδικών αριθμών σε ό,τι έχει να κάνει με εγκλήματα σχετιζόμενα με ΑΤΜ πρβλ. *Θ. Σάμιο*, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο – Η de lege lata αξιολόγηση της αθέμιτης κτήσης και χρήσης καρτών αυτόματης συναλλαγής για ανάληψη μετρητών από ΑΤΜ, Ποινικές Μελέτες, Τομέας Ποινικών και Εγκληματολογικών Επιστημών ΔΠΘ, εκδ. Π. Ν. Σάκκουλα, 2010, ιδίως σελ. 67.

[392] Αναφορικά με το "phising" και για παραδείγματα με εικόνες screenshot από οθόνη ηλεκτρονικού υπολογιστή βλ. *Chuck Easttom and Det. Jeff Taylor*, Computer Crime, Investigation and the Law, Course Technology PTR, A part of Cengage Learning, 2011, pp. 7 f.

[393] Αναλυτικά για τα φαινόμενα phising και pharming βλ. *"Phising and pharming: A guide to understanding and managing the risks"*, CPNI (Centre for the Protection of National Infrastructure), July 2010, url: http://www.cpni.gov.uk/Documents/Publications/2010/2010019-Phishing_pharming_guide.pdf.

[394] Σε κάθε περίπτωση στη γλώσσα των hackers, όπως αναφέρεται και σε έτερο σημείο της παρούσας, οι hackers αντικαθιστούν το γράμμα f με τον δίφθογγο ph – άρα, το "phising"είναι ίσως "fishing", δηλαδή «ψάρεμα» των στοιχείων που επιδιώκουν οι hackers (*Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 416).

[395] Βλ. και *Michael Kunz & Patrick Wilson*, Computer Crime and Computer Fraud, Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004, url: http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf, p. 14.

λογαριασμού του, τον προσωπικό αριθμό αναγνώρισης (PIN) κ.ά.[396]. Άλλοι τρόποι «ψαρέματος» των στοιχείων των χρηστών εκ μέρους των hackers είναι πρακτικές οι οποίες καλούνται «νιγηριανά e-mails»[397] [(με κεντρικό τους πυρήνα το αίτημα τάχα για παροχή βοήθειας σε κάποιον με υπόσχεση οικονομικού οφέλους ή έχοντας παραβιάσει λογαριασμό κάποιου φίλου του υποψήφιου θύματος και ζητώντας δήθεν

[396] Βλ. ενδεικτικά για μια γνωστή περίπτωση phising το ρεπορτάζ του *Γ. Ανδριτσόπουλου* «Σκάνδαλο στο twitter - Χάκερ έκλεψαν τα δεδομένα χιλιάδων χρηστών», εφημερίδα «ΤΑ ΝΕΑ», Δευτέρα 4 Φεβρουαρίου 2013, σελ. 18 όπου, μετά από μια επίθεση από hackers στο δίκτυο κοινωνικής δικτύωσης twitter κατά την οποία φέρεται να έχει αποκτηθεί πρόσβαση σε δεδομένα 250.000 λογαριασμών, όταν το twitter γνωστοποίησε ότι θα ειδοποιήσει μέσω ηλεκτρονικού ταχυδρομείου τους χρήστες που είχαν πληγεί, επιτήδειοι άρχισαν να στέλνουν e-mail προερχόμενα δήθεν από το twitter ζητώντας τους να τους αποστείλουν τον κωδικό πρόσβασης που χρησιμοποιούν.

[397] Η πρακτική αυτή εκδηλώνεται αρκετές φορές ως εξής: άτομα (στην αρχή της πρακτικής αυτής τάχα από τη Νιγηρία αλλά έπειτα πλέον δηλώνοντας διάφορες χώρες δήθεν προέλευσης) αποστέλλουν ηλεκτρονική επιστολή (e-mail) και αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους (τα οποία δύνανται να προέρχονται και από εγκληματικές πράξεις), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Για τον σκοπό αυτό, κάνουν χρήση και επικαλούνται τίτλους επίσημων φορέων της χώρας τους (Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κ.λπ.) και χρησιμοποιούν τα ονόματα ακόμη και κυβερνητικών ή στρατιωτικών παραγόντων (πολλές φορές μάλιστα ανύπαρκτων στην πραγματικότητα προσώπων) ή προφασίζονται τάχα σχέση τους με «διάσημα» ή «σημαντικά» πρόσωπα. Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν προσωπικά τους στοιχεία, τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κ.λπ. προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών...» (έτσι στην ιστοσελίδα της ΕΛ.ΑΣ. – url: http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_content&perform=view – βλ. και *Russell G. Smith*, Travelling in Cyberspace on a False Passport: Controlling Transnational Identity related crime, The British Criminology Conference: Selected Proceedings. Volume 5, Papers from the British Society of Criminology Conference, Keele, July 2002, published August 2003. Editor: Roger Tarling. ISSN 1464-4088).

Άλλος τρόπος εκδήλωσης αυτής της συμπεριφοράς είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), τα οποία περιέχουν διάφορες παραπλανητικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ειδικότερα, το υποψήφιο θύμα λαμβάνει ένα ηλεκτρονικό μήνυμα (e-mail), με το οποίο ο δράστης υπόσχεται μεγάλη χρηματική αμοιβή αν το θύμα τον βοηθήσει να μεταφέρει χρήματα από τον λογαριασμό του δράστη στο λογαριασμό του θύματος. Συνήθως οι λόγοι που επικαλείται ο δράστης για τη μεταφορά αυτή αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή πλούσιες οικογένειες που πρέπει δήθεν να εγκαταλείψουν τη χώρα τους εξαιτίας πολιτικών συγκρούσεων. Πριν το θύμα εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο δράστης της νιγηριανής απάτης πρέπει να καταβάλει κάποιο ποσό για τα έξοδα μεταφοράς ή να δώσει τα στοιχεία του τραπεζικού του λογαριασμού, με συνέπεια να είναι πολύ πιθανό να του αποσπάσει ο δράστης το σύνολο των κατατεθειμένων χρημάτων στο λογαριασμό αυτό. Μετά την αποστολή αυτή των χρημάτων διακόπτεται η επικοινωνία δράστη – θύματος (βλ. Χ. Τσουραμάνης, Ψηφιακή Εγκληματικότητα, όπ. π. σελ. 22-23 καθώς και urls: www.potifos.com/fraud, www.e-telescope.gr/gr/cat03/art03_010622.htm).

Τέλος, η πιο δημοφιλής πρακτική απόσπασης χρημάτων ή αναφορικά με χωρίς δικαίωμα πρόσβαση στιχείων πρόσβασης είναι η εξής: ο hacker έχει ήδη παραβιάσει τον λογαριασμό e-mail ή άλλου ηλεκτρονικού μέσου επικοινωνίας κάποιου χρήστη και μέσω αυτού στέλνει ψεύτικο μήνυμα σε όλες τις επαφές του εν λόγω χρήστη, λέγοντας ότι βρίσκεται σε κάποια απομακρυσμένη χώρα (π.χ. Νιγηρία), ότι π.χ. του έχουν κλέψει τα χρήματα και ότι έχει άμεση ανάγκη από χρήματα ζητώντας, επομένως, είτε χρήματα είτε κωδικούς πιστωτικών καρτών για να κάνει χρήση ως δήθεν φίλος τους (ιδού το "phising" – «ψάρεμα στοιχείων»).

Τα νιγηριανά e-mails ονομάζονται και «419» διότι πολλές φορές οι συμπεριφορές αυτές τιμωρούνται με βάση το άρθρο 419 του Νιγηριανού Ποινικού Κώδικα περί απάτης (βλ. το εν λόγω άρθρο του Πονικού Κώδικα της Νιγηρίας στο url: http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm).

βοήθεια, είτε χρηματική, είτε με την παροχή προσωπικών κωδικών (π.χ. κωδικοί πιστωτικής κάρτας)] ή «ισπανικό λόττο»[398], ως διαδικασία δηλαδή για την αλίευση στοιχείων που θα χρησιμοποιηθούν για τη χωρίς δικαίωμα πρόσβαση σε δεδομένα ή, έτι περαιτέρω, για αποδέσμευση ποσού το οποίο φέρεται τάχα να ανήκει στο θύμα. [399]

Το "phising" στην παρούσα εργασία έχει καταταχθεί στις *εξωπρογραμματιστικές πρακτικές hacking* καθώς, όπως είδαμε, συνίσταται στην εξαπάτηση κάποιου για να αποκαλυφθούν οι κωδικοί του χωρίς κάποια τεχνική επενέργεια με τη χρήση προγράμματος ή τεχνικού εργαλείου[400].

2.11.2.2 Γνήσιες πρακτικές hacking (χρήση ηλεκτρονικών προγραμμάτων και εντολών)

Σχεδόν όλοι οι hackers γνωρίζουν ότι ένας από τους βασικούς λόγους της επιτυχίας τους είναι η αδυναμία των διαφόρων συστημάτων να εμποδίσουν την εισβολή τους σε αυτά. Ένα σύστημα λειτουργεί σωστά από τη στιγμή που ο μηχανισμός αναγνώρισης της ταυτότητας των νόμιμων χρηστών του είναι αξιόπιστος. Για τον

---

[398] Μορφή απάτης ή phising μέσω του διαδικτύου είναι και το «ισπανικό ΛΟΤΤΟ». Η απαρχή αυτής της πρακτικής φέρεται να αναφέρεται σε αφρικανούς κατοίκους Ισπανίας οι οποίοι αποστέλλουν στα υποψήφια θύματά τους e-mails στα οποία αναφέρεται ότι τα τελευταία δήθεν κέρδισαν στο ισπανικό ΛΟΤΤΟ ένα μεγάλο ποσό και ζητούν από το θύμα τους τα προσωπικά στοιχεία και τον αριθμό του τραπεζικού του λογαριασμού για να καταθέσουν το υποτιθέμενο ποσό ή/και την κατάθεση από το θύμα χρηματικού ποσού για την κάλυψη δήθεν διαδικαστικών εξόδων. Περαιτέρω, αρκετές φορές αποστέλλονται μηνύματα σε τυχαίους χρήστες του διαδικτύου τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας (μακρινός συγγενής του ή όχι) έχει αποβιώσει και ο παραλήπτης του μηνύματος έχει επιλεγεί να κληρονομήσει αυτός την περιουσία είτε ότι έχουν κερδίσει κάποιο μεγάλο ποσό σε διαδικτυακή κλήρωση – με αυτήν τη πρόφαση, λοιπόν, οι δράστες αιτούνται είτε την καταβολή ποσών τάχα για διαδικαστικά έξοδα είτε την αποκάλυψη προσωπικών στοιχείων (αριθμός λογαριασμού, κωδικός κ.ά.) προκειμένου τάχα να κατατεθεί το κερδιθέν ποσό στον λογαριασμό αυτόν (βλ. σχετικά την ιστοσελίδα της ΕΛ.ΑΣ. url: http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_content&perform=view, το άρθρο του *Γ. Σουλιώτη*, www.Ηλεκτρονικές απάτες.gr, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 26 Νοεμβρίου 2004, url: http://www.kathimerini.gr/201674/article/epikairothta/ellada/wwwhlektronikes-apatesgr και το url: https://sites.google.com/site/elektronikoenklema2012/morphes-tou-elektronikou-enklematos/enklemata-me-ten-chrese-e-y-os-boethetiko-meso).

[399] Δεν πρέπει να παραγνωρίζεται το ότι πολλές φορές ο υπολογιστής και το διαδίκτυο δύναται να χρησιμοποιηθεί προκειμένου να τελεστεί απάτη χωρίς όμως να υπάρξει χωρίς δικαίωμα πρόσβασης σε δεδομένα [π.χ. περιπτώσεις επικοινωνίας μέσω υπολογιστή από την οποία δημιουργείται πλάνη σε πρόσωπο το οποίο προβαίνει σε περιουσιακή διάθεση – βλ. αναλυτικά *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 421].

[400] Αναφορικά με το phising βλ. και *David S. Wall*, Hunting, shooting and phising: new cybercrime challenges for cybercanadians in the 21st century, British Library, 2008.

λόγο αυτό η εξουδετέρωση του ως άνω μηχανισμού αποτελεί τον κύριο στόχο κάθε hacker.

Ανεξάρτητα από τον λόγο για τον οποίο ένας hacker εισβάλει σε ένα σύστημα, προκειμένου να επιτύχει τους στόχους του θα χρειαστεί να χρησιμοποιήσει σε πολλές περιπτώσεις κάποια προγράμματα (κακόβουλο λογισμικό – "malicious software"[401] ή, μετά από σύνδεση των δύο αυτών λέξεων, "malware"[402]), τα οποία, εγκαθιστάμενα σε αυτό, θα του προσφέρουν σημαντική βοήθεια[403]. Αυτά τα προγράμματα –πολλές φορές κατασκευασθέντα από τους ίδιους τους hackers[404] – εντάσσονται στην παρούσα εργασία στις *γνήσιες πρακτικές hacking*, καθώς γίνεται άμεση χρήση των δυνατοτήτων της τεχνολογίας για τη διείσδυση στο σύστημα.

Δυνάμει των ανωτέρω, είναι γεγονός ότι η εξέλιξη της τεχνολογίας απαιτεί συνεχή παρακολούθηση και ενημέρωση προκειμένου οποιοσδήποτε να προβεί στην αποτελεσματική χρήση της. Δεν είναι τυχαίο, επομένως, ότι σημαντική πηγή πληροφόρησης για τους hackers αποτελούν οι δημοσιεύσεις για θέματα ασφάλειας συστημάτων ηλεκτρονικών υπολογιστών, οι οποίες λαμβάνουν χώρα σε επιστημονικά περιοδικά, σε πρακτικά συνεδρίων, σε βιβλία, σε fora, σε newgroups και σε mailing lists από επιστήμονες πληροφορικής και γενικότερα από ειδικούς του χώρου αυτού. Γνωρίζοντας με τον τρόπο αυτό οι hackers τα μέτρα που λαμβάνονται για την αντιμετώπιση των παραβιάσεων, είναι σε θέση να λάβουν τα κατάλληλα αντί-μέτρα. Ειδικά όταν πρόκειται για εταιρείες – στόχους, οι hackers παρακολουθούν ακόμη και συνεργασίες των στόχων αυτών με εταιρείες λογισμικών προκειμένου να γνωρίζουν ακριβώς ποια είναι τα μέτρα ασφαλείας που λαμβάνει η συγκεκριμένη επιχείρηση και να προετοιμάσουν το έδαφος για την παράνομη διείσδυσή τους σε αυτά[405].

Τέλος, οι hackers διαθέτουν αρκετό από το χρόνο τους αναζητώντας να βρουν σε δικτυακούς τόπους πληροφορίες, τις οποίες έχουν θέσει στη διάθεσή τους άλλοι

---

[401] Βλ. το κεφάλαιο 5 με τίτλο «Παρουσίαση των κακόβουλων λογισμικών» εις *Steven Furnell*, όπ. π. σελ. 183 επ. καθώς και αναπτύξεις στην παράγραφο 2.11.2 του παρόντος πονήματος.

[402] Βλ. *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ.6-7.

[403] Βλ. *Χρήστος Ε. Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, όπ. π., σελ. 127.

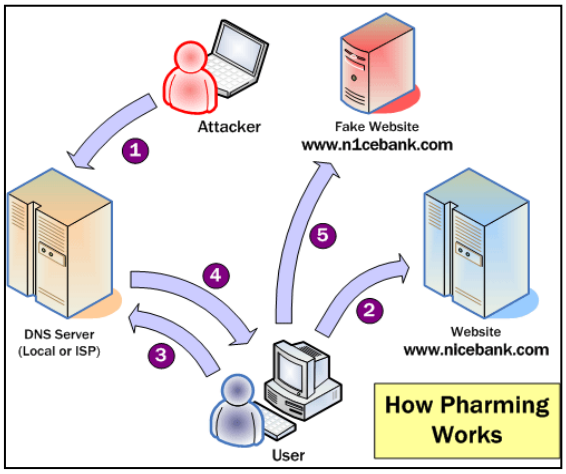
[404] ... τους elite hackers ή τους makecrafters (βλ. παραγράφους της παρούσας 2.3.3 και 2.3.4 αντίστοιχα).

[405] Είναι και εδώ πολύ χρήσιμες οι πρακτικές τύπου footprinting (βλ. ανωτέρω).

συνάδελφοί τους[406]. Είναι γεγονός ότι ιστοσελίδες (sites) και βίντεο με πληροφορίες και εργαλεία (tools) για hacking αφθονούν στον παγκόσμιο ιστό[407]. Ακόμη πολλοί hackers συνεργάζονται μεταξύ τους ανταλλάσσοντας πληροφορίες με ηλεκτρονικό ταχυδρομείο (e-mail) ή συνομιλώντας σε ειδικά chat rooms.

2.11.2.2.1 Pharming

"Pharming" είναι η εκμετάλλευση του τρωτού ηλεκτρονικού προγράμματος (software) ενός DNS (Domain Name System)[408] server που επιτρέπει σε κάποιον να ανακατευθύνει τους επισκέπτες μιας ιστοσελίδας (website) σε άλλη[409]. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή (ή την ψηφιακή συσκευή) του θύματος και τον επηρεάζει κατά τέτοιο τρόπο, ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφθεί, θεωρώντας πως βρίσκεται σε ασφαλή διαδικτυακό χώρο, ο συγκεκριμένος υπολογιστής τον "οδηγεί" σε κάποια «πλαστή» ιστοσελίδα. Δηλαδή, ο δράστης τροποποιεί το Domain Name Code με αποτέλεσμα οι χρήστες που



[406] Ακόμη και συνέδρια με θέμα το hacking λαμβάνουν χώρα – βλ. *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π. – η συγκεκριμένη έρευνα έλαβε χώρα σε ένα τέτοιο συνέδριο.

[407] Ενδεικτικά urls: http://www.breakthesecurity.com/p/hacking-tutorials-for-beginners.html, http://www.wikihow.com/Hack, http://www.youtube.com/watch?v=Z2xJaaNqItk, http://learnhacking.in/, κ.ά.

[408] Για τον ορισμό και τη λειτουργία του συστήματος ονομάτων χώρων [αγγλ. Domain Name System (DNS)] βλ. *Εμμ. Μεταξάκη*, Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου, ΠοινΧρ ΞΔ/ 2014, σελ. 8 επ. και ιδίως υποσ. 6.

[409] Με δεδομένη την αντικατάσταση του γράμματος f με τον δίφθογγο ph, το pharming μάλλον είναι τελικώς farming, η κατεύθυνση δηλαδή των χρηστών σε μια συγκεκριμένη και οριοθετημένη περιοχή (farm). Ο Κιούπης «μεταφράζει» το "pharming" ως «καλλιέργεια» (*Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 418).

αναζητούν μια ιστοσελίδα με αλλοιωμένη την αριθμητική της διεύθυνση (numerical address) να κατευθύνονται αυτόματα σε άλλη ιστοσελίδα[410].

Ειδικότερα, με τη μέθοδο *DNS Spoofing*[411] ο hacker τροποποιεί το Domain Name Code, το οποίο είναι η αριθμητική, δυαδικά ψηφιοποιημένη διεύθυνση της ιστοσελίδας, με συνέπεια όταν οι χρήστες αναζητούν την ιστοσελίδα αυτή που έχει αλλοιωθεί η αριθμητική της διεύθυνση (numerical address) να επισκέπτονται άλλη ιστοσελίδα αυτόματα. Αποτέλεσμα αυτού, πέρα από την απώλεια εσόδων για την ιστοσελίδα που δεν κατόρθωσε να επισκεφθεί ο χρήστης, τελικά, και μέσω της δημιουργίας ενός ακριβούς αντιγράφου κάποιας ιστοσελίδας (mirror site), είναι τα δεδομένα τα οποία πληκτρολογεί και καταχωρεί ο χρήστης στην ψεύτικη σελίδα (π.χ. username και password) να γίνονται γνωστά στον hacker[412] – άρα, τελικώς μπορεί να υποστηριχθεί ότι το "phising"[413] είναι η ολοκλήρωση του "pharming". Οι τεχνικές pharming αρκετές φορές δεν μένουν μόνο στην υποκλοπή της ταυτότητας αλλά, σε περιπτώσεις για παράδειγμα ιστοσελίδας τράπεζας, η προσπάθεια του θύματος να πραγματοποιήσει τις συναλλαγές του μέσω on-line banking μπορεί να καταλήξει στη μεταφορά των χρημάτων του απευθείας στους δράστες.[414]

2.11.2.2.2 Επιθέσεις άρνησης υπηρεσίας (DoS και DDoS attacks)

Σε επίπεδο πλήγματος στη διαθεσιμότητα των ηλεκτρονικών δεδομένων, με τη μέθοδο επίθεσης ***Denial of service (DoS attack)***[415] οι hackers εκτελούν πολλαπλά

---

[410] Srivasta Tushar Vishesh, *"Phishing and Pharming – The deadly duo"*, Sans Institute Reading Room site, January 2007, url. http://www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil-twins_1731.

[411] Αναφορικά με το dns spoofing βλ. ενδεικτικά url: http://www.menandmice.com/resources/dns-spoofing/.

[412] Βλ. «Τρόποι και κόλπα των hackers!», url: http://projecthackers-hacking.blogspot.gr/2012/10/blog-post_11.html.

[413] Βλ. ανωτέρω παράγραφο 2.11.2.1.2 της παρούσας.

[414] Chaudhari Nilesh, *"Pharming on the Net"*, March 2006, http://palizine.plynt.com/issues/2006Mar/pharming/.

[415] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 16 καθώς και *Michael Kunz & Patrick Wilson*, Computer Crime and Computer Fraud, Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004, url: http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf, p. 17, *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 139-141

προγράμματα με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών, τα οποία «βομβαρδίζουν» το δίκτυο με δεδομένα και έτσι το υπερφορτώνουν και το επιβαρύνουν, με αποτέλεσμα να αδυνατεί να ανταποκριθεί[416] [417]. Επομένως, κάνουν το σύστημα να «κρασάρει» (όπως λέγεται στη «αργκό» γλώσσα όσων ασχολούνται με την πληροφορική - να μη μπορεί, δηλαδή, να λειτουργήσει) καθιστώντας τα ηλεκτρονικά δεδομένα μη διαθέσιμα. Αντίστοιχη μέθοδος «κρασαρίσματος» είναι και η επίθεση με ***Distributed denial of service (DDoS attack)***[418]: οι hackers μέσω της χρήσης δούρειων ίππων ("Trojan horses" – βλ. κατωτέρω[419]) ελέγχουν πολλούς υπολογιστές χρηστών και σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο μετά από την υπερβολική αυτή ζήτηση καταρρέει[420] [421].

2.11.2.2.3 Joomla bugs

Οι hackers αποκτούν πρόσβαση σε μία ιστοσελίδα που έχει δημιουργηθεί και ανανεώνεται/ τροφοδοτείται από το σύστημα διαχείρισης περιεχομένου ("content manager system" – "cms") "Joomla". Μέσω του συστήματος ιστοσελίδας "joomla" υπάρχει η δυνατότητα να τοποθετηθούν κακόβουλα λογισμικά «bugs» και

και *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 7.

[416] Βλ. «Τρόποι και κόλπα των hackers!», url: http://projecthackers-hacking.blogspot.gr/2012/10/blog-post_11.html.

[417] Μια από τις πιο κοινές τεχνικές άρνησης εξυπηρέτησης (Denial of Service) είναι η resource mismatch. Ορισμένες φορές απαιτούνται σημαντικά περισσότεροι πόροι (resources) για τη μια πλευρά μιας σύνδεσης όσον αφορά μια κίνηση δικτύου (network traffic) ή δικτύου CPU. Ένας hacker μπορεί να εκμεταλλευτεί το γεγονός αυτό προκειμένου να καταστρέψει αυτούς του πόρους του θύματος χωρίς να έχει αντίκτυπο στη δική του συσκευή (βλ. url: http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/resource_mismatch/default.htm).

[418] Το 2007 εκτιμήθηκε ότι περίπου 10.000 DDoS επιθέσεις λαμβάνουν χώρα κάθε μέρα σε όλο τον κόσμο *(Ian Brown, Lilian Edwards and Chris Marsden* Information security and cybercrime, University of Essex, p. 4).

[419] Βλ. και *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal Theory, Working Paper No. 249030, url: http://papers.ssrn.com/paper.taf?abstract_id=249030, p. 25.

[420] Βλ. «Τρόποι και κόλπα των hackers!», url: http://projecthackers-hacking.blogspot.gr/2012/10/blog-post_11.html.

[421] Χαρακτηριστικές είναι, βέβαια, ορισμένες απαντήσεις των hackers κατωτέρω (σε ερώτηση η οποία αφορά την κολεκτίβα "Anonymous") σύμφωνα με τις οποίες οι επιθέσεις αυτού του τύπου «δεν είναι hacking» (βλ. συγκεκριμένα στην παράγραφο 7.8.4.1 τις απαντήσεις στην ερώτηση 13).

μετατρέπουν την ιστοσελίδα σε phishing ή malware παγίδα για τους επισκέπτες της, χωρίς να απαιτείται οι ίδιοι οι επισκέπτες να έχουν δικό τους λογαριασμό "Joomla"[422].

2.11.2.2.4 Packet sniffers

Χρήσιμο εργαλείο για τους hackers αποτελούν και τα προγράμματα "*packet sniffer*" τα οποία επιτρέπουν στο χρήση να προσλαμβάνει και να ερμηνεύει «πακέτα» πληροφοριών που διακινούνται στο διαδίκτυο. Κάθε πληροφορία που κοινοποιείται σε ένα δίκτυο υπολογιστών, όπως για παράδειγμα το όνομα χρήστη, ο κωδικός εισόδου, το e-mail μεταφράζεται σε «πακέτα», τα οποία αποστέλλονται στο δίκτυο. Το internet λειτουργεί κυρίως μέσω του πρωτοκόλλου παράδοσης "ethernet" και ως εκ τούτου όταν κάποιος χρήστης αποστείλει ένα «πακέτο» πληροφοριών[423] στο "ethernet" κάθε μηχάνημα στο δίκτυο αντιλαμβάνεται το «πακέτο» αυτό. Κάθε «πακέτο» πληροφοριών που αποστέλλεται μέσω διαδικτύου έχει μία αριθμητική διεύθυνση, ώστε ο σωστός υπολογιστής να λαμβάνει τη σωστή πληροφορία. Το «Ethernet Packet Sniffer» είναι λογισμικό που επιτρέπει στο hacker ή το διαχειριστή του δικτύου να έχει πρόσβαση σε πληροφορίες, οι οποίες δεν προορίζονται για τη δική του διεύθυνση.

2.11.2.2.5 Οι «δούρειοι ίπποι» ("Trojan horses")[424]

Στα πλέον γνωστά εργαλεία των hackers για πρόσβαση σε ηλεκτρονικά δεδομένα συγκαταλέγονται οι δούρειοι ίπποι (*Trojan horses*)[425]. Πρόκειται για προγράμματα,

[422] Βλ. σχετικώς url: http://krebsonsecurity.com/2013/08/simple-hack-threatens-oudated-joomla-sites/.

[423] Για τον ορισμό του διαδικτυακού πακέτου βλ. την αναλυτική υποσημείωση υπ' αρ. 59 στο πόνημα του *Εμμ. Μεταξάκη*, Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου, ΠοινΧρ ΞΔ/ 2014, σελ. 13.

[424] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 16.

[425] Βλ. και *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal

τα οποία «μεταμφιέζει» ο hacker σε άλλα προγράμματα (σαν τον Δούρειο Ίππο της «Ιλιάδας» του Ομήρου), ώστε να οδηγήσει το χρήστη να εγκαταστήσει το συγκεκριμένο πρόγραμμα. Μόλις το πρόγραμμα αυτό («ίππος») εγκατασταθεί στον υπολογιστή του χρήστη – θύματος, ο hacker αποκτά πρόσβαση στις πληροφορίες του σκληρού δίσκου ή στο e-mail του χρήστη[426]. Επίσης, ο hacker μπορεί να αποκτήσει πρόσβαση και σε άλλα συστήματα ή και να πραγματοποιήσει DDoS επιθέσεις. Οι χρήστες παρέχουν «το όνομα χρήστη» και τον κωδικό πρόσβασης με την πεποίθηση ότι συνδέονται στο σύστημα, ενώ στην πραγματικότητα τα στοιχεία αυτά καταγράφονται από τον «ίππο» και τα χρησιμοποιεί ο hacker. Ο πιο γνωστός, ίσως, ίππος είναι ο "Black Orifice", ο οποίος δημιουργήθηκε από το hacker group με την ονομασία «Cult of the Dead Cow»[427] και μέσω αυτού ο hacker αποκτά πρόσβαση και ελέγχει κάθε προσωπικό υπολογιστή με λειτουργικό σύστημα windows 95/98 και επόμενα.

2.11.2.2.6 «Ιοί» (viruses) και «σκουλήκια» (worms)[428]

Οι «ιοί»[429] και τα «σκουλήκια» είναι προγράμματα[430] που αυτοαναπαράγονται και εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο.

Οι ιοί ("viruses")[431] των ηλεκτρονικών υπολογιστών είναι προγράμματα που έχουν σχεδιασθεί με σκοπό να «μολύνουν» άλλα προγράμματα με αντίγραφά τους, έχοντας

Theory, Working Paper No. 249030, url: http://papers.ssrn.com/paper.taf?abstract_id=249030, p. 25 και *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 6.

[426] Βλ. url: http://www.gohacking.com/make-trojan-horse/ - στην ιστοσελίδα αυτή δίνονται οδηγίες για την κατασκευή «δούρειου ίππου».

[427] Βλ. σχετικά url: http://www.cultdeadcow.com/tools/bo.html.

[428] Βλ. και *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal Theory, Working Paper No. 249030, url: http://papers.ssrn.com/paper.taf?abstract_id=249030, p. 22 f.

[429] Οι δημιουργοί ιών (virus writers) αποτελούν μια ξεχωριστή κατηγορία χωρίς ομοιογενή κουλτούρα και, ενώ μοιράζονται κοινές μεθοδολογίες με τους καλύτερους hackers, έχουν αναπτύξει διαφορετικές πορείες. Οι δημιουργοί των ιών χρησιμοποιούν τα κενά ασφαλείας τα οποία έχουν ανακαλύψει οι hackers και έπειτα προβαίνουν στη δημιουργία των αντίστοιχων ιών (βλ. *Cynthia Fitch*, M.Ed., Crime and Punishment: The Psychology of Hacking in the New Millennium, url: http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795, pp. 7).

[430] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 7.

ως αποστολή τους τη δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων και τη διαγραφή αρχείων ή του συνόλου του περιεχομένου ψηφιακών αποθηκευτικών χώρων (π.χ. σκληρών δίσκων). Συνήθως οι ιοί είναι συνδεδεμένοι με κάποιο πρόγραμμα και επηρεάζουν τον υπολογιστή μόλις αυτό το πρόγραμμα εκτελεστεί[432]. Έχουν τη δυνατότητα να αναπαράγονται συνεχώς και, επομένως, μπορούν να μεταδοθούν εύκολα από ένα σύστημα σε άλλο και αντιγράφονται από υπολογιστή σε υπολογιστή χωρίς να απαιτούν τη συμβολή κανενός άλλου προγράμματος ή αρχείου.

Τα "worms" – "σκουλήκια"[433] είναι προγράμματα ηλεκτρονικών υπολογιστών που χρησιμοποιούνται ως μηχανισμός μεταφοράς άλλων προγραμμάτων (συνήθως ιών) – η διαφορά με τους ιούς είναι ότι δεν χρειάζεται η εκτέλεση κάποιου προγράμματος για να εισέλθουν σε έναν υπολογιστή[434]. Το πιο γνωστό «σκουλήκι» με την ονομασία «ILOVEYOU»[435] υπολογίζεται ότι επηρέασε περίπου 45 εκατομμύρια υπολογιστές.

2.11.2.2.7 IP Spoofing[436]

Μία επιπλέον δημοφιλής μέθοδος πρόσβασης των hackers στο ξένο σύστημα στηρίζεται στην εκμετάλλευση της σχέσης εμπιστοσύνης μεταξύ των υπολογιστών, το οποίο σημαίνει ότι ένας υπολογιστής εκτελεί διαταγές που εισέρχονται στο σύστημα χωρίς να απαιτεί κωδικό, εφόσον οι εντολές αυτές προέρχονται μόνο από γνωστούς σε αυτόν υπολογιστές (IP spoofing)[437]. Η ψευδής αυτή ταύτιση επιτυγχάνεται με την κατάλληλη χρήση των αριθμών IP (Internet Protocol), οι οποίοι συνιστούν μία αριθμική διεύθυνση και προσδιορίζουν όλους τους ηλεκτρονικούς

---

[431] Βλ. ενδεικτικά url: http://www.webopedia.com/TERM/V/virus.html.

[432] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 16.

[433] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 16.

[434] Βλ. The Difference Between a Computer Virus, Worm and Trojan Horse, url: http://www.webopedia.com/DidYouKnow/Internet/virus.asp.

[435] Βλ. το σχετικό λήμμα της ηλεκτρονικής εγκυκλοπαίδειας "Wikipedia" στο url: http://en.wikipedia.org/wiki/ILOVEYOU.

[436] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 16.

[437] Για το IP Spoofing βλ. ενδεικτικώς *Farha Ali*, Lander University, IP Spoofing, url: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html και *Matthew Tanase*, IP Spoofing: An introduction, url: http://www.symantec.com/connect/articles/ip-spoofing-introduction.

υπολογιστές που χρησιμοποιούν το διαδίκτυο και συνδέονται on–line. Ο hacker, δηλαδή, χρησιμοποιεί ή «πλαστογραφεί» την αλληλουχία αριθμών που συνιστούν τη διεύθυνση διαδικτυακού πρωτοκόλλου (IP address)[438] την οποία αποδέχεται και στην οποία χορηγεί άδεια πρόσβασης το σύστημα ηλεκτρονικών πληροφοριών και με αυτόν τον τρόπο «αυθεντικοποιείται»[439] και αποκτά χωρίς δικαίωμα πρόσβαση.

2.11.2.2.8 SQL (Structured Query Language) injection

Το «SQL Injection» άρχισε να χρησιμοποιείται ως τεχνική το έτος 1998 και είναι, ίσως, μία από τις πλέον κοινώς εφαρμοσμένες τεχνικές επίθεσης που χρησιμοποιούνται σήμερα. Με το SQL injection ο hacker εκμεταλλεύεται την ακατάλληλη κωδικοποίηση σε γλώσσα προγραμματισμού ηλεκτρονικών υπολογιστών κάποιων εφαρμογών του διαδικτύου που χρησιμοποιεί το θύμα[440] και έτσι αποκτά πρόσβαση στα δεδομένα του θύματος[441].

Ειδικότερα και ως παράδειγμα, όταν ο χρήστης υποβάλλει τα στοιχεία του για είσοδο σε σύστημα ηλεκτρονικών δεδομένων, η διαδικτυακή εφαρμογή που ελέγχει τη σελίδα σύνδεσης επικοινωνεί με βάση δεδομένων[442] μέσω μιας σειράς προγραμματισμένων εντολών έτσι ώστε να επαληθεύσει το όνομα χρήστη και τον κωδικό πρόσβασης. Αν είναι έγκυρα τα στοιχεία, ο χρήστης έχει τη δυνατότητα πρόσβασης. Μέσω της SQL Injection, ο hacker δημιουργεί εντολές SQL παρακάμπτοντας τη διαδικασία επαλήθευσης του χρήστη (login). Αυτό είναι δυνατό στην περίπτωση που η διαδικασία αυτή επαλήθευσης έχει τρωτά σημεία και κενά ασφαλείας.

---

[438] Αναφορικά με τη διεύθυνση IP βλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 206 επ.

[439] Βλ. ορισμό της «αυθεντικοποίησης» στον Κανονισμό 460/2004 της ΕΕ (παράγραφος 6.3.6 του παρόντος πονήματος).

[440] Βλ. το λήμμα "SQL injection" στη ηλεκτρονική εγκυκλοπαίδεια Wikipedia (url: http://en.wikipedia.org/wiki/SQL_injection) όπου και σχετικά παραδείγματα.

[441] Βλ. και url: http://www.acunetix.com/websitesecurity/sql-injection/

[442] Για την νομική προστασία των βάσεων δεδομένων πρβλ. *Μαρία Κανελλοπούλου – Μπότη,* Νομική προστασία βάσεων δεδομένων, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004.

Το SQL Injection είναι περισσότερο γνωστό για επίθεση σε ιστοσελίδες, αλλά μπορεί να χρησιμοποιηθεί από τους hackers για να επιτεθούν σε οποιοδήποτε τύπο βάσης δεδομένων SQL, εκμεταλλευόμενοι τα κενά ασφαλείας της.

2.11.2.2.9 Hacking shells

Τα hacking shells είναι τμήμα κώδικα (γλώσσας προγραμματισμού π.χ. PHP, Python, Ruby), το οποίο εισάγουν οι hackers σε μία ιστοσελίδα και με αυτόν τον τρόπο αποκτούν πρόσβαση στα αρχεία που είναι αποθηκευμένα εκεί, με δυνατότητα να επεξεργαστούν, να διαγράψουν ή να αποθηκεύσουν τα αρχεία της ιστοσελίδας ή να ανεβάσουν δικά τους αρχεία στο συγκεκριμένο ιστότοπο[443]. Τα hacking shells βοηθούν τον εισβολέα – hacker να διατηρεί την πρόσβαση στα αρχεία κάποιας ιστοσελίδας για μεγάλο χρονικό διάστημα. Υπάρχουν πολλοί τύποι hacking shells, όπως τα DDOS shells, τα symlink shells κ.λπ. Με τα hacking shells ο εισβολέας - hacker μπορεί να καταστρέψει ολόκληρη τη βάση ηλεκτρονικών δεδομένων της ιστοσελίδας.

2.11.2.2.10 Exploits

Το «exploit» (από το αγγλικό ρήμα «εκμεταλλεύομαι» ή περιφραστικά «χρησιμοποιώ κάτι προς όφελός μου») είναι ένα τμήμα λογισμικού, ένα μέρος δεδομένων ή μια αλληλουχία εντολών που εκμεταλλεύεται μια βλάβη ή αδυναμία του ηλεκτρονικού συστήματος προκειμένου να προκαλέσει ακούσια ή μη αναμενόμενη συμπεριφορά σε σύστημα ηλεκτρονικών υπολογιστών. Μια τέτοια συμπεριφορά οδηγεί συχνά στην απόκτηση του ελέγχου ενός συστήματος πληροφοριών και στην παραχώρηση προνομίων στο σύστημα αυτό ή σε μια επίθεση DoS[444].

---

[443] Βλ. ενδεικτικά urls: http://en.wikipedia.org/wiki/Backdoor_Shell, http://www.hackforsecurity.net/2012/10/what-is-shell-and-how-to-use-it.html και http://www.go4expert.com/articles/shells-impressive-web-hacking-method-t19226/.

[444] Βλ. Wikipedia – The Free encyclopedia, url. http://en.wikipedia.org/wiki/Exploit_(computer_security).

Τα «exploits» συνήθως κατηγοριοποιούνται με κριτήρια το είδος της ευπάθειας του συστήματος που εκμεταλλεύονται, το αν λειτουργούν στην ίδια συσκευή - μηχάνημα με το πρόγραμμα στο οποίο εντοπίζεται το τρωτό σημείο (local exploit) ή αν μπορούν να επιτεθούν σε πρόγραμμα που εκτελείται σε ένα άλλο μηχάνημα (remote exploit) και το αποτέλεσμα που επέρχεται από την εκτέλεση ("run") του "exploit" (EoP, DoS, spoofing κ.λπ.).

2.11.2.2.11 «Κλείδωμα πλήκτρων» ("Key logger")

Το "key logger" είναι είδος κακόβουλου προγράμματος - λογισμικού παρακολούθησης (θεωρείται ότι είναι λογισμικό ή spyware) που εκτελείται χωρίς να αφήνει ίχνη, καταγράφει όλες τις πληροφορίες που πληκτρολογεί ο χρήστης του υπολογιστή στο πληκτρολόγιό του και, στη συνεχεία, αποστέλλει πληροφορίες στον hacker που έχει επιτεθεί με το λογισμικό αυτό. Πιο συγκεκριμένα, τα keyloggers καταγράφουν πληροφορίες όπως κωδικοί πρόσβασης σε διάφορες ιστοσελίδες, ποιες ιστοσελίδες έχει επισκεφθεί το θύμα κ.λπ., μέσω της ανίχνευσης των πλήκτρων που χρησιμοποιεί το θύμα στο πληκτρολόγιό του και την καταγραφή κάθε χρήσης πλήκτρου από το θύμα σε ένα αρχείο καταγραφής, συνήθως κρυπτογραφημένο[445]. Μπορεί, συνεπώς, να καταγράψει τα άμεσα μηνύματα, τα e-mail, καθώς και κάθε πληροφορία που πληκτρολογεί το θύμα οποιαδήποτε στιγμή χρησιμοποιώντας το πληκτρολόγιο του υπολογιστή του. Το αρχείο καταγραφής που δημιουργείται από το keylogger στη συνέχεια δύναται να αποστέλλεται σε καθορισμένο δέκτη, τον hacker, ακόμη και μέσω e-mail. Ορισμένα προγράμματα keylogger μπορούν, επίσης, να καταγράψουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί το θύμα, καθώς και τα URL των ιστοσελίδων που επισκέπτεται. Τα keyloggers είναι ιδιαιτέρα επικίνδυνα για όλους όσους χρησιμοποιούν ηλεκτρονικούς δικτυακούς τόπους μέσω των οποίων προβαίνουν σε χρηματικές συναλλαγές[446].

---

[445] Έτσι προκύπτει προφανώς και το όνομα αυτών των προγραμμάτων: keylogger = αυτό που «κλειδώνει» τα πλήκτρα.

[446] Βλ. σχετικά urls: http://www.inout.gr/showthread.php?t=24288, http://www.techopedia.com/definition/4000/keylogger. και http://www.webopedia.com/TERM/K/keylogger.html καθώς και το url: http://thanasaras13.blogspot.gr/2011/07/keylogger.html από blog στο οποίο προσφέρονται οδηγίες για εγκατάσταση προγράμματος keylogger.

2.11.2.2.12 «Λογικές βόμβες» (“Logic bombs”)

Τα “Logic bombs” είναι κακόβουλα προγράμματα που έχουν εισαχθεί αλλά παραμένουν ανενεργά στη μνήμη μιας ηλεκτρονικής συσκευής πληροφορικής και ενεργοποιούνται είτε σε προκαθορισμένη χρονική στιγμή (time bombs) είτε μετά από κάποιο συγκεκριμένο χειρισμό[447]. Σκοπός τους είναι η καταστροφή αρχείων εξαιτίας της οποίας προκαλείται η σταδιακή κατάρρευση του συστήματος[448].

2.11.2.2.13 Snoopers

Snoopers καλούνται προγράμματα που παρακολουθούν δεδομένα που διακινούνται μέσα σε ένα σύστημα, ψάχνοντας να βρουν ένα συγκεκριμένο είδος πληροφοριών[449]. Ένα τέτοιο πρόγραμμα μπορεί να εγκατασταθεί στον κεντρικό εξυπηρετητή ενός δικτύου ή στο σκληρό δίσκο ενός ηλεκτρονικού υπολογιστή και να παρακολουθεί με τον τρόπο αυτό τα δεδομένα που διακινούνται σε αυτά.

2.11.2.2.14 «Ανίχνευση ευπαθειών» (“Vulnerability scanning”)

Η ανίχνευση ευπαθειών (“vulnerability scanning”) είναι μια τεχνική ασφαλείας που χρησιμοποιείται για τον εντοπισμό των αδυναμιών της ασφάλειας σε ένα σύστημα υπολογιστών[450]. Η συγκεκριμένη τεχνική μπορεί να χρησιμοποιηθεί από ιδιώτες ή διαχειριστές δικτύου είτε για λόγους ασφαλείας, είτε από hackers που προσπαθούν να

---

[447] Βλ. και *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal Theory, Working Paper No. 249030, url: http://papers.ssrn.com/paper.taf?abstract_id=249030, p. 24.

[448] Βλ. url: http://www.techopedia.com/definition/4010/logic-bomb.

[449] Βλ. url: http://www.yourdictionary.com/snooper.

[450] Βλ. ανωτέρω σχετικές αναπτύξεις για έλεγχο των κενών ασφαλείας δικτύων στο πλαίσιο χακτιβισμού και ethical hacking καθώς και σχετική ανάπτυξη για “backdoors” στην παράγραφο 1.3.1 του παρόντος πονήματος.

αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ηλεκτρονικών υπολογιστών[451]. Η ανίχνευση ευπαθειών συνήθως αφορά σε συστήματα που είναι συνδεδεμένα στο διαδίκτυο αλλά μπορεί, επίσης, να παραπέμπει και σε έλεγχο συστημάτων σε εσωτερικά δίκτυα (intranets[452]) που δεν είναι συνδεδεμένα στο διαδίκτυο, προκειμένου να εκτιμηθεί η απειλή από κακόβουλα λογισμικά[453].

Υπάρχουν ακριβά αλλά και δωρεάν εργαλεία για vulnerability scanning. Το vulnerability scanning μπορεί να πραγματοποιηθεί με διάφορους τρόπους όπως το "Port Scanner". Ειδικότερα, ο όρος port scanning[454] αναφέρεται σε μία από τις πιο δημοφιλείς τεχνικές ανίχνευσης ανοικτών δικτυακών θυρών, που χρησιμοποιείται από τους εισβολείς με στόχο την άντληση πληροφοριών σε ένα απομακρυσμένο δίκτυο (remote network). Όλες οι συσκευές που βρίσκονται συνδεδεμένες σε ένα τοπικό δίκτυο (LAN – Local Area Network) ή στο διαδίκτυο ενεργοποιούν ηλεκτρονικές εντολές, οι οποίες απευθύνονται σε κάποιες γνωστές ή μη θύρες (ports). Η «σάρωση» των θυρών (port scanning) βοηθά τον εισβολέα να βρει τις διαθέσιμες ελεύθερες, ώστε να αποκτήσει πρόσβαση στον υπολογιστή κάποιου χρήστη και να λειτουργήσει κακόβουλα. Η τεχνική του "Port Scanning" προσπαθεί να ανιχνεύσει τις αδυναμίες του χρήστη, ενώ η αποστολή μηνύματος ανίχνευσης σε μία θύρα, καθώς και η απάντηση στο απεσταλμένο μήνυμα καταδεικνύει την κατάσταση στην οποία βρίσκεται η θύρα (ανοικτή ή κλειστή). Επιπλέον, συλλέγονται πληροφορίες για το είδος του λειτουργικού συστήματος, το οποίο χρησιμοποιεί ο χρήστης.

2.11.2.2.15 Source rooting

Το "source rooting" αποτελεί τεχνική με την οποία ο αποστολέας ενός «πακέτου» πληροφοριών μπορεί να καθορίσει μερικώς ή πλήρως τη διαδρομή που θα ακολουθήσει το «πακέτο» μέσα στο δίκτυο. Η πιο συνηθισμένη μορφή της τεχνικής αυτής είναι η "loose source record root- LSRR" με την οποία ο αποστολέας καθορίζει

[451] Βλ. url: http://www.techopedia.com/definition/4160/vulnerability-scanning.

[452] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 128.

[453] Βλ. url: http://www.webopedia.com/TERM/V/vulnerability_scanning.html.

[454] Αναλυτικά για το port scanning βλ. *Cynthia Bailey*, *Lee Chris Roedel & Elena Silenok*, Detection and Characterization of Port Scan Attacks, Department of Computer Science & Engineering - University of California, San Diego, url: http://cseweb.ucsd.edu/~clbailey/PortScans.pdf.

έναν ή περισσότερους σταθμούς από τους οποίους πρέπει να διέλθει το «πακέτο». Η τεχνική αυτή μπορεί να χρησιμοποιηθεί από hackers προκειμένου η διαδρομή του «πακέτου» να παρακάμψει τοίχους προστασίας (firewalls[455])[456].

2.11.2.2.16 Bouncing

Το bouncing αποτελεί τεχνική με την οποία καλύπτεται η πηγή της σύνδεσης δικτύου ενός χρήστη και αξιοποιείται από hackers προκειμένου να κρύψουν τυχόν επερχόμενη επίθεση τους. Η τεχνική αυτή υποστηρίζεται από αντίστοιχο λογισμικό. Συγκεκριμένα, το bouncer (BNC) αποτελεί ειδικό λογισμικό, το οποίο χρησιμοποιείται προκειμένου ο χρήστης να κρύβει την αυθεντική πηγή της σύνδεσής του προστατεύοντας έτσι την ιδιωτικότητά του. Επιπρόσθετα, η τεχνική αυτή εφαρμόζεται προκειμένου να αποκρυφθεί ο στόχος[457].

2.11.2.2.17 Rootkits

Το rootkit αποτελεί έναν τύπο κακόβουλου λογισμικού, το οποίο ενεργοποιείται κάθε φορά που εκκινείται ένα σύστημα και έχει σχεδιαστεί για να κρύβει την ύπαρξη ορισμένων διαδικασιών ή προγραμμάτων από τις κανονικές μεθόδους ανίχνευσης και να επιτρέψει τη συνεχόμενη προνομιακή πρόσβαση σε έναν υπολογιστή. Η εγκατάσταση ενός προγράμματος rootkit μπορεί να λάβει χώρα αυτόματα ή αν κάποιος παραβιαστής έχει αποκτήσει πρόσβαση τύπου διαχειριστή. Τα rootkits είναι δύσκολο να ανιχνευθούν επειδή ενεργοποιούνται πριν να εκκινήσει εντελώς το λειτουργικό σύστημα. Τα rootkits επιτρέπουν την εγκατάσταση κρυφών αρχείων,

---

[455] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 114.

[456] Βλ. urls: http://linux.about.com/cs/linux101/g/source_route.htm και http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm.

[457] Βλ. url: http://www.irc-junkie.org/2009-12-22/irc-bouncer-comparison/.

διεργασιών και λογαριασμών, ενώ είναι σε θέση να υποκλέψουν δεδομένα από τις συνδέσεις του δικτύου και το πληκτρολόγιο[458].

2.11.2.2.18 Υπερχείλιση προσωρινής μνήμης (buffer overflow)[459]

Η συγκεκριμένη πρακτική μπορεί να υποστηριχθεί ότι είναι μια εξειδικευμένη περίπτωση επίθεσης DoS. Συγκεκριμένα, η υπερχείλιση προσωρινής μνήμης (buffer overflow) λαμβάνει χώρα όταν ένα πρόγραμμα ή μια διαδικασία επιχειρεί να αποθηκεύσει περισσότερα δεδομένα σε μια προσωρινή περιοχή αποθήκευσης δεδομένων (buffer) και από όσα αυτή έχει τη δυνατότητα να διατηρήσει. Εφόσον τα buffers έχουν δημιουργηθεί για να διατηρούν μια συγκεκριμένη ποσότητα δεδομένων, οι επιπλέον πληροφορίες μπορεί να υπερχειλίσουν σε παρακείμενα buffers, αντικαθιστώντας τα δεδομένα που βρίσκονται σε αυτά. Στις επιθέσεις με υπερχείλιση προσωρινής μνήμης, τα επιπλέον δεδομένα ενδέχεται να περιέχουν κωδικούς που έχουν σχεδιαστεί για να προκαλέσουν ορισμένες επιβλαβείς δράσεις. Στην πραγματικότητα, στέλνονται νέες οδηγίες στον υπό επίθεση υπολογιστή, οι οποίες θα μπορούσαν, για παράδειγμα, να καταστρέψουν τα αρχεία του χρήστη, να μετατρέψουν δεδομένα ή να αποκαλύψουν εμπιστευτικές πληροφορίες[460].

2.11.3 Ο hacker μέσα στο σύστημα πληροφοριών

---

[458] Βλ. σχετικώς urls: http://en.wikipedia.org/wiki/Rootkit και http://www.webopedia.com/TERM/R/rootkit.html.

[459] Βλ. Microsoft Corporation with *Andy Ruth & Kurt Hudson*, Security+ Certification, training kit, Microsoft, 2003, σελ. 204.

[460] Τον Ιούλιο του 2000, ένα ευπαθές σημείο σε επίθεση υπερχείλισης προσωρινής μνήμης ανακαλύφθηκε στο Microsoft Outlook και το Outlook Express. Ένα ελάττωμα στον προγραμματισμό κατέστησε δυνατό για έναν εισβολέα να θέσει σε κίνδυνο την ακεραιότητα του υπολογιστή-στόχου με μια απλή αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου, καταφέρνοντας, έτσι, να εκτελούν οποιοδήποτε τμήμα κώδικα προγραμματισμού επιθυμούσαν στον υπολογιστή του παραλήπτη του e-mail. Η διαδικασία αυτή ενεργοποιείτο μόλις ο παραλήπτης «κατέβαζε» το e-mail από τον διακομιστή (σχετικά με το buffer overflow βλ. το url: http://searchsecurity.techtarget.com/definition/buffer-overflow).

Από τη στιγμή που ο hacker αποκτήσει πρόσβαση στο σύστημα του στόχου του, η συνέχεια εξαρτάται από τον σκοπό και το κίνητρο του hacker. Η χρησιμοποίηση των δυνατοτήτων ενός συστήματος από τον ίδιο τον hacker έχει συνήθως σχέση με την επιθυμία του να το ελέγξει -έστω και λίγο- ή/και να εμποδίσει τη χρήση του από τους νόμιμους χρήστες του. Είναι, επίσης, βέβαιο ότι ο hacker μεταξύ άλλων θα συγκεντρώσει πληροφορίες και για τη λειτουργία του συστήματος αυτού καθώς και ότι θα προσπαθήσει να εκμεταλλευτεί τις δυνατότητές του και γενικότερα τα δικαιώματα που παρέχονται στους νόμιμους χρήστες του. Ολοκληρώνοντας την «επίσκεψή» του ο hacker θα προσπαθήσει να εξαφανίσει τα ίχνη του και παράλληλα να διατηρήσει τη δυνατότητα («να αφήσει ανοικτή την πόρτα») και για μελλοντικές ανάλογες δραστηριότητες στο ίδιο σύστημα[461].

Ειδικότερα, ο hacker, ευρισκόμενος μέσα στο σύστημα του στόχου του, έχει ήδη επιτύχει τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Περαιτέρω, όμως, είναι γεγονός ότι θα έχει την ευχέρεια – πέρα από το να δει και να συγκεντρώσει τις πληροφορίες που τον ενδιαφέρουν – να διαστρεβλώσει τις ήδη υπάρχουσες εκεί πληροφορίες, να εγκαταστήσει κακόβουλα προγράμματα, να εξαφανίσει τα ίχνη της «επίσκεψής» του και να δημιουργήσει κερκόπορτες (backdoors) χρήσιμες για ανάλογες μελλοντικές δραστηριότητές του. Υπάρχει βέβαια και η πιθανότητα ανάλογες πληροφορίες να εισάγονται περιοδικά στο σύστημα, οπότε στην περίπτωση αυτή ο hacker το επισκέπτεται σε τακτά χρονικά διαστήματα, προσπαθώντας να μην αφήνει ίχνη κάθε φορά ή έχει εγκαταστήσει σε αυτό ειδικά προγράμματα (π.χ. Snoopers), τα οποία του επιτρέπουν να παρακολουθεί την κίνηση των δεδομένων.

Σε περίπτωση που ο αποκτήσας χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα θέλει να αλλοιώσει το περιεχόμενο πληροφοριών του συστήματος με σκοπό να ζημιώσει τον κάτοχο των πληροφοριών στις οποίες απέκτησε πρόσβαση, είναι προφανές ότι μπορεί να προβεί σε καταλυτικές επεμβάσεις και οι ζημιές που θα επέλθουν από τη χρήση εσφαλμένων στοιχείων που θα έχει εισαγάγει σε αυτά θα είναι σημαντικές για τον κάτοχο και διαχειριστή των δεδομένων αυτών.

Μπορεί σε κάθε περίπτωση να υποστηριχθεί ότι η εκμετάλλευση του συστήματος από τον hacker, ο οποίος έχει αποκτήσει χωρίς δικαίωμα πρόσβαση, δύναται να λάβει *δύο μορφές*: Κατά την πρώτη μορφή, ο hacker περιορίζει τη δράση του «τοπικά» στον

[461] Βλ. *Χρήστος Ε.Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, όπ. π., σελ. 126.

υπολογιστή, όταν βλέπει ή καταστρέφει τα δεδομένα του. Στη δεύτερη και πιο σύνθετη μορφή, ο hacker επιδιώκει να χρησιμοποιήσει τον υπολογιστή ως σημείο αναφοράς για εκτενέστερη δράση στο διαδίκτυο. Σε τέτοιου είδους επιθέσεις χρησιμοποιούνται πολλοί υπολογιστές στους οποίους έχουν εγκατασταθεί προγράμματα, τα οποία οδηγούν στην αυτόματη υπερφόρτωση ενός υπολογιστή – στόχου[462] (βλ. botnet[463]).

Στο τελευταίο στάδιο της παρουσίας του μέσα στο σύστημα πληροφοριών ο hacker έχει ως στόχο την εξαφάνιση των ιχνών της πρόσβασης καθώς δεν επιδιώκει συνήθως την ολοκληρωτική καταστροφή του συστήματος. Αυτό επιτυγχάνεται με τη μετατροπή ή το σβήσιμο των δεδομένων του Πρωτοκόλλου. Δυνατές είναι εξάλλου πολλές παρεμβάσεις, όπως η αντικατάσταση των προγραμμάτων του συστήματος (root kits), τα οποία μπορούν να καλύψουν την παρουσία του εισβολέα για μεγάλο χρονικό διάστημα. Είναι, δε, τόσο εξαιρετικές οι επιδόσεις των hackers όσον αφορά την εξαφάνιση στοιχείων – ιχνών, που πολλοί hackers φέρεται να έχουν στρατολογηθεί κατά καιρούς από το FBI προκειμένου να εντοπίσουν άλλους hackers[464]. Βασικό μέλημα λοιπόν του hacker είναι να σβήσει όσα περισσότερα ίχνη μπορεί αλλά και όσα απομένουν να τα περιπλέξει με τέτοιο τρόπο ώστε να μην μπορούν να τον αποκαλύψουν. Γνωρίζοντας ο hacker ότι η αποκάλυψη της ταυτότητάς του θα καταστρέψει το «έργο» του, οι προσπάθειές του για την εξάλειψη των ιχνών της παρουσίας του ξεκινούν από τη στιγμή της εισόδου του στο σύστημα και ολοκληρώνονται με την έξοδό του από αυτό.

Βέβαια, η εξαφάνιση των ιχνών για την αποφυγή της αποκάλυψης της ταυτότητάς του δεν σημαίνει ότι ο hacker δεν αφήνει την υπογραφή του! Πολλές φορές οι hackers αφήνουν μηνύματα (π.χ. με τη μορφή «ο …Χ… ήταν εδώ» - "…Χ… was here")[465], τα οποία είναι δηλωτικά της παρουσίας τους χρησιμοποιώντας το ψευδώνυμό τους, προκειμένου να αποκτήσουν φήμη[466].

---

[462] Βλ. *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, όπ. π., σελ. 192.

[463] Βλ. ανωτέρω περιγραφή των υπολογιστών zombies και των botnets.

[464] Βλ. Εφημερίδα «Τα ΝΕΑ – Πρόσωπα», Τεύχος 131 της 8/9/2001, σελ. 14.

[465] *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 142-143.

[466] *Suelette Dreyfus*, Computer hackers: Juvenile Deliquents or International Saboteurs?, εισήγηση η οποία παρουσιάστηκε στο συνέδριο "Internet Crime" το οποίο έλαβε χώρα στη Μελβούρνη της

Τέλος, από τη στιγμή που ένας hacker αποκτά τη δυνατότητα πρόσβασης σε ένα σύστημα, συχνά επιθυμία του είναι να εξακολουθήσει να έχει πρόσβαση στο σύστημα αυτό ακόμα και εάν αποκαλυφθεί η παράνομη είσοδός του. Για να το πετύχει αυτό ο hacker συνήθως δημιουργεί ο ίδιος τις λεγόμενες *κερκόπορτες (backdoors),* δηλαδή εναλλακτικούς τρόπους παράνομης επαναδιείσδυσής του στο σύστημα. Για τον λόγο αυτό πολλοί hackers έχουν στη διάθεσή τους ή κατασκευάζουν τα κατάλληλα προγράμματα με τα οποία θα μπορέσουν να εκμεταλλευτούν τα προβλήματα ασφαλείας του συστήματος και γενικότερα τις ατέλειές του και με τον τρόπο αυτό θα μπορέσουν να ανοίξουν και άλλες διόδους πρόσβασης σε αυτό[467].

Σε κάθε περίπτωση, αποτελεί κοινό τόπο ότι η μεθοδολογία του hacking είναι αδύνατον να καλυφθεί εξ ολοκλήρου. Τούτο διότι αυτή ανανεώνεται καθημερινά από τους hackers, η φαντασία των οποίων περισσεύει – εξάλλου, η συνεχής αναζήτηση καινοτόμων πρακτικών πάντοτε παραμένει άξονας του hacking!

Αυστραλίας στις 16-17 Φεβρουαρίου 1998 και διοργανώθηκε από το Australian Institute of Criminology.

[467] Βλ. *Χρήστος Ε. Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του διαδικτύου, όπ. π., σελ. 128.

3. ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΕΣ ΘΕΩΡΙΕΣ ΓΙΑ ΤΗ ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ

Παρά το γεγονός ότι η ποικιλία και ο αριθμός των ευκαιριών αναφορικά με το έγκλημα στο διαδίκτυο έχουν αυξηθεί αλματωδώς τα τελευταία χρόνια, έχουν υπάρξει ελάχιστες προσπάθειες για την ανάπτυξη και την εφαρμογή των εγκληματολογικών θεωριών[468] σε ό,τι αφορά το ψηφιακό έγκλημα[469]. Αυτό ίσως να οφείλεται ακόμη και στο γεγονός ότι και ο ίδιος ο χώρος του διαδικτύου τα τελευταία χρόνια μεταβάλλεται συνεχώς ακόμη και ως προς τη χρήση του. Για παράδειγμα, θεωρώ ότι η δυνατότητα που απέκτησε ο χρήστης του διαδικτύου να γίνεται ο ίδιος εύκολα δημιουργός του περιεχομένου του με τις εφαρμογές του web 2 μετάλλαξε την άποψη του χρήστη και τη συμπεριφορά του ως προς τη διαχείριση των προσωπικών του πληροφοριών: από την στάση «*είμαι πολύ σημαντικός και δεν σας επιτρέπω να δείτε ποιος είμαι και τι κάνω μέσω του διαδικτύου*» (άρα ενισχυμένη θέληση για προστασία του απορρήτου των πληροφοριών) έχουμε πλέον μεταβεί στη στάση «*είμαι πολύ σημαντικός - δείτε τι κάνω μέσω του διαδικτύου*» (επομένως, μεγαλύτερη ανάγκη για προστασία των προσωπικών δεδομένων).

Δυνάμει αυτών των αλλαγών, είναι λογικό ότι και το πεδίο στο οποίο δρουν οι ψηφιακοί «παραβιαστές» είναι ρευστό και οι επιστήμονες προσπαθούν πρώτα να

---

[468] Ο ρόλος της θεωρίας στην ερευνητική διαδικασία είναι σημαντικός. Η θεωρία προσφέρει το πλαίσιο για τη συστηματική ερμηνεία των εμπειρικών δεδομένων, αναφέρεται στη μορφή που μπορεί να προσλάβει το κοινωνικό φαινόμενο, εξηγεί τους λόγους για τους οποίους εμφανίζεται και τις συνθήκες υπό τις οποίες υπάρχει.

Αναφορικά με την έννοια της θεωρίας και ιδίως στις κοινωνικές επιστήμες πρβλ. *Jonathan H. Turner*, The Structure of Sociological Theory, University of California, Riverside, The Dorsey Press Homewood, Illinois, Irwin-Dorsey Limited, Georgetown, Ontario, Revised Edition, 1978, *David Nachmias & Chava Nachmias*, Research methods in the social sciences, St. Martin's Press, New York, 3rd edition, 1987, *Ι. Λαμπιρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, εκδ. Αντ. Ν. Σάκκουλα. 1995, σελ. 134 επ.

[469] Έτσι η *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, url: http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf, όπως παραπέμπει στους Taylor, Caeti, Loper, Fritsch & Liederbach, σελ. 1.

ανιχνεύσουν αυτές τις αλλαγές προτού πάρουν σαφή θέση[470]. Για αυτό και δεν υπάρχουν ευρέως αποδεκτές θεωρίες ή θεωρητικά πλαίσια αναφορικά με το πώς εξελίσσονται οι hackers[471]. Άρα, φαίνεται αναγκαία η διενέργεια συναφών ερευνών, καθώς η σχέση μεταξύ θεωρίας και έρευνας είναι αμφίδρομη, με την έρευνα να ανατροφοδοτεί τη θεωρία.

Ακολούθως, λοιπόν, παρουσιάζονται ενδεικτικώς εγκληματολογικές θεωρίες[472] οι οποίες «φωτίζουν» πτυχές του hacking και μπορούν να αξιοποιηθούν σε επίπεδο ερμηνείας και πρόληψης στις περιπτώσεις hacking και χωρίς δικαίωμα πρόσβασης σε δεδομένα.

3.1 Θεωρία ορθολογικής επιλογής και παράγωγες θεωρίες

3.1.1 Θεωρία ορθολογικής επιλογής[473]

Σε επίπεδο θεωρητικού πλαισίου, η ορθολογική επιλογή[474] περιστρέφεται γύρω από την έννοια ότι το έγκλημα εμφανίζεται σαν μια υποσχετική και ανταποδοτική εναλλακτική στον δράστη σε σύγκριση με το κόστος του. Με άλλα λόγια, η ανάλυση κόστους – οφέλους (cost – benefit analysis)[475] έχει μια μεγάλη παράδοση στην

[470] Πρβλ. *Γ. Πανούση*, Εγκληματολογία, εγκληματολογική έρευνα και ΜΜΕ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1999, σελ. 142 όπου και αναπτύσσεται η προβληματική της ανάπτυξης εγκληματολογικών θεωριών.

[471] *Qing Hu, Zhengchuan Xu & Ali Alper Yayla*, Why college students commits computer hacks: Insights from a cross culture analysis, url: http://www.pacis-net.org/file/2013/PACIS2013-104.pdf.

[472] Αναφορικά με την έννοια και τη λειτουργία της επιστημονικής θεωρίας και τον αποθετικό ορισμό της πρβλ. *Μ. Κρανιδιώτη*, Η ολοκλήρωση – Μέθοδος ανάπτυξης θεωρίας στην εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2007, σελ. 10-11.

[473] Αναφορικά με τη θεωρία ορθολογικής επιλογής και ιδίως τις φιλοσοφικές της ρίζες πρβλ. το αναλυτικό πόνημα των *Αρ. Χατζή & Γ. Φωκά – Καβαλιεράκη*, Θεωρία ορθολογικής επιλογής – Πανεπιστημιακές σημειώσεις, Τμήμα Μεθοδολογίας, Ιστορίας και Θεωρίας της Επιστήμης Ε.Κ.Π.Α., Αθήνα 2012, url: http://www.aristideshatzis.net/2010/04/blog-post_2909.html.

[474] Βλ. *Κ. Δ. Σπινέλλη,* Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 177-178.

[475] Βλ. σχετικά με την ανάλυση κόστους και οφέλους εκ μέρους των δραστών *Κ. Δ. Σπινέλλη,* Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 189.

οικονομική όσο και στην κοινωνιολογική και την εγκληματολογική σκέψη[476] και εκφράζεται μέσα από τη θεωρία της ορθολογικής επιλογής κατά τις διάφορες εκφάνσεις της[477].

Ειδικότερα, η θεωρία της ορθολογικής επιλογής[478] αναπτύχθηκε στη δεκαετία του 1970 και υποστηρίζει ότι ο δράστης αποφασίζει τη διάπραξη του αδικήματος έχοντας υπολογίσει τα προσδοκώμενα οφέλη του εγκλήματος σε συνάρτηση με το ενδεχόμενο κόστος και ιδίως αυτό της σύλληψης και τιμώρησής του. Για τον λόγο αυτόν υποστηρίζεται ότι η αυστηρή τιμώρηση τέτοιου είδους εγκλημάτων είναι αποτελεσματική για την πρόληψη της εγκληματικότητας και λειτουργεί αποτρεπτικά για τους δράστες[479]. Σύμφωνα με τη θεωρία της ορθολογικής επιλογής, κατά τη διάπραξη ενός εγκλήματος η στάθμιση κόστους-οφέλους ως ανωτέρω λαμβάνει χώρα σε κάθε βήμα / στάδιο της συμπεριφοράς. Ο hacker φαίνεται να υπολογίζει το κόστος της ενέργειάς του σε συνάρτηση με το όφελος το οποίο θα έχει, λαμβάνοντας υπόψιν τα χαρακτηριστικά που ευνοούν την διάπραξη εγκληματικών ενεργειών στο διαδίκτυο (π.χ. ανωνυμία, ταχύτητα κ.ά.)[480]. Ως εκ τούτου, για την πρόληψη των εγκλημάτων θα ήταν πολύ χρήσιμη η επεξεργασία των επιλογών που πρέπει να γίνουν σε κάθε στάδιο π.χ. για την χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα[481].

---

[476] Η περιγραφή των δραστών ως ορθολογικώς σταθμίζοντες τις εναλλακτικές τους χάριν του συμφέροντός τους ανάγεται στους κλασικούς συγγραφείς όπως ο Beccaria (1764) και ο Bentham (1789) [για τους Beccaria και Bentham πρβλ. *Ν. Κουράκη,* Ποινική Καταστολή, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2009, 5η εκδ., σελ. 140 επ. και 156 επ. αντίστοιχα - για τον Beccaria και τον Bentham και την αρχή του ωφελιμισμού (ulitarismus) βλ. και *Κ. Δ. Σπινέλλη,* Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 183-186].

[477] Αναλυτικά για τη θεωρία ορθολογικής επιλογής βλ. *Μ. Γαλανού*, Περί της οικονομικής ανάλυσης του συστήματος της ποινικής δικαιοσύνης, ΠοινΔικ 1/2008, σελ. 81-82.

[478] Για τη θεωρία ορθολογικής επιλογής αναφορικά με το hacking βλ. αναλυτικά *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 8.

[479] Η Lowman (όπ. π.) παραπέμπει στον Keel, ο οποίος υποστηρίζει ότι νόμοι των ΗΠΑ που αναφέρονται στη λογική "*three strikes and you're out*" βασίζονται σε αυτήν την θεωρία (για την πρακτική "*three strikes and you're out*" πρβλ. *Ν. Κουράκη,* Ποινική Καταστολή, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, σελ. 389 και για κριτική στην εν λόγω πρακτική βλ. *Αγγ. Πιτσελά,* Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002, σελ. 119).

[480] Βλ. χαρακτηριστικά τις αναπτύξεις του *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 410 καθώς και *Χρ. Τσουραμάνη*, Ψηφιακή εγκληματικότητα, όπ. π., σελ. 7-8 για τις διαφορές των ψηφιακών εγκλημάτων από τα παραδοσιακά, χαρακτηριστικά τα οποία αποτελούν στην ουσία στοιχεία που διευκολύνουν την διάπραξη ψηφιακών εγκλημάτων.

[481] Τούτο προφανώς σημαίνει ότι είναι απαραίτητη η πολύ καλή γνώση του modus operandi των δραστών (βλ. ανωτέρω παράγραφο 2.11 της διατριβής) και ενδεχομένως η τιμώρηση προπαρασκευαστικών ενεργειών, όπως η προμήθεια και διάθεση προγραμμάτων ("malware") που

3.1.2 Θεωρία της καθημερινής δραστηριότητας ("routine activity theory")

Η θεωρία της καθημερινής δραστηριότητας (routine activity theory) των Lawrence Cohen και Marcus Felson (1979) βασίζεται στη θεωρία της ορθολογικής επιλογής[482] και είναι μια από τις πιο ριζοσπαστικές εγκληματολογικές θεωρίες, υπό την έννοια ότι αποδίδει την αύξηση των εγκληματικών δραστηριοτήτων στον εκσυγχρονισμό και την αστικοποίηση της κοινωνίας. Εν προκειμένω, στη θεωρία αυτή υποστηρίζεται ότι το έγκλημα είναι μια κανονική κατάσταση και το μόνο το οποίο απαιτείται για αυτό είναι η ευκαιρία. Οι συνήθεις δραστηριότητες της σύγχρονης ζωής δημιουργούν έναν μεγάλο αριθμό *κατάλληλων στόχων (suitable targets)* χωρίς την παρουσία *κατάλληλων φυλάκων (capable guardians)* (του στόχου ή του δυνητικού παραβάτη) ικανών να αποτρέψουν τους *παραβάτες με κίνητρα (motivated offenders)*[483]. Όταν ο χώρος και ο χρόνος των τριών αυτών στοιχείων συγκλίνουν, το έγκλημα είναι πιθανό να λάβει χώρα[484].

Η σύγκλιση αυτή των ανωτέρω στοιχείων λαμβάνει χώρα κατά τη χρήση του διαδικτύου[485]. Γίνεται, επομένως, αντιληπτό ότι υπάρχει άμεση εφαρμογή των ανωτέρω στο έγκλημα στο διαδίκτυο[486], λαμβανομένης υπόψη της ταχύτατης και συνεχώς εξελισσόμενης χρήσης του διαδικτύου και των υπολογιστικών συστημάτων:

διευκολύνουν τη χωρίς δικαίωμα πρόσβαση σε δεδομένα ή την «παγίδευση» ηλεκτρονικών δεδομένων (hacking tools, key loggers κ.λπ.).

[482] Έτσι η *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 8.

[483] Βλ. την εμπεριστατωμένη ανάλυση των τριών αυτών στοιχείων στο πόνημα του *Majid Yar*, The Novelty of "Cybercrime" - An Assessment in Light of Routine Activity Theory, European Journal of Criminology, Volume 2 (4): 407–427: 1477-3708, European Society of Criminology and SAGE Publications, London, Thousand Oaks CA, and New Delhi 2005.

[484] Αντίστοιχη και η προσέγγιση του Grabosky κατά τον οποίο το έγκλημα με υπολογιστή μπορεί να εξηγηθεί με τον συνδυασμό τριών παραγόντων: κίνητρο, ευκαιρία και ελλιπής φύλαξη (έτσι *Peter Grabosky*, Computer Crime in a World Without Borders, Platypus Magazine, The journal of the Australian Federal Police, June 2000).

[485] Βλ. χαρακτηριστικά *Χρ. Τσουραμάνη*, Η ψηφιακή (ηλεκτρονική) εγκληματικότητα στο πλαίσιο της "θεωρίας της καθημερινής δραστηριότητας" ("Routine Activity Theory"), εις: *Σ. Γεωργούλα*, Η εγκληματολογία στην Ελλάδα σήμερα – Τιμητικός τόμος για τον Στέργιο Αλεξιάδη, εκδ. ΚΨΜ, Αθήνα, 2007, σελ. 155 επ.

[486] Έτσι και *Ronald V. Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research 10: 55–63, 2004, Kluwer Academic Publishers, p. 58 και *Soumyo D. Moitra*, Developing Policies for Cybercrime - Some Empirical Issues, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13/3, 2005, p. 449.

η ταχεία ανάπτυξη των συστημάτων και εφαρμογών πληροφορικής είχε ως αποτέλεσμα την αφθονία κενών ασφαλείας στα συστήματα που αποθηκεύονται πολύτιμα ψηφιακά στοιχεία, άρα και την ύπαρξη ελκυστικών στόχων για δυνητικούς παραβάτες[487] [488].

Βασικό στοιχείο, επομένως, της ως άνω θεωρίας είναι και η *απουσία* αυτού του κατάλληλου φύλακα. Στη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, αυτός ο κατάλληλος φύλακας μπορεί να είναι τα μέτρα ασφαλείας (π.χ. κωδικός πρόσβασης). Ωστόσο, σε περίπτωση "insider", ο οποίος έχει κωδικούς πρόσβασης, η απουσία του κατάλληλου φύλακα μπορεί να αποδοθεί στην φυσική απουσία του προϊσταμένου του υπαλλήλου ή στην έλλειψη ελέγχου του υπαλλήλου αυτού από τον προϊστάμενό του[489].

3.1.3 Ορθολογική επιλογή προοπτικής ("rational choice perspective")

Από τις εκφάνσεις της θεωρίας ορθολογικής επιλογής ο Bachmann[490] επιλέγει στην έρευνά του να προσπαθήσει να εξηγήσει το hacking μέσα από τη θεωρία της ορθολογικής επιλογής προοπτικής (rational choice perspective) των Cornish και Clarke. Πυρήνα της εν λόγω θεωρίας αποτελούν οι εξής έξι αρχές:

1. Τα εγκλήματα διαπράττονται σκοπίμως και εσκεμμένως με σκοπό την αποκόμιση οφέλους από τον δράστη.

2. Στην προσπάθειά τους να αποκομίσουν όφελος, οι παραβάτες δεν καταφέρνουν πάντα να λαμβάνουν τις καλύτερες αποφάσεις λόγω των

[487] *Qing Hu, Zhengchuan Xu & Ali Alper Yayla*, Why college students commits computer hacks: Insights from a cross culture analysis, url: http://www.pacis-net.org/file/2013/PACIS2013-104.pdf.

[488] Για τη συσχέτιση εγκλημάτων στο διαδίκτυο και θεωρίας της καθημερινής δραστηριότητας και ανάλυση αυτής βλ. *Adam M. Bossler & Thomas J. Holt*, Malware Victimization - A Routine Activities Framework, εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf, pp. 317 f.

[489] *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 9.

[490] Βλ. το αναλυτικό ερευνητικό πόνημα του *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking underground, όπ. π., σελ. 48 επ., στο οποίο ελέγχει την εφαρμογή της εν λόγω θεωρίας σε δείγμα hackers.

κινδύνων και της αβεβαιότητας που ενέχουν οι καταστάσεις στις οποίες εμπλέκονται.

3. Οι αποφάσεις του δράστη ποικίλουν σημαντικά ανάλογα με τη φύση του εγκλήματος.

4. Οι αποφάσεις εμπλοκής σε συγκεκριμένα είδη εγκλήματος (αποφάσεις συμμετοχής - ανάμειξης) είναι εντελώς διαφορετικές από εκείνες που αφορούν στη διάπραξη συγκεκριμένης εγκληματικής πράξης.

5. Οι αποφάσεις συμμετοχής μπορούν να χωριστούν σε τρεις κατηγορίες: εμπλοκής για πρώτη φορά (έναρξη), συνεχούς συμμετοχής (έξη) και παύσης – καθεμία από αυτές μελετάται ξεχωριστά καθώς επηρεάζεται από διαφορετικά σύνολα μεταβλητών.

6. Οι αποφάσεις διάπραξης περιλαμβάνουν μια σειρά από επιλογές που γίνονται σε κάθε στάδιο της εγκληματική πράξης (π.χ. προετοιμασία, επιλογή στόχων, τέλεση της πράξης, μετέπειτα διαφυγή).

Η αφετηρία σκέψης αυτής της θεωρίας δηλώνει ουσιαστικά ότι τα εγκλήματα δεν είναι παράλογες ή τυχαίες πράξεις. Αντίθετα, θεωρούνται σκόπιμες πράξεις προς όφελος του δράστη. Το όφελος αυτό είναι εύκολα αναγνωρίσιμο και προφανές στις περιπτώσεις οικονομικού ανταλλάγματος ή υλικών αγαθών. Στην περίπτωση, όμως, της χωρίς δικαίωμα πρόσβασης σε δεδομένα έχει υποστηριχθεί ότι αυτό το όφελος μπορεί να συνίσταται στον ενθουσιασμό, τη διασκέδαση, το κύρος, τη σεξουαλική ικανοποίηση κ.ά.[491]

3.2 Κριτική εγκληματολογία

Σύμφωνα με την κριτική εγκληματολογία, ορισμένες μορφές συμπεριφοράς χαρακτηρίζονται ως εγκληματικές επειδή απειλούν το καπιταλιστικό σύστημα και την κυρίαρχη άρχουσα τάξη. Επίσης, κατά την κριτική εγκληματολογία, σε ορισμένα

[491] *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking underground, όπ. π., σελ. 50.

άτομα επικολλάται η ετικέτα του εγκληματία[492] επειδή ο στιγματισμός τους εξυπηρετεί τα συμφέροντα της άρχουσας τάξης και όχι επειδή η συμπεριφορά τους έχει υπερβεί τα όρια της κοινωνικής ανοχής του κοινωνικού συνόλου[493]. Εν προκειμένω, οι hackers, με ηθική και ιδεολογία η οποία υποστηρίζει την ελευθερία της πληροφορίας[494] και με δεδομένο ότι η ηλεκτρονική πληροφορία στο καπιταλιστικό σύστημα έχει οικονομική αξία και είναι δεκτική ιδιοκτησίας[495], συνιστούν απειλή για το υπάρχον καπιταλιστικό σύστημα[496] [497]. Επομένως, οι συμπεριφορές τους περικλείονται από εγκληματικό μανδύα για αυτόν ακριβώς τον λόγο.

Οι κριτικοί εγκληματολόγοι υποστηρίζουν σθεναρά ότι το έγκλημα μπορεί να γνωρίσει ουσιαστική μείωση μόνον εάν συνδυαστεί με τη ριζική απώθηση της καταπίεσης και εκμετάλλευσης σε όλες της τις μορφές (οικονομική, πολιτική, πολιτισμική, φιλική, ψυχική) και σχέσεις. Εκτιμούν, επίσης, ότι το πρόβλημα του εγκλήματος είναι αντιμετωπίσιμο μόνο στο ευρύτερο πλαίσιο αλλαγών στο συσχετισμό των κοινωνικών δυνάμεων σχετικά με τη μορφή και το ρόλο του ποινικού συστήματος ή ακόμα και ριζοσπαστικών αλλαγών στην οργάνωση της κοινωνίας[498].

Συνεπώς, η δράση των hackers, στο βαθμό και στις περιπτώσεις που στέκεται απέναντι στο ισχύον σύστημα (ή και στην κυρίαρχη κουλτούρα[499]) φαίνεται να εντάσσεται και να ερμηνεύεται στους κόλπους της κριτικής εγκληματολογίας. Ειδικά

---

[492] Βλ. κατωτέρω υποσ. αναφορικά με τη θεωρία της ετικέτας.

[493] Έτσι *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, 2η εκδ. σελ. 43, όπου και περιεκτική ανάλυση των θέσεων της κριτικής εγκληματολογίας.

[494] Βλ. ανωτέρω παράγραφο 2.6 του παρόντος πονήματος.

[495] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 1 της παρούσας.

[496] ... καθώς τίθενται ενάντια στην κυρίαρχη κουλτούρα – βλ. ανωτέρω ανάπτυξη αναφορικά με την (υπο)κουλτούρα του hacking.

[497] Κατά τον Taylor, η ποινικοποίηση της χωρίς δικαίωμα πρόσβασης έλαβε χώρα διότι οι hackers με τις αντιλήψεις τους περί ελευθερίας της πληροφορίας (όπως αναλύθηκαν ανωτέρω) απείλησαν ένα από τα βασικά «δεκανίκια» του καπιταλισμού, τα δικαιώματα ιδιοκτησίας (έτσι *Paul Taylor*, Hackers, distributed in Computer Underground Digest, Vol. 9 Issue 59, σελ. 5).

[498] Βλ. *Γρηγόρης Λάζος*, Κριτική Εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2007, σελ. 119. Όπως ενδεικτικά αναφέρει: *«η κριτική εγκληματολογία μετέχει στην προσπάθεια της ευρύτερης κριτικής κοινωνικής επιστήμης για την άρση (και όχι τη φίμωση) της απόγνωσης και για τον εξορθολογισμό (και όχι την καταστολή) της οργής. Στο πλαίσιο αυτό τα κοινωνικά συναισθήματα της απόγνωσης και της οργής δεν ξενίζουν, ούτε κατωτεροποιούνται ή τίθενται σε αιώρηση. Αντίθετα, μετέχουν στους τρόπους κριτικής εγκληματολογικής έκφρασης. Κι αυτό διότι η κριτική εγκληματολογία βρίσκεται σε μία αέναη εγρήγορση ώστε να μην μεταπέσει σε "φύλακα στο ζωολογικό κήπο της κοινωνικής απόκλισης"»* (όπ. π. σελ. 122).

[499] Βλ. παράγραφο 2.8 ανωτέρω.

αναφορικά με την κατοχή ηλεκτρονικών δεδομένων, αν αυτή ερμηνευθεί ως έκφανση ιδιοκτησίας[500] σύμφωνα με το καπιταλιστικό σύστημα, η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα φαίνεται να καταρρίπτει επί της ουσίας αυτήν τη «συστημική ανωμαλία» της ανελευθερίας στην πρόσβαση στην πληροφορία. Το τελευταίο ενισχύεται αν λάβει κανείς υπόψη ότι η αντιμετώπιση φαινομένων, όπως είναι η κάμψη του κράτους πρόνοιας και η ενίσχυση του κράτους επιτήρησης και καταστολής, η απαλλοτρίωση του κυβερνοχώρου από το κεφάλαιο, η καταστροφή του περιβάλλοντος, η διευρυνόμενη εξαθλίωση εκατομμυρίων ανθρώπων, η εντεινόμενη ανεργία και η ενίσχυση του ρατσισμού, τίθεται στο επίκεντρο τόσο της κριτικής εγκληματολογίας όσο και της δράσης και της ιδεολογίας ομάδων hackers[501].

3.3 Θεωρία τεχνικών ηθικής ουδετεροποίησης

Η εγκληματολογική θεωρία των τεχνικών ουδετεροποίησης (neutralization theory) – «εξουδετέρωσης» των Sykes και Matza (1957)[502] προσφέρεται και αυτή για ερμηνεία συμπεριφορών των hackers[503].

Συγκεκριμένα, από τη θεωρία αυτή προσδιορίζονται «τεχνικές ουδετεροποίησης» που επινοήθηκαν από τους δράστες ώστε να μειώνεται η επιρροή των ετικετών που τους αποδίδονται σύμφωνα με την οικεία θεωρία της ετικέτας (ή του χαρακτηρισμού ή της

[500] Το ηλεκτρονικό έγκλημα προσδιορίζεται βάσει των σχέσεων ιδιοκτησίας (έτσι *Αγγ. Κίτσιου &Χρ. Κουρούτζας*, Μελετώντας το ηλεκτρονικό έγκλημα στο πλαίσιο της κοινωνίας της πληροφορίας. Πιλοτική έρευνα αναπαραστάσεων σε φορείς του νομού Λέσβου, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τομ. Ι., σελ. 324 επ., όπως παραπέμπουν στους Michalowski και Pfuhl).

[501] Π.χ. βλ. το κίνημα του χακτιβισμού (παράγραφος 2.9.2 του παρόντος πονήματος).

[502] Βλ. Gresham M. Sykes and David Matza, Techniques of Neutralization: A Theory of Delinquency, ***American Sociological Review***, Vol. 22, No. 6 (Dec., 1957), published by: American Sociological Association, pp. 664-670. Βλ. παρουσίαση και ανάλυση της θεωρίας της ηθικής ουδετεροποίησης / «εξουδετέρωσης» στο εγχειρίδιο εγκληματολογίας της Κ. Δ. Σπινέλλη, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 268 επ. καθώς και σε Στ. Αλεξιάδη, Εγκληματολογία, εκδ. Σάκκουλα, 4η εκδ. Θεσσαλονίκη, 2004, σελ. 68 επ.

[503] Βλ. το σχετικό πόνημα του *Robert G. Morris*, Computer Hacking and the Techniques of Neutralization: An Empirical Assessment, url: http://www.utdallas.edu/~rgm071000/index_files/Morris%20-%20Hacking%20and%20Neutralization.pdf όπου και ειδική ανάλυση της θεωρίας των Matza & Sykes και η συσχέτισή της με το hacking.

διάδρασης - labeling ή interactionism theory)[504]. Ειδικότερα, φαίνεται ότι αυτοί που παραβιάζουν τους κανόνες, προκειμένου να αποβάλουν τις ετικέτες, χρησιμοποιούν πέντε τεχνικές ουδετεροποίησης[505], όπως αυτές περιγράφονται ακολούθως:

---

[504] Οι ετικέτες είναι οι χαρακτηρισμοί που αποδίδονται σε εκείνους που παραβιάζουν τους κοινωνικούς κανόνες και που στοχεύουν να ενθαρρύνουν ή να υποχρεώσουν τους παραβάτες να συμμορφωθούν προς αυτούς.

Με τη θεωρία της αλληλεπίδρασης ή του χαρακτηρισμού είναι συνδεδεμένα τα ονόματα των Tannebaum, Lemert, Becker, Schur και άλλων. Ο H. Becker ονόμασε τη θεωρία της αλληλεπίδρασης και θεωρία της ετικέτας (labeling theory) δίνοντας έτσι μεγάλη έμφαση στο στοιχείο του χαρακτηρισμού μιας συμπεριφοράς ως προβληματικής καθώς και της κοινωνικής αντίδρασης που η συμπεριφορά αυτή επισύρει. Σύμφωνα, λοιπόν, με τον H. Becker, δημιουργό της θεωρίας της ετικέτας (labeling theory), «*Παρέκκλιση δεν είναι μια ιδιότητα της πράξης που διαπράττει το άτομο αλλά μάλλον μια συνέπεια της εφαρμογής από άλλους των κανόνων και κυρώσεων σε έναν παραβάτη. Παρεκκλίνων είναι κάποιος στον οποίο εφαρμόσθηκε με επιτυχία η ετικέτα και παρεκκλίνουσα η συμπεριφορά που οι άνθρωποι έτσι "ετικετάρουν"*».

Βλ. παρουσίαση και ανάλυση της θεωρίας της ετικέτας και της διάδρασης στο εγχειρίδιο εγκληματολογίας της *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 275, *Ηλ. Δασκαλάκη*, Η εγκληματολογία της κοινωνικής αντίδρασης, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1985, *Αν. Χάιδου*, Θετικιστική εγκληματολογία. Αιτιολογικές προσεγγίσεις του εγκληματικού φαινομένου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996, σελ. 239 επ. και *Μ. Αρχιμανδρίτου*, Η διαχρονική εξέλιξη της προσέγγισης της ετικέτας, εκδ. Σάκκουλα, Θεσσαλονίκη, 1996.

Αναφορικά με την ετικετοποίηση των hackers, έχει υποστηριχθεί ότι το hacking είναι και μια κοινωνικά κατασκευασμένη ταμπέλα. Ο όρος hacker έχει εξελιχθεί με τα χρόνια - αρχικά, ο όρος αντιπροσώπευε τα κίνητρα των βιρτουόζων προγραμματιστών να υπερβαίνουν τα εμπόδια, σήμερα, όμως αντιπροσωπεύει τη μη εξουσιοδοτημένη πρόσβαση σε δίκτυα υπολογιστών και συστήματα πληροφοριών (βλ. και παραγράφους 2.2 και 2.4 της διατριβής). Υποστηρίζεται ότι η ετικέτα "hacker" έχει αποκτήσει αρνητική χροιά αναφορικά με ηλεκτρονικούς βανδαλισμούς (Chandler, 1996), ως απειλή για την εθνική ασφάλεια και για την πνευματική ιδιοκτησία (Halbert, 1997). Από την άλλη πλευρά, όμως, ο Skibell (2002) υποστηρίζει ότι η ετικέτα αυτή του hacker αποτελεί μύθο και αναφέρει ότι λίγοι hackers διαθέτουν επαρκείς δεξιότητες ή επιθυμούν να διαπράττουν εγκλήματα και να προκαλούν ζημία.

Ειδικότερα, οι hackers ανέπτυξαν το διαδίκτυο και τους προσωπικούς υπολογιστές (Wall, 2001) και έχει λεχθεί ότι θα μπορούσε ακόμη και να υποτεθεί ότι ο προσωπικός υπολογιστής να μην είχε υπάρξει χωρίς τη συμβολή και την κουλτούρα των hackers (Chandler, 1996, σελ. 229). Οι παλαιότερες γενιές των hackers (Jordan & Taylor, 2004, Levy, 1984) με πάθος ήθελαν ηλεκτρονικούς υπολογιστές και συστήματα υπολογιστών και πληροφοριών εύχρηστα και προσβάσιμα. Επίσης, οι hackers έχουν δημιουργήσει με επιτυχία αρκετά χρηστικά και μοναδικά software προγράμματα και έχουν ενισχύσει το κίνημα του ανοιχτού κώδικα ως εναλλακτικό και επιτυχή τρόπο για την ανάπτυξη και διανομή software, το οποίο έχει τις ρίζες του στην κουλτούρα των hackers από τις αρχές της δεκαετίας του 1960 (Levy, 1984). Ωστόσο, στην πορεία η ετικέτα του hacker έχει αλλάξει από θετική σε αρνητική (βλ. και παράγραφο 2.4 αναφορικά με την εξέλιξη των hackers).

Κάνοντας χρήση της θεωρίας της ετικέτας, σύμφωνα με τον Becker (1963), τα άτομα που χαρακτηρίζονται ως αποκλίνοντα αυτοπροσδιορίζονται πρώτα από όλα τα ίδια ως αποκλίνοντα. Ο Becker υποστηρίζει ότι η παραβίαση του ποινικού νόμου είναι ένας λόγος για να χαρακτηριστεί κάποιος αποκλίνων, αλλά το αν αυτό πραγματοποιείται και σε ποιο βαθμό εξαρτάται τελικά από βασικές παραμέτρους όπως η ηλικία, η κοινωνικοοικονομική κατάσταση κ.ά. Τέλος, οι hackers είναι ένα καλό παράδειγμα της προσέγγισης του Becker καθώς η επισήμανση μιας δραστηριότητας ως αποκλίνουσας βασίζεται στη δημιουργία κοινωνικών ομάδων και όχι στην ποιότητα της ίδιας της δραστηριότητας. Ο Becker (1963) χρησιμοποιεί τον όρο "αουτσάιντερ" για να περιγράψει τους ετικετοποιημένους αποκλίνοντες που αποδέχονται την ετικέτα που τους επισυνάπτεται και βλέπουν τους εαυτούς τους ως κάτι διαφορετικό από το "καθιερωμένο".

(έτσι *Orly Turgeman-Goldschmidt*, Identity construction among hackers, όπ. π., σελ. 32-34, όπως παραπέμπει και στους συγγραφείς που αναφέρονται εντός του κειμένου).

[505] Βλ. *Allen Ball*, «An empirical exploration of Neutralization Theory», Criminology 7/4/2006, δημοσιευμένη σε http://onlinelibrary.wiley.com/subject και *Phil Bartle*, «Τεχνικές ουδετεροποίησης –

1. «***Δεν φταίω εγώ***» – **άρνηση της ευθύνης**. Ο παραβάτης ισχυρίζεται ότι κάποιος άλλος φέρει ευθύνη για την παρανομία ή ότι η πράξη του αποτελεί ατύχημα. Συχνά το άτομο αυτό βλέπει τον εαυτό του περισσότερο ως θύμα παρά ως δράστη. Αναφορικά με τους hackers, η ιδεολογία τους σχετικά με την ελευθερία της πληροφορίας δύναται να συνδυαστεί με την εν λόγω τεχνική προκειμένου να κατηγορηθεί το «σύστημα», το οποίο αποκλείει από την πρόσβαση στην πληροφορία και, συνεπώς, ο μόνος τρόπος για αυτούς είναι η χρήση τεχνικών hacking. Επίσης, η άρνηση αυτή της ευθύνης μπορεί ενδεχομένως να βασιστεί και στον πειραματισμό αναφορικά με την χρήση της τεχνολογίας, με επιχείρημα ότι είναι η ίδια η τεχνολογία ανεξέλεγκτη και όχι αυτός που προσπαθεί να βρει τρόπους αξιοποίησής της και ερμηνείας των δυνατοτήτων της.

2. «***Κανείς δεν έπαθε τίποτα***» – **άρνηση της ζημίας ή της βλάβης**. Οι hackers μπορούν να επικαλεστούν ότι μόνη η πρόσβαση σε πληροφορία δεν προκαλεί ζημία, σύμφωνα με την ιδεολογία τους για ελευθερία της πληροφορίας[506].

3. «***Κανείς δεν έπαθε τίποτα***» – **άρνηση της ύπαρξης θύματος**. Η άρνηση της ύπαρξης θύματος μπορεί να είναι ιδιαιτέρως εμφανής στα κυβερνοεγκλήματα, διότι η τεχνική αυτή μπορεί να χρησιμοποιηθεί όταν το θύμα δεν είναι φυσικά ορατό ή είναι άγνωστο ή αφηρημένο[507]. Στην περίπτωση των ηλεκτρονικών πληροφοριών η δεοντική άποψη των hackers για μη δυνατότητα ιδιοκτησίας επί αυτών σημαίνει ότι δεν υπάρχει θύμα σε αυτές τις περιπτώσεις[508].

Μειώνοντας τη σοβαρότητα ενός εγκλήματος», Μετάφραση Αποστολία Γουγούση, στην ιστοσελίδα **http://cec.vcn.bc.ca/mpfc/modules/cri-neug.htm** καθώς και *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 268 επ.

[506] Βλ. ανωτέρω αναπτύξεις στις παραγράφους 2.6 και 2.7.

[507] Ως παράδειγμα, ο Dabney (1995) διαπίστωσε ότι οι εργαζόμενοι είχαν την τάση να χρησιμοποιούν αυτήν την τεχνική εξουδετέρωσης για να δικαιολογήσουν το ότι έπαιρναν αντικείμενα τα οποία βρίσκονταν εντός του χώρου της εταιρείας, για τα οποία όμως δεν ήταν ξεκάθαρο ποιος είναι ο ιδιοκτήτης (δηλαδή άλλος υπάλληλος ή η εταιρεία). Έτσι *Robert G. Morris*, Computer Hacking and the Techniques of Neutralization: An Empirical Assessment, όπ. π., σελ. 7-8.

[508] Έτσι *J. J. Bloombecker*, Computer Crime Update: The View as we exit 1984, New England Law Review, 1985, σελ. 627.

4. «***Δεν έχετε δικαίωμα να με κρίνετε***» **– καταδίκη όσων καταδικάζουν τον δράστη**. Η αρνητική κριτική την οποία ασκούν οι hackers (π.χ. οι ομάδες των "Anonymous"[509]) για το «σύστημα» το οποίο δεν επιτρέπει την ελευθερία στην πρόσβαση στην πληροφορία προφανώς αντανακλά και την μη αποδοχή της εξουσίας των δημιουργών και εκφραστών του. Δηλαδή, οι hackers μπορούν να υιοθετούν την τεχνική αυτή θεωρώντας τους κατηγόρους τους ως υποκριτές που διαπράττουν καθημερινά άδικες πράξεις.

5. «***Το έκανα από πίστη σε έναν ανώτερο σκοπό***» **– επίκληση της πίστης και αφοσίωση σε έναν ανώτερο θεσμό**. Είναι προφανές ότι οι hackers, και ιδίως οι χακτιβιστές, έχοντας καθαρή συνείδηση και κανένα αίσθημα ενοχής, υιοθετούν ως ένα βαθμό το δημοφιλές σύνδρομο του «Ρομπέν των Δασών»[510] αφού υπεραμύνονται ασθενέστερων κοινωνικών ομάδων, επιζητούν και υποστηρίζουν την διαφάνεια, πολεμούν μεταξύ άλλων τη διαφθορά (κυβερνητική ή μη), την κάθε είδους βία και την παραβίαση των ανθρωπίνων δικαιωμάτων. Επιδιώκουν με τις πράξεις τους την υποστήριξη ομάδων ή/και ιδεών και δικαιολογούν τις πράξεις τους με την επίκληση αυτής της υποστήριξης[511].

Αρκετοί εγκληματολόγοι έχουν επεκτείνει με την πάροδο των χρόνων τον «κατάλογο» τεχνικών εξουδετέρωσης, με πιο πρόσφατες έρευνες και μελέτες. Ενδεικτικά, μια ακόμη τεχνική εξουδετέρωσης, η οποία μπορεί να συνδέεται άμεσα με το κυβερνοέγκλημα γενικότερα και με το hacking ειδικότερα, είναι η «υπεράσπιση της αναγκαιότητας» (Minor, 1981). Σύμφωνα με την τεχνική αυτή, αν μια πράξη θεωρείται αναγκαία, τότε δεν χρειάζεται ο δράστης να αισθάνεται ενοχή για τη διάπραξή της, έστω και αν θεωρείται ηθικά λανθασμένη[512]. Μία επιπλέον τεχνική

---

[509] Για την κολεκτίβα των "Anonymous" πρβλ. *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756.

[510] Βλ. *Suzan J. Harrington*, Software Piracy: Are Robin Hood & Responsibility Denial at Work?, Ethical Issues of Information Systems, IRM Press, Hershey, USA 2002, p. 179.

[511] Βλ. χαρακτηριστικά ιδέες και δράσεις της κολεκτίβας των "Anonymous" στο πόνημα *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756.

[512] *Robert G. Morris*, Computer Hacking and the Techniques of Neutralization: An Empirical Assessment, όπ. π., σελ. 7.

ουδετεροποίησης είναι αυτή της ανταπόδοσης: σε αυτήν την περίπτωση, ο δράστης βλέπει τον εαυτό του ως έναν εκδικητή που διορθώνει τα λάθη που ισχυρίζεται ότι διέπραξε παλαιότερα το θύμα. Η πρακτική αυτή είναι συνήθης στους hackers που αντεπιτίθενται εναντίον ιστοσελίδων οι οποίες πρεσβεύουν αξίες αντίθετες από την ιδεολογία τους και πιστεύουν ότι μέσα από τις δράσεις τους αποδίδεται δικαιοσύνη (π.χ. η έκφραση "justice is coming" της κολεκτίβας "Anonymous").

Συμπεριφορές και αντιδράσεις, δηλαδή, οι οποίες αποδίδονται στους hackers (π.χ. ο έλεγχος των συστημάτων για την ασφάλειά τους δεν είναι επιζήμιος)[513] προσιδιάζουν στις ανωτέρω τεχνικές ουδετεροποίησης. Τέλος, ο Morris βάσιμα αναφέρει ότι η εν λόγω θεωρία δεν είναι ξεκάθαρο αν μπορεί να χρησιμοποιηθεί για προληπτική ερμηνεία μιας πράξης hacking ή μετά από αυτή. Εξάλλου, εκτιμάται βάσιμα ότι η εν λόγω θεωρία δρα συμπληρωματικά με άλλες θεωρίες ερμηνευτικές του hacking.[514]

3.4 Εγκλήματα «λευκού περιλαιμίου»

Η θεωρία των εγκλημάτων λευκού περιλαιμίου αναπτύχθηκε από τον Edwin Sutherland και αναφέρεται σε έγκλημα που διαπράττεται από πρόσωπο με υψηλή κοινωνική θέση και κατά τη διάρκεια της κατοχής της θέσης αυτής[515]. Χρησιμοποιήθηκε κυρίως προκειμένου να εξηγήσει εγκληματικές συμπεριφορές στο πλαίσιο επιχειρηματικής δραστηριότητας[516].

Δεδομένου ότι το ηλεκτρονικό έγκλημα συχνά λαμβάνει χώρα στο πλαίσιο της επαγγελματικής δραστηριότητας (και κυρίως για την αποκόμιση οφέλους) δεν θα μπορούσε να μην κατατάσσεται στα εγκλήματα λευκού περιλαιμίου[517]. Ειδικότερα,

---

[513] Βλ. σχετικές αντιδράσεις των hackers στο πόνημα των *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

[514] *Robert G. Morris*, Computer Hacking and the Techniques of Neutralization: An Empirical Assessment, όπ. π.

[515] *Edwin Sutherland*, White-Collar Crime, Holt, Rinehart & Winston, New York, 1949.

[516] Βλ. σχετικές αναπτύξεις για το "white-collar crime" του *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 13 επ.

[517] *Orly Turgeman-Goldschmidt*, Between Hackers and White-Collar Offenders, Bar-Ilan University, Israel, 2012, όπως παραπέμπει στους Rosoff, Pontell & Tillman, 2002, σελ. 417 και στους Clinard & Quinney, 1973, αντίστοιχα (βλ. σχετικό απόσπασμα στα url: http://www.igi-

συσχέτιση εγκλημάτων πληροφορικής και εγκλημάτων λευκού περιλαιμίου[518] πραγματοποιείται από τον Wasik, ο οποίος προτείνει τρεις σχετικούς τύπους[519]:

Κατά πρώτον, ο Wasik αναφέρεται σε εγκλήματα επιχείρησης (στελεχών δηλαδή της επιχείρησης) προς όφελος αυτής με βασικό παράδειγμα τη βιομηχανική κατασκοπεία (πρακτική που συνδέεται άμεσα με χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα - η πρόσβαση αυτή αποτελεί στην ουσία βασικό εργαλείο βιομηχανικής κατασκοπείας).

Κατά δεύτερον, ο Wasik αναφέρεται στα εγκλήματα εργαζομένων στο πλαίσιο της απασχόλησής τους εις βάρος των εργοδοτών τους (εγκλήματα από insiders)[520].

Κατά τρίτον, γίνεται αναφορά σε εξωτερικούς ως προς την επιχείρηση εγκληματίες (outsiders)[521], οι οποίοι αποκτούν εξ αποστάσεως μη εξουσιοδοτημένη πρόσβαση (unauthorized remote access).

Οι Pontell και Rosoff (2009)[522] συνέδεσαν την εγκληματικότητα του λευκού περιλαιμίου με την τέλεση εγκλημάτων πληροφορικής (όπως η απάτη στο διαδίκτυο, η κατασκοπεία και οι "Denial of Service" επιθέσεις[523]) αναφερόμενοι κυρίως σε νεαρούς παραβάτες μεσαίας και ανώτερης κοινωνικής τάξης[524].

Ωστόσο, οι παραβάτες λευκού περιλαιμίου συνήθως ενεργούν προκειμένου να αποκομίσουν οικονομικό κέρδος – άρα, ζήτημα υπάρχει αναφορικά με την ένταξη της απλής χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα στα εγκλήματα λευκού περιλαιμίου όταν οι hackers ενεργούν για διασκέδαση, περιέργεια και για να

---

global.com/chapter/between-hackers-white-collar-offenders/46418 και http://www.igi-global.com/chapter/between-hackers-white-collar-offenders/61024).

[518] Βλ. και σχετική ανάπτυξη των *Robert S. Snoyer & Glenn A. Fischer*, Managing microcomputer security, ed. Chantico Publishing Company, Inc., 1993, σελ. 46 επ.

[519] Έτσι η σχετική αναλυτική ανάπτυξη από τον *Γ. Λάζο*, Πληροφορική και Έγκλημα, όπ. π., σελ. 57 επ.

[520] Βλ. την μοναδική δημοσιευμένη απόφαση στην Ελλάδα αναφορικά με χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα (αποφ. Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 75, όπως αναλύεται κατωτέρω), κατά την οποία κελευστής καταδικάστηκε για το αδίκημα του 370Γ παρ. 2 επειδή απέκτησε χωρίς δικαίωμα πρόσβαση σε δεδομένα αποθηκευμένα σε υπολογιστή του χώρου εργασίας του.

[521] Αναφορικά με τους insiders και τους outsiders βλ. παράγραφο 2.11 ανωτέρω.

[522] *Orly Turgeman-Goldschmidt*, Between Hackers and White-Collar Offenders, όπ. π.

[523] Βλ. σχετικά παράγραφο 2.11.2.2.2 ως ανωτέρω.

[524] Ενδεικτικά πρβλ. το άρθρο της *Jennifer Booton*, "From the Streets to Cyberspace: U.S. Gangs Turn to White-Collar Crime", FoxBusiness, 28 Οκτωβρίου 2011, url: http://www.foxbusiness.com/technology/2011/10/28/from-streets-to-cyberspace-us-gangs-turn-to-white-collar-crime/.

«τσεκάρουν» ή/και να εξελίξουν τη δεξιοτεχνία τους στον προγραμματισμό χωρίς όμως να αποκομίσουν άμεσο περιουσιακό όφελος.[525]

3.5 Η θεωρία της «ηθικής ανάπτυξης» ("moral development theory")

Η θεωρία της "ηθικής ανάπτυξης" αναπτύχθηκε από τον Lawrence Kohlberg και υποστηρίζει ότι τα άτομα αναπτύσσουν την ηθική συλλογιστική τους σε μια σειρά από διαδοχικά στάδια κατά την ωρίμανσή τους και την κοινωνικοποίησή τους. Η άποψη για το «σωστό» και το «λάθος» είναι διαφορετική σε κάθε στάδιο μέχρι την πρώιμη ενήλικη ζωή. Η εγκληματική συμπεριφορά προκύπτει όταν παρουσιάζεται μια ευκαιρία για προσβολή και υπάρχει συνάμα καθυστέρηση στην ανάπτυξη του ηθικού διαλογισμού στο άτομο (Hollin, 1989)[526]. Ο Kohlberg υποστήριξε ότι οι εγκληματίες σταματούν συχνά την «ηθική ανάπτυξή» τους σε νωρίτερο στάδιο σε σχέση με όσους δεν προβαίνουν σε παραβατικές συμπεριφορές[527].

Η Lowman υποστηρίζει ότι η εγκληματικότητα στο διαδίκτυο, η οποία περιλαμβάνει ζητήματα αίσθησης κατοχής δικαιώματος για την επίδειξη παρεκκλίνουσας συμπεριφοράς (π.χ. «η πληροφορία είναι ελεύθερη άρα έχω δικαίωμα για πρόσβαση οπουδήποτε»), μπορεί να εξηγηθεί από τη θεωρία ηθικής ανάπτυξης. Ωστόσο, κριτικά και ελεγκτικά διατυπώνεται και πάλι το πρόβλημα των ασαφών ηθικών νορμών που οδηγούν σε δημοφιλή πεποίθηση αναφορικά με την παρέκκλιση στο διαδίκτυο[528].

---

[525] *Orly Turgeman-Goldschmidt*, Between Hackers and White-Collar Offenders, όπ. π.

[526] Βλ. *Marc Rogers*, Psychological Theories of Crime and "Hacking", url: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.32.3697. Στο εν λόγω πόνημα αναφέρεται ότι η θεωρία αυτή προκρίνεται για την ερμηνεία της παραβατικότητας ενδεχομένως σε περιπτώσεις αδικημάτων στην υπηρεσία κ.ά. (όπως παραπέμπει στους Balckburn, 1993 και Clinnard & Quinney, 1986).

[527] *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 9.

[528] Βλ. όπως και παραπάνω *του γράφοντος*, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

3.6 Η θεωρία της έντασης ("strain theory" / "blocked opportunity theory" - Robert Merton)

Ο Merton διατύπωσε την άποψη ότι δημιουργείται ψυχική ένταση που μπορεί να οδηγήσει προς το έγκλημα σε περίπτωση διάστασης μέσων και στόχων που θέτει μία κοινωνία και των διαθέσιμων νόμιμων μέσων για την πραγματοποίησή τους, ιδίως ελλείψει ίσων ευκαιριών μεταξύ των μελών της κοινωνίας[529] [530]. Οι στόχοι αυτοί μπορεί να αφορούν υλικά αγαθά ή ακόμη και δυνατότητες εκπαίδευσης (μεθερμηνεύοντάς το, δηλαδή, ως ελεύθερη πρόσβαση στην πληροφορία, σύμφωνα και με την ιδεολογία των hackers)[531].

Αναφορικά με το πρόβλημα της ανομίας, η οποία προκύπτει από την ως άνω διάσταση μέσων και στόχων, ο Merton διέκρινε πέντε δυνατές προσαρμογές:

> Κατά πρώτον, την κομφορμιστική προσαρμογή, κατά την οποία το άτομο συμμορφώνεται με τους στόχους και τα κοινωνικώς και νομίμως αποδεκτά μέσα για την κατάκτησή τους – άρα, είναι σχεδόν απίθανο υπό αυτήν την θεώρηση να λάβουν χώρα παραβατικές πράξεις.
>
> Κατά δεύτερον, την καινοτομία, κατά την οποία το άτομο αποδέχεται τους στόχους αλλά είτε απορρίπτει τα θεμιτά και νόμιμα μέσα, είτε αναζητά εναλλακτικά μέσα, τα οποία μπορεί να κινούνται στα όρια του νόμου ή της παρέκκλισης.
>
> Κατά τρίτον, την τυπολατρία, κατά την οποία το άτομο δεν δίνει σημασία στους στόχους αλλά ακολουθεί πιστά και τυφλά τους θεσμοθετημένους νομικούς ή κοινωνικούς κανόνες.

Επίσης, βλ. αντίστοιχα για τις διαφορετικές προσεγγίσεις – οι οποίες αταλάντευτα συνδέονται με τα (υπό διαμόρφωση) διαδικτυακά ήθη – αναφορικά με τη νομική αντιμετώπιση του πληροφορικού εγκλήματος *Γ. Λάζου*, Πληροφορική και Έγκλημα, όπ. π., σελ. 83 επ.

[529] Βλ. σχετικώς την εμπεριστατωμένη ανάλυση της *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 252.

[530] Βλ. και *Ashley Crossman*, Structural Strain Theory - An Overview, url: http://sociology.about.com/od/Sociological-Theory/a/Structural-Strain-Theory.htm.

[531] *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 10.

Κατά τέταρτον, τον αναχωρητισμό, ο οποίος εκφράζει τη συλλήβδην απόρριψη στόχων και μέσων κατάκτησής τους.

Κατά πέμπτον, την εξέγερση, κατά την οποία το άτομο απορρίπτει μέσα και στόχους ως ανωτέρω, θέτει, όμως, νέους δικούς του στόχους και νέα μέσα και μεθόδους για να τους κατακτήσει.

Η απόλυτη ελευθερία της πληροφορίας στο διαδίκτυο αποτελεί στόχο για τους hackers, ο οποίος σύμφωνα με τις κρατούσες αρχές φαίνεται ανέφικτος – το μέσον για να την πετύχουν είναι η δράση τους αναφορικά με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Έτσι, υπάρχει η δυνατότητα να εξηγηθεί η συμπεριφορά των hackers και με τη διάσταση της καινοτομίας και με τη διάσταση του αναχωρητισμού αλλά και με τη διάσταση της εξέγερσης (βλ. για ακόμη μια φορά το παράδειγμα των "Anonymous"). Η θέλησή τους αυτή για απόλυτη ελευθερία της πληροφορίας στο διαδίκτυο, η οποία έρχεται σε αντίθεση με τα ισχύοντα ρυθμιστικά πλαίσια του διαδικτύου, δημιουργεί ένταση και καθεστώς ανομίας.

Έχει υποστηριχθεί, επιπρόσθετα, ότι η διάσταση του καινοτόμου ή νεωτεριστή εξηγούν και τη βιομηχανική κατασκοπεία σε επίπεδο χωρίς δικαίωμα πρόσβασης σε δεδομένα. Ενώ, δηλαδή, η θεωρία του Merton αρχικώς χρησιμοποιήθηκε περισσότερο προκειμένου να εξηγήσει το έγκλημα στα χαμηλότερα κοινωνικά στρώματα, φαινόμενα έντασης και ανομίας εντοπίζονται και στα μεσαία και ανώτερα στρώματα καθώς υπάρχει διάσταση μεταξύ των στόχων να αποκτήσουν περαιτέρω επιτυχία και των νομίμων μέσων για την επίτευξη αυτών[532].

3.7 Η θεωρία έλλειψης αυτοελέγχου ("self-control theory"- Michael Gottfredson and Travis Hirschi)

Για την ερμηνεία και πρόβλεψη των συμπεριφορών hacking έχει, επίσης, χρησιμοποιηθεί και η θεωρία αυτοελέγχου του εγκλήματος (self-control theory) - γνωστή και ως γενική θεωρία του εγκλήματος των Gottfredson και Hirschi (1990).

[532] *Sarah Lowman*, Criminology of Computer Crime, Μάιος 2010, όπ. π., σελ. 10 όπως παραπέμπει στους Taylor, Caeti, Loper, Fritsch και Liederbach.

Σύμφωνα με την εν λόγω θεωρία, αυτό που διαφοροποιεί τους εγκληματίες από μη εγκληματίες είναι τα χαρακτηριστικά του χαμηλού αυτο-ελέγχου, τα οποία εντοπίζονται στους παραβαίνοντες τους κανόνες. Τα χαρακτηριστικά αυτά του χαμηλού αυτοελέγχου υποστηρίζεται ότι σχηματίζονται συνήθως σε μικρή ηλικία και τείνουν να είναι σταθερά καθ' όλη τη διάρκεια της ζωής ενός ατόμου. Περιλαμβάνουν, δε, παρορμητικότητα, ανάληψη κινδύνων, εγωκεντρισμό, υψηλή/ιδιαίτερη ψυχραιμία κ.ά.[533] [534] Σε έρευνες των Bossler και Burruss (2011) καθώς και των Holt et al. (2011) καταγράφηκε ότι ο χαμηλός αυτοέλεγχος είναι σημαντικός στις περιπτώσεις διάπραξης hacking[535].

3.8 "Situational action theory" – "Moral Beliefs and Moral Judgment Theory"

Μια άλλη ενδιαφέρουσα εγκληματολογική θεωρία που ενσωματώνει και την ορθολογική επιλογή είναι η θεωρία της περιπτωσιολογικής δράσης (situational action theory), η οποία διατυπώθηκε από τον Wikström (2004, 2006)[536]. Σύμφωνα με αυτή, για να εξηγηθούν οι εγκληματικές πράξεις πρέπει πρώτα να εξηγηθεί τι παρακινεί τα άτομα να παραβούν τους κανόνες[537] – επίσης, οι άνθρωποι παρακινούνται σε δράση (συμπεριλαμβανομένων των εγκληματικών πράξεων) σύμφωνα με τις εναλλακτικές επιλογές δράσης τους, λαμβανομένων υπόψιν των ιδιαιτεροτήτων του περιβάλλοντος. Ως εκ τούτου, αυτό που διαφοροποιεί τους εγκληματίες από τους νομοταγείς έγκειται στις εναλλακτικές λύσεις τις οποίες βρίσκουν και στις επιλογές στις οποίες προβαίνουν σε ένα συγκεκριμένο περιβάλλον. Η θεωρία αυτή υποστηρίζει, επίσης, ότι οι εναλλακτικές επιλογές εξαρτώνται από τις γνώσεις, την ικανότητα, την

[533] Ενδεικτικά και αναλυτικά για την εν λόγω θεωρία και τη σύγχρονη προσέγγισή της βλ. το άρθρο των *Per-Olof H. Wikström and Kyle Treiber*, The Role of Self-Control in Crime Causation, European Journal of Criminology 2007; 4; 237, url: http://www.sagepub.com/isw6/articles/ch6wikstrom.pdf.

[534] Για κριτική προσέγγιση της εν λόγω θεωρίας βλ. *Gilbert Geis*, On the absence of self-control as the basis for a general theory of crime: A critique, url: http://www.soc.umn.edu/~uggen/Geis_TC_00.pdf.

[535] Βλ. *Qing Hu, Zhengchuan Xu & Ali Alper Yayla*, Why college students commits computer hacks: Insights from a cross culture analysis, όπ. π.

[536] *Per-Olof H. Wikström & Kyle H. Treiber*, Violence as Situational action, International Journal of Conflict and Violence (IJCV): Vol. 3 (1) 2009, pp. 75 – 96, url: http://ijcv.org/index.php/ijcv/article/viewFile/49/49.

[537] Βλ. ανωτέρω παράγραφο 2.5 αναφορικά με τα κίνητρα των hackers.

εμπειρία, το ηθικό υπόβαθρο κ.ά. του υποκειμένου καθώς και από χαρακτηριστικά του περιβάλλοντος (π.χ. ευκαιρίες, ηθικό πλαίσιο).

Το θέμα του ηθικού κριτηρίου έχει αναφερθεί σε έρευνες για το hacking. Σύμφωνα με τον Yar (2005), επισημαίνονται δύο κύριες αιτίες του «νεανικού προβλήματος» (της συμμετοχής, δηλαδή, εφήβων) στο hacking. Κατά πρώτον, η εφηβεία είναι περίοδος αναπόφευκτης ψυχολογικής αναταραχής και κρίσης, η οποία συνδράμει να ερμηνευθεί η συμμετοχή των ανηλίκων σε διάφορες μορφές «παραβατικής» και «αντικοινωνικής» συμπεριφοράς[538]. Κατά δεύτερον, υπάρχει «ηθικό έλλειμμα» στους νεαρούς που υιοθετούν παρεκκλίνουσες συμπεριφορές. Το επιχείρημα αυτό είναι σύμφωνο με τις εγκληματολογικές θεωρίες της αναπτυξιακής ψυχολογίας, η οποία υποστηρίζει ότι κατά τη μετάβαση από την παιδική ηλικία στην ενηλικίωση, οι ανήλικοι περνούν από διάφορα στάδια ηθικής μάθησης[539] και εξαρτάται από την «ωριμότητα» το κατά πόσον τα άτομα αυτά μπορούν να είναι πλήρως σε θέση να εκτιμήσουν και να εφαρμόσουν ηθικές αρχές.

Σε μελέτη του Xu και των συνεργατών του (2013) προκύπτει ότι οι hackers υποκινούνται από μια ποικιλία παραγόντων όπως η διασκέδαση, η περιέργεια, η μάθηση, η εκδίκηση, η δικαιοσύνη και το κέρδος. Ωστόσο, ένας βασικός παράγοντας που διαφοροποιεί ένα διερευνητικό φοιτητή που παίζει με τους υπολογιστές και τα συστήματα από έναν hacker, ο οποίος διαπράττει εγκλήματα πληροφορικής, είναι οι ηθικές πεποιθήσεις. Ως εκ τούτου, σύμφωνα με τη θεωρία της περιπτωσιολογικής δράσης, ένα στοιχείο που μπορεί να επηρεάσει σημαντικά την απόφαση για το αν κάποιος θα προβεί σε ενέργειες hacking ή όχι είναι η ηθική πεποίθηση του ατόμου για το αν η ενέργεια αύτη είναι σωστή ή λάθος.[540]

[538] Βλ. και σχετικές αναπτύξεις στην παράγραφο 8.4 του παρόντος πονήματος καθώς και σχετικές υποσημειώσεις σχετικά με τα ευρήματα της ηλικίας των συμμετεχόντων hackers στην κατωτέρω έρευνα στην παράγραφο 7.8.4.1 του παρόντος πονήματος.

[539] Πρβλ. και *Σπύρου Γεωργουσόπουλου και του γράφοντος*, Ποιος είναι ο Jean Piaget, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr, τεύχος 18, Απρίλιος 2011, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1303923164.

[540] *Qing Hu, Zhengchuan Xu & Ali Alper Yayla*, Why college students commits computer hacks: Insights from a cross culture analysis, όπ. π.

3.9 Θεωρία του «διαφορικού συγχρωτισμού» ή της «διαφοροποιούσας συναναστροφής ("differential association theory" – Edwin Sutherland)

Η θεωρία του «διαφορικού συγχρωτισμού» ή της «διαφοροποιούσας συναναστροφής» ("differential association theory") για την εξήγηση του εγκλήματος διατυπώθηκε από τον Ed. Sutherland. Η θεωρία αυτή του Sutherland θεωρείται ότι συνέβαλε θετικά στην εξέλιξη των εγκληματολογικών θέσεων σχετικά με την αιτιολόγηση του εγκλήματος, ιδιαίτερα διότι επεσήμανε τη σημασία των κοινωνικών παραγόντων, καθώς το έγκλημα δεν είναι δυνατό να ερμηνευθεί αποκλειστικά με βάση τους όρους της προσωπικότητας, και έστρεψε την προσοχή στις ομοιότητες που υπάρχουν στη διαδικασία της εκμάθησης τόσο της «εγκληματικής» όσο και της «νομοταγούς» συμπεριφοράς.

Κατά τη θεωρία αυτή, η εγκληματική συμπεριφορά μαθαίνεται με τη συναναστροφή με άλλα άτομα μέσω της ανθρώπινης επικοινωνίας, με τη διάδραση με άλλα άτομα και η εκμάθησή της απαιτεί στενές προσωπικές σχέσεις. Ειδικότερα, οι νέοι θα επιλέξουν το είδος παραβατικής υποπολιτισμικής ομάδας[541] στην οποία θα συμμετάσχουν σύμφωνα με τις ευκαιρίες για παράνομες δραστηριότητες στην (ψηφιακή πλέον) γειτονιά τους[542]. Οι ομάδες εντός των οποίων λαμβάνει χώρα το κύριο μέρος της εκμάθησης της εγκληματικής συμπεριφοράς είναι «κλειστές» και τα μέλη τους συνδέονται με προσωπικούς δεσμούς (οι οποίοι δεσμοί μπορεί να είναι τελικώς μονό διαδικτυακοί με δεδομένο ότι η ψηφιακή επικοινωνία έχει αντικαταστήσει σε μεγάλο βαθμό την πραγματική επικοινωνία για τους χρήστες του διαδικτύου). Επίσης, στην εκμάθηση της εγκληματικής συμπεριφοράς περιλαμβάνονται οι «τεχνικές» για τη διάπραξη εγκλημάτων και η συγκεκριμένη κατεύθυνση των κινήτρων, των αναγκών, των επεξηγήσεων και των διαθέσεων του ατόμου για την παράβαση του νόμου – στην περίπτωση του hacking και της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα οι τεχνικές αυτές είναι απαραίτητες αλλά και «γοητευτικές» διότι αρκετές από αυτές απαιτούν οξύνοια και συνίστανται

[541] Βλ. ανωτέρω αναφορικά με τις υποομάδες των hackers στο κεφάλαιο 2 του παρόντος πονήματος.

[542] *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, 2η έκδ., Αθήνα-Κομοτηνή, Αντ. Ν. Σάκκουλας, 2005, σελ. 256-257.

σε ρηξικέλευθες πρακτικές. Σύμφωνα με την εν λόγω θεωρία, το άτομο παρεκκλίνει διότι οι αντιλήψεις του για τη μη εφαρμογή του νόμου, τις οποίες μαθαίνει με τη συναναστροφή (εν προκειμενω η υποστήριξη της ιδεολογίας του hacking, η οποία ενδεχομένως προκρίνει ιδανικά τα οποία υπολαμβάνονται από τους hackers ως «ανώτερα» αυτών που ο νόμος προστατεύει), επικρατούν των αντίθετων αντιλήψεων για σεβασμό και τήρηση του νόμου. Περαιτέρω, η συναναστροφή του ατόμου με διάφορες ομάδες μπορεί να διαφέρει κατά περίπτωση σε συχνότητα, διάρκεια, προτεραιότητα και ένταση[543].

Αναφορικά με τη συσχέτιση της εν λόγω θεωρίας με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα και γενικότερα με πράξεις hacking, πρόσφατες έρευνες έχουν καταδείξει ότι η αυξημένη συναναστροφή με παραβατικούς συμμαθητές/συμφοιτητές συνδέεται σημαντικά με τη συμμετοχή σε ποικίλες πράξεις hacking σε υπολογιστή[544]. Η δράση, άρα, σε υποομάδες[545] έχει τη δική της ιδιαίτερη σημασία στην εκδήλωση του hacking σε επίπεδο παραβατικής συμπεριφοράς και, επομένως, φαίνεται σύμφωνα και με αυτή τη θεωρία, βάσιμος ο προβληματισμός των Arief και Besnard, οι οποίοι θεωρούν ότι η δράση των hackers σε υποομάδες αποτελεί βασικό στοιχείο του προβλήματος της παραβατικής συμπεριφοράς των hackers[546].

3.10 Διαχειριστική εγκληματολογία

Κατά τη διαχειριστική εγκληματολογία το πρόβλημα της εγκληματικότητας εντοπίζεται σε τρία κυρίως στοιχεία: στη φύση του συμβάντος, στον τόπο (ή αλλιώς χώρο – π.χ. τον κυβερνοχώρο) τέλεσης του εγκλήματος και στην παραδοχή ότι ο δράστης είναι έλλογο ον που προβαίνει σε ανάλυση κόστους-οφέλους προκειμένου

[543] *Στ. Αλεξιάδης*, Εγκληματολογία, 4η έκδοση, Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα, 2004, σελ. 66-67.

[544] Έτσι όπως παραπέμπει στους Morris & Blackburn (2009) ο *Robert G. Morris*, Computer Hacking and the Techniques of Neutralization: An Empirical Assessment, όπ. π., σελ. 13.

[545] Βλ. *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 21 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) και *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 41-42 και 164 για την εσωτερική οργάνωση των ομάδων αυτών.

[546] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 11.

να προβεί στη διάπραξη ενός εγκλήματος[547]. Επομένως, με την εφαρμογή της κατάλληλης αντεγκληματικής πολιτικής το έγκλημα μπορεί να γίνει λιγότερο ελκυστικό για τον δράστη[548].

Οι στόχοι της διαχειριστικής εγκληματολογίας[549] είναι η χειραγώγηση του άμεσου περιβάλλοντος προκειμένου να εξασφαλιστεί ότι οι πιθανές τιμωρίες υπερτερούν του δυνητικού κέρδους – αυξάνοντας την ορατή παρουσία της αστυνομίας, την εγκατάσταση και χρήση τεχνολογιών επιτήρησης, βελτιώνοντας την ασφάλεια της ιδιοκτησίας, κ.ο.κ. – καθώς και οι παρεμβάσεις στον τρόπο ζωής των (ακόμη και δυνητικών) παραβατών προκειμένου να περιοριστούν οι παρορμήσεις τους προς αποκλίνουσες επιλογές (π.χ. ποινικοποίηση προπαρασκευαστικών συμπεριφορών, έμφαση στην πρόληψη κ.ά.). Με άλλα λόγια, οι παρεμβάσεις αυτές αποσκοπούν στην ενίσχυση των «εσωτερικών περιορισμών», έτσι ώστε οι αποκλίνουσες επιλογές να γίνονται λιγότερο επιβραβεύτικες από ψυχολογική, συναισθηματική και πνευματική άποψη[550]. Επιπρόσθετα, υποστηρίζεται σχετικά και μια διαχειριστική τάση στην ποινική δικαιοσύνη αναφορικά με την αποδοτικότητα και την αποτελεσματικότητα της διοικητικής της οργάνωσης[551].

Οι στόχοι της διαχειριστικής εγκληματολογίας στο πεδίο της ψηφιακής παραβατικότητας εν γένει και ιδίως σε ότι έχει να κάνει με την χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα και το hacking μπορούν να δώσουν αφορμή για ποικίλες δράσεις αναφορικά με την πρόληψη εγκληματικών συμπεριφορών. Ωστόσο, με δεδομένο ότι δεν υπάρχει εν προκειμένω απόλυτη ερμηνεία των πράξεων, είναι το δίχως άλλο παράτολμο να κινηθούμε περιοριστικά χωρίς να έχουμε καταγράψει

---

[547] Αναλυτικά για τη διαχειριστική εγκληματολογία βλ. *Μ. Γαλανού*, Περί της οικονομικής ανάλυσης του συστήματος της ποινικής δικαιοσύνης, ΠοινΔικ 1/2008, σελ. 82-83.

[548] Βλ. αναλυτικότερα *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 52 επ.

[549] *Martin O'Brien and Majid Yar*, Criminology – The key concepts, Routledge ed., 2008, p. 5.

[550] Βλ. στο ίδιο πνεύμα τις ενδιαφέρουσες παρατηρήσεις του Clarke αναφορικά με την οπτική των θεωριών που μπορούν να ερμηνεύσουν το έγκλημα το οποίο συνδέεται με την χρήση της τεχνολογίας και την υποστήριξη της άποψης ότι «παραδοσιακές» εγκληματολογικές θεωρίες, οι οποίες αναζητούν τα αίτια, δεν έχουν να προσφέρουν τόσα όσα οι θεωρίες οι οποίες εστιάζουν στην κατανόηση της διενέργειας του εγκλήματος και στην αποτροπή του (*Ronald V. Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research 10: 55–63, 2004,Kluwer Academic Publishers).

[551] Βλ. σχετικά *Ευστράτιου Παπαθανασόπουλου*, Διοικητισμός και ποινικότητα, εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 723 επ. καθώς και αναφορικά με το «διαχειριστικό ιδεώδες» στην ποινική δικαιοσύνη την κριτική ανάλυση του *A. K. Bottomley*, Έγκλημα και Ποινική Δικαιοσύνη στο ξεκίνημα του 21ου αιώνα: «Αυστηροί με το έγκλημα – Αυστηροί με τα αίτια του εγκλήματος»; ΠοινΔικ 6/2002, ιδίως σελ. 643-644.

προηγουμένως στάσεις, απόψεις και θέσεις των εμπλεκομένων μερών και κυρίως των ειδικών, όπως στοχεύει η ακόλουθη έρευνα. Σε κάθε περίπτωση, πάντως, η δεύτερη δέσμη στόχων της διαχειριστικής εγκληματολογίας στους οποίους συμπεριλαμβάνεται και η ενημέρωση και εκπαίδευση των χρηστών ηλεκτρονικών διασυνδεδεμένων συσκευών (υπολογιστών κ.λπ.) μπορεί να ελεγχθεί ερευνητικά εάν και κατά πόσο προτείνεται από τα μέρη του δείγματος που ακολουθούν.

4. ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

Το ποινικό δίκαιο προσαρμοζόμενο στις εξελίξεις της πληροφορικής αντιμετώπισε την αθέμιτη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα ως αξιόποινη πράξη[552]. Ο Koops επισημαίνει ότι ειδικά με την ποινικοποίηση χρήσεων της τεχνολογίας, το ποινικό δίκαιο έχει μετατραπεί από ultimum refugium σε κυρίαρχο εργαλείο κοινωνικού ελέγχου[553]. Η επιλογή του νομοθέτη να ποινικοποιήσει την απλή πρόσβαση (χωρίς, δηλαδή, περαιτέρω επενέργεια στα ηλεκτρονικά στοιχεία, περιουσιακό όφελος ή ζημία) έχει οδηγήσει κατά καιρούς στη δημιουργία πολλών και σημαντικών αντιδράσεων[554]. Ένα εκ των βασικότερων επιχειρημάτων των αντιδράσεων αυτών είναι ότι ο νομοθέτης ποινικοποιεί ενέργειες που θα μπορούσαν να ορισθούν ως προκαταρκτικές για την τέλεση ενός εγκλήματος, προωθώντας κατ' αυτόν τον τρόπο το ποινικό δίκαιο σε χώρους και κατευθύνσεις που προηγουμένως καλύπτονταν μάλλον από το αστικό δίκαιο[555]. Κατά τον Taylor, στην περίπτωση των hackers, η ποινικοποίηση της χωρίς δικαίωμα πρόσβασης (με ή χωρίς την διάρρηξη μέτρων ασφαλείας, ανάλογα με την εκάστοτε εθνική νομοθεσία) έλαβε χώρα διότι με τις αντιλήψεις τους περί ελευθερίας της πληροφορίας (όπως αναλύθηκαν ανωτέρω)

---

[552] Η Λαμπροπούλου επισημαίνει ότι αφορμή «για την επικοινωνία δικαίου και κοινωνίας» δίνουν οι συγκρούσεις και η έγερση δικαιικών αξιώσεων (βλ. τις σχετικές αναπτύξεις της *Έφης Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 97 επ.).

[553] *Bert-Jaap Koops*, Technology and the Crime Society: Rethinking Legal Protection, TILT Law & Technology Working Paper No. 010/2009, 23 March 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 006/2009, url: http://ssrn.com/abstract=1367189.

[554] Αναφορικά με τους σχετικούς προβληματισμούς και την αναζήτηση ουσιαστικών κριτηρίων για τον προσδιορισμό της έννοιας του εγκλήματος πρβλ. *Ν. Κουράκη*, Η ουσιαστική έννοια του εγκλήματος ως έρεισμα για τη διάκριση γνησίων και μη γνησίων ποινών, εις: *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π., σελ. 70, με σχετική αναφορά στον Χωραφά κατά τον οποίο τα ουσιαστικά αυτά κριτήρια του εγκλήματος συνδέονται αναπόφευκτα με την αριστοτέλεια διασφάλιση «*κοινή συμφέροντος*».

[555] Βλ. *Γρηγόρης Λάζος*, Πληροφορική & Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2001, σελ. 106.

απείλησαν ένα από τα βασικά «δεκανίκια» του καπιταλισμού, τα δικαιώματα ιδιοκτησίας[556] [557].

4.1 Τιμώρηση είτε κατά την ωφελιμιστική είτε κατά την ανταποδοτική θεώρηση

Η ποινικοποίηση της απλής χωρίς εξουσιοδότηση ή δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή ή άλλη ψηφιακή συσκευή ή μνήμη (και με την εξέλιξη της τεχνολογίας σε σύστημα πληροφοριών) έχει δημιουργήσει έντονους προβληματισμούς ως προς το κατά πόσον βρίσκεται μέσα στα όρια των κοινωνικών αξιών και ηθικών συντεταγμένων της σύγχρονης κοινωνίας. Όπως υποστηρίζει εύστοχα η Brenda Nelson, ήδη από το 1991, η ποινική αντιμετώπιση του hacking εντείνει οριακά τις δυνατότητες του νόμου: κατά τη Nelson, «*τόσο οι ανταποδοτικές όσο και οι ωφελιμιστικές θεωρήσεις είναι χρήσιμες στο να μας βοηθήσουν να κατανοήσουμε τη σύγκρουση που προκύπτει μεταξύ δύο ομάδων αξιών, αυτών που προστατεύονται μέσω του συστήματος της ποινικής δικαιοσύνης και αυτών που σχετίζονται με τις βασικές αρχές της ελευθερίας από παρεμβάσεις, της ελεύθερης πληροφόρησης και της ελευθερίας στην έκφραση*»[558].

Σύμφωνα με την ανταποδοτική θεώρηση, η κοινωνία πάντα νομιμοποιείται να επιβάλλει ποινές σε όσους παραβιάζουν την ηθική τάξη. Ωστόσο, η θέση «*καλύτερη δράση είναι η δράση με βάση καθολικούς κανόνες*»[559] προϋποθέτει τον σαφή ορισμό της ηθικής τάξης, την οποία ο νόμος καλείται να προστατεύσει. Ήδη, όμως, έχει αναφερθεί ανωτέρω ότι «*ελλείπει –ή είναι, μάλλον, υπό διαμόρφωση– αυτή η ανεπίσημη νόρμα που απορρέει από μια δημοφιλή πεποίθηση η οποία θα αποτελέσει την "λυδία λίθο" για τον χαρακτηρισμό μιας συμπεριφοράς στο διαδίκτυο ως*

[556] *Paul Taylor*, Hackers, distributed in Computer Underground Digest Vol. 9 Issue 59, σελ. 5

[557] Βλ. στο παρόν πόνημα αναπτύξεις για την οικονομική διάσταση και αξία της ηλεκτρονικής πληροφορίας (παράγραφος 1.2) και για την κριτική εγκληματολογία (παράγραφος 3.2).

[558] Βλ. *B. Nelson*, Straining the capacity of the law: The idea of computer crime in the age of the computer worm, Computer and Law Journal, 1991, σελ. 300.

[559] Βλ. *James Rachels*, The best action is one in accord with universal rules, in: *M. D. Ermann, M.B. Williams, M. S. Schauf* (επιμ.), Computer, ethics and society, Oxford University Press, 1997, σελ. 42.

παρεκκλίνουσας»[560] λαμβάνοντας υπόψιν τη συνεχή εξέλιξη της τεχνολογίας και των συστημάτων πληροφοριών [πριν από μερικά έτη οι λειτουργίες του συμμετοχικού διαδικτύου (web 2.0)[561], πρόσφατα το «διαδίκτυο των πραγμάτων» ("internet of things" κ.ο.κ.][562].

Θα μπορούσε, ίσως, να υποστηριχθεί ότι το hacking ως συμπεριφορά είναι εκτός κρατούσας ηθικής επειδή παραβιάζει την αξιοπρέπεια αυτών που εργάσθηκαν για να παράγουν κάτι χρήσιμο για τα ηλεκτρονικά συστήματα στα οποία προσδοκούν να έχουν κάποιο έλεγχο ή επειδή το hacking παραβιάζει το δικαίωμα της ιδιωτικότητας[563], της ασφάλειας και του απορρήτου στα ηλεκτρονικά δεδομένα. Η αντίθετη όμως άποψη, μία «εναλλακτική ηθική», συνίσταται στο ότι το hacking αποτελεί έκφραση μιας βασικής ανθρώπινης παρόρμησης για γνώση και καινοτομία και για την άρνηση του αυτονόητου και του κατεστημένου.

Αλλά και η ωφελιμιστική θεώρηση κατά την οποία «*καλύτερη δράση είναι η δράση με τα καλύτερα αποτελέσματα*»[564] φαίνεται να έχει ισχυρό αντίλογο ως προς το να δικαιολογήσει απολύτως την ποινικοποίηση της εξερεύνησης των συστημάτων πληροφοριών. Η αποτροπή και η αναμόρφωση αποτελούν βασικά συστατικά της

---

[560] Βλ. *του γράφοντος*, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

Επίσης, βλ. αντίστοιχα για τις διαφορετικές προσεγγίσεις –οι οποίες αταλάντευτα συνδέονται με τα (υπό διαμόρφωση) διαδικτυακά ήθη- αναφορικά με τη νομική αντιμετώπιση του πληροφορικού εγκλήματος *Γ. Λάζου*, Πληροφορική και Έγκλημα, όπ. π., σελ. 83 επ.

Επίσης, κατά την εύστοχη διατύπωση του Κιούπη «*Λόγω της ταχύτατης εξέλιξης του διαδικτύου δεν έχουν διαμορφωθεί ακόμη καθολικά ισχύοντες και παγιωμένοι κώδικες σωστής συμπεριφοράς. Το αποτέλεσμα είναι ότι πολλές αξιόποινες πράξεις που τελούνται στο διαδίκτυο (ίσως οι λιγότερο σοβαρές) δεν φορτίζονται αρνητικά με την ηθική απαξία που θα είχαν αντίστοιχες συμπεριφορές στον φυσικό κόσμο. Οι ηθικές / αξιολογικές αναστολές είναι ακόμη λιγότερες, καθώς οι περισσότεροι δράστες είναι νεαρής ηλικίας και και δεν έχουν (ακόμη) εγκολπωθεί βασικές αξιακές επιλογές "της κοινωνίας των μεγάλων" ή ανήκουν σε κάποιες μικρές μειοψηφίες φανατικών χρηστών των υπολογιστών, οι οποίοι δρουν αποκλειστικά στον αξιολογικά ουδέτερο χώρο που ορίζουν οι τεχνικές παράμετροι του Internet.*» (έτσι *Δημ. Κιούπης*, Ποινικό Δίκαιο και Internet, όπ. π., σελ., 122).

[561] Βλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013, σελ. 4.

[562] Βλ. σχετικές αναπτύξεις στην παράγραφο 1.1 του παρόντος πονήματος.

[563] Ο Δαγτόγλου υποστηρίζει χαρακτηριστικά ότι «*Χωρίς ιδιωτική σφαίρα το άτομο χάνει την ατομικότητά του και μετατρέπεται σε ανώνυμο και άβουλο ποσοστό του συνόλου. Είναι λογικώς επόμενο, ότι τα ολοκληρωτικά καθεστώτα περιορίζουν σημαντικά και σε πολλές περιπτώσεις αίρουν την ιδιωτική σφαίρα του ατόμου.*» (Π. Δ. Δαγτόγλου, Ατομικά Δικαιώματα, τομ. Α', εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1991, σελ. 320).

[564] Σύμφωνα με τον *John Hospers* "*The best action is the one with the best consequences*" (*John Hospers*, Utilitarian theory, εις: *M. David Ermann, Mary B. William & Claudio Gutierrez*, Computer, ethics and society, Oxford University Press, Inc. New York, NY, USA, 1990, σελ. 33).

ωφελιμιστικής θεώρησης. Ο νόμος φαίνεται να έχει τη δυνατότητα να προσφέρει μία ειδική αποτροπή σε σχέση με το hacking αλλά και μία γενική αποτροπή που οδηγεί σε μία τακτική συμπεριφορά με βάση τον νόμο. Όμως, οι επικριτές της αποτροπής αμφιβάλλουν ως προς το κατά πόσον η τιμωρία πραγματικά αποτρέπει το έγκλημα[565]. Επίσης, οι επικριτές της αναμόρφωσης, στηριζόμενοι κυρίως στα υψηλά ποσοστά υποτροπής, αμφισβητούν τον αναμορφωτικό χαρακτήρα της ποινής[566] [567] [568].

Σύμφωνα, λοιπόν, με την ανωτέρω άποψη, ούτε η ανταποδοτική ούτε η ωφελιμιστική επιχειρηματολογία προσφέρουν σαφή νομιμοποίηση για την επιβολή ποινικών κυρώσεων σε βάρος των hackers. Με βάση τις προηγούμενες διαπιστώσεις, η Brenda Nelson έρχεται να καταθέσει τη δική της σύνθετη άποψη σε ό,τι αφορά στην αντιμετώπιση του hacking τονίζοντας ότι «*ένας νόμος που επιτρέπει την τιμωρία του hacker ως εγκληματία υπάρχει ως ανωμαλία στο ποινικό σύστημα ως όλο*». Θεωρεί, δε, ότι ο νόμος πρέπει να στηρίζεται σε μία αρετή αυτοσυγκράτησης, όπως αυτή εκφράζεται από τις περιοριστικές αρχές *mens rea* και *actus reus*. Προκειμένου, δε, να εξασφαλίσει το κύρος και τη νομιμότητά του, ο νόμος σε σχέση με το hacking πρέπει να προχωρήσει σε εκτεταμένη χρήση της αυτοσυγκράτησης[569].

4.2 Οι hackers και ο ποινικός νόμος

Το hacking αποτελεί ενδιαφέρον μιας μερίδας ατόμων ή ομάδων με κοινή (υπο)κουλτούρα με κοινές αρχές και επικοινωνιακούς κώδικες, όπως αναλύεται

[565] Στην έρευνα που ακολουθεί θα ανιχνευθεί μεταξύ άλλων σε πεδίο αυτοομολογούμενης παραβατικότητας και η ένταση της αποτρεπτικής λειτουργίας της ελληνικής ποινικής νομοθεσίας σε έλληνες hackers.

[566] Ειδικά για το ηλεκτρονικό έγκλημα βλ. *Γρηγόρης Λάζος*, Πληροφορική & Έγκλημα, όπ. π., σελ. 108 και *Ειρ. Βασιλάκη*, Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής τους καταστολής – Προετοιμάζοντας το ποινικό δίκαιο του 21ου αιώνα;, εις: *Ν. Κουράκη* (εκδ. επιμ.), Αντεγκληματική πολιτική ΙΙ, σειρά «Ποινικά», αρ. 59, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή 2000, σελ. 31.

[567] Προς αυτήν την κατεύθυνση και η θεώρηση του *Michael Jacobson*, Reply to Kevin D. Haggerty, Theoretical Criminology, 2004, SAGE Publications, London, Thousand Oaks and New Delhi, Vol. 8(2): 233–238; 1362–4806, αναφορικά με την αύξηση στο μέλλον της χρήσης εναλλακτικών της φυλάκισης ποινών, οι οποίες θα συνδράμουν στη μείωση της υποτροπής.

[568] Αναφορικά με την «υποχώρηση» του «αναμορφωτικού ιδεώδους» πρβλ. *Ν. Κουράκη*, Εισαγωγή στη θεωρία της ποινής, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 32.

[569] Βλ. *B. Nelson*, Straining the capacity of the law: The idea of computer crime in the age of the computer worm, όπ. π., σελ. 301.

ανωτέρω[570]. Στο σύνολό τους, οι νομοθετικές ρυθμίσεις που αφορούν στο hacking δεν εστιάζουν την προσοχή τους στους hackers ως κοινωνική κατηγορία ή ως άτομα που εκδηλώνουν περιφρόνηση για τον νόμο και την κατεστημένη κοινωνία αλλά στη hack-ιστική συμπεριφορά από τεχνοκοινωνική σκοπιά, κυρίως λόγω του ότι – και στο βαθμό που – αποτελεί τη βασικότερη προϋπόθεση για τη διάπραξη μιας σειράς πληροφορικών εγκλημάτων. Ουσιαστικά, η μεγαλύτερη μερίδα πληροφορικών εγκλημάτων έχουν ως πρώτο βήμα κατά την τέλεσή τους την πρόσβαση χωρίς εξουσιοδότηση σε ηλεκτρονικά δεδομένα[571]. Ωστόσο, καταγράφονται περιστατικά κατά τα οποία εσφαλμένως κινήθηκαν ποινικές διαδικασίες εναντίον hackers – ως αποτέλεσμα, έχει σε ορισμένες περιπτώσεις υπονομευθεί το κύρος των διωκτικών αρχών και έχει δοθεί στους hackers σοβαρό επιχείρημα αναφορικά με το ότι έχουν παρεξηγηθεί οι δραστηριότητές τους[572].

Ο νομικός ορισμός του hacking ως εγκλήματος, σε συνδυασμό με την απόδοση στερεοτύπων και την ετικετοποίηση των hackers από μέρος των ΜΜΕ[573], φαίνεται να επιδρά και στον τρόπο σκέψης και δράσης των hackers, στον τρόπο που οι τελευταίοι σχετίζονται με την ευρύτερη κοινωνία αλλά και μεταξύ τους καθώς και στον τρόπο που συγκροτούν την κοινότητά τους στο διαδίκτυο[574]. Η εγκληματοποίηση είναι πολύ πιθανό ότι πέτυχε να αποτρέψει μία ίσως σημαντική μερίδα νέων από την υιοθέτηση hack-ιστικών (καινοτομιστικών) αρχών και μεθόδων δράσης στον τρόπο ζωής τους. Από την άλλη πλευρά, συνέβαλε στη βελτίωση των μεθόδων δράσης των hackers ώστε να είναι δύσκολος ο εντοπισμός τους από τις διωκτικές αρχές. Η επίθεση διωκτικών αρχών, ιδεολογικών μηχανισμών του κράτους και ΜΜΕ εναντίον του hacking πιθανότατα άλλαξε ως ένα βαθμό την αντίληψη των hackers για την κοινωνία στην οποία ζουν, τη διεύρυνε και συγχρόνως της προσέθεσε ριζοσπαστικά

---

[570] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 2 και συγκεκριμένα στην παράγραφο 2.8 του παρόντος πονήματος.

[571] *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 409.

[572] Βλ. *Steven Furnell*, όπ. π., σελ. 275-280.

[573] Βλ. αναπτύξεις για τους ηθικούς πανικούς σε συνάρτηση με τα ΜΜΕ σε σχετική υποσημείωση στην παράγραφο 7.3.1.5 του παρόντος πονήματος.

[574] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 3 για τη θεωρία της ετικέτας αλλά και το γεγονός ότι ο όρος cracker δημιουργήθηκε από τους hackers προκειμένου να διαχωριστούν με αφορμή την υπερβολική και εσφαλμένη χρήση του όρου hacker από τους δημοσιογράφους! [*Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 9 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf)].

και αντικαθεστωτικά στοιχεία[575]. Μία άλλη επίπτωση είναι ότι μερικοί hackers οδηγήθηκαν και οδηγούνται στην αποδοχή του στερεότυπου του εγκληματία[576].

Τέλος, οι Duff και Gardiner στέκονται ενάντια στην ποινικοποίηση του hacking καθώς υποστηρίζουν ότι η ποινικοποίηση της μη εξουσιοδοτημένης πρόσβασης σε συστήματα ηλεκτρονικών υπολογιστών και του "hacking" αποτελεί ακόμη ένα βήμα στη διαδικασία για την επαύξηση της επιτήρησης[577].

4.3 Ειδικές προβληματικές του ποινικού δικαίου σχετικά με το hacking

Πέρα από την ποινικοποίηση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking, θα αναφερθούμε πρώτα ενδεικτικά σε δύο ειδικότερα σχετικά με το hacking ζητήματα[578], όπως ο ακριβής προσδιορισμός του τόπου τέλεσης σε συνδυασμό με την παραβίαση ή μη της θεμελιώδους αρχής *ne bis in idem* καθώς και ο καθορισμός των ορίων της ποινικής ευθύνης του παρόχου της πρόσβασης στο διαδίκτυο.

4.3.1 Τόπος τέλεσης του hacking και αρχή ne bis in idem

Καταρχάς, ζήτημα τίθεται όσον αφορά τον τόπο τέλεσης του εγκλήματος της απομακρυσμένης χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, όταν π.χ.

[575] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38 όπου καταγράφεται η αντίθεση των hackers κατά του status quo.

[576] Βλ. *Γρηγόρης Λάζος*, Πληροφορική & Έγκλημα, όπ. π., σελ. 105.

[577] *Orly Turgeman-Goldschmidt*, Between Hackers and White-Collar Offenders, όπ. π., όπως παραπέμπει στους Duff και Gardiner.

[578] Αναφορικά με σχετικούς προβληματισμούς βλ. και το άρθρο του *K Vishnu Konoorayar*, Regulating Cyberspace: The Emerging Problems and Challenges, Cochin University Law Review, 2003, pp. 413-435.

αυτή τελείται μέσω της χρήσης διαδικτύου (unauthorized remote access)[579] (σε συνάρτηση με τον εφαρμοστέο κανόνα δικαίου και το αρμόδιο δικαστήριο[580]). Το γεγονός, μάλιστα, ότι η πλειονότητα των hackers χρησιμοποιεί το διαδίκτυο ως κύριο εργαλείο προκειμένου να αποκτήσει πρόσβαση σε ξένα πληροφορικά συστήματα καθιστά αυτομάτως εντονότερη την προβληματική σχετικά με τον προσδιορισμό του τόπου τέλεσης του σχετικού εγκλήματος[581] και με δεδομένο ότι κατά την εύστοχη διατύπωση του Αγγελή «*...όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ τους ολόκληρος ο πλανήτης αποτελεί "μία χώρα"»*[582].

Η ρύθμιση για τον τόπο τέλεσης του εγκλήματος της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, όταν αυτή τελείται μέσω διαδικτύου, δικαιολογημένα απασχολεί ως πρόβλημα που, κατά την Καϊάφα-Γκμπάντι, δεν έχει βρει ακόμη την αξιόπιστη λύση του[583]. Ειδικότερα, η ύπαρξη ενός πολύ μεγάλου αριθμού τόπων τέλεσης, οι οποίοι προσδιορίζονται από την ενέργεια του δράστη – hacker, τη ροή της πληροφορίας μέσω του διαδικτύου και τους πλείονες του ενός τόπους επέλευσης του εγκληματικού αποτελέσματος, είναι ικανή να αποτελέσει βάση δικαιοδοσίας για τη δίωξη του hacking σε αντίστοιχα μεγάλο αριθμό κρατών[584] με αντίστοιχα διαφορετικές εθνικές νομοθεσίες. Ταυτόχρονα τίθεται ζήτημα παραβίασης ή μη της αρχής *ne bis in idem*, σύμφωνα με την οποία κανείς δεν πρέπει να διώκεται ή να δικάζεται δύο φορές για τις ίδιες πράξεις, πραγματικά περιστατικά ή συμπεριφορά[585].

---

[579] Βλ. σχετικές προσεγγίσεις αναφορικά και με την άσκηση ποινικής δίωξης αλλά τη δικαστική συνεργασία κρατών στο πόνημα του *Peter Grabosky*, Requirements of prosecution services to deal with cyber crime, Crime Law Soc Change (2007) 47: 201-223.

[580] Βλ. τις σχετικές αναπτύξεις του *Γ. Γιαννόπουλου*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 31 και 37 επ.

[581] Αναφορικά με τη διεθνή δικαιοδοσία στο διαδίκτυο σε επίπεδο ιδιωτικού διεθνούς δικαίου πρβλ. *Θεόδωρος Σιδηρόπουλος*, Το δίκαιο του διαδικτύου, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2008, β' έκδ., σελ. 133 επ.

[582] *Ιωάν. Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 12/2001, 1299.

[583] Βλ. *Μ. Καϊάφα – Γκμπάντι*, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμενόπουλος 2007, σελ. 1059-1060.

[584] Βλ. *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, Ποινικά υπ' αρ. 57, Εκδόσεις Αντ. Σάκκουλα, Αθήνα – Κομοτηνή 1999, σελ. 75.

[585] Η αρχή *ne bis in idem* κατοχυρώνεται ως ατομικό δικαίωμα στα διεθνή νομικά κείμενα των ανθρώπινων δικαιωμάτων, όπως ενδεικτικά στο Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (άρθρο 14, παράγραφος 7) της 19ης Δεκεμβρίου 1966, στο έβδομο πρωτόκολλο (άρθρο 4) της Σύμβασης για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών και στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (άρθρο 50). Αναγνωρίζεται, δε, από όλα τα νομικά συστήματα που διαπνέονται από την ιδέα σεβασμού και προστασίας των θεμελιωδών δικαιωμάτων και αποτελεί ουσιαστική θωράκιση έναντι της καταχρηστικής άσκησης των κρατικών εξουσιών επί των πολιτών.

Ο Καράκωστας παρουσιάζει στο πόνημά του θεωρίες αναφορικά με τον καθορισμό του τόπου τελέσεως του αδικήματος αναφορικά με συμπεριφορές στο διαδίκτυο[586] – «*στην περίπτωση αδικήματος πολλαπλής τοπικής σύνδεσης*», όπως αναφέρει – και προκρίνει, ως φαίνεται, την «θεωρία του βαρύνοντος τόπου» σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος στο οποίο εκδηλώνεται κατά την κύρια σημασία του. Αναγνωρίζει, βέβαια, τις δυσκολίες στον καθορισμό αυτού του βαρύνοντος τόπου, ο οποίος δύναται επί της ουσίας να είναι ο τόπος εισαγωγής των ζημιογόνων δεδομένων, ο τόπος όπου είναι εγκατεστημένος ο server, ο τόπος που έχει την κατοικία του ή την έδρα του ο δράστης, ο τόπος όπου κατοικεί ή συνήθως διαμένει ο ζημιωθείς κ.ά.

Όλως προσφάτως, ο έλληνας νομοθέτης, προσπαθώντας να επιλύσει τα ανωτέρω ζητήματα που ανακύπτουν από την τέλεση πράξεων μέσω διαδικτύου, με το ά. 2 του ν. 4267/2014 προέβη στην προσθήκη τρίτης παραγράφου στο άρθρο 5 του ελληνικού ποινικού κώδικα κατά την οποία «*Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους*». Η διατύπωση της διάταξης αυτής με μια πρώτη ματιά κρίνεται τουλάχιστον άτεχνη καθώς, σύμφωνα με τη γραμματική της ερμηνεία, φαίνεται η ελληνική επικράτεια ως τόπος τέλεσης όλων ανεξαιρέτως των πράξεων που τελούνται μέσω διαδικτύου ανά την υφήλιο αφού στην Ελλάδα παρέχεται πρόσβαση στο διαδίκτυο. Η διάταξη αυτή, δηλαδή, δεν αναφέρεται έστω στα επίδικα δεδομένα αλλά ορίζει ότι από τη στιγμή που στην Ελλάδα υπάρχει πρόσβαση στο μέσο επικοινωνίας (π.χ. διαδίκτυο) τότε εφαρμόζονται οι ελληνικοί ποινικοί νόμοι, μολονότι δεν έχει υπάρξει καμία επενέργεια της πράξης σε ελληνικό έδαφος, σε έλληνα πολίτη, σε μέσο εγκατεστημένο και διαχειριζόμενο καθοιονδήποτε τρόπο στην Ελλάδα κ.λπ. Η διάταξη αυτή διευρύνει υπερβολικά την ποινική δικαιοδοσία, σε τέτοιο βαθμό μάλιστα κατά τον οποίο η ελληνική δικαιοσύνη δύναται να καταστεί αντικείμενο forum shopping, καθώς σε επίπεδο αρμοδιότητας θα μπορεί π.χ. να ασχοληθεί με κάποιον βιετναμέζο, κάτοικο Ιαπωνίας, ο οποίος από τον υπολογιστή του σπιτιού του στην Ιαπωνία απέκτησε χωρίς δικαίωμα πρόσβαση σε δεδομένα ενός υπολογιστή στην Αργεντινή μέσω του διαδικτύου, χρησιμοποιώντας server

[586] Βλ. αναλυτικότερα *Ι. Καράκωστας*, Δίκαιο & Ίντερνετ, Νομικά ζητήματα του διαδικτύου, εκδ. Π. Ν. Σάκκουλα, 3η εκδ., Αθήνα 2009, σελ. 265-267.

εγκατεστημένο στις Η.Π.Α.! Για την εν λόγω διάταξη εκτιμώ πως θα εκφραστεί σφοδρή κριτική οσονούπω.

4.3.2 Ποινική ευθύνη ή μη του παρόχου πρόσβασης

Με το hacking μέσω διαδικτύου σχετίζεται, επίσης, το θέμα της τυχόν ποινικής ευθύνης των παρόχων πρόσβασης στο διαδίκτυο για αξιόποινες πράξεις που τελούνται από τους χρήστες των υπηρεσιών τους, εν προκειμένω για την πράξη της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα από τους hackers[587]. Στο παρόν σημείο πρέπει να διευκρινιστεί ότι η έκφραση «ποινική ευθύνη των παρόχων πρόσβασης» χρησιμοποιείται για λόγους συντομίας, αφού το ελληνικό ποινικό δίκαιο είναι αυστηρά προσανατολισμένο στην απονομή ποινικής ευθύνης με το κλασικό πρότυπο της ατομικής ενοχής, πράγμα που σημαίνει ότι ποινική ευθύνη έχουν μόνο τα φυσικά πρόσωπα[588] [589].

Οι πάροχοι πρόσβασης στο διαδίκτυο αποτελούν τους ενδιάμεσους σταθμούς μεταξύ των χρηστών παγκοσμίως και, ουσιαστικά, τους κεντρικούς διαύλους διεξαγωγής αυτής της παγκόσμιας επικοινωνίας, που χρησιμοποιούν στις περιηγήσεις τους οι μεμονωμένοι χρήστες. Γενικότερα για τις περιπτώσεις ευθύνης των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας[590], ο έλληνας νομοθέτης οριοθέτησε τα ανακύπτοντα ζητήματα με το Π.Δ. 131/2003 σε προσαρμογή της Οδηγίας 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (Οδηγία για το ηλεκτρονικό εμπόριο). Στο εν λόγω προεδρικό διάταγμα, βέβαια, δεν προβλέπονται ποινικές ευθύνες αλλά στο α. 19

[587] Αναφορικά με την έννοια του παρόχου πρβλ. *Θ. Σιδηρόπουλο*, Το δίκαιο του διαδικτύου, όπ. π., σελ. 155 επ.

[588] Βλ. ενδεικτικά *Αγάπιος Αν. Παπανεοφύτου*, Ποινική ευθύνη των νομικών προσώπων ή των υπολόγων για τη δράση τους φυσικών προσώπων; εις: Ποινικό Δίκαιο-Ελευθερία-Κράτος Δικαίου, Τιμητικός Τόμος για τον Γ. Α. Μαγκάκη, Εκδόσεις Αντ. Ν. Σάκκουλα 1996, σελ. 204.

[589] Ο Μυλωνόπουλος επισημαίνει ότι στην Ευρώπη το αξιόποινο των νομικών προσώπων αναγνωρίζεται ευρέως και ότι η Γερμανία και η Ελλάδα συνιστούν μειοψηφία. Αναλυτικά για την προβληματική αυτή βλ. τις πολύ ενδιαφέρουσες αναπτύξεις του εις *Χρ. Μυλωνόπουλου*, Το Ευρωπαϊκό Ποινικό Δίκαιο μετά τη Συνθήκη της Λισαβόνας, ΠοινΧρ ΞΑ/2011, σελ. 87.

[590] Βλ. σχετικά και αναλυτικά *Γ. Γιαννόπουλος*, Η ευθύνη των παρόχων υπηρεσιών στο internet, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013.

διαλαμβάνεται ότι «*Οι παραβάτες των διατάξεων του παρόντος Π.Δ. τιμωρούνται με τις προβλεπόμενες στην παραγρ. 3 του άρθρου 14 του Ν. 2251/94 (ΦΕΚ Α/191) κυρώσεις, καθώς και με τις κυρώσεις που προβλέπονται στον Αγορανομικό Κώδικα όπως αυτός ισχύει*».

Υποστηρίζεται ότι δεν μπορεί με βάση τις κείμενες ελληνικές διατάξεις να θεμελιωθεί πειστικά ποινική ευθύνη των παρόχων πρόσβασης στο διαδίκτυο για τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Για τη χάραξη των ορίων ευθύνης τους και τον καθορισμό συγκεκριμένων υποχρεώσεών τους απαιτείται νομοθετική παρέμβαση περιεχομένου ανάλογου με όσα ισχύουν για άλλα τηλεπικοινωνιακά μέσα με την απαραίτητη επισήμανση της τεχνικής πρωτοτυπίας του διαδικτύου[591]. Ταυτόχρονα, όμως, είναι αναγκαίο να διαφυλαχθεί και να κατοχυρωθεί η όσο το δυνατόν μεγαλύτερη ελευθερία στο διαδίκτυο, το οποίο αποτελεί ένα εξαιρετικό forum ανταλλαγής ιδεών, γνώσεων, πληροφοριών και έκφρασης του ατόμου[592]. Εξάλλου, και κατά τον Σιδηρόπουλο, η επιβολή (στους παρόχους) της υποχρέωσης άμεσης απόσυρσης ή απενεργοποίησης της πρόσβασης σε πληροφορίες ή δραστηριότητες, που φέρονται να έχουν παράνομο περιεχόμενο, συνεπάγεται αμέσως την επιφόρτιση των παρόχων με αρμοδιότητες δικαστικής φύσεως, γεγονός το οποίο το δίχως άλλο δημιουργεί προβλήματα[593].

---

[591] Διάταξη από την οποία προβλέπεται ευθύνη εκπροσώπων ή εργαζομένων σε νομικό πρόσωπο για σχετικά ζητήματα είναι αυτή του ά. 11 παρ. 2 του ν. 3917/2011 (ΦΕΚ 22/Α/21.2.2011) για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις και έχει ως εξής:

> «*2. Αν ο δράστης των πράξεων της παραγράφου 1 είναι νόμιμος εκπρόσωπος ή μέλος της διοίκησης ή υπεύθυνος ασφάλειας δεδομένων ή εργαζόμενος ή συνεργάτης του παρόχου ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε σε οικονομικό ή άλλο αντάλλαγμα, τιμωρείται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από 55.000 μέχρι 200.000 ευρώ.*»

Η, δε, παράγραφος 1 στην οποία παραπέμπει η παράγραφος 2 έχει ως εξής:

> «*1. Όποιος, κατά παράβαση των διατάξεων του παρόντος κεφαλαίου, λαμβάνει γνώση των δεδομένων που διατηρούνται από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών, τα συλλέγει, αποθηκεύει, αντιγράφει, αφαιρεί, μεταφέρει, αλλοιώνει, βλάπτει, καταστρέφει, μεταδίδει, ανακοινώνει ή με άλλο τρόπο τα επεξεργάζεται, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με κάθειρξη μέχρι δέκα ετών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.*»

Βλ. στο επόμενο κεφάλαιο του παρόντος πονήματος σχετική ανάλυση της τελευταίας διάταξης.

[592] Βλ. *Δημήτρης Κιούπης*, Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet, ΠοινΧρ ΜΗ/1998, σελ. 720.

[593] Έτσι *Θ. Σιδηρόπουλος*, Το δίκαιο του διαδικτύου, όπ. π. σελ. 160-161.

4.4 Επισκόπηση εννόμων τάξεων αναφορικά με το hacking

Η ιδιαίτερη αξία που απέκτησε η ηλεκτρονική πληροφορία και το γεγονός ότι οι πρακτικές hacking χρησιμοποιούνται πλέον για πράξεις κυβερνοτρομοκρατίας[594], cyber bullying κ.ά. οδήγησε τις νομοθεσίες να ανταποκριθούν με νέες διατάξεις για την ποινικοποίηση πράξεων όπως η διαγραφή ή η με οποιοδήποτε τρόπο επέμβαση σε ηλεκτρονικά δεδομένα και ακόμη και η απλή απόκτηση πρόσβασης σε στοιχεία υπολογιστή[595].

4.4.1 Ελλάδα

4.4.1.1 Ο νόμος 1805/1988

Στην Ελλάδα τα ποινικά ζητήματα όσον αφορά στη χρήση υπολογιστών και διαδικτύου αντιμετωπίστηκαν κυρίως από τον νόμο 1805/1988, ο οποίος, βασισμένος σε γερμανικά πρότυπα, θέσπισε σημαντικές διατάξεις όπως το άρθρο 370Β και 370Γ ΠΚ που αφορούν τη παράνομη αντιγραφή και παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών καθώς και το 386Α που έχει ως αντικείμενο την απάτη με υπολογιστή[596]. Αναλυτικότερα, ο νόμος 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes). Μολονότι έχουν περάσει πάνω από 25 χρόνια από την ψήφιση του

[594] Βλ. και παράγραφο 2.3.3 αναφορικά με τους κυβερνοτροοκράτες.

[595] Αναφορικά με νομοθεσίες σχετικές με χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα και γενικότερα εγκλήματος μέσω υπολογιστή βλ. τον αναλυτικό πίνακα στο πόνημα των *Kim-Kwang Raymond Choo, Russell G. Smith & Rob McCusker*, Future directions in technology-enabled crime: 2007–09, Research and Public Policy Series No 78, Australian Institute of Criminology, pp. 73-74.

[596] Βλ. *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες. Β΄: Πραγματολογική προσέγγιση και επιμέρους ζητήματα, Δεύτερη Ανανεωμένη Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ. 188, *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, Ποινικά υπ' αρ. 57, Εκδόσεις Αντ. Σάκκουλα, Αθήνα – Κομοτηνή 1999 και *Χρήστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Εκδόσεις Σάκκουλας, 1991.

εν λόγω νόμου και, σε μια πρώτη θεώρηση, θα μπορούσε κάποιος να υποστηρίξει ότι είναι αναχρονιστικός – λαμβάνοντας υπόψιν τους ραγδαίους ρυθμούς με τους οποίους εξελίσσεται η τεχνολογία και πιο συγκεκριμένα το διαδίκτυο –, οι διατάξεις αυτές έχουν συνταχθεί με προοπτικές προσαρμοστικότητας στα νέα δεδομένα που τυχόν θα παρουσιάζονταν. Επομένως, στην περίπτωση που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου, τότε τα άρθρα αυτά εφαρμόζονται και στις περιπτώσεις αυτές. Η εξέλιξη, ωστόσο, των ηλεκτρονικών εγκλημάτων έχει καταστήσει τις διατάξεις αυτές σε ορισμένες περιπτώσεις ανεπαρκείς[597] και με αναπόφευκτες αλληλεπικαλύψεις με μεταγενέστερες διατάξεις.

Ειδικότερα, αναφορικά με τους hackers και την πρόσβαση που μπορεί να αποκτήσουν σε δεδομένα ισχύει το ά. 370Γ παρ. 2 η οποία τιμωρεί την χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα[598]. Για πράξεις πέραν της πρόσβασης όπως η αντιγραφή, η χρήση, η αποκάλυψη σε τρίτον στοιχείων ή προγραμμάτων υπολογιστών που συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα ισχύει το άρθρο 370Β[599].

[597] Ενδεικτικά, δεν υπάρχει ακόμη και σήμερα στο ελληνικό ποινικό δίκαιο διάταξη για την αλλοίωση ηλεκτρονικών δεδομένων παρά το ότι προβλέπεται η ύπαρξη τέτοιας στο ά. 4 της Σύμβασης του Συμβουλίου της ευρώπης για το έγκλημα στον Κυβερνοχώρο (βλ. κατωτέρω παράγραφο 6.2.2). Ο Κιούπης αποδίδει την έλλειψη αυτή στο γεγονός ότι ο έλληνας νομοθέτης δεν είχε συνειδητοποιήσει τις διαστάσεις του προβλήματος [βλ. σχετικά *Δημ. Κιούπης*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 422-423].

[598] Σύμφωνα με τις παρ. 2, 3 και 4 του ά. 370 Γ ΠΚ

> *«2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) ΕΥΡΩ" [10.000 δρχ.]*. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.*
>
> *3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.*
>
> *4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.»*

[599] Σύμφωνα με την παρ. 1 ά. 370Β ΠΚ

> «*1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.»*

4.4.1.2 Το άρθρο 4 του νόμου 2246/1994

Στη συνέχεια και ιδίως αναφορικά με την προστασία του περιεχομένου της επικοινωνίας και για την τιμώρηση πράξεων οι οποίες στρέφονται εναντίον των πληροφοριών που μεταβιβάζονται διά τηλεπικοινωνιακών συστημάτων εισήχθη στην ελληνική έννομη τάξη το άρθρο 4 του νόμου 2246/1994[600]. Στο εν λόγω άρθρο επιδιώκεται η προστασία μιας ευρείας γκάμας αγαθών (εχεμύθεια, σεβασμός της ιδιωτικής ζωής, τήρηση του απορρήτου και διαφύλαξη της πνευματικής ιδιοκτησίας του περιεχομένου των μηνυμάτων και δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων) που ο νομοθέτης διείδε την περίοδο εκείνη ότι «απειλούνται» από την εξέλιξη της πληροφορικής επιστήμης. Πιστεύω ότι η γενική διατύπωση της διάταξης αυτής, ιδίως σε περιπτώσεις χωρίς δικαίωμα πρόσβασης, την καθιστά εξ ορισμού ανεφάρμοστη[601] ένεκα της αρχής της ειδικότητας, κατά την οποία οι ακόλουθες διατάξεις, και ιδίως η διάταξη του ά. 370Γ παρ. 2 ΠΚ, κατά περίπτωση υπερισχύουν.

4.4.1.3 Ο νόμος 3674/2008 και η εισαγωγή του άρθρου 292Α ΠΚ

Με το άρθρο 13 ν. 3674/2008[602] προβλέπεται η κατάρτιση Εθνικού Σχεδίου Ασφαλείας Επικοινωνιών (ΕΣΑΕ) ως προς τις κρίσιμες υποδομές των επικοινωνιών

---

[600] Συγκεκριμένα, στις παραγράφους 2 και 3 του ά. 4 ν. 2246/1994 ορίζεται ότι

> «*2. Όποιος με οποιονδήποτε τρόπο παραβαίνει τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής, τήρησης του απορρήτου και διαφύλαξης της πνευματικής ιδιοκτησίας του περιεχομένου των μηνυμάτων και δεδομένων, που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων, που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο (2) ετών και χρηματική ποινή πέντε εκατομμυρίων (5.000.000) έως είκοσι εκατομμυρίων (20.000.000) δραχμών, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις. Σε περίπτωση που ο παραβάτης της παρούσας διάταξης ανήκει στο προσωπικό τηλεπικοινωνιακής επιχείρησης, η επιβαλλομένη ποινή φυλάκισης είναι τουλάχιστον τριών (3) ετών και η χρηματική ποινή τουλάχιστον δέκα εκατομμύρια (10.000.000) δραχμές.*
>
> *3. Ο τεχνικός εξοπλισμός και τα μέσα που χρησιμοποιήθηκαν για την τέλεση των παραπάνω αξιοποίνων πράξεων κατάσχονται και δημεύονται.»*

[601] Για αυτόν τον λόγο και δεν θα λάβει χώρα περαιτέρω ανάλυση στο πλαίσιο της παρούσας διατριβής.

[602] Άρθρο 13 - «Εθνικό σχέδιο ασφάλειας ηλεκτρονικών επικοινωνιών»:

> «*1. Το εθνικό σχέδιο ασφάλειας των επικοινωνιών (ΕΣΑΕ) καταρτίζεται με σκοπό την αποτελεσματική θωράκιση των υποδομών και μέσων στον τομέα των ηλεκτρονικών*

της χώρας, για την περίπτωση διακινδύνευσης της ασφάλειας των επικοινωνιών από οποιαδήποτε επίθεση[603] και με το ά. 9 παρ. 3 του ίδιου νόμου προστέθηκε στον ελληνικό Ποινικό Κώδικα το ά. 292Α [604]. Το εν λόγω άρθρο, το οποίο έχει τίτλο:

επικοινωνιών. Στο ΕΣΑΕ περιλαμβάνονται ιδίως τα όργανα, οι στόχοι, οι γενικές αρχές και κατευθύνσεις, τα πρότυπα, τα μέσα, οι κίνδυνοι που έχουν αναγνωριστεί, τα μέτρα οργανωτικού και εκπαιδευτικού χαρακτήρα, οι υποχρεώσεις για την ενημέρωση του κοινού, οι κυρώσεις και εν γένει οι κανόνες, οι οποίοι διέπουν την πολιτική ασφάλειας για τις ηλεκτρονικές επικοινωνίες των δημόσιων υπηρεσιών, των Ν.Π.Δ.Δ., των επιχειρήσεων του ευρύτερου δημόσιου τομέα και των παροχών δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών.

2. Το ΕΣΑΕ εγκρίνεται και αναθεωρείται με προεδρικό διάταγμα ύστερα από πρόταση των Υπουργών Εσωτερικών, Οικονομίας και Οικονομικών, Εξωτερικών, Εθνικής Άμυνας, Ανάπτυξης, Δικαιοσύνης, Μεταφορών και Επικοινωνιών, Εμπορικής Ναυτιλίας, Αιγαίου και Νησιωτικής Πολιτικής.

3. Οι δημόσιες υπηρεσίες, τα Ν.Π.Δ.Δ., τα νομικά πρόσωπα του δημόσιου τομέα που λειτουργούν με τη μορφή Ν.Π.Ι.Δ. και οι πάροχοι δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούνται να προσαρμόζουν τις πολιτικές ασφάλειας που εφαρμόζουν για την προστασία των ηλεκτρονικών επικοινωνιών στις αρχές και κατευθύνσεις του ΕΣΑΕ το αργότερο εντός έξι (6) μηνών από την έγκριση του. Οι πολιτικές ασφάλειας και τα ειδικά σχέδια που εφαρμόζονται από ορισμένες ή όλες τις υπηρεσίες των Υπουργείων Εσωτερικών, Οικονομίας και Οικονομικών, Εξωτερικών, Εθνικής Άμυνας, Εμπορικής Ναυτιλίας, Αιγαίου και Νησιωτικής Πολιτικής, δύνανται να εξαιρούνται από την υπαγωγή τους στο ΕΣΑΕ.

4. Συνιστάται ειδική νομοπαρασκευαστική επιτροπή με σκοπό την κατάρτιση του ΕΣΑΕ. Η επιτροπή συγκροτείται με απόφαση του Υπουργού Μεταφορών και Επικοινωνιών, είναι εννεαμελής και αποτελείται από ανώτατο δικαστικό λειτουργό ή καθηγητή Α.Ε.Ι., εν ενεργεία ή μη, ως Πρόεδρο, από υπαλλήλους της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης και της Γενικής Γραμματείας Δημόσιας Τάξης του Υπουργείου Εσωτερικών, της Γενικής Γραμματείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομίας και Οικονομικών, της Γενικής Γραμματείας Ερευνας και Τεχνολογίας του Υπουργείου Ανάπτυξης, της Γενικής Γραμματείας Επικοινωνιών του Υπουργείου Μεταφορών και Επικοινωνιών, της ΑΠΔΠΧ, της ΑΔΑΕ και της ΕΕΤΤ ως μέλη. Με την ίδια απόφαση ορίζεται ως γραμματέας της επιτροπής υπάλληλος του Υπουργείου Μεταφορών και Επικοινωνιών ή δικηγόρος. Για τις πολιτικές ασφαλείας και τα ειδικά σχέδια που εφαρμόζονται από κάθε Υπουργείο, δημόσια υπηρεσία, Ο.Τ.Α., Περιφέρειες και Ν.Π.Δ.Δ., που είναι αποδέκτες εθνικού ή συμμαχικού διαβαθμισμένου υλικού, όπως το υλικό αυτό ορίζεται από τον Εθνικό Κανονισμό Ασφαλείας (ΕΚΑ), εξακολουθούν να εφαρμόζονται οι διατάξεις του Κανονισμού αυτού.»

[603] Βλ. ανωτέρω στο κεφάλαιο 1 του παρόντος πονήματος αναφορικά με την προστασία υποδομών ζωτικής σημασίας καθώς και τις αναπτύξεις περί κυβερνοτρομοκρατίας στο οικείο κεφάλαιο 2.

[604] Άρθρο 292Α ΠΚ:

«*1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, και με τον τρόπο αυτόν θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή από είκοσι χιλιάδες (20.000) μέχρι πενήντα χιλιάδες (50.000) ευρώ. Αν ο υπαίτιος της πράξης του προηγούμενου εδαφίου είναι ο εργαζόμενος ή συνεργάτης του παρόχου υπηρεσιών τηλεφωνίας, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή από είκοσι χιλιάδες (20.000) μέχρι εκατό χιλιάδες (100.000) ευρώ.*

2. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού, ο οποίος παραβιάζει διάταξη κανονισμού της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ή όρο της Γενικής Άδειας ή του δικαιώματος χρήσης ραδιοσυχνότητας ή του δικαιώματος χρήσης αριθμού, που αναφέρονται στην ασφάλεια των ηλεκτρονικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή από εκατό χιλιάδες (100.000) μέχρι πεντακόσιες χιλιάδες (500.000) ευρώ.

3. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού ή ο υπεύθυνος διασφάλισης του απορρήτου των επικοινωνιών κατά το άρθρο 3 του παρόντος νόμου, που

«Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών», προβλέπει μεταξύ άλλων ως αξιόποινη πράξη τη χωρίς δικαίωμα πρόσβαση σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή υπηρεσιών τηλεφωνίας και με τον τρόπο αυτόν θέτει σε κίνδυνο την ασφάλεια αυτών των επικοινωνιών. Στην παράγραφο 3 τιμωρείται ως γνήσιο έγκλημα παράλειψης η μη λήψη των αναγκαίων μέτρων προστασίας από τις πράξεις της παραγράφου 1. Η παράγραφος 4 του ίδιου άρθρου εισάγει το υποκειμενικό στοιχείο του αδίκου του σκοπού παράνομου περιουσιακού οφέλους, η παράγραφος 5 αναφέρεται στην διακινδύνευση του Πολιτεύματος και η παράγραφος 6 τιμωρεί την διάθεση προγραμμάτων ή άλλων μέσων για την επίτευξη χωρίς δικαίωμα πρόσβασης σε σύστημα που αφορά τηλεφωνικές υπηρεσίες καθώς και τη διαφήμιση ή τη δημόσια προσφορά σχετικών υπηρεσιών.

4.4.1.4 Ο νόμος 3917/2011

Με τον ν. 3917/2011 η Ελλάδα ενσωμάτωσε την Οδηγία 2006/24/ΕΚ αναφορικά με τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με

παραλείπει να λάβει τα αναγκαία μέτρα για την αποτροπή πράξης της παραγράφου 1, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή από πενήντα χιλιάδες (50.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ, εφόσον η πράξη τελέστηκε ή έγινε απόπειρα τελέσεως αυτής, ανεξάρτητα αν ο δράστης τιμωρηθεί.

4. Αν ο υπαίτιος των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή από εκατό χιλιάδες (100.000) μέχρι τριακόσιες χιλιάδες (300.000) ευρώ. Εφόσον το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των εβδομήντα τριών χιλιάδων (73.000) ευρώ, ο υπαίτιος τιμωρείται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από εκατό χιλιάδες (100.000) μέχρι πεντακόσιες χιλιάδες (500.000) ευρώ.

**** ΠΡΟΣΟΧΗ: Το ποσό των εβδομήντα τριών χιλιάδων (73.000) ευρώ του δεύτερου εδαφίου της παραγράφου 4 αναπροσαρμόζεται στο ποσό των εκατό είκοσι χιλιάδων (120.000) με την παρ. 1 περ.ι` άρθρου 24 Ν.4055/2012,ΦΕΚ Α 51/12.3.2012.Εναρξη ισχύος 2 Απριλίου 2012.»*

5. Αν από τις πράξεις των προηγούμενων παραγράφων μπορεί να τεθούν σε κίνδυνο Θεμελιώδεις αρχές και θεσμοί του Πολιτεύματος, όπως μνημονεύονται στο άρθρο 134Α του Ποινικού Κώδικα ή απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή στην ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.

6. Όποιος αθέμιτα διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει προς εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων της παραγράφου 1 ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεση τους, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή από δέκα χιλιάδες (10.000) μέχρι πενήντα χιλιάδες (50.000) ευρώ.»

τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις. Στο ά. 11 τιμωρείται, και μάλιστα με κάθειρξη μέχρι δέκα ετών, ακόμη και αυτός που λαμβάνει γνώση δεδομένων που διατηρούνται από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών[605] - η πράξη αυτή, δε, τιμωρείται ακόμη και όταν τελείται από αμέλεια, κατά την παρ. 4 του ίδιου άρθρου.

4.4.1.5 Ο νόμος 3471/2006

Με τον ν. 3471/2006[606] ενσωματώθηκε στην ελληνική έννομη τάξη η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[607]. Στο ά. 15 του νόμου αυτού[608] προβλέπονται ποινικές κυρώσεις. Η παράγραφος 1 αναφέρεται

---

[605] Άρθρο 11 - Ποινικές κυρώσεις - (Άρθρο 13 της Οδηγίας 2006/24/ΕΚ):

«*1. Όποιος, κατά παράβαση των διατάξεων του παρόντος κεφαλαίου, λαμβάνει γνώση των δεδομένων που διατηρούνται από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών, τα συλλέγει, αποθηκεύει, αντιγράφει, αφαιρεί, μεταφέρει, αλλοιώνει, βλάπτει, καταστρέφει, μεταδίδει, ανακοινώνει ή με άλλο τρόπο τα επεξεργάζεται, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με κάθειρξη μέχρι δέκα ετών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.*

2. Αν ο δράστης των πράξεων της παραγράφου 1 είναι νόμιμος εκπρόσωπος ή μέλος της διοίκησης ή υπεύθυνος ασφάλειας δεδομένων ή εργαζόμενος ή συνεργάτης του παρόχου ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε σε οικονομικό ή άλλο αντάλλαγμα, τιμωρείται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από 55.000 μέχρι 200.000 ευρώ.

3. Αν από τις πράξεις των παραγράφων 1 και 2 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή από 55.000 μέχρι 300.000 ευρώ.

4. Αν οι πράξεις των παραγράφων 1 και 2 έχουν τελεστεί από αμέλεια, επιβάλλεται φυλάκιση τουλάχιστον δύο ετών.»

[606] Πρβλ. *Γρ. Τσόλια*, Επεξεργασία και προστασία των εξωτερικών στοιχείων της επικοινωνίας και των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, εις: *Λ. Κοτσαλή & Γ. Τριανταφύλλου*, Ανθρώπινα δικαιώματα και ποινικό δίκαιο, σειρά Ποινικά αρ. 75, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2007, σελ. 441 επ.

[607] Η Οδηγία διαθέσιμη στο url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF.

[608] Άρθρο 15 – «Ποινικές κυρώσεις»:

«*1. Όποιος, κατά παράβαση του παρόντος νόμου, χρησιμοποιεί, συλλέγει, αποθηκεύει, λαμβάνει γνώση, αφαιρεί, αλλοιώνει, καταστρέφει, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, ή τα καθιστά προσιτά σε μη δικαιούμενα*

σε ενέργειες επί προσωπικών δεδομένων ενώ η παράγραφος 2 δεν έχει να κάνει με δεδομένα αλλά με μη συμόρφωση σε πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

4.4.2 Ηνωμένο Βασίλειο

Στο Ηνωμένο Βασίλειο ήδη από το 1990 έχει τεθεί σε ισχύ η "Computer Misuse Act"[609] (29 Αυγούστου 1990). Τροποποιήθηκε με την "Criminal Justice and Public Order Act"[610] (1994) και την "Police Justice Act"[611] (2006).

Με το νομοθέτημα αυτό τιμωρούνται η μη εξουσιοδοτημένη πρόσβαση στο υλικό του υπολογιστή (φυλάκιση 6 μηνών ή χρηματική ποινή), η μη εξουσιοδοτημένη πρόσβαση με πρόθεση τη διάπραξη ή διευκόλυνση της διάπραξης νέων αξιόποινων πράξεων και η μη εξουσιοδοτημένη τροποποίηση του υλικού του υπολογιστή. Η δεύτερη από τις διατάξεις της "Computer Misuse Act" τιμωρεί τη μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη ή τη διευκόλυνση της διάπραξης περαιτέρω αξιόποινων πράξεων. Η τρίτη διάταξη στοχεύει στο να αποτρέψει την

πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων ευρώ (10.000) μέχρι και εκατό χιλιάδων ευρώ (100.000), αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

2. Υπεύθυνος επεξεργασίας και τυχόν εκπρόσωπος του που δεν συμμορφώνεται με τις πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που επιβάλλουν τις διοικητικές κυρώσεις της προσωρινής ανάκλησης αδείας, της οριστικής ανάκλησης αδείας και της καταστροφής αρχείου ή διακοπής επεξεργασίας και καταστροφής των σχετικών δεδομένων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον δώδεκα χιλιάδων ευρώ (12.000) μέχρι και εκατόν είκοσι χιλιάδων ευρώ (120.000).

3. Εφόσον ο δράστης των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτο, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000) μέχρι και εκατόν πενήντα χιλιάδων ευρώ (150.000). Αν προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή πενήντα χιλιάδων ευρώ (50.000) μέχρι και τριακοσίων πενήντα χιλιάδων ευρώ (350.000).

4. Εφόσον οι πράξεις των παραγράφων 1 και 2 του παρόντος άρθρου τελεσθούν από αμέλεια, επιβάλλεται φυλάκιση μέχρι δεκαοκτώ (18) μηνών και χρηματική ποινή μέχρι και δέκα χιλιάδων ευρώ (10.000).»

[609] Βλ. την "Computer Misuse Act" στο url: http://www.legislation.gov.uk/ukpga/1990/18/contents

[610] Βλ. την "Criminal Justice and Public Order Act" στο url: http://www.legislation.gov.uk/ukpga/1994/33/contents.

[611] Βλ. την "Police Justice Act" στο url: http://www.legislation.gov.uk/ukpga/2006/48/contents.

παρακώλυση ή παρεμπόδιση της πρόσβασης σε δεδομένα που είναι αποθηκευμένα σε έναν υπολογιστή. Το αδίκημα της § 3 απευθύνεται ειδικά σε αυτούς που δημιουργούν ή/και κυκλοφορούν έναν ιό υπολογιστή (virus), κάποιο «σκουλήκι» (worm), κάποιον "δούρειο ίππο" (Trojan horse) ή γενικώς κάποιο πρόγραμμα (από τα λεγόμενα "hacking tools" ή "malware"[612]), το οποίο μπορεί να περιορίσει με οποιονδήποτε τρόπο την πρόσβαση στα δεδομένα υπολογιστή. Η μόνη προϋπόθεση προκειμένου να θεμελιωθεί το ποινικώς υπεύθυνο είναι η γνώση του δράστη για το ότι αποπειράται μη εξουσιοδοτημένη πρόσβαση.

4.4.3 Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ)

Οι Ηνωμένες Πολιτείες ήταν ίσως το πρώτο χρονικά κράτος του οποίου η νομοθεσία κλήθηκε να προβλέψει την τιμώρηση πράξεων που αποδίδονται στους hackers. Συγκεκριμένα, το 1984 θεσπίστηκε το νομοθέτημα "Counterfeit Access Device and Computer Fraud and Abuse Act (Counterfeit Access Device Act)"[613]. Το 1986 το Κογκρέσο τροποποίησε τον νόμο αυτό με τη θέσπιση της "Computer Fraud and Abuse Act (CFAA)"[614]. Ο νόμος αυτός τροποποιήθηκε το 1996 από το νομοθέτημα "National Information Infrastructure Act" και το 2001 από την "USA Patriot Act". Η πιο πρόσφατη τροποποίηση έγινε το 2008 με την ψήφιση της "Identity theft enforcement and Restitution Act".

Με την "Computer Fraud and Abuse Act" τιμωρούνται η εν γνώσει χωρίς άδεια πρόσβαση σε ηλεκτρονικό υπολογιστή προκειμένου να αποκτηθούν δεδομένα εθνικής ασφάλειας και η σκόπιμη χωρίς άδεια πρόσβαση σε ηλεκτρονικό υπολογιστή για την απόκτηση πληροφοριών οικονομικής φύσεως που εμπεριέχονται σε αρχεία χρηματοπιστωτικού ιδρύματος ή καταναλωτικών ενώσεων, πληροφοριών από

[612] Βλ. παράγραφο 4.4.2 του παρόντος πονήματος.

[613] Βλ. στο url: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA) μια σύντομη παρουσίαση του νομοθετήματος "Counterfeit Access Device and Computer Fraud and Abuse Act (Counterfeit Access Device Act)" καθώς και σχετικών υποθέσεων που έχουν εκδικαστεί βάσει αυτού.

[614] Ο εν λόγω νόμος χαρακτηρίζεται μάλιστα στο άρθρο του *Dave Smith*, "Computer Fraud And Abuse Act 2013: New CFAA Draft Aims To Expand, Not Reform, The 'Worst Law In Technology' " (url: http://www.ibtimes.com/computer-fraud-abuse-act-2013-new-cfaa-draft-aims-expand-not-reform-worst-law-technology-1158515) ως «ο χειρότερος νόμος για την τεχνολογία» καθώς η κυβέρνηση μπορεί να διώξει και να φυλακίσει όποιον χρήστη του διαδικτύου επιθυμεί!

οποιαδήποτε υπηρεσία των Ηνωμένων Πολιτειών καθώς και πληροφοριών από κάθε προστατευόμενο υπολογιστή, αν αυτές αποτελούν στοιχεία διακρατικής ή επικοινωνίας ή επικοινωνίας μεταξύ ξένων κρατών. Επίσης, τιμωρούνται η σκόπιμη χωρίς άδεια πρόσβαση σε κυβερνητικούς υπολογιστές και ο επηρεασμός της χρήσης και της λειτουργίας του υπολογιστή. Επιπρόσθετα, ποινικώς κολάσιμη πράξη είναι η εν γνώσει πρόσβαση σε προστατευμένο υπολογιστή με την πρόθεση της απάτης.

Εν συνεχεία, τιμωρείται από το εν λόγω νομοθέτημα όποιος εν γνώσει του προκάλεσε τη μετάδοση προγράμματος, πληροφορίας, κωδικού ή εντολής που προκαλεί ζημία ή όποιος με σκοπό αποκτά πρόσβαση χωρίς άδεια σε έναν υπολογιστή, και, ως αποτέλεσμα της συμπεριφοράς αυτής προκαλείται:

- Ζημία για ένα ή περισσότερα πρόσωπα κατά τη διάρκεια περιόδου ενός έτους συνολικής αξίας τουλάχιστον 5.000 δολαρίων.
- Τροποποίηση της ιατρικής αντιμετώπισης σε σχέση με την ιατρική εξέταση, διάγνωση, θεραπεία ή φροντίδα ασθενούς.
- Σωματική βλάβη σε οποιοδήποτε πρόσωπο.
- Απειλή για τη δημόσια υγεία ή τη δημόσια ασφάλεια.
- Βλάβη που επηρεάζει το κρατικό-κυβερνητικό σύστημα ηλεκτρονικών υπολογιστών
- Εν γνώσει και με την πρόθεση της απάτης εμπορία κωδικού πρόσβασης ή παρόμοιων πληροφοριών, μέσω των οποίων μπορεί να επιτευχθεί πρόσβαση χωρίς άδεια σε υπολογιστή.

4.4.4 Γερμανία

Μέχρι το 1986 στη Γερμανία δεν είχε θεσπιστεί καμία ειδική διάταξη για τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα και για την αλλοίωση αυτών. Το κενό αυτό καλύφθηκε με τη θέσπιση του δεύτερου νόμου για την καταπολέμηση της οικονομικής εγκληματικότητας (2. WiKG- Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität). Με τον νόμο αυτόν προστέθηκε σημαντικός αριθμός

διατάξεων και ειδικότερα για την τιμώρηση της κατασκόπευσης δεδομένων (Ausspähen von Daten 202a StGB)[615], της παραποίησης δεδομένων (Datenveränderung, 303a StGB)[616] καθώς και της δολιοφθοράς Η/Υ (Computersabootage, 303b StGB)[617].

Έτι περαιτέρω, και μόνο η διατύπωση του ά. 202a StGB «όποιος χωρίς άδεια *αποκτά*… δεδομένα…» στην ποινική διάταξη που εφαρμόζεται για το hacking στη Γερμανία καταδεικνύει την αρχική βούληση του νομοθέτη να μην τιμωρείται η απλή χωρίς δικαίωμα πρόσβαση «χάριν γούστου» από τους hackers[618] αλλά το «κατέβασμα» των δεδομένων (Hauptmann) ή η δυνατότητα αναπαραγωγής του ουσιαστικού τους περιεχομένου (Hilgendorf). Ωστόσο, ο Αργυρόπουλος επισημαίνει άριστα τις τεχνικές δυσκολίες αυτών των προσεγγίσεων και προτείνει την σαφέστερη διατύπωση της διάταξης προς την τιμώρηση και του «απλού» hacking (πρόσβαση σε ηλεκτρονικό σύστημα πληροφοριών)[619].

---

[615] Σύμφωνα με το ά. **202ª StGB – Χωρίς άδεια απόκτηση δεδομένων:**

«*1) Όποιος χωρίς άδεια αποκτά για τον ίδιο ή για κάποιον άλλο δεδομένα, τα οποία δεν προορίζονται για αυτόν και προστατεύονται ιδιαίτερα έναντι κάθε χωρίς εξουσιοδότηση πρόσβασης, τιμωρείται με φυλάκιση μέχρι τριών ετών ή με χρηματική ποινή.*

2) Δεδομένα, κατά την έννοια της παραγράφου 1, είναι μόνο αυτά τα οποία είναι αποθηκευμένα ή μεταβιβάζονται με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, που δεν μπορούν να διαβαστούν άμεσα.»

[616] Σύμφωνα με το ά. **303a StGB – Παραποίηση δεδομένων**

«*1) Όποιος παράνομα διαγράφει, υπεξάγει, αχρηστεύει ή παραποιεί δεδομένα (202a παρ. 2) τιμωρείται με ποινή φυλάκισης μέχρι δύο ετών ή με χρηματική ποινή.*

2) Η απόπειρα τιμωρείται.»

[617] Σημαντική η ανάλυση των εν λόγω διατάξεων από τον Αργυρόπουλο (βλ. *Αν. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 57 επ.).

[618] Έτσι ο Αργυρόπουλος, όπου και σχετική ανάλυση (βλ. *Αν. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 79).

[619] *Αν. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 83.

5. ΤΟ ΕΓΚΛΗΜΑ ΤΗΣ ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

5.1 Η διάταξη του άρθρου 370Γ παρ. 2 ΠΚ.

5.1.1 Εισαγωγικά

Ο Έλληνας νομοθέτης με την ψήφιση των ά. 3 και 4 του ν. 1805/1988[620] προέβη για πρώτη φορά στην ποινικοποίηση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, εισάγοντας στο εικοστό δεύτερο κεφάλαιο του Ποινικού Κώδικα δύο καινοτόμες για την εποχή εκείνη ποινικές διατάξεις, αυτές των άρθρων 370Β και 370Γ παρ. 2 ΠΚ αντίστοιχα. Κατά τον χρόνο θέσπισης του ως άνω νόμου η χρήση του διαδικτύου αλλά και των ηλεκτρονικών υπολογιστών δεν είχε λάβει τις διαστάσεις που κατέχει σήμερα. Ωστόσο, οι διατάξεις του συγκεκριμένου νόμου χαρακτηρίζονται καταρχήν από διορατικότητα, η οποία εμφαίνεται από την ευρύτητα στη διατύπωσή τους, προκειμένου να δύνανται να καλύψουν στο πεδίο εφαρμογής τους ένα ευρύ πλέγμα μελλοντικών εγκληματικών συμπεριφορών, το οποίο τελικώς και δημιουργήθηκε από τις καλπάζουσες τεχνολογικές εξελίξεις μέσα στην εικοσαετία και πλέον που ακολούθησε. Δηλαδή, ο έλληνας ποινικός νομοθέτης έλαβε από νωρίς σαφή θέση υπέρ της ποινικοποίησης της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα[621], σε αντίθεση ενδεχομένως με αντίθετες φωνές, οι οποίες

[620]Δημοσιεύτηκε στο Φ.Ε.Κ. Α' 199 της 31.08.1988.

[621] Σύμφωνα με την αιτιολογική έκθεση του ν. 1805/1988 κρίθηκε αναγκαία η θέσπιση της εν λόγω διάταξης λαμβανομένης υπόψη της μεγάλης δαπάνης η οποία απαιτείτο για την παραγωγή προγραμμάτων για την προστασία της ηλεκτρονικής πληροφορίας καθώς και του οξύτατου ανταγωνισμού που είχε αναπτυχθεί στον κλάδο αυτό!

θεωρούσαν, και θεωρούν ίσως ακόμη, την ως άνω συμπεριφορά ως ένα «ακίνδυνο παιχνίδι»[622].

Συγκεκριμένα, η διάταξη του ά. 370Γ παρ. 2 ΠΚ συνιστά τη βασική ποινική ρύθμιση για το υπό εξέταση θέμα στην οποία ορίζεται ότι « *Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών [29,00 ευρώ]. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148*». Αναφορικά με το ά. 370Β ΠΚ[623], όπως ειπώθηκε και ανωτέρω και θα εξηγηθεί ειδικότερα κατωτέρω, απο την ίδια τη γραμματική ακόμη διατύπωση προκύπτει ότι η απλή και μόνο πρόσβαση στα δεδομένα δεν συμπεριλαμβάνεται στους τρόπους τέλεσης του οικείου εγκλήματος. Για την εφαρμογή της εν λόγω διάταξης απαιτείται ο ειδικότερος απόρρητος χαρακτήρας των δεδομένων (κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα καθώς και όσα ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα)[624].

5.1.2 Προστατευόμενο έννομο αγαθό

[622] Βλ. σχετικές αναπτύξεις στην παράγραφο 4.1. του παρόντος πονήματος.

[623] Άρθρο 370Β ΠΚ:

> «*1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.*
>
> *2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.*
>
> *3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.*
>
> *4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση.*»

[624] Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, Υπερ/2000, σελ. 968 καθώς και κατωτέρω αναπτύξεις για τη σχέση ά. 370Β και 370Γ παρ. 2 ΠΚ.

Η προσπάθεια προσδιορισμού του προστατευόμενου εννόμου αγαθού[625] του ά. 370Γ παρ. 2 ΠΚ έχει οδηγήσει στη διατύπωση διαφορετικών απόψεων, άλλοτε αλληλοσυμπληρούμενων και άλλοτε αντιτιθέμενων, ως εξής:

Κατά τη μάλλον επικρατέστερη άποψη, το προστατευόμενο από το σύνολο του ά. 370Γ ΠΚ έννομο αγαθό είναι αυτό του απορρήτου υπό τυπική έννοια, δηλαδή το τυπικό δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό ουσιαστική έννοια και χωρίς να έχουν τα δεδομένα αυτά αποκλειστικά οικονομική αξία[626] [627]. Αντίστοιχη φαίνεται να είναι και η θέση ότι προστατεύεται η τυπική εξουσία διαθέσεως του κατόχου των στοιχείων ή των προγραμμάτων υπολογιστών, ο οποίος δυνάμει του δικαιώματός του στο πνευματικό περιεχόμενό τους ορίζει αυτός σε ποιον μπορούν να γίνουν προσιτά. Κατά συνέπεια, η ίδια η πληροφορία αποτελεί την ουσιαστική αξία και εν τέλει αυτή προστατεύεται. Αποκτά, δε, αξία από την αξιολόγηση από τον κάτοχό της, ο οποίος με τον τρόπο αυτό αποκτά εξουσία διαθέσεώς της, δυνατότητα εξουσιάσεώς της και το δικαίωμα να αποκλείει κάθε ανάμειξη τρίτου σε αυτή χωρίς τη συγκατάθεσή του[628]. Με την ανωτέρω θέση συντάσσεται και η νομολογία[629] επικαλούμενη την ίδια την Εισηγητική Έκθεση του ν. 1805/1988, η οποία αναφέρει ότι με τη διάταξη του ά. 370Γ παρ. 2 ΠΚ αποσκοπείται η τιμώρηση της παραβιάσεως μυστικών που έχουν σχέση με προγράμματα ηλεκτρονικών υπολογιστών και προστατεύεται το ουσιαστικό απόρρητο αυτών των προγραμμάτων.

---

[625] Βλ. σχετικά αναφορικά με την ασφάλεια στο διαδίκτυο και τις αναπτύξεις του Αγγελή και ιδίως την υποσ. 5 όπου και παραπέμπει στον Χωραφά για τον ορισμό του εννόμου αγαθού (*Ιωάννης Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 12/2001, 1293 επ.).

[626] Βλ. *Χρήστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Εκδόσεις Σάκκουλας 1991, σελ. 92, *Αριστοτέλης Χαραλαμπάκης - Ιωάννης Γιαννίδης*, Ποινικός Κώδικας και Νομολογία, Εκδόσεις Δίκαιο και Οικονομία, Π.Ν. Σάκκουλας, Αθήνα 2009, σελ. 1623, *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ2/2003 (Έτος 6ο) σελ. 193. Την ίδια άποψη υποστηρίζει και ο Ιγγλεζάκης (βλ. *Ιωάν. Ιγγλεζάκης*, Δίκαιο της πληροφορικής, β' έκδοση, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2008, σελ. 279), ο οποίος παραπέμπει ως ανωτέρω στον Μυλωνόπουλο.

[627] Αντίστοιχο και το προστατευόμενο έννομο αγαθό της σχετικής γερμανικής ποινικής διάταξης (παρ. 202a StGB), όπως αναφέρει ο Αργυρόπουλος (βλ. *Αν. Αργυρόπουλο*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 61-62). Ωστόσο, είναι γεγονός ότι η γερμανική ποινική διάταξη δεν αναφέρεται στην «πρόσβαση» σε δεδομένα αλλά στην «απόκτηση» δεδομένων.

[628] Βλ. *Αθανάσιος Κονταξής*, Ποινικός Κώδικας [Συνδυασμός θεωρίας και πράξης], Τόμος Β΄, Έκδοση Γ', Αθήνα, 2000, σελ. 3153- 3154 και *Μιχαήλ Μαργαρίτης*, Ποινικός Κώδικας – Ερμηνεία και Εφαρμογή, Εκδόσεις Δίκαιο και Οικονομία, Π. Ν. Σάκκουλας, Αθήνα, 2009, σελ. 1034.

[629] Βλ. απόφ. Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 75.

Σύμφωνα με δεύτερη διατυπωθείσα άποψη, το προστατευόμενο αυτοτελές έννομο αγαθό της σχετικής διάταξης είναι το απόρρητο των ηλεκτρονικών δεδομένων[630] (ασχέτως τυχόν περαιτέρω σκοπών του δράστη)[631], ως έκφανση της ιδιότητάς τους να ανήκουν σε κάποιον, ο οποίος έχει τη δυνατότητα – ανεξάρτητα από το εάν τα δεδομένα αυτά αφορούν τον ίδιο ή άλλους – να αποκλείει την πρόσβαση σε αυτά.

Κατά μία άλλη, αρκετά ενδιαφέρουσα, άποψη, το ά. 370Γ ΠΚ και ιδιαίτερα η δεύτερη παράγραφος αποτελεί τον πυρήνα του ελληνικού ποινικού δικαίου της πληροφορικής. Η προστασία των ηλεκτρονικών στοιχείων δεν είναι αυτοσκοπός αλλά προστατευτέα είναι η πληροφορία που ενσωματώνεται σε αυτά. Με αυτόν τον τρόπο η πληροφορία και ειδικότερα το δικαίωμα εξουσίασης και διάθεσής της συνιστούν ένα νέο έννομο αγαθό στο σύστημα του ποινικού δικαίου[632]. Πιο συγκεκριμένα, η εν λόγω διάταξη προστατεύει «*τα στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών*». Από τη γραμματική διατύπωση του νόμου φαίνεται σαφής η προσπάθεια του νομοθέτη να οριοθετήσει μία περιοχή συγκέντρωσης και κυκλοφορίας στοιχείων, στην οποία ο νόμιμος κάτοχος δύναται να δημιουργήσει ένα είδος κυριαρχίας και να έχει την πρακτική δυνατότητα να απαγορεύσει την πρόσβαση. Είναι, δε, αυτονόητο ότι, με την απόκτηση πρόσβασης στην ως άνω περιοχή, διακινδυνεύεται η κυριαρχία του νόμιμου κατόχου επί των στοιχείων. Επειδή όμως, όπως και παραπάνω σημειώθηκε, ο ουσιαστικός σκοπός του νομοθέτη δεν υποστηρίζεται ότι είναι η προστασία των στοιχείων, η υπό έρευνα διάταξη εξυπηρετεί κατά πρώτον το συμφέρον του νόμιμου κατόχου να διαθέτει τις πληροφορίες που προκύπτουν από τα στοιχεία σε όποιον αυτός επιθυμεί και κατά δεύτερον το δικαίωμα να μην παρενοχλούνται τα στοιχεία σε συγκεκριμένους χώρους τους οποίους ο νόμιμος κάτοχος δικαιούται να εποπτεύει[633]. Συγκλίνουσα με την προηγούμενη άποψη φαίνεται να είναι και η θέση κατά την οποία το έννομο αγαθό

[630] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμενόπουλος, 2007, σελ. 1066.

[631] Βλ. *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, Ποινικά 57, Εκδόσεις Αντ. Σάκκουλα, Αθήνα – Κομοτηνή 1999, σελ. 127.

[632] Βλ. *Χρίστος Μυλωνόπουλος*, Ο ποινικός κώδικας ανάμεσα στο παρόν και στο μέλλον, ΠοινΛόγος 1/2002, σελ. 10.

[633] Βλ. *Ειρήνη Ε. Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 1993, σελ. 83-84.

που προστατεύεται εν προκειμένω είναι η πληροφορία και το δικαίωμα εξουσίασης και διάθεσής της[634].

Έχοντας ως βάση τη σύντομη ανάπτυξη των ως άνω απόψεων, ο καθορισμός του προστατευόμενου εννόμου αγαθού του ά. 370Γ παρ. 2 ΠΚ δεν είναι τόσο απλός όσο φαίνεται αρχικά. Το βέβαιο είναι ότι δεν πρόκειται για την προστασία κάποιου περιουσιακού αγαθού. Στη διαπίστωση αυτή συνηγορεί και η ίδια η συστημική θέση της διάταξης στο 22ο κεφάλαιο του ΠΚ για την παραβίαση απορρήτων καθώς και το γεγονός ότι δεν απαιτείται τα στοιχεία να έχουν περιουσιακή αξία και το υποκείμενο του εγκλήματος να έχει πρόθεση αποκόμισης περιουσιακού οφέλους.

Σε κάθε περίπτωση, η προσπάθεια προσέγγισης του προστατευόμενου έννομου αγαθού δεν πρέπει να βασίζεται αποκλειστικά και μόνο στη διατύπωση της υπό έρευνα διάταξης ή στη συστημική της ένταξη στον Ποινικό Κώδικα. Στη συγκεκριμένη περίπτωση η προσέγγιση (πρέπει να) καταλήγει σε μία αναγωγή σε νέα έννομα αγαθά για το ποινικό δίκαιο, όπως είναι η *ασφάλεια των ηλεκτρονικών πληροφοριών* (των δεδομένων-στοιχείων) και το δικαίωμα του έχοντος την εξουσία διάθεσης επί των δεδομένων αυτών στην άρτια και απεριόριστη δυνατότητα χρησιμοποίησής τους. Η από τεχνική άποψη ασφάλεια (security) είναι η προστασία ενός συστήματος πληροφοριών και των στοιχείων που περιέχονται σε αυτό. Ασφάλεια των στοιχείων σημαίνει ότι θα πρέπει να διασφαλίζεται η εμπιστευτικότητα [confidentiality - άλλως το απόρρητο των πληροφοριών που ενσωματώνουν], η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) των στοιχείων[635]. Ειδικότερα, εμπιστευτικότητα (confidentiality) των στοιχείων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος. Ακεραιότητα (integrity) των στοιχείων είναι η ιδιότητά τους να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε, δέ, αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας. Τέλος, διαθεσιμότητα (availability) των στοιχείων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμα σε κάθε εξουσιοδοτημένο χρήστη του συστήματος. Προκειμένου να υπάρχει ασφάλεια στα συστήματα πληροφοριών είναι απαραίτητες και οι τρεις αυτές εκφάνσεις – άρα, και μόνο μία εκ των τριών αν πληγεί μπορεί να

[634] *Μ. Παπαδόπουλος*, Wardriving, Warchalking & Wireless Hacking, 2ο εθνικό συνέδριο με διεθνή συμμετοχή, ΕΒΕΑ, 16-17 Μαρτίου 2006, Ηλεκτρονική Δημοκρατία, Προκλήσεις της ψηφιακής εποχής, σελ. 28.

[635] Όπως ήδη αναλύθηκε στην παράγραφο 1.3 του παρόντος πονήματος, με σχετικές παραπομπές.

θεωρηθεί ότι πλήττεται η ασφάλεια των πληροφοριών. Με αυτόν τον τρόπο προστατεύονται σφαιρικά τα ηλεκτρονικά στοιχεία και ιδίως οι πληροφορίες που αυτά εμπεριέχουν.

Μήπως, όμως, αυτή η τελευταία άποψη της προηγούμενης παραγράφου δεν περιγράφει απλώς την πρόσβαση στην οποία αναφέρεται η διάταξη του ά. 370Γ παρ. 2 ΠΚ; Αν υποθέσουμε ότι η εμπιστευτικότητα συνιστά ουσιαστικά το απόρρητο των πληροφοριών, τότε μπορούμε να πούμε ότι η πρόσβαση πλήττει την ακεραιότητα ή/και τη διαθεσιμότητα; Η απάντηση έρχεται μέσω παραδειγμάτων: αναφορικά με τη διαθεσιμότητα, αυτή πλήττεται, πέρα από τη χρήση ιών και άλλων επιβλαβών ηλεκτρονικών προγραμμάτων, αν ο δράστης εισέλθει χωρίς δικαίωμα σε δεδομένα και με αυτόν τον τρόπο αποκλείσει την πρόσβαση στον πραγματικό δικαιούχο επειδή το σύστημα επιτρέπει μόνο έναν χρήστη (π.χ. η βάση νομικών δεδομένων NOMOS στην οποία αν ο χρήστης έχει εισέλθει στο σύστημα κανείς άλλος δεν μπορεί να εισέλθει στον λογαριασμό του). Η ακεραιότητα των δεδομένων μπορεί αντιστοίχως να πληγεί σε περίπτωση που το ηλεκτρονικό σύστημα χρησιμοποιηθεί ως "zombie" σε περιπτώσεις επιθέσεων "botnet" καθώς και στις περιπτώσεις κατά τις οποίες ανανεώνεται ο κωδικός πρόσβασης κατά την τελευταία πρόσβαση του χρήστη στο σύστημα. Σε ό,τι αφορά στο δεύτερο παράδειγμα, αν, δηλαδή, ο δράστης αποκτήσει χωρίς δικαίωμα πρόσβαση στο σύστημα πληροφοριών, με αυτόν τον τρόπο πλήττει κατά μία έννοια την ακεραιότητα των δεδομένων καθώς με την ενέργειά του αυτή επιτρέπει την τροποποίηση του κωδικού πρόσβασης του χρήστη από το σύστημα, κωδικό πρόσβασης που ο χρήστης δεν μπορεί μετέπειτα να γνωρίζει εξαιτίας της παράνομης συμπεριφοράς του έχοντος αποκτήσει χωρίς δικαίωμα πρόσβαση.

Με βάση τα ανωτέρω είναι δεδομένο ότι η ασφάλεια των πληροφοριών πρέπει να αναχθεί σε έννομο αγαθό υπό την τεχνική της έννοια. Προς τον σκοπό αυτόν και έχοντας ως παράδειγμα νομοθεσίες ξένων χωρών οι οποίες τιμωρούν και την παρεμπόδιση της πρόσβασης (π.χ. Ηνωμένο Βασίλειο) καθώς και τα παραδείγματα ως άνω, de lege ferenda χρειάζεται ίσως ανανέωση της διάταξης του ά. 370Γ παρ. 2 για την εναργέστερη προστασία της ασφάλειας των ηλεκτρονικών δεδομένων (π.χ. και όλως ενδεικτικώς με την συμπερίληψη της φράσης «ή αποκλείει την πρόσβαση» στην αντικειμενική υπόσταση του εγκλήματος).

Φορέας του εννόμου αγαθού είναι ο έχων την εξουσία διαθέσεως των δεδομένων που περιλαμβάνονται στο ηλεκτρονικό σύστημα[636]. Για τον ακριβέστερο προσδιορισμό του είναι απαραίτητη η διάκριση ανάμεσα σε αποθηκευμένα δεδομένα [σε αυτήν την περίπτωση δικαιούχος είναι αυτός στον οποίον ανήκει η θέση αποθήκευσης – σε περίπτωση, δε, νεφελοειδούς συστήματος αποθήκευσης (cloud computing) ο δικαιούχος του αντίστοιχου λογαριασμού] και σε δεδομένα που βρίσκονται σε «διαβιβαστική βάση» [περίπτωση κατά την οποία δικαιούχος διαθέσεως μπορεί να είναι και ο παραλήπτης τους κατά το «κατέβασμα» (downloading) ή την ολοκλήρωση της λήψης τους][637].

5.1.3 Έννοια και στοιχεία της αντικειμενικής υπόστασης του εγκλήματος

Όπως ήδη αναφέρθηκε ανωτέρω, το έγκλημα της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα ορίζεται από τον ποινικό νομοθέτη στη δεύτερη παράγραφο του ά. 370Γ ΠΚ, όπου νοείται η απόκτηση πρόσβασης σε στοιχεία που έχουν εισαχθεί σε ηλεκτρονικό υπολογιστή ή σε περιφερειακή μνήμη του ή μεταδίδονται με συστήματα τηλεπικοινωνιών, χωρίς δικαίωμα και ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που έχει λάβει ο νόμιμος κάτοχός τους[638].

Το έγκλημα αυτό είναι «κοινό»[639] καθώς η διατύπωση ξεκινάει με τη λέξη «όποιος» και συνεπώς δεν απαιτείται ο δράστης να έχει κάποιες ιδιαίτερες ιδιότητες προκειμένου να θεωρηθεί αξιόποινη η πράξη του. Επίσης, το εν λόγω έγκλημα είναι μονοπρόσωπο, συμπεριφοράς[640] και ενέργειας[641] (καθώς πιστεύω δεν δύναται να νοηθεί τεχνικά η έστω και με ενδεχόμενο δόλο απόκτηση πρόσβασης σε ηλεκτρονικά

[636] Βλ. κατωτέρω αναλυτικά αναφορικά με την έννοια «νομίμου κατόχου» των στοιχείων.

[637] Βλ. *Αν. Αργυρόπουλο*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 63 και ειδικότερα σελ. 68.

[638] Βλ. *Μιχαήλ Μαργαρίτης*, Ποινικός Κώδικας – Ερμηνεία και Εφαρμογή, οπ. παρ, σελ. 1035.

[639] Για τον ορισμό του κοινού εγκλήματος βλ. ενδεικτικά *Νικόλαο Κ. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, 2006, σελ. 165 επ. και *Λ. Κοτσαλή*, Ποινικό Δίκαιο – Γενικό Μέρος, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, τομ. 1, σελ. 88 επ.

[640] Σχετικά με τα εγκλήματα συμπεριφοράς βλ. ενδεικτικά *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., σελ. 169 επ. και *Λ. Κοτσαλή*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., τομ. 1, σελ. 90 επ.

[641] Σχετικά με τα εγκλήματα ενέργειας βλ. ενδεικτικά *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., σελ. 179 επ.

δεδομένα με παράλειψη, με δεδομένο ότι η χρήση υπολογιστή ή άλλων ηλεκτρονικών συσκευών, και ιδίως στο διαδίκτυο, απαιτεί έστω μια ελάχιστη κίνηση ενεργοποίησης και παροχής εντολής για την περιήγηση σε δεδομένα συστήματος πληροφοριών).

Σύμφωνα με την αιτιολογική έκθεση του ν. 1805/1988 «*κατά το νέο αρθρ. 370 παράγραφος 2 ΠΚ τιμωρείται ως* ***έγκλημα διακινδύνευσης*** *η πρόσβαση σε στοιχεία που έχουν αποθηκευθεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών*»[642]. Συνεπώς, κατά τον νομοθέτη δεν απαιτείται να έχει επέλθει βλάβη από την υπό κρίση συμπεριφορά – δεν απαιτείται, δηλαδή, ο δράστης να αντιγράψει, να καταστρέψει ή να προβεί σε άλλη επιζήμια συμπεριφορά για το περιεχόμενων των στοιχείων[643]. Αρκεί εξαιτίας της πράξης ή των πράξεων του δράστη να δημιουργήθηκε ο κίνδυνος τέλεσης κάποιας άλλης παρόμοιας πράξης[644] - επί της εν λόγω απόψεως, ωστόσο, πιστεύω ότι πρέπει να επισημανθεί πως η γραμματική διατύπωση της διάταξης δεν αναφέρεται σε σκοπό καμίας περαιτέρω πράξης. Υποστηρίζεται, τέλος, ότι πρόκειται για κοινώς επικίνδυνο έγκλημα[645] [646].

Ωστόσο, σε αντίθεση με την πρόβλεψη του νομοθέτη στην αιτιολογική έκθεση, πιστεύω ότι δεν θα ήταν αδόκιμο να υποστηριχθεί και η άποψη ότι η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα είναι ***έγκλημα βλάβης***, εφόσον θεωρηθεί βλάβη και επιζήμια συμπεριφορά αυτή καθεαυτή η απόκτηση πρόσβασης. Δηλαδή, το γεγονός ότι για τη στοιχειοθέτηση του εγκλήματος δεν απαιτείται περαιτέρω η διαγραφή των ηλεκτρονικών στοιχείων δεν καθιστά το υπό κρίση έγκλημα διακινδύνευσης, αφού το προστατευόμενο έννομο αγαθό (απόρρητο, ασφάλεια ή δυνατότητα εξουσίας των δεδομένων) έχει ήδη τρωθεί από τη χωρίς σχετικό δικαίωμα απόκτηση πρόσβασης και συνακόλουθα γνώσης[647] των στοιχείων αυτών από τρίτα πρόσωπα. Η διατυπωθείσα αυτή άποψη προφανώς οφείλεται σε σύγχυση

---

[642] Σε έγκλημα διακινδύνευσης αναφέρεται και ο *Ιωάν. Ιγγλεζάκης*, Δίκαιο της πληροφορικής, όπ. π., σελ. 279.

[643] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156.

[644] Βλ. *Ειρήνη Ε. Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 86.

[645] Βλ. *Μ. Παπαδόπουλος*, Wardriving, Warchalking & Wireless Hacking, 2ο εθνικό συνέδριο με διεθνή συμμετοχή, ΕΒΕΑ, 16-17 Μαρτίου 2006, Ηλεκτρονική Δημοκρατία, Προκλήσεις της ψηφιακής εποχής, σελ. 28.

[646] Για τα κοινώς επικίνδυνα εγκλήματα βλ. *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., σελ. 178.

[647] Αναφορικά με την ανάλυση και συσχέτιση των εννοιών πρόσβαση και γνώση βλ. ειδικότερα κατωτέρω παράγραφο 5.1.3.2 του παρόντος πονήματος.

ανάμεσα στην προσβολή του προστατευόμενου έννομου αγαθού και τον κίνδυνο που η πράξη αυτή εμπεριέχει για την προσβολή άλλων έννομων αγαθών, όπως η περιουσία. Πράγματι, σε πολλές περιπτώσεις, η απόκτηση πρόσβασης σε ξένα στοιχεία αποτελεί το πρώτο βήμα για μια σύνθετη συμπεριφορά με σκοπό την απόκτηση παράνομου περιουσιακού οφέλους. Ωστόσο, η διάταξη του ά. 370Γ παρ. 2 ΠΚ τυποποιεί συμπεριφορά η οποία δεν περιλαμβάνει αυτά τα στοιχεία – βέβαια, ενδεχομένως να μπορεί να θεωρηθεί βλάβη το γεγονός ότι λαμβάνουν χώρα εντολές που τροποποιούν τη λειτουργία του ηλεκτρονικού συστήματος πληροφοριών προκειμένου να επιτραπεί η πρόσβαση.

Όσον αφορά τη διάκριση των εγκλημάτων σε εγκλήματα συμπεριφοράς (τυπικά) και αποτελέσματος (ουσιαστικά), ορθότερος φαίνεται να είναι ο χαρακτηρισμός του εγκλήματος της παρ. 2 του ά. 370Γ ΠΚ ως ***εγκλήματος συμπεριφοράς***. Κι αυτό διότι, όπως θα αναλυθεί κατωτέρω, η εγκληματική συμπεριφορά του δράστη, ήτοι η χωρίς δικαίωμα απόκτηση πρόσβασης σε στοιχεία, δεν προϋποθέτει κάποια επενέργεια στο υλικό αντικείμενο του εγκλήματος (στοιχεία). Δεν απαιτείται, δηλαδή, η μεταβολή της κατάστασης των στοιχείων (π.χ. διαγραφή, αλλοίωση, αντιγραφή). Αρκεί ο δράστης να έφτασε σε τέτοιο σημείο δια της πρόσβασης ώστε να απέκτησε τη δυνατότητα να επιφέρει τη ως άνω μεταβολή.

Ως προς την ιδιότητα του εξεταζόμενου εγκλήματος ως εγκλήματος στιγμιαίου ή διαρκούς[648], υποστηρίζεται η άποψη ότι πρόκειται μάλλον περί ***στιγμιαίου εγκλήματος***, αφού τιμωρείται η χωρίς δικαίωμα πρόσβαση του δράστη στα στοιχεία και όχι η διατήρηση της παράνομης κατάστασης που δημιουργείται[649], σύμφωνα και με τη γραμματική διατύπωση του νόμου *«Όποιος αποκτά πρόσβαση…»*.

5.1.3.1 Έννοια «στοιχείων» στο ά. 370Γ παρ. 2

Η διατάξη του ά. 370Γ παρ. 2 αναφέρεται στη δεύτερη παράγραφο στα *«στοιχεία» που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται*

[648] Βλ. σχετικά με τα «στιγμιαία εγκλήματα» και τα «διαρκή εγκλήματα» *Νικόλαο Κ. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, όπ. π., σελ. 181 και *Λ. Κοτσαλή*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., τομ. 1, σελ. 93 επ.

[649] Βλ. *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, Τόμος Δεύτερος, Νομική Βιβλιοθήκη 2011, σελ. 1732.

με σύστημα τηλεπικοινωνιών. Πρόκειται για μία γενική διάταξη, η οποία αφορά όλη τη σφαίρα επεξεργασίας στοιχείων από συστήματα υπολογιστή, αφενός εκείνων που είναι καταγεγραμμένα στους χώρους του υπολογιστή (πρωτεύουσες μνήμες, δευτερεύουσες μνήμες, κεντρικός επεξεργαστής, περιφερειακές μνήμες) αφετέρου εκείνων που βρίσκονται σε «κίνηση», μεταδίδονται δηλαδή με συστήματα τηλεπικοινωνιών.

Καταρχάς, είναι απαραίτητο να προβούμε στον εννοιολογικό προσδιορισμό του ηλεκτρονικού υπολογιστή όπως αυτός γίνεται αντιληπτός από τον μέσο χρήστη. Ο ηλεκτρονικός υπολογιστής (και πλέον οι ηλεκτρονικές συσκευές με δυνατότητα διασύνδεσης μεταξύ τους και σύνδεσης στο διαδίκτυο) λειτουργεί κατ' ουσίαν με λογισμικό, δηλαδή ειδικότερα προγράμματα και δεδομένα (ή αλλιώς «στοιχεία»)[650]. Και ενώ τα προγράμματα επιτρέπουν στον υπολογιστή να λειτουργήσει (λειτουργικά προγράμματα[651]) ή να εκτελέσει τις διάφορες ειδικότερες λειτουργίες που ενδιαφέρουν τον χρήστη[652], τα δεδομένα ή στοιχεία αποτελούν τα προϊόντα λειτουργίας των προγραμμάτων, πληροφορίες δηλαδή που δημιουργούμε ή ανακτούμε χάρη σε αυτά[653]. Βεβαίως, κατά την άποψή μου, στοιχεία δύνανται να αποτελούν και τα ίδια τα λειτουργικά προγράμματα του υπολογιστή ή των ψηφιακών συσκευών αναφορικά με την προγραμματιστική δομή τους, την εκτέλεσή τους από τη συσκευή κ.λπ.

Στις δύο πρώτες κατηγορίες στοιχείων ανήκουν όλα εκείνα τα στοιχεία που είναι αποθηκευμένα ή υφίστανται επεξεργασία από έναν υπολογιστή και τα οποία είναι καταγεγραμμένα σε εσωτερικές ή εξωτερικές μνήμες του υπολογιστή, όπως χαρακτηριστικά ήταν παλαιότερα οι μαγνητοταινίες ή δισκέτες, οι μνήμες τυχαίας προσπέλασης και οι διάτρητες κάρτες και σήμερα είναι οι μνήμες usb sticks, τα cd

---

[650] Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 960.

[651] Τέτοια είναι π.χ. τα γνωστά MS-DOS, Windows, Unix, Linux - βλ. υποσ. 4, *Δημήτρης Κιούπης*, όπ. π., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, σελ. 960.

[652] Τέτοια είναι π.χ. τα προγράμματα επεξεργασίας κειμένου, τα λογιστικά φύλλα, οι βάσεις δεδομένων, τα προγράμματα σχεδίασης και επεξεργασίας εικόνων, περιήγησης στο διαδίκτυο, διαχείρισης ηλεκτρονικού ταχυδρομείου κ.λπ. Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 960, υποσ. 5.

[653] Παραδείγματος χάριν τα κείμενα που γράφουμε ή διαβάζουμε, οι εικόνες, οι ήχοι, τα αριθμητικά δεδομένα, οι πίνακες κ.λπ. Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 960, υποσ. 6.

roms κ.ά. Στη τρίτη, δέ, κατηγορία (ανακτώμενες πληροφορίες) ανήκουν τα στοιχεία που μεταδίδονται διαμέσου συστημάτων τηλεπικοινωνιών. Η εν λόγω μετάδοση μπορεί να σημαίνει τρεις ξεχωριστές λειτουργίες: πρώτον *την απομακρυσμένη επεξεργασία στοιχείων,* δεύτερον *την απόκτηση στοιχείων από τράπεζες στοιχείων και* τρίτον *την επικοινωνία μέσω ηλεκτρονικών συστημάτων επικοινωνιών*. Πιο συγκεκριμένα, στην πρώτη περίπτωση τα στοιχεία μεταφέρονται από ένα τερματικό σε έναν υπολογιστή, ο οποίος βρίσκεται σε διαφορετικό χώρο και αποκτά σε αυτά τεχνική δυνατότητα επεξεργασίας. Τα αποτελέσματα της επεξεργασίας είτε επαναφέρονται στην αρχική μονάδα αποστολής είτε παραμένουν στον κεντρικό υπολογιστή. Σημαντική τεχνική προϋπόθεση για την απομακρυσμένη επεξεργασία στοιχείων αποτελεί το σύστημα διαμοιρασμού του χρόνου, το οποίο δύναται να εξυπηρετήσει πολλούς χειριστές συγχρόνως. Σημειώνεται ότι σε κάθε απομακρυσμένη επεξεργασία στοιχείων είναι αδιάφορο αν η μεταφορά στοιχείων από ένα τερματικό γίνεται προς έναν κεντρικό επεξεργαστή που ευρίσκεται στο διπλανό δωμάτιο ή σε απόσταση πολλών εκατοντάδων χιλιομέτρων. Στη δεύτερη περίπτωση η πρόσβαση στα στοιχεία γίνεται μέσω ενός δικτύου επικοινωνίας ενώ απαιτείται και διαδικασία ελέγχου, η οποία συνήθως είναι η αναφορά ενός κλειδάριθμου για την αναγνώριση του δικαιώματος εισόδου σε έναν χρήστη. Πρόκειται κατ' ουσίαν για ένα σύστημα, το οποίο προσφέρει σε μία ομάδα χρηστών την ικανότητα να καταθέτουν και να αποκτούν στοιχεία που αφορούν ένα συγκεκριμένο θέμα. Η τρίτη περίπτωση αφορά τη μεταφορά στοιχείων μέσω ειδικών συστημάτων επικοινωνιών, όπως είναι το ηλεκτρονικό ταχυδρομείο (electronic mail), το τηλεκείμενο (teletext), η διαδικτυακά αναμεταδιδόμενη συζήτηση – τηλεδιάσκεψη (Internet Relay Chat IRC) και η τηλεπαροχή επικοινωνιών (videotext) με σκοπό την εξυπηρέτηση ανταλλαγής μηνυμάτων μέσω συστημάτων υπολογιστών[654]. Στην τρίτη αυτή κατηγορία εντάσσονται πλέον και τα νεφελοειδή συστήματα αποθήκευσης (cloud computing).

Τέλος, στην προστασία των στοιχείων εντάσσεται χαρακτηριστικά και ο προγραμματιστικός κώδικας (γλώσσα προγραμματισμού) των λειτουργικών προγραμμάτων του ηλεκτρονικού υπολογιστή. Σε όλες τις ως άνω κατηγορίες

[654] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 85-86.

στοιχείων ο νόμιμος κάτοχος δύναται να δημιουργήσει ένα είδος κυριαρχίας και μία δυνατότητα απαγορεύσεως πρόσβασης σε αυτά[655].

5.1.3.2 Έννοια απόκτησης πρόσβασης

Με τη διάταξη του ά. 370Γ παρ. 2 ΠΚ τιμωρείται per se η απόκτηση πρόσβασης σε ηλεκτρονικά δεδομένα. Καταρχάς, υποκείμενο του εγκλήματος δύναται να είναι οποιοδήποτε πρόσωπο, όπως άλλωστε προκύπτει από την ίδια τη διατύπωση της διάταξης «*Όποιος αποκτά πρόσβαση……*»[656].

Πρόσβαση σε στοιχεία είναι κάθε τεχνική και φυσική δυνατότητα επίδρασης στον αποθηκευτικό χώρο των στοιχείων και η φυσική δυνατότητα εισόδου στο σύστημα στο οποίο φυλάσσονται ή η δυνατότητα θεώρησής τους με τεχνικά μέσα οπουδήποτε και αν βρίσκονται[657]. Βάσει της κατηγοριοποίησης των στοιχείων που προηγήθηκε, η πρόσβαση δύναται να είναι αφενός σε δεδομένα που βρίσκονται αποθηκευμένα σε υπολογιστή (illegal access) αφετέρου σε δεδομένα που μεταδίδονται μεταξύ υπολογιστών στο διαδίκτυο (illegal interception). Σε αρκετές, δε, περιπτώσεις, η απόκτηση πρόσβασης σε δεδομένα ηλεκτρονικού υπολογιστή ταυτίζεται με τη χρησιμοποίηση ενός ηλεκτρονικού υπολογιστή[658].

---

[655] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3154.

[656] Βλ. *Φίλιππος Ν. Ανδρέου*, Ποινικός Κώδικας, κατ' άρθρο Ερμηνεία - Νομολογία - Βιβλιογραφία, Τέταρτη Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα 2005, σελ. 1509.

[657] Το ζήτημα του πότε υφίσταται πρόσβαση σε συγκεκριμένα δεδομένα στον εικονικό κόσμο των ηλεκτρονικών υπολογιστών, όπου ουσιαστικά όλοι οι ηλεκτρονικοί υπολογιστές είναι συνδεδεμένοι και αλληλεπιδρούν μεταξύ τους με την μετάδοση δεδομένων δεν είναι τόσο ξεκάθαρο όπως στον πραγματικό κόσμο, βλ. σχετικά *Orin S. Kerr,* Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. NYU Law Review, Vol. 78, No 5, 1646-1647, ο οποίος θεωρεί ότι ο χρήστης αποκτά πρόσβαση σε ηλεκτρονικό υπολογιστή όταν αποστέλλει συγκεκριμένη εντολή σε ηλεκτρονικό υπολογιστή και αυτή εκτελείται επιτυχημένα ("a user accesses a computer any time the user sends a command to that computer that the computer executes") και ορίζει την πρόσβαση ως οποιαδήποτε επιτυχημένη αλληλεπίδραση με ηλεκτρονικό υπολογιστή ("access as any successful interaction with the computer"). Την ερμηνεία αυτή αποδέχτηκαν εμμέσως τα αμερικανικά δικαστήρια στην υπόθεση United States vs. Morris, 928 F.2d 504 (2d Cir. 1991). Με βάση τους ορισμούς αυτούς ακόμη και αυτός που απλώς εισέρχεται στην αρχική ιστοσελίδα μιας εταιρείας, όπου πρέπει να υποβάλλει το username και το password του αποκτά πρόσβαση στους ηλεκτρονικούς υπολογιστές της συγκεκριμένης εταιρείας, αφού έλαβε δεδομένα από τους ηλεκτρονικούς υπολογιστές της εταιρείας αυτής. Στην περίπτωση όμως αυτή ενδεχομένως δεν υπάρχει αξιόποινη συμπεριφορά, αφού κάθε τρίτος (μπορεί να) έχει πρόσβαση στα δεδομένα αυτά και συνεπώς έχει τη δυνατότητα και το δικαίωμα να αλληλεπιδρά με τον τρόπο αυτό με τους ηλεκτρονικούς υπολογιστές της συγκεκριμένης εταιρείας.

[658] Βλ. *Orin S. Kerr,* Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. NYU Law Review, Vol. 78, No 5, σελ. 1621, ο οποίος αναφέρει ότι η έννοια της

Με βάση την ερμηνεία του γράμματος της σχετικής διάταξης ως ***πρόσβαση εννοούμε τη συμπεριφορά εκείνη δια της οποίας κάποιος κατορθώνει να προσεγγίσει δεδομένα του υπολογιστή ενός τρίτου, χωρίς να απαιτείται κάποια πρόσθετη ενέργεια ή σκοπός*** (όπως οι αντίστοιχα αναφερόμενοι στο ά. 370Β ΠΚ, δηλαδή αντιγραφή, αποτύπωση, αποθήκευση, χρησιμοποίηση ή άλλοι, όπως διαγραφή στοιχείων, «κλοπή» χρόνου χρήσεως σύνδεσης στο διαδίκτυο, εξασφάλιση ψευδούς ψηφιακής ταυτότητας για την τέλεση άλλων αξιόποινων πράξεων κ.λπ.)[659]. Δεν απαιτείται, δηλαδή, η πρόσβαση του δράστη να γίνεται με πρόθεση βλάβης. Καθεαυτή η ως άνω διείσδυση είναι φορέας αυτοτελούς αδίκου[660].

Επίσης, δεν απαιτείται ο αποκτών πρόσβαση να λάβει γνώση των στοιχείων[661]. Έχει υποστηριχθεί ότι αρκεί η δραστηριότητά του να έφτασε σε τέτοιο σημείο ώστε το επόμενο βήμα να είναι η τέλεση μιας από τις παραπάνω ή κάποιας άλλης παρόμοιας πράξης - άρα, υπό αυτή την έννοια ως πρόσβαση πρέπει να θεωρηθεί η δυνατότητα ανάγνωσης, απόκτησης ή αλλοίωσης στοιχείων[662]. Ωστόσο, όπως επισημάνθηκε ήδη, στην αντικειμενική υπόσταση δεν περιγράφεται ως υποκειμενικό στοιχείο του αδίκου σκοπός περαιτέρω επεξεργασίας των ηλεκτρονικών πληροφοριών αλλά η διάταξη της παραγράφου 2 του ά. 370Γ ΠΚ τιμωρεί την χωρίς δικαίωμα πρόσβαση per se.

Ένα δεύτερο συστατικό στοιχείο της (χωρίς δικαίωμα) πρόσβασης είναι η αντίθεσή της προς τη θέληση του νόμιμου κατόχου των στοιχείων, ο οποίος δεν επιτρέπει την είσοδο σε αυτά, δημιουργώντας έτσι ένα είδος φράγματος έναντι στη δραστηριότητα του δράστη. Ειδικότερα, απαιτείται ο κάτοχος των στοιχείων να έχει εκφράσει με αντικειμενικά διαγνώσιμο τρόπο τη βούλησή του να απαγορεύσει την πρόσβαση σε τρίτους σε συγκεκριμένα στοιχεία[663]. Το ως άνω φράγμα δεν είναι απαραίτητο να αποτελείται από εξωτερικά στοιχεία. Κατά αυτή την έννοια, η μη εγγραφή επάνω σε

πρόσβασης ("access") δεν ορίσθηκε επακριβώς από τον αμερικανό νομοθέτη και συνεπώς η οριοθέτηση του ακριβούς περιεχομένου της εμφανίζει αρκετές δυσκολίες.

[659] Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 968.

[660] Βλ. *Χρήστος Μυλωνόπουλος*, όπ. π., σελ. 93.

[661] *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1733, *Μαρία Καϊάφα-Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμενόπουλος 2007, σελ. 1066.

[662] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156, *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1732.

[663] Βλ. *Χρήστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π. σελ. 92-93, προφανώς επηρεασμένος από την ερμηνεία της αντίστοιχης διάταξης του γερμανικού ΠΚ (202a StGB).

μαγνητικό δίσκο (π.χ. «απαγορεύεται η ανάγνωση των καταγεγραμμένων στοιχείων» ή «απαγορεύεται η χρήση της μαγνητικής ταινίας») δεν σημαίνει ότι ο νόμιμος κάτοχος του περιεχομένου της επιτρέπει την πρόσβαση σε αυτά[664]. Ωστόσο, για να μπορέσει να γίνει γνωστή η ως άνω απαγορευτική θέληση του νόμιμου κατόχου των στοιχείων θα πρέπει με κάποιον τρόπο να εξωτερικεύεται. Αρκεί η ύπαρξη μιας εντολής που να προειδοποιεί τον χρήστη, κατά τη ροή στοιχείων ή πριν από αυτήν, ότι το περιεχόμενό τους είναι ιδιωτικό και απαγορεύεται η χωρίς δικαίωμα πρόσβαση (π.χ. ύπαρξη κλειδάριθμων). Ακόμη, όμως, και στην περίπτωση που δεν υπάρχει καμία γνωστοποίηση της θέλησης του νόμιμου κατόχου, που δεν έχει δηλαδή εξωτερικευθεί με οποιοδήποτε τρόπο η βούληση του κατόχου των στοιχείων να διαφυλαχθεί η προστατευόμενη πληροφορία στη σφαίρα της ιδιωτικότητάς του, δέον είναι να ερευνηθεί εάν με βάση τις εκάστοτε συνθήκες θα έπρεπε να περιμένει κανείς ελευθερία εισόδου ή απαγόρευση σε ορισμένα στοιχεία. Θα πρέπει, δηλαδή, να αναζητηθεί και να ερμηνευθεί μία υποθετική – μη εξωτερικευμένη βούληση του νόμιμου κατόχου[665].

Σε αυτό, όμως, το σημείο ανακύπτει το ερώτημα σχετικά με το ποια είναι τα όρια που διαχωρίζουν τη θέληση από την αυθαιρεσία, ώστε συνάμα να διασφαλίζεται η βασική αρχή ότι η απόκτηση και η πρόσβαση στην πληροφορία είναι ελεύθερες. Το βέβαιο είναι ότι καθώς δεν υπάρχει ένας ορισμένος υλικός χώρος, στο πλαίσιο του οποίου να μπορεί να καθοριστεί μία φυσική κυριαρχία (ειδικά σε ό,τι αφορά τον κυβερνοχώρο), αντικειμενικά κριτήρια δεν μπορούν να δοθούν. Για τον λόγο αυτόν κάθε περίπτωση θα πρέπει να εξετάζεται in concreto και εξαρτώμενη από τις ειδικές συνθήκες, προκειμένου να εξαχθεί το συμπέρασμα εάν η απαγόρευση πρόσβασης προς ορισμένα πρόσωπα από τον νόμιμο κάτοχο στοιχείων αποτελεί έκφραση του δικαιώματος διαφύλαξης και διάθεσης των στοιχείων ή αυθαίρετη απαγόρευση της ελεύθερης ροής της πληροφορίας[666].

Πιο συγκεκριμένα, το γεγονός της σύνδεσης των στοιχείων με τον ιδιωτικό χώρο του νομίμου κατόχου τους (π.χ. όταν αυτά αποθηκεύονται στον ηλεκτρονικό υπολογιστή που βρίσκεται στην κατοικία του ή στον επαγγελματικό του χώρο) πρέπει να ερμηνευθεί ως βούλησή του να περιληφθούν αυτά στη σφαίρα ιδιωτικότητάς του. Σε

[664] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 87.

[665] Βλ. *Μ. Παπαδόπουλος*, όπ. π., σελ. 232

[666] Βλ. *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., σελ. 94.

κάθε περίπτωση, από την ίδια τη διατύπωση της διάταξης («ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους») συνάγεται ότι δεν πρέπει να απαιτείται η υπερνίκηση εμποδίων ή μέτρων ασφαλείας. Η αναφορά αυτή έχει αξία ιδίως στις περιπτώσεις άμεσης φυσικής πρόσβασης του δράστη στα δεδομένα, όπως π.χ. στην περίπτωση που κάποιος υπάλληλος εταιρίας εισέρχεται σε απαγορευμένο για αυτόν χώρο και θέτει σε λειτουργία υπολογιστή του οποίου επιτρέπεται η χρήση μόνο σε περιορισμένο αριθμό αρμοδίων υπαλλήλων[667].

Με βάση την ως άνω παραδοχή αποφεύγονται τα δυσεπίλυτα προβλήματα που προκύπτουν στην αντίστοιχη γερμανική ποινική διάταξη, η οποία αφορά μόνο τα δεδομένα τα οποία «προστατεύονται ιδιαίτερα έναντι κάθε ανεξουσιοδότητης πρόσβασης». Έτσι, στη Γερμανία υποστηρίζεται ότι ορισμένα είδη firewall, τα οποία έχουν μια εσωτερική λειτουργία προστασίας, που δεν είναι εξωτερικά αναγνωρίσιμη, δεν αποτελούν ιδιαίτερο μέτρο ασφαλείας. Επίσης, ανεπαρκή θεωρούνται και τα μέτρα ασφαλείας τα οποία μπορεί να υπερνικήσει ακόμη και ένας μη ειδικός μέσος άνθρωπος ή υποστηρίζεται ότι ένα θεωρητικά εύκολο password (π.χ. 1234) δεν αποτελεί «ιδιαίτερη προστασία»[668] έναντι μη εξουσιοδοτημένης πρόσβασης[669].

Ωστόσο, έχει υποστηριχθεί και η άποψη πως τέτοιου είδους ερμηνείες θα περιόριζαν το πεδίο προστασίας της ερευνώμενης διάταξης και θα οδηγούσαν στο να μείνουν απροστάτευτοι όσοι δεν έχουν ιδιαίτερες γνώσεις πληροφορικής και, συνεπώς, δεν μπορούν να προστατεύσουν τους ηλεκτρονικούς υπολογιστές με τεχνικά μέσα και δεν γνωρίζουν πότε τα μέτρα που λαμβάνουν είναι εύκολο να υπερνικηθούν[670] [671].

---

[667] Έτσι και η νομολογία στη μοναδική δημοσιευμένη απόφαση Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 75 (βλ. κατωτέρω την παράγραφο 5.5 του παρόντος πονήματος).

[668] Υποστηρίζεται ότι για τη δημιουργία ενός ισχυρού κωδικού πρόσβασης πρέπει να γίνεται χρήση τουλάχιστον 8 χαρακτήρων με συνδυασμό κεφαλαίων και πεζών γραμμάτων, συμβόλων και αριθμών και η λέξη που σχηματίζεται να έχει όσο το δυνατόν λιγότερο γλωσσικό νόημα. Επίσης, καλό είναι ο χρήστης να προβαίνει σε συχνή αλλαγή του (βλ. αναλυτικά το άρθρο της *Marian Merritt*, Τα «Πρέπει» και τα «Μη» των κωδικών πρόσβασης, url: http://gr.norton.com/dos-donts-passwords/article).

[669] Βλ. *Ανδρέας Δ. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα: τα αδικήματα της χωρίς άδεια απόκτησης δεδομένων (202a StGB), της παραποίησης δεδομένων (303a StGB) και της δολιοφθοράς Η/Υ (303b StGB) σε σχέση με το hacking και τη μετάδοση ηλεκτρονικών ιών στο internet, σελ. 73-74, με περαιτέρω παραπομπές σε Hildendorf, Grundfalle zum Computerstraftrecht, Μέρος ΙΙ, Jus 1996, σελ. 702-706, Koch, Aspekte des technischen und starftlichen Zugriffsschutzes vin EDV –

Systemen, RDV 1996, σελ. 123-131 και v. Gravenreuth, ο οποίος παρομοιάζει έναν εύκολο κωδικό πρόσβασης με «μια κλειδαριά στην οποία το κλειδί βρίσκεται ακόμη επάνω».

[670] Τα ανωτέρω γίνονται αντίστοιχα δεκτά και στο πλαίσιο του αμερικανικού δικαίου, βλ. *Winn Peter A.*, The Guilty Eye: Unauthorized access, Trespass and Privacy. Business Lawyer, Vol. 62, 2007, σελ. 1420.

Έντονη προβληματική προκαλεί και το ζήτημα της χάραξης των ορίων της απόπειρας της απόκτησης πρόσβασης και κατ' επέκταση της απόπειρας τέλεσης του σχετικού εγκλήματος. Στο πλαίσιο της προσπάθειας καθορισμού των ως άνω ορίων αναγκαία φαίνεται να είναι μία περιγραφή της διαδικασίας σύνδεσης (log-on) με ένα σύστημα υπολογιστή. Αρχικά ο χρήστης δίνει την αναγνωριστική του κωδική ονομασία (username) και τον κλειδάριθμό του (password). Στο δεύτερο στάδιο ακολουθεί η αναγνώριση του συνδυασμού από το σύστημα. Εάν ο συνδυασμός επαληθεύεται προσφέρεται στον χρήστη ένας πίνακας επιλογών (menu) ή η δυνατότητα να εισέλθει και να χρησιμοποιήσει τις λειτουργίες ή τις πληροφορίες του συστήματος. Τις περισσότερες φορές και για λόγους ασφαλείας σε αυτή τη φάση εμφανίζεται στην οθόνη ένα μήνυμα που προειδοποιεί ότι από εδώ και πέρα η χρήση επιτρέπεται σε πρόσωπα που έχουν το σχετικό δικαίωμα. Το τρίτο στάδιο αρχίζει με τη χρησιμοποίηση από τον δράστη των δυνατοτήτων που του προσφέρθηκαν κατά το αμέσως προηγούμενο στάδιο.

Ξεκινώντας από το τέλος δεν υπάρχει αμφιβολία ότι κατά το τρίτο στάδιο ο δράστης έχει ήδη αποκτήσει πρόσβαση. Κατά το δεύτερο στάδιο ο δράστης έχει «προκαλέσει» το σύστημα να του παρουσιάσει τις λειτουργίες του και έχει την πρακτική δυνατότητα να τις χρησιμοποιήσει. Σε αυτό το σημείο ο δράστης έχει διαπράξει αυτό που η διάταξη ονομάζει «απόκτηση πρόσβασης», εφόσον το επόμενο βήμα είναι η απόκτηση πληροφοριών. Κατά το πρώτο, δε, στάδιο ο δράστης προσπαθεί ακόμα να εισέλθει στο σύστημα. Προκαλεί, δηλαδή, κάποιες παρενοχλήσεις στη λειτουργία του προκειμένου να υλοποιήσει τους περαιτέρω σκοπούς του. Άρα, η δραστηριότητα του δράστη κατά το πρώτο στάδιο παραμένει ακόμη στο χώρο της απόπειρας απόκτησης πρόσβασης[672]. Ωστόσο, πρέπει να επισημανθεί ότι η απόπειρα του εγκλήματος της παρ. 2 του άρθρου 370 ΠΚ μπορεί να μείνει ατιμώρητη σύμφωνα με την παρ. 3 του άρθρου 42 ΠΚ, η οποία συνιστά λόγο δικαστικής άφεσης του αξιοποίνου[673].

Με βάση, δε, τη διατύπωση και τη γραμματική ερμηνεία της σχετικής διάταξης πρέπει να γίνει δεκτό ότι η πλήρωση του αντικειμενικού στοιχείου της απόκτησης πρόσβασης δεν απαιτεί ο δράστης να έχει έλθει σε γνώση, οπτικά ή ακουστικά, των

---

[671] Βέβαια, σήμερα η πρόσβαση στην πληροφορία είναι αρκετά εύκολη. Θεωρώ, λοιπόν, ότι όποιος επιθυμεί να προστατεύσει το σύστημα πληροφοριών που διαχειρίζεται μπορεί να λάβει, ακόμη και χωρίς τη συνδρομή τεχνικού, κάποια βασικά μέτρα ασφαλείας.

[672] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π. σελ. 87.

[673] Βλ. *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1734.

στοιχείων ούτε να τα έχει «αποκτήσει» με την έννοια π.χ. της αφαίρεσης και της πρόσκτησης – ιδιοποίησης του εγκλήματος της κλοπής[674] (π.χ. με τη μεταφορά τους σε δικό του υλικό φορέα ή με την απόκτηση κατοχής του υλικού φορέα στον οποίο είναι αυτά αποθηκευμένα) ή με αντιγραφή τους. Στην περίπτωση, όμως, κατά την οποία τα εν λόγω στοιχεία είναι κωδικοποιημένα - κρυπτογραφημένα[675], θα πρέπει να γίνει δεκτό ότι ο δράστης αποκτά πρόσβαση μόνο όταν καταφέρει να τα αποκωδικοποιήσει ή να τα αποκρυπτογραφήσει[676] (όταν δηλαδή έχει στην κατοχή του και το «κλειδί» που απαιτείται για την αποκωδικοποίηση-αποκρυπτογράφησή τους).

Στην πραγματικότητα αρκετές φορές είναι δύσκολο έως αδύνατο να γίνει διάκριση ανάμεσα στην απλή απόκτηση χωρίς δικαίωμα πρόσβασης σε στοιχεία και στη γνώση των στοιχείων αυτών[677]. Κατά την είσοδο του δράστη σε ένα σύστημα πληροφοριών εμφανίζονται στην οθόνη αυτόματα και υποχρεωτικά, ανεξάρτητα δηλαδή από τη δική του βούληση, τα πρώτα δεδομένα που είναι αποθηκευμένα σε αυτό. Το περιεχόμενο των στοιχείων αυτών, ή τουλάχιστον ενός μέρους αυτών, ο δράστης το διαβάζει σε κάθε περίπτωση καθώς μόνο έτσι μπορεί να καταλάβει εάν όντως η εισβολή του είναι επιτυχημένη και βρίσκεται στο σύστημα που ήθελε να εισέλθει. Γι' αυτό και μπορεί να υποστηριχθεί ότι πρακτικά σε ό,τι αφορά τη γνώση των στοιχείων η «διείσδυση» είναι πολύ δύσκολο να διακριθεί από το «κατέβασμα» (downloading) των στοιχείων (εξάλλου, σε περίπτωση απομακρυσμένης πρόσβασης τμήμα των στοιχείων δύναται να «κατέβει» σε προσωρινή μνήμη αποθήκευσης του υπολογιστή του δράστη).

5.1.3.3 Προσέγγιση της έννοιας «χωρίς δικαίωμα»

Η φράση «χωρίς δικαίωμα» αποτελεί στοιχείο της αντικειμενικής υπόστασης του εγκλήματος του ά. 370Γ παρ. 2 ΠΚ. Αναφορικά προς την πρώτη έννοιά της είναι

[674] Αναφορικά με το έγκλημα της κλοπής πρβλ. την εμπεριστατωμένη ανάλυση του *Χρήστου Μυλωνόπουλου*, Ποινικό Δίκαιο - Ειδικό μέρος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2001, σελ. 4 επ.

[675] Για την κρυπτογράφηση βλ. και σχετική ανάπτυξη στην παράγραφο 9.1.5 του παρόντος πονήματος.

[676] Βλ. *Ανδρέας Δ. Αργυρόπουλος*, όπ. π., σελ. 78, με περαιτέρω παραπομπές σε *Hilgendorf* (υποσ. 225), σελ. 705.

[677] Βλ. και παράγραφο 5.3.2 για τις αποδεικτικές δυσχέρειες αναφορικά με την περιέλευση σε γνώση των ηλεκτρονικών στοιχείων.

βέβαιον ότι πρόκειται για συγκατάθεση[678], η οποία αποκλείει την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος και δεν αίρει απλώς τον άδικο χαρακτήρα της πράξεως, αφού, όταν αυτή συντρέχει, δεν υφίσταται καν προσβολή του εννόμου αγαθού[679]. Σύμφωνη με την παραδοχή αυτή είναι και η νομολογία, η οποία συμπληρώνει ότι *«η χρησιμοποίηση προγραμμάτων που ανήκουν σε άλλους τιμωρείται σε κάθε περίπτωση που λαμβάνει χώρα, χωρίς σχετικό δικαίωμα, γεγονός που διευρύνει υπερβολικά το αξιόποινο και οδηγεί στο συμπέρασμα ότι με τη διάταξη αυτή δεν κολάζονται μόνο οι σοβαρές προσβολές (π.χ. δημόσια εκτέλεση ενός προγράμματος) αλλά και οι πλέον μηδαμινές (π.χ. χρησιμοποίηση του προσωπικού υπολογιστή συναδέλφου που απουσιάζει, του υπολογιστή τσέπης άλλου κ.λπ.)».*[680]. Ωστόσο, οι όποιες τυχόν δυσμενείς συνέπειες της διεύρυνσης του αξιοποίνου σαφώς περιορίζονται από το γεγονός ότι το έγκλημα διώκεται κατ' έγκληση, όπως προβλέπεται στην τελευταία παράγραφο του οικείου άρθρου.

Άλλη μία απόδειξη του ότι το στοιχείο «χωρίς δικαίωμα» συνιστά μέρος της αντικειμενικής υπόστασης του εγκλήματος αποτελεί η ίδια η βούληση του ποινικού νομοθέτη, ο οποίος, όπως σημειώθηκε ανωτέρω, θέλησε μέσω της σχετικής διάταξης να απαγορεύσει την πρόσβαση σε στοιχεία που βρίσκονται σε ορισμένους χώρους και υπό την κυριαρχία ενός ορισμένου προσώπου και όχι απλά «την πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή» γενικώς. Το δεύτερο θα οδηγούσε αναπόφευκτα σε μονοπώλιο της πληροφορίας και κατά συνέπεια σε αποτελέσματα που ένας νομοθέτης, ως εκφραστής του δημοκρατικού πολιτεύματος, δεν θα μπορούσε ποτέ να επιδιώξει[681].

---

[678] Για τη διάκριση μεταξύ συγκατάθεσης και συναίνεσης στο ποινικό δίκαιο βλ. *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, όπ. π., σελ. 336 επ.

[679] Βλ. *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., σελ. 95, *Αριστοτέλης Χαραλαμπάκης – Ιωάννης Γιαννίδης*, όπ. π., σελ. 1624, *Αλέξανδρος Π. Κωστάρας*, Ποινικός Κώδικας και Ειδικοί Ποινικοί Νόμοι, Εκδόσεις Αντ. Ν. Σάκκουλα 2008, σελ. 751, *Ιωάννης Μανωλεδάκης*, Ερμηνεία κατ' άρθρο των όρων του Ειδικού μέρους του Ποινικού Κώδικα, Εκδόσεις Π. Ν. Σάκκουλα Α.Ε., 1996, σελ. 29, *Φίλιππος Ν. Ανδρέου*, όπ. π., σελ. 1509. Ο *Ανδρέας Δ. Αργυρόπουλος*, Ηλεκτρονική Εγκληματικότητα, όπ. π. σελ. 84, σχετικά με το στοιχείο «χωρίς άδεια» της γερμανικής διάταξης 202 a StGB, αναφέρει ότι η συναίνεση του δικαιούχου στην απόκτηση των δεδομένων από το δράστη αποτελεί στην ουσία συγκατάθεση, η οποία αίρει την τυπικότητα της πράξης και αποκλείει την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος.

[680] Βλ. απόφ. Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 76, με την οποία καταδικάστηκε για παράνομη χρησιμοποίηση προγράμματος υπολογιστή ο κατηγορούμενος κελευστής, ο οποίος εισήλθε στο γραφείο του Κυβερνήτη του πλοίου, όπου υπηρετούσε, αν και δεν περιλαμβανόταν στο εξουσιοδοτημένο προσωπικό, έθεσε σε λειτουργία τον ηλεκτρονικό υπολογιστή και χρησιμοποιώντας εγκατεστημένο πρόγραμμα προέβη σε εκτύπωση ορισμένων εγγράφων.

[681] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 90.

Η μη συγκατάθεση του νόμιμου κατόχου δεν είναι απαραίτητο να εκδηλώνεται με εξωτερικά στοιχεία, και δη επί των υλικών φορέων, αλλά αρκεί να εκδηλώνεται και από άλλα στοιχεία ή δύναται να συνάγεται και από τις εκάστοτε συγκεκριμένες συνθήκες[682]. Το βέβαιον είναι ότι η θέληση του νομίμου κατόχου πρέπει να συνίσταται στη βούλησή του κατά τον χρόνο τέλεσης να μην περιέλθουν τα στοιχεία στη σφαίρα εξουσίας του δράστη.

Ταυτόχρονα, ο νομοθέτης προέβη και σε μία ενδεικτική αναφορά (*ιδίως*) περιπτώσεων της χωρίς δικαίωμα πρόσβασης, όπως είναι *η παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχος*. Στην περίπτωση του διαδικτύου (internet), η ως άνω αναφορά θα πρέπει να περιορισθεί στη λήψη μέτρων ασφαλείας από το νόμιμο κάτοχο. Τούτο διότι μόνο τα τελευταία δύνανται να εμποδίσουν ουσιαστικά τη διαδικτυακή διείσδυση (π.χ. κωδικοί εισόδου, κωδικοποίηση δεδομένων, ειδικά σημεία ανίχνευσης, μαγνητικές κάρτες, κλείδωμα ηλεκτρονικού υπολογιστή, του πληκτρολογίου ή της οθόνης κ.λπ.)[683]. Βέβαια, η χωρίς δικαίωμα πρόσβαση στα στοιχεία είναι αξιόποινη και χωρίς παραβίαση μέτρων ασφαλείας, αρκεί η αντίθετη βούληση του κατόχου να έχει εκδηλωθεί με αντικειμενικά διαγνώσιμο τρόπο[684]. Η παραβίαση απαγορεύσεων έχει κυρίως αξία στις περιπτώσεις άμεσης φυσικής πρόσβασης του δράστη στα δεδομένα (π.χ. στην περίπτωση που κάποιος υπάλληλος εταιρείας εισέρχεται σε απαγορευμένο γι' αυτόν χώρο και θέτει σε λειτουργία υπολογιστή του οποίου επιτρέπεται η χρήση σε αυστηρά κλειστό αριθμό υπαλλήλων)[685].

Ωστόσο, η απάντηση στο ερώτημα εάν κάποιο πρόσωπο πράττει με ή χωρίς δικαίωμα όταν εισέρχεται σε στοιχεία που είναι αποθηκευμένα σε σύστημα υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών δεν είναι πάντοτε εύκολη. Κι αυτό διότι είναι εξαιρετικά δύσκολο να δοθούν γενικά κριτήρια. Συνήθως, το δικαίωμα παρέχεται από τον ίδιο τον νόμιμο κάτοχο στοιχείων, όπως συμβαίνει στην περίπτωση κατά την οποία ένας τρίτος αποκτά τη δυνατότητα, κατόπιν αμοιβής, να χρησιμοποιεί ορισμένα στοιχεία (τράπεζες στοιχείων). Στην περίπτωση τώρα που ο τρίτος επεξεργαστεί τα στοιχεία, εφόσον η πράξη του αυτή ξεπερνάει τα όρια της

[682] Βλ. παράγραφο 5.1.3.2 του παρόντος πονήματος.

[683] Βλ. *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., σελ. 98.

[684] *Μ. Καϊάφα Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, όπ. π., σελ. 1065.

[685] Βλ. *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, όπ. π., σελ. 126.

σύμβασης, μπορεί να τιμωρηθεί σύμφωνα με άλλες νομικές διατάξεις[686] και όχι επειδή τέλεσε τη χωρίς δικαίωμα πρόσβαση σε στοιχεία.

Ζήτημα δημιουργείται στην περίπτωση που ο δράστης έχει δικαίωμα πρόσβασης στα στοιχεία, αλλά χρησιμοποιεί την εξουσιοδότηση για διαφορετικό σκοπό (ulterior purpose)[687] από αυτόν που του έχει δοθεί (π.χ. υπάλληλος τράπεζας που έχει πρόσβαση στο αρχείο των υποχρεώσεων των πελατών της εταιρείας, χρησιμοποιεί δολίως τη δυνατότητά του αυτή για να δώσει πληροφορίες σε τρίτα πρόσωπα, τα οποία δεν έχουν δικαίωμα να λάβουν γνώση). Εάν η εξουσιοδότηση πρόσβασης έχει δοθεί σιωπηρά ή ρητά για την επίτευξη συγκεκριμένου σκοπού και για συγκεκριμένο κομμάτι των αρχείων, η απόκτηση πρόσβασης για την εκπλήρωση διαφορετικού σκοπού θα πρέπει να θεωρηθεί ότι γίνεται χωρίς δικαίωμα. Εάν όμως δεν έχει ορισθεί συγκεκριμένος σκοπός δεν θα πρέπει να θεωρηθεί ότι γίνεται χωρίς δικαίωμα[688]. Συνεπώς, η καθ' υπέρβαση των σαφών ορίων της θέλησης του νόμιμου κατόχου πρόσβαση συνιστά πρόσβαση χωρίς δικαίωμα[689].

Αντίθετη φαίνεται να είναι η άποψη σύμφωνα με την οποία εάν ο υπάλληλος, στον οποίο είναι εμπεπιστευμένα τα στοιχεία από τον ίδιο τον νόμιμο κάτοχο, γνωστοποιήσει σε τρίτους το περιεχόμενο των στοιχείων ή το εκμεταλλεύεται ο ίδιος πέρα από τα όρια των υπαλληλικών του δικαιωμάτων, θα έχουμε να κάνουμε με παράνομη συμπεριφορά προβλεπόμενη από άλλους νομικούς κανόνες και όχι με την αξιόποινη συμπεριφορά του ά. 370Γ παρ. 2 ΠΚ[690].

Λύση στο ως άνω θέμα δίνει η ίδια η διάταξη της παρ. 3 του ά. 370Γ ΠΚ, εισάγοντας ειδικό λόγο περιορισμού της αντικειμενικής υπόστασης του εγκλήματος[691]. Συγκεκριμένα, στη συνήθη περίπτωση που ο εργαζόμενος αποκτά μια de facto πρόσβαση σε στοιχεία του εργοδότη – νόμιμου κατόχου, ως φυσική συνέπεια της

---

[686] Π.χ. με τον ν. 2472/1997 για την προστασία δεδομένων προσωπικού χαρακτήρα.

[687] Βλ. *Alex Steel,* Vaguely Going Where No-One Has Gone: The expansive New Computer Offences, σελ. 80-81.

[688] Έτσι και το Supreme Court of Victoria στην υπόθεση Director of Public Prosecutions v. Murdoch [1993] 1 V.R. 406, Βλ. *Peter A. Winn*, The Guilty Eye: Unauthorized access, Trespass and Privacy. Business Lawyer, Vol. 62, 2007, σελ. 1410.

[689] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156.

[690] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 91.

[691] Άρθρο 370Γ παρ. 3: «*Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του*».

εργασιακής του σχέσης η πρόσβαση τιμωρείται μόνο εφόσον απαγορεύεται ρητώς από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του. Η εν λόγω διάταξη εξειδικεύει την αντικειμενική υπόσταση του εγκλήματος σε ορισμένες περιπτώσεις και συνιστά μια νομικοπολιτικού χαρακτήρα επιλογή από πλευράς του ποινικού νομοθέτη. Κι αυτό διότι συχνά οι εργαζόμενοι δεν δίνουν ιδιαίτερη σημασία στα όρια μέσα στα οποία δικαιούνται να ασκήσουν το δικαίωμα πρόσβασης στα στοιχεία του εργοδότη τους ή από αμέλεια δεν συνειδητοποιούν πότε τα υπερβαίνουν. Τα όρια ανάμεσα στην επιτρεπόμενη και μη συμπεριφορά του υπαλλήλου δύνανται να καθοριστούν και από τη σχετική σύμβαση εργασίας του[692]. Πρέπει να γίνει δεκτό ότι η ως άνω διάταξη αφορά μόνο τα στοιχεία του νομίμου κατόχου που έχουν σχέση με την επαγγελματική του δραστηριότητα και όχι άλλα προσωπικά του στοιχεία που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του. Ωστόσο, η εφαρμογή της διάταξης αυτής ως προς το τελευταίο καθίσταται δυσχερής γιατί πολλές φορές είναι πιθανό, παραδείγματος χάριν σε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται για εταιρικούς σκοπούς, να περιέχονται τόσο επαγγελματικά όσο και προσωπικά ηλεκτρονικά μηνύματα. Σε αυτές τις περιπτώσεις προκύπτει ζήτημα εάν προστατεύονται τα προσωπικά μηνύματα του κατόχου ή υφίσταται εικαζόμενη συναίνεση-συγκατάθεση του κατόχου (αφού γνωρίζει ότι πρόκειται για εταιρικό λογαριασμό ηλεκτρονικού ταχυδρομείου, στον οποίο ενδεχομένως έχουν πρόσβαση και άλλοι υπάλληλοι) που αποκλείει την πλήρωση της αντικειμενικής υπόστασης ή εάν ο δράστης μπορεί να επικαλεστεί πραγματική πλάνη, αφού πίστευε ότι ανοίγει έναν εταιρικό λογαριασμό ηλεκτρονικού ταχυδρομείου με μηνύματα αμιγώς επαγγελματικού περιεχομένου. Σε αυτήν την περίπτωση καθοριστική θα είναι η τυχόν υπάρχουσα απαγόρευση χρήσης του εταιρικού λογαριασμού ηλεκτρονικού ταχυδρομείου για μη επαγγελματικούς σκοπούς, οπότε θα είναι ευκολότερο να στοιχειοθετηθεί η πραγματική πλάνη[693] του δράστη.

Ιδιαίτερης μνείας χρήζει η περίπτωση που το δικαίωμα πρόσβασης ανήκει σε πλείονα πρόσωπα (ακόμη και στο ευρύ κοινό), αλλά η συγκατάθεση του κατόχου εξαρτάται από ορισμένες προϋποθέσεις, όπως παραδείγματος χάριν από την καταβολή

[692] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 92.

[693] Για την πραγματική πλάνη βλ. *Λ. Κοτσαλή*, Ποινικό Δίκαιο – Γενικό Μέρος, τομ. 1, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005 σελ. 529 επ. και *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, τομ. 1, όπ. π., σελ. 502 επ.

τιμήματος (παροχή πληροφοριών από databank). Στην περίπτωση αυτή το έγκλημα του ά. 370Γ παρ.2 ΠΚ τελείται με την πρόσβαση χωρίς την πλήρωση της σχετικής προϋπόθεσης[694].

Ως προς τη δεύτερη έννοια του στοιχείου «χωρίς δικαίωμα», δηλαδή τη μη ύπαρξη δικαιώματος που παρέχεται από τον νόμο, προφανώς και εξαιρούνται περιπτώσεις όπου η πρόσβαση σε στοιχεία είναι νόμιμη διότι αναγνωρίζεται ρητώς από σχετική νομική διάταξη (π.χ. ανακριτικές πράξεις).

Τέλος, δύναται πράξη του ά. 370Γ παρ. 2 ΠΚ να τελεστεί χωρίς δικαίωμα αλλά να αρθεί το άδικό της αν πληρούνται οι προϋποθέσεις κάποιου λόγου άρσης του αδίκου (ά. 25 ΠΚ, ά. 253 ΚΠΔ, ά. 262 ΚΠΔ)[695].

5.1.3.4 Η έννοια του «νόμιμου κατόχου»

Ο εννοιολογικός προσδιορισμός του *νόμιμου κατόχου* κρίνεται εξίσου αναγκαίος διότι, σύμφωνα με τα αμέσως προεκτεθέντα, η από μέρους του συγκατάθεση ή μη οδηγεί στην πλήρωση ή μη αντίστοιχα της αντικειμενικής υπόστασης του εξεταζόμενου εγκλήματος.

Συγκεκριμένα, η κατοχή – με δεδομένη την άυλη φύση της πληροφορίας - νοείται ως η πραγματική κατάσταση, η οποία παρέχει σε κάποιον τη δυνατότητα να απολαμβάνει την κάθε είδους ωφέλεια του εννόμου αγαθού. Όπως ήδη επισημάνθηκε κατά την εννοιολογική προσέγγιση του προστατευόμενου εννόμου αγαθού, ο νόμιμος κάτοχος είναι το πρόσωπο που έχει την τυπική εξουσία, το δικαίωμα διαθέσεως των στοιχείων, με την έννοια ότι έχει τη δυνατότητα να ορίζει σε ποιους αποκλείεται και σε ποιους επιτρέπεται η πρόσβαση σε αυτά. Συνεπώς, ο νόμιμος κάτοχος δεν είναι άλλος παρά ο φορέας του προστατευόμενου έννομου αγαθού της διάταξης του ά. 370Γ παρ. 2 ΠΚ.

Για τον ειδικότερο προσδιορισμό του νόμιμου κατόχου θα πρέπει να γίνει διάκριση ανάμεσα στα στοιχεία που είναι αποθηκευμένα σε σύστημα υπολογιστή ή στις

[694] *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., σελ. 94, *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1733.
[695] Βλ. *Ι. Ιγγλεζάκη*, Δίκαιο της πληροφορικής. όπ. π., σελ. 280.

βοηθητικές του μνήμες και στα στοιχεία που βρίσκονται σε διαδικασία διαβίβασης. Στην πρώτη περίπτωση, ο βασικός δικαιούχος είναι ο δικαιούχος της θέσης αποθήκευσης, εκείνος δηλαδή που συγκεντρώνει κάθε φορά τα δεδομένα και τα αποθηκεύει στον υλικό φορέα τους ή τουλάχιστον αυτός κατ' εντολήν του οποίου πραγματοποιείται η πράξη εγγραφής[696]. Στη δεύτερη περίπτωση, δικαιούχος διαθέσεως μπορεί να είναι και ο παραλήπτης τους κατά το «κατέβασμα» ή την ολοκλήρωση της λήψης τους[697]. Η τοποθέτηση απαγορεύσεων και οργανωτικών ή τεχνικών μέτρων ασφαλείας εκδηλώνει ότι τα στοιχεία βρίσκονται στην κατοχή κάποιου και ότι αυτός θέλει να απαγορεύσει πρόσβαση άλλου σε αυτά χωρίς τη θέλησή του (π.χ. σε περίπτωση λογαριασμού ηλεκτρονικού ταχυδρομείου ή νεφελοειδούς αποθήκευσης ηλεκτρονικών στοιχείων). Επίσης, νόμιμος κάτοχος είναι όχι μόνο ο παραγωγός αλλά και αυτός που αποκτά το δικαίωμα χρήσης, το δικαίωμα δηλαδή να έρχεται σε πρόσβαση κατά ορισμένο τρόπο με τα ηλεκτρονικά στοιχεία - πληροφορίες[698].

Σημειώνεται ότι *ο βοηθός κατοχής*[699] ή *φύλακας κατοχής* δεν έχει το δικαίωμα εξουσίας, έστω κι αν έχει πρόσβαση στα στοιχεία, δεδομένου ότι αυτός βοηθά μόνο τον κάτοχο να επενεργεί στα στοιχεία.

Η κυριότητα και η κατοχή των υλικών φορέων στα οποία είναι καταγεγραμμένα τα στοιχεία ή δια των οποίων αυτά μεταδίδονται δεν ενδιαφέρει εν προκειμένω. Εξάλλου, πλέον τα τελευταία έτη έχουν αναπτυχθεί στο διαδίκτυο τα λεγόμενα νεφελοειδή συστήματα αποθήκευσης ("cloud computing")[700] όπου ο χρήστης δύναται να αποθηκεύει πληροφορίες σε έναν ή περισσότερους servers στο διαδίκτυο (ακόμη και έναντι χρηματικού αντιτίμου για τη δυνατότητα αποθήκευσης δεδομένων μεγάλου όγκου σε bytes). Ο μοναδικός σύνδεσμος του νόμιμου κατόχου των στοιχείων με τους υλικούς φορείς που τα περιέχουν είναι τα τεχνικά μέτρα ασφαλείας

---

[696] Βλ. *Ανδρέας Δ. Αργυρόπουλος*, όπ. π., σελ. 94-95, με περαιτέρω παραπομπές σε Meier (υποσ.110), σελ. 661.

[697] Βλ. *Ανδρέας Δ. Αργυρόπουλος*, όπ. π. σελ. 94-95, με περαιτέρω παραπομπές σε Mühle, Schönke-Schröder-Leckner (υποσ.110), σελ. 63.

[698] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3155.

[699] Για την έννοια του βοηθού κατοχής στο αδίκημα της κλοπής πρβλ. *Χρ. Μυλωνόπουλο*, Ποινικό δίκαιο – Ειδικό μέρος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2001, σελ. 36 επ.

[700] Π.χ. η ιστοσελίδα www.dropbox.com ή η λειτουργία Drive της Google.

που εμποδίζουν την πρόσβαση τρίτων σε αυτά (π.χ. username και password)[701]. Επίσης, είναι αδιάφορο ποιον αφορά το περιεχόμενο των στοιχείων. Συνεπώς, ακόμη και εάν πρόκειται για στοιχεία που αφορούν κάποιο πρόσωπο[702], το πρόσωπο το οποίο αφορούν δεν δικαιούται κατά τη διάταξη του ά. 370Γ παρ. 2 ΠΚ να διεισδύει σε αυτά, εφόσον δεν του παρέχεται άδεια από τον νόμιμο κάτοχό τους. Προστασία του προσώπου που αφορούν τα προσωπικά στοιχεία από τυχόν αυθαιρεσίες του νόμιμου κατόχου τους δίνεται μέσα από το πλαίσιο ειδικών νομικών διατάξεων που προφυλάσσουν και χαράζουν τα όρια της ηλεκτρονικής επεξεργασίας προσωπικών στοιχείων[703].

Τέλος, όπως ειπώθηκε ήδη, αν ο δικαιούχος επιτρέψει την πρόσβαση στα ηλεκτρονικά του δεδομένα τότε πρόκειται για συγκατάθεση, καθώς αίρεται η ίδια η τυπικότητα της πράξης και δεν πληρούται η αντικειμενική υπόσταση του εν λόγω εγκλήματος[704].

5.1.4 Υποκειμενική υπόσταση του εγκλήματος

Για την πλήρωση της υποκειμενικής υπόστασης του εγκλήματος της παρ. 2 του ά. 370Γ ΠΚ και δεδομένης της τυποποίησης του ως πλημμελήματος (ποινή φυλάκισης ή χρηματική ποινή) απαιτείται, από τον συνδυασμό των διατάξεων των άρθρων 26 παρ. 1 και 27 παρ.1 ΠΚ, δόλος οποιουδήποτε βαθμού, ο οποίος πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος. Αρκεί, δηλαδή, και η ύπαρξη ενδεχόμενου δόλου εκ μέρους του δράστη[705]. Υποστηρίζεται και η αντίθετη άποψη ότι δεν αρκεί ενδεχόμενος δόλος αλλά απαιτείται άμεσος δόλος (α΄ ή β΄ βαθμού) του δράστη διότι η παράνομη πράξη της πρόσβασης πρέπει να γίνεται χωρίς

[701]Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 84.

[702] ...τα οποία βέβαια έχουν συννόμως αρχειοθετηθεί και τεθεί σε επεξεργασία σύμφωνα και με τις διατάξεις του ν. 2472/1997 για την προστασία δεδομένων προσωπικού χαρακτήρα.

[703] Όλως ενδεικτικώς ν. 2472/1997 για την προστασία των δεδομένων προσωπικού χαρακτήρα.

[704] Έτσι και ο Αργυρόπουλος αναφορικά με την αντίστοιχη γερμανική διάταξη (βλ. *Αν. Αργυρόπουλος*, Ηλεκτρονική εγκληματικότητα, όπ. π., σελ. 84).

[705] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156, *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 971 και *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1733.

δικαίωμα, απαιτείται δηλαδή η γνώση ορισμένου περιστατικού, η οποία ως γνωστόν αποκλείει τον ενδεχόμενο δόλο (ά. 27 παρ. 2 εδάφιο α' ΠΚ)[706].

Ωστόσο, ορθή φαίνεται να είναι η πρώτη άποψη, αφού η εν λόγω διάταξη της παρ. 2 του ά. 370Γ ΠΚ ποινικοποιεί ως εγκληματική συμπεριφορά τη χωρίς δικαίωμα πρόσβαση σε στοιχεία καθεαυτή χωρίς να απαιτείται για την πλήρωση της υποκειμενικής υπόστασης οποιοδήποτε άλλο πρόσθετο υποκειμενικό στοιχείο του αδίκου (π.χ. γνώση των στοιχείων ή σκοπός παράνομου περιουσιακού οφέλους ή σκοπός αλλοίωσης ή διαγραφής των στοιχείων) και ιδίως γνώση της τυχόν έλλειψης δικαιώματος εκ μέρους του δράστη.

5.1.5 Ποινή του εγκλήματος - Σύγκριση και συρροή με άλλα εγκλήματα

Ο ποινικός νομοθέτης τυποποιεί το έγκλημα της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά στοιχεία σε βαθμό πλημμελήματος, ορίζοντας το πλαίσιο της ποινής σε φυλάκιση μέχρι τρεις μήνες ή σε χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών [πλέον 29,00 ευρώ]. Ωστόσο, πρέπει να επισημανθεί η αναντιστοιχία που αναδεικνύεται εάν συγκρίνει κανείς τις προβλεπόμενες ποινές άλλων σχετικών αξιόποινων πράξεων, όπως εκείνων των ά. 370Α ΠΚ (παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας)[707] και 370 ΠΚ (παραβίαση του απορρήτου των επιστολών) αναφορικά με το ότι στα δύο τελευταία εγκλήματα προβλέπονται πιο αυστηρές ποινές.

Συγκεκριμένα, η χωρίς δικαίωμα πρόσβαση του δράστη σε στοιχεία υπολογιστή, τα οποία μεταδίδονται μέσω διαδικτύου, φαίνεται να είναι αντίστοιχη – ως προς το απαξιολογικό της περιεχόμενο – με την «παγίδευση» ακόμη και συστήματος υλικού ή λογισμικού για την παρακολούθηση τηλεφωνικής συνδιαλέξεως (ά. 370Α παρ. 1

[706] Βλ. *Ειρήνη Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, όπ. π., σελ. 93.

[707] Βλ. για το ά. 370Α ΠΚ το άρθρο της *Δ. Παπαδοπούλου*, Η νομική προστασία του δικαιώματος για ελεύθερη επικοινωνία, ΠοινΔικ 2/2009, σελ. 210 επ.

ΠΚ)[708]. Αρχικά, σε κάθε περίπτωση, θεωρώ ότι η χωρίς δικαίωμα πρόσβαση δεν δύναται να συμπεριλαμβάνεται στην έννοια της παγίδευσης ή με οποιονδήποτε άλλο τρόπο παρέμβασης σε σύστημα υλικού ή λογισμικού καθώς η πρόσβαση μοναχά δεν μπορεί να ενταχθεί εννοιολογικά στην έννοια της παρέμβασης. Σε τέτοια, εξάλλου, περίπτωση θα πρέπει να εφαρμοστεί η διάταξη του ά. 370Γ παρ. σύμφωνα και με την αρχή της ειδικότητας, αφού η διάταξη αυτή αναφέρεται συγκεκριμένα σε πρόσβαση. Υπάρχει όμως και η περίπτωση αληθινής πραγματικής συρροής των δύο διατάξεων όταν κάποιος αποκτά χωρίς δικαίωμα πρόσβαση και «παγιδεύει» ή «παρεμβαίνει» σε υλικό ή λογισμικό παροχής τηλεφωνικών υπηρεσιών με σκοπό να πληροφορηθεί το περιεχόμενο της τηλεφωνικής συνδιάλεξης (βέβαια, πρέπει να θεωρηθεί ότι από τη χωρίς δικαίωμα πρόσβαση αυτή δεν προέκυψε κίνδυνος για την ασφάλεια των τηλεφωνικών επικοινωνιών προκειμένου να μην εφαρμοστεί το ά. 292Α ΠΚ)[709]. Στο πλαίσιο της συστημικής συνύπαρξης των ποινικών διατάξεων, θα μπορούσε να υποστηριχθεί ότι η σημαντική αυτή απόκλιση ποινής (κακούργημα το ά. 370 Α παρ. 1

[708] Άρθρο 370Α - Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας.

«*1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.*

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.

3. Με κάθειρξη μέχρι δέκα ετών τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από πενήντα πέντε χιλιάδες (55.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ.

5. Αν οι πράξεις των παραγράφων 1 και 3 αυτού του άρθρου συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, τιμωρούνται κατά τα άρθρα 146 και 147 του Ποινικού Κώδικα.».

[709] Βλ. και κατωτέρω παράγραφο 5.2.4.

ΠΚ[710], πλημμέλημα το ά. 370Γ παρ. 2 ΠΚ), είναι εντελώς αδικαιολόγητη. Δυνάμει των ανωτέρω, ο Κιούπης υποστηρίζει ότι αυτό το χαμηλό πλαίσιο ποινής δημιουργεί ένα τεράστιο κενό ποινικής προστασίας[711].

Επίσης, η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά στοιχεία ομοιάζει και με το έγκλημα της παραβίασης του απορρήτου των επιστολών, όπως αυτό τυποποιείται στο ά. 370 ΠΚ[712]. Δεδομένης, δε, της διευρυμένης έννοιας του εγγράφου στο ά. 13 εδάφιο

---

[710] Το ά. 370Α ΠΚ διευρύνθηκε υποκειμενικά και αντικειμενικά και αναβαθμίστηκε σε κακούργημα με το ά. 10 του ν. 3674/2008 (βλ. σχετικά και *Δ. Παπαδοπούλου*, Η νομική προστασία του δικαιώματος για ελεύθερη επικοινωνία, όπ. π., σελ. 214 επ.). Η προηγούμενη διατύπωσή του είχε ως εξής:

«Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση. Η χρησιμοποίηση από το δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκε με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνητά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων, τιμωρείται με φυλάκιση. Με την ίδια ποινή τιμωρείται και όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου. Το δεύτερο εδάφιο της παραγρ. 1 αυτού του άρθρου εφαρμόζεται και σ' αυτή την περίπτωση.

3. Με φυλάκιση τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Η πράξη της παραγρ.3 δεν είναι άδικη αν η χρήση έγινε ενώπιον οποιουδήποτε δικαστηρίου, ανακριτικής ή άλλης δημόσιας αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος που δε μπορούσε να διαφυλαχθεί διαφορετικά και ιδίως σε ποινικό δικαστήριο για την υπεράσπιση του κατηγορουμένου και γενικά αν η χρήση έγινε για την εκπλήρωση καθήκοντος του κατηγορουμένου ή για τη διαφύλαξη έννομου ή άλλου δικαιολογημένου ουσιώδους δημοσίου συμφέροντος.

5. Η ποινική δίωξη της πράξης της παραγράφου 3 γίνεται μόνο με έγκληση.

6. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι ιδιωτικός αστυνομικός ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή απέβλεπε στην είσπραξη αμοιβής επιβάλλεται φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή.

7. Όποιος διαθέτει στο εμπόριο ή μ' άλλο τρόπο προσφέρει για εγκατάσταση τεχνικά μέσα ειδικά μόνο για την τέλεση των πράξεων των παραγράφων 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους, τιμωρείται με φυλάκιση και με χρηματική ποινή.»

Κατά τον Παύλου, αυτή η αυστηροποίηση των ποινικών κυρώσεων καταχωρίζεται ως έκφανη των δυσοίωνων προοπτικών του ελληνικού ποινικού δικαίου (πρβλ. σχετικά *Στ. Παύλου*, Ένας φαύλος κύκλος χωρίς τέλος: Οι τροποποιήσεις του ΠΚ (για την επιτάχυνση της δικαιοσύνης και την αποσυμφόρηση των φυλακών), ΠοινΔικ 10/2012, σελ. 921 επ.).

[711] Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 969.

[712] Άρθρο 370 - Παραβίαση του απορρήτου των επιστολών.

«*1. Όποιος αθέμιτα και με σκοπό να λάβει γνώση του περιεχομένου τους ανοίγει κλειστή επιστολή ή άλλο κλειστό έγγραφο ή παραβιάζει τον κλειστό χώρο στον οποίο είναι φυλαγμένα ή με οποιονδήποτε τρόπο εισχωρεί σε ξένα απόρρητα διαβάζοντας ή αντιγράφοντας ή αποτυπώνοντας με άλλο τρόπο επιστολή ή άλλο έγγραφο τιμωρείται με χρηματική ποινή ή με φυλάκιση μέχρι ενός έτους.*»

γ' ΠΚ[713] θα μπορούσε να υποστηρίξει κανείς ότι όποιος αποκτά αθέμιτη πρόσβαση σε ηλεκτρονικά στοιχεία πληροί την αντικειμενική υπόσταση του εγκλήματος του ά. 370 ΠΚ, όταν δηλαδή κάποιος παραβιάζοντας του κωδικούς πρόσβασης διαβάζει τα ψηφιακά έγγραφα (ηλεκτρονικές επιστολές, αρχεία κειμένου κ.λπ.) που είναι αποθηκευμένα στο υπολογιστή ή μεταδίδονται μέσω διαδικτύου. Ενώ λοιπόν η συμπεριφορά αυτή επισύρει ποινή φυλάκισης μέχρι ενός έτους, ο νομοθέτης προέβλεψε για τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά στοιχεία πολύ χαμηλότερο πλαίσιο ποινής.

Η επίλυση του προβλήματος της φαινομενικής συρροής των δύο ως άνω διατάξεων με την εφαρμογή της ειδικότερης του ά. 370Γ παρ. 2 ΠΚ προσφέρει μεν συστηματική διέξοδο, ωστόσο καθιστά σαφή την έκδηλη νομοθετική αντιφατικότητα ενώπιον της συγκεκριμένης εγκληματικής συμπεριφοράς[714]. Σύμφωνα με αντίθετη άποψη, σχέση ειδικότητας μεταξύ των ως άνω διατάξεων δεν υπάρχει, διότι το ά. 370 ΠΚ χρειάζεται για την κατάφασή του και έναν επιπρόσθετο σκοπό, «να λάβει ο δράστης γνώση του περιεχομένου», στοιχείο που δεν περιλαμβάνεται στη νομοτυπική μορφή του ά. 370Γ παρ. 2 ΠΚ. Έτσι, ορθότερο είναι να δεχθεί κανείς ότι υπερισχύει η διάταξη του ά. 370 ΠΚ[715]. Συνεπώς, με βάση την τελευταία άποψη, η χωρίς δικαίωμα πρόσβαση και το διάβασμα ενός ξένου ηλεκτρονικού μηνύματος από την προσωπική αλληλογραφία κάποιου χρήστη του διαδικτύου, όταν έχει τα χαρακτηριστικά του εγγράφου, θα πρέπει να αντιμετωπίζεται με βάση το ά. 370 ΠΚ.

Δυσαναλογία από πλευράς ποινής παρατηρείται και κατά τη σύγκριση του εξεταζόμενου εγκλήματος με ένα τρίτο «παραδοσιακό» έγκλημα, εκείνο της διατάραξης της οικιακής ειρήνης κατ' ά. 334 ΠΚ[716]. Συγκεκριμένα, ο ηλεκτρονικός

---

[713] Άρθρο 13 - Έννοια όρων του Κώδικα

> «*... γ)... Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή των στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.*»

[714] Βλ. *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., υποσ. 31, σελ. 91 και *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, όπ. π., σελ. 134.

[715] Βλ. *Μαρία Καϊάφα –Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, όπ. π., σελ. 1067.

[716] Άρθρο 334. Διατάραξη οικιακής ειρήνης.

> «*1. Όποιος εισέρχεται παράνομα ή παραμένει παρά τη θέλησή του δικαιούχου στην κατοικία άλλου ή στο χώρο που αυτός χρησιμοποιεί για την εργασία του ή σε χώρο περικλεισμένο που αυτός κατέχει τιμωρείται με φυλάκιση μέχρι ενός έτους ή με χρηματική ποινή.*»

εισβολέας «εισέρχεται» παράνομα σε χώρο «περικλεισμένο» που άλλος «κατέχει». Η αθέμιτη αυτή πρόσβαση σε ξένα ηλεκτρονικά στοιχεία αποτελεί ταυτόχρονα παράνομη είσοδο στον ψηφιακό χώρο της απόλυτης εξουσίασης του θύματος. Εξάλλου, ο χώρος που κατέχει ο χρήστης ειδικά στο διαδίκτυο δεν συνιστά μόνο χώρο πληροφοριακού αυτοκαθορισμού του αλλά και χώρο ανάπτυξης της προσωπικότητάς του. Και είναι τόσο σαφής η δομική ομοιότητα των δύο ως άνω συμπεριφορών ώστε να μπορεί κανείς να χρησιμοποιήσει ακόμη και την έκφραση «*διατάραξη ηλεκτρονικής οικιακής ειρήνης*»[717].

Συνεπώς, σε σχέση με άλλες ποινικές διατάξεις η προβλεπόμενη ποινή του ά. 370Γ παρ. 2 ΠΚ μπορεί να θεωρηθεί επιεικής. Άρα, είναι απαραίτητη η συστημική προσέγγιση των ως άνω εγκλημάτων προκειμένου να δύνανται να επιτύχουν με συνέπεια τον αντεγκληματικό τους στόχο και την προληπτική τους λειτουργία.

Προκειμένου, δε, ο νομοθέτης να ρυθμίσει την παράνομη διείσδυση σε δεδομένα προσωπικού χαρακτήρα τυποποίησε το ειδικότερο έγκλημα της διάταξης του ά. 22 παρ. 4 του ν. 2472/1997 (προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα)[718]. Αν θεωρηθεί ότι με τον όρο «*χωρίς δικαίωμα επέμβαση*» της εν λόγω διάταξης εννοείται και κατά την γραμματική ερμηνεία και η πρόσβαση (ως έννοια μερικότερη αυτής της επέμβασης) και αν γίνει δεκτό ότι στους τρόπους τέλεσης και η απλή παράνομη διείσδυση σε αρχείο δεδομένων προσωπικού χαρακτήρα, η οποία δεν οδηγεί σε γνώση των δεδομένων, υπάγεται στην ευρύτερη διατύπωση της διάταξης της παρ. 4 του ά. 22 «*όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα…*», τότε, σε περίπτωση χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά αρχεία δεδομένων προσωπικού χαρακτήρα θα εφαρμόζεται η εν λόγω διάταξη – με την επιφύλαξη ότι η ίδια πράξη δεν τιμωρείται βαρύτερα από άλλη διάταξη – και όχι η διάταξη του ά. 370Γ παρ. 2 ΠΚ, η οποία και απορροφάται από την αντίστοιχη του ά. 22 παρ. 4 ν.

[717] Βλ. *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 970.

[718] Άρθρο 22 παρ. 4 ν. 2472/1997:

> «*Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και εάν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως δέκα εκατομμυρίων δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις*».

2472/1997 με βάση την αρχή της ειδικότητας που εφαρμόζεται στις περιπτώσεις συρροής εγκλημάτων.

Ζήτημα φαίνεται να δημιουργεί το ερώτημα εάν η περίπτωση της απλής χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά στοιχεία εμπίπτει και στην αντικειμενική υπόσταση του ά. 370Β παρ. 1 ΠΚ, αποτελώντας ειδικότερα τον πέμπτο τρόπο τέλεσής του «*Όποιος αθέμιτα…ή οπωσδήποτε παραβιάζει στοιχεία…*». Κατά μία άποψη βέβαια η μορφή αυτή παραβίασης των στοιχείων θα πρέπει να ερμηνευθεί περιοριστικά, ώστε να αναφέρεται σε πράξεις ίσης απαξίας με εκείνες των τεσσάρων πρώτων τρόπων τέλεσης του εγκλήματος (αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη)[719]. Το ζήτημα αυτό αποκτά ακόμη μεγαλύτερο ενδιαφέρον εάν ληφθεί υπόψη και το δεύτερο εδάφιο της πρώτης παραγράφου «*Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο συμφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους*». Ουσιαστικά τίθεται το εξής ερώτημα: Με ποια από τις δύο ποινικές διατάξεις θα τιμωρηθεί ο δράστης, ο οποίος παράνομα διεισδύει σε απόρρητα του νόμιμου κατόχου, για τα οποία ο τελευταίος έχει λάβει μέτρα προκειμένου να παρεμποδίζονται οι τρίτοι να λάβουν γνώση τους;

Η σημασία, δέ, της απάντησης είναι εξαιρετική λόγω της σημαντικής διαφοράς του πλαισίου ποινής, αφού στην περίπτωση του ά. 370Β παρ. 1 ΠΚ προβλέπεται φυλάκιση από τρεις μήνες μέχρι πέντε έτη ενώ στην περίπτωση του ά. 370Γ παρ. 2 ΠΚ προβλέπεται φυλάκιση μέχρι τρεις μήνες. Με βάση τη συστηματική ερμηνεία των δύο διατάξεων καταλήγουμε στη παραδοχή ότι η ως άνω περίπτωση καλύπτεται από τη διάταξη του ά. 370Γ παρ. 2 ΠΚ, το οποίο άλλως θα έμενε ανεφάρμοστο. Το τελευταίο, δε, συστηματικό επιχείρημα οδηγεί στο συμπέρασμα ότι στο πλαίσιο του ά. 370Β παρ. 1 ΠΚ προστατεύονται μόνο τα κρατικά, επιστημονικά ή επαγγελματικά απόρρητα, καθώς και τα απόρρητα επιχειρήσεων καθώς και ότι ο χαρακτηρισμός ως απορρήτων των δεδομένων των οποίων έχει απαγορευθεί η πρόσβαση αναφέρεται τελικά μόνο σε δεδομένα αυτών των κατηγοριών[720].

Στο δεύτερο εδάφιο της δεύτερης παραγράφου του ά. 370Γ ΠΚ ο νομοθέτης προβλέπει ότι αν πράξη της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους τιμωρείται κατά το

[719] Βλ. *Χρίστος Μυλωνόπουλος*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, όπ. π., σελ. 77.
[720] Βλ. *Δημήτρης Κιούπης*, Ποινικό Δίκαιο και Internet, όπ. π., σελ. 132.

άρθρο 148 ΠΚ, με τις βαρύτατες ποινές, δηλαδή, της κατασκοπείας. Σημειώνεται ότι με τον όρο ασφάλεια, ο νομοθέτης εννοεί την εξωτερική ασφάλεια[721]. Στην ουσία πρόκειται για ρητή παραπομπή αναφορικά με το κυρωτικό μέρος[722].

5.1.6 Δικονομικά ζητήματα[723]

Σύμφωνα με την παρ. 4 του άρθρου 370Γ ΠΚ, το έγκλημα της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα διώκεται κατ' έγκληση[724], οπότε τυγχάνουν εφαρμογής οι διατάξεις των άρθρων 117-120 ΠΚ. Δικαιούμενο πρόσωπο στην υποβολή της σχετικής έγκλησης είναι σύμφωνα με το άρθρο 118 παρ. 1 ΠΚ ο παθών από την αξιόποινη πράξη. Τέτοιος θεωρείται ο φορέας του εννόμου αγαθού. Εν προκειμένω, ως φορέας του εννόμου αγαθού φέρεται ο νόμιμος κάτοχος των στοιχείων[725].

Σχετικά με την παράσταση πολιτικής αγωγής, η διάταξη του ά. 370 Γ παρ.2 ΠΚ έχει θεσπιστεί για την προστασία του ιδιωτικού συμφέροντος και όχι του «κοινωνικού». Συνακόλουθα από την παράβαση της εν λόγω διάταξης δεν γεννάται αξίωση αποζημίωσης ή χρηματικής ικανοποίησης λόγω ηθικής βλάβης του Ελληνικού Δημοσίου[726]. Ωστόσο και το Δημόσιο θα μπορούσε να αποτελεί νόμιμο κάτοχο, όπως ένα οποιοδήποτε νομικό πρόσωπο, που λειτουργεί στο πλαίσιο ενός συμφέροντος ιδιωτικής φύσης, όπως για παράδειγμα περιουσιακό[727].

---

[721] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156, *Ιωάννης Μανωλεδάκης*, όπ. π., σελ. 135.

[722] Βλ. *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1734.

[723] Αναφορικά με τη δωσιδικία των εγκλημάτων στο διαδίκτυο πρβλ. *Susan W. Brenner & Bert-Jaap Koops*, Appoaches to Cybercrime Jurisdiction, 4 J. High Tech. L. 1, 2004 και *Susan W. Brenner*, Cybercrime jurisdiction, Crime Law Soc Change (2006) 46:189–206.

[724] Αναφορικά με την έγκληση βλ. *Ν. Ανδρουλάκη*, Θεμελιώδεις έννοιες της ποινικής δίκης, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1994, σελ. 48 επ. και *Αρ. Καρρά*, Ποινικό Δικονομικό Δίκαιο, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1998, σελ. 306 επ.

[725] Βλ. *Αθανάσιος Κονταξής*, όπ. π., σελ. 3156.

[726] Βλ. απόφ. Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 75.

[727] *Αριστοτέλης Χαραλαμπάκης*, Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, όπ. π., σελ. 1735.

5.2 Το άρθρο 292Α ΠΚ και η σχέση του με το άρθρο 370Γ παρ. 2 ΠΚ

5.2.1 Εισαγωγικά

Με τον ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις»[728] [729] και συγκεκριμένα με το ά. 9 παρ. 3 προστέθηκε στο δέκατο τέταρτο κεφάλαιο του Ποινικού Κώδικα το ά. 292Α. Σύμφωνα με την αιτιολογική έκθεση του εν λόγω νόμου[730], η προσθήκη της διάταξης αυτής έλαβε χώρα λόγω της ανάγκης ανάληψης πρόσθετων νομοθετικών μέτρων για την ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, εξ αφορμής των «*γνωστών γεγονότων των υποκλοπών*»[731] (όπως κατά λέξη αναφέρεται στην αιτιολογική έκθεση)[732] [733].

5.2.2 Χαρακτηρολογικά στοιχεία των εγκλημάτων του ά. 292Α ΠΚ τα οποία αφορούν σε χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα

[728] ΦΕΚ Α' 136/10.07.2008.

[729] Αναλυτικά για τον ν. 3674/2008 βλ. *Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου*, Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών (Η ελληνική νομική ρύθμιση ενόψει και του πρόσφατου Ν. 3674/2008), ΔιΜΜΕ 4/2008, σελ. 446 επ.

[730] Η αιτιολογική έκθεση του ν. 3674/2008 βρίσκεται δημοσιευμένη στον Κώδικα Νομικού Βήματος (ΚΝοΒ) 2008 – βλ. συγκεκριμένα σελίδα 1461.

[731] Πρβλ. σχετικά με τα «γνωστά γεγονότα» το δημοσίευμα της ενημερωτικής ιστοσελίδας www.in.gr με τίτλο: «Ελληνικό Γουοτεργκέιτ... Πολιτικός σεισμός από το σκάνδαλο παρακολούθησης κινητών τηλεφώνων» (url: http://news.in.gr/greece/article/?aid=681341) καθώς και το λήμμα της ελεύθερης διαδικτυακής εγκυκλοπαίδειας «Βικιπαιδεία»: «Σκάνδαλο τηλεφωνικών υποκλοπών 2004-2005» (url: http://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%AC%CE%BD%CE%B4%CE%B1%CE%BB%CE%BF_%CF%84%CE%B7%CE%BB%CE%B5%CF%86%CF%89%CE%BD%CE%B9%CE%BA%CF%8E%CE%BD_%CF%85%CF%80%CE%BF%CE%BA%CE%BB%CE%BF%CF%80%CF%8E%CE%BD_2004-2005).

[732] Έτσι *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, ερμηνεία κατ' άρθρο, τομ. 2, εκδ. Νομική Βιβλιοθήκη, Αθήνα 2011, σελ. 839.

[733] Βλ. και *Μ. Μαργαρίτη*, Ποινικός Κώδικας, Ερμηνεία – εφαρμογή, όπ. π., σελ. 854.

Στο α' εδάφιο της πρώτης παραγράφου του ά. 292Α ΠΚ[734] το περιγραφόμενο έγκλημα παίρνει χαρακτηριστικά «κοινού» και μονοπρόσωπου εγκλήματος (με τη χρήση της λέξεως «όποιος»)[735]. Επίσης, πρόκειται για έγκλημα ενέργειας και συμπεριφοράς[736]. Σύμφωνα με την αιτιολογική έκθεση του νόμου το εν λόγω έγκλημα είναι συγκεκριμένης διακινδύνευσης (δεν απαιτείται να έχει επέλθει βλάβη από την υπό κρίση συμπεριφορά) και υπαλλακτικώς μικτό.

Στο β' εδάφιο της πρώτης παραγράφου του ά. 292Α ΠΚ[737] περιγράφεται διακεκριμένη περίπτωση του εγκλήματος του α' εδαφίου της πρώτης παραγράφου ως *μη γνήσιο ιδιαίτερο* έγκλημα καθώς η ιδιότητα του δράστη ως συνεργάτη ή εργαζομένου[738] του παρόχου υπηρεσιών τηλεφωνίας επαυξάνει το αξιόποινο.

Για την τέλεση του εγκλήματος της παρ. 1 ά. 292Α ΠΚ αρκεί και ενδεχόμενος δόλος, ο οποίος, βέβαια, πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

Άμεσα συνδεδεμένο με το έγκλημα της παραγράφου 1 ως ανωτέρω είναι αυτό της παραγράφου 3 του ίδιου άρθρου[739]. Στην εν λόγω παράγραφο περιγράφεται ως εγκληματική πράξη η παράλειψη της λήψης αναγκαίων μέτρων[740] (έγκλημα γνήσιας παράλειψης) από τον πάροχο ή τον νόμιμο εκπρόσωπο αυτού ή τον υπεύθυνο διασφάλισης του απορρήτου[741] (ιδιαίτερο έγκλημα). Επίσης, ως εξωτερικός όρος του

---

[734] Άρθρο 292Α - Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών:

> *«1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, και με τον τρόπο αυτόν θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή από είκοσι χιλιάδες (20.000) μέχρι πενήντα χιλιάδες (50.000) ευρώ. ...»*

[735] Έτσι *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, όπ. π., σελ. 840. Για σχετικές υποσημειώσεις πρβλ. αυτές τις παραγράφου 4.3 ως ανωτέρω.

[736] Έτσι *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, όπ. π., σελ. 840. Για σχετικές υποσημειώσεις πρβλ. αυτές τις παραγράφου 4.3 ως ανωτέρω.

[737] «*... Αν ο υπαίτιος της πράξης του προηγούμενου εδαφίου είναι ο εργαζόμενος ή συνεργάτης του παρόχου υπηρεσιών τηλεφωνίας, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή από είκοσι χιλιάδες (20.000) μέχρι εκατό χιλιάδες (100.000) ευρώ*».

[738] Σύμφωνα με τις διατάξεις του εργατικού δικαίου ή σε περίπτωση παροχής υπηρεσιών στον πάροχο αναφορικά με αυτές καθεαυτές τις τηλεφωνικές υπηρεσίες.

[739] «*3. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού ή ο υπεύθυνος διασφάλισης του απορρήτου των επικοινωνιών κατά το άρθρο 3 του παρόντος νόμου, που παραλείπει να λάβει τα αναγκαία μέτρα για την αποτροπή πράξης της παραγράφου 1, τιμωρείται με Φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή από πενήντα χιλιάδες (50.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ, εφόσον η πράξη τελέστηκε ή έγινε απόπειρα τελέσεως αυτής, ανεξάρτητα αν ο δράστης τιμωρηθεί*».

[740] Αναφορά των μέτρων αυτών υπάρχει στα ά. 2 και 3 ν. 3674/2008. Ωστόσο επισημαίνεται ότι η γραμματική διατύπωση της διάταξης αναφέρεται στα *αναγκαία* μέτρα και όχι σε αυτά που τυχόν ορίζονται από νόμο.

[741] Στο ά. 8 παρ. 8 Π.Δ. 47/2005 προβλέπεται ο ορισμός υπαλλήλου του παρόχου ως εξουσιοδοτημένου προσώπου για την τήρηση του απορρήτου, στο ά. 7 παρ. 2 εδ. β' ν. 3917/2011

αξιοποίνου εισάγεται η τέλεση ή η απόπειρα τέλεσης της πράξης του ά. 1, ανεξαρτήτως αν ο δράστης της εν λόγω πράξης τιμωρήθηκε. Από πλευράς υποκειμενικής υπόστασης αρκεί ενδεχόμενος δόλος, ο οποίος πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

Στις παραγράφους 4[742] και 5[743] του ά. 292Α ΠΚ προβλέπονται διακεκριμένες και επιβαρυντικές περιστάσεις των εγκλημάτων του ά. 292Α ΠΚ.

Τέλος, στην παράγραφο 6 του ά. 292Α ΠΚ προβλέπεται ως έγκλημα η αθέμιτη διάθεση ειδικών τεχνικών μέσων για την τέλεση πράξεων της παραγράφου 1 του ά. 292Α ΠΚ[744]. Το έγκλημα είναι κοινό, μονοπρόσωπο, ενέργειας, συμπεριφοράς και υπαλλακτικώς μικτό. Η εν λόγω διάταξη τιμωρεί τη διάθεση των λεγόμενων «εργαλείων χωρίς δικαίωμα πρόσβασης» (hacking tools), ως προπαρασκευαστική πράξη του εγκλήματος της παραγράφου 1 ά. 292Α ΠΚ και μόνον όταν η διάθεση ή εγκατάσταση αυτών αποσκοπεί στην παραβίαση της ασφάλειας συστήματος του παρόχου ως ανωτέρω. Ωστόσο, η εν λόγω διάταξη αναφέρεται μόνο στη χωρίς δικαίωμα πρόσβαση της παραγράφου 1 του ά. 292Α ΠΚ, σε περιπτώσεις, δηλαδή, που το hacking αφορά λογισμικό δικτύων τηλεφωνίας. Σε άλλες περιπτώσεις χωρίς δικαίωμα πρόσβασης, στις οποίες δεν προσβάλλεται λογισμικό παρόχου τηλεφωνικών υπηρεσιών, δεν υπάρχει στο ελληνικό δίκαιο αντίστοιχη τιμωρητική διάταξη.

προβλέπεται ο ορισμός εκ μέρους του παρόχου «υπεύθυνου ασφαλείας δεδομένων» και υφιστάμενες κανονιστικές πράξεις της ΑΔΑΕ προβλέπουν τον ορισμό «υπευθύνου ασφαλείας» (βλ. αναλυτικά *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, όπ. π., σελ. 851). Οι ως άνω είναι προφανώς αυτοί που έχουν τις ιδιότητες προκειμένου να τελέσουν το έγκλημα της παραγράφου 3 του ά. 292Α ΠΚ.

[742] «*4. Αν ο υπαίτιος των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή από εκατό χιλιάδες (100.000) μέχρι τριακόσιες χιλιάδες (300.000) ευρώ. Εφόσον το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των εβδομήντα τριών χιλιάδων (73.000) ευρώ, ο υπαίτιος τιμωρείται με Κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από εκατό χιλιάδες (100.000) μέχρι πεντακόσιες χιλιάδες (500.000) ευρώ*».

[Το ποσό των εβδομήντα τριών χιλιάδων (73.000) ευρώ του δεύτερου εδαφίου της παραγράφου 4 αναπροσαρμόζεται στο ποσό των εκατό είκοσι χιλιάδων (120.000) ευρώ με την παρ.1 περ. ι' άρθρου 24 Ν.4055/2012,ΦΕΚ Α 51/12.03.2012. Έναρξη ισχύος 2 Απριλίου 2012].

[743] «*5. Αν από τις πράξεις των προηγούμενων παραγράφων μπορεί να τεθούν σε κίνδυνο θεμελιώδεις αρχές και θεσμοί του Πολιτεύματος, όπως μνημονεύονται στο άρθρο 134Α του Ποινικού Κώδικα ή απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή στην ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη*».

[744] «*Όποιος αθέμιτα διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει προς εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων της παραγράφου 1 ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεση τους, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή από δέκα χιλιάδες (10.000) μέχρι πενήντα χιλιάδες (50.000) ευρώ*».

5.2.3 Περιορισμοί στην εφαρμογή της διάταξης

Η εν λόγω διάταξη αφορά στη χωρίς δικαίωμα πρόσβαση σε σύνδεση ή δίκτυο ή συστήματα υλικού ή λογισμικού του παρόχου υπηρεσιών τηλεφωνίας. Επομένως, το πεδίο εφαρμογής του άρθρου αυτού δεν επεκτείνεται στην ασφάλεια όλων των μορφών ηλεκτρονικών επικοινωνιών αλλά αφορά μόνο τις υπηρεσίες τηλεφωνίας[745], σύμφωνα με την περιγραφή της αντικειμενικής υπόστασης (ενδεικτικά, υποστηρίζεται βασίμως η άποψη ότι το ά. 292Α ΠΚ δεν τυγχάνει εφαρμογής σε περιπτώσεις πρόσβασης στο διαδίκτυο μέσω κινητής τηλεφωνικής υπηρεσίας). Επιπρόσθετα, η εν λόγω διάταξη αναφέρεται στους «παρόχους», ήτοι στις εταιρείες ή επιχειρήσεις «*υπηρεσιών που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις*». Άρα, και ως προς αυτό το σκέλος η διάταξη περιορίζει το πεδίο εφαρμογής της, καθώς αποκλείονται οι περιπτώσεις ιδιωτικών δικτύων επικοινωνίας (intranets) π.χ. του εσωτερικού δικτύου επικοινωνίας μιας επιχείρησης[746].

5.2.4 Σχέση ά. 292Α ΠΚ με ά. 370Γ παρ. 2 ΠΚ και ά. 370Α ΠΚ – Το ζήτημα της συρροής

Η ιδιαίτερη σύνδεση της εν λόγω διάταξης με τη χωρίς δικαίωμα πρόσβαση σε *ηλεκτρονικά* δεδομένα ουσιαστικά εντοπίζεται στην αναφορά της αντικειμενικής υπόστασης της διάταξης σε σύστημα λογισμικού. Το «λογισμικό» (software) αποτελεί ουσιαστικά το πρόγραμμα βάσει του οποίου λειτουργούν οι υπολογιστές του παρόχου αναφορικά με τις υπηρεσίες που παρέχουν. Ειδικότερα, λειτουργικό σύστημα (operating System ή OS) ονομάζεται στην επιστήμη της πληροφορικής το λογισμικό του υπολογιστή που είναι υπεύθυνο για τη διαχείριση και τον συντονισμό

[745] Έτσι η αιτιολογική έκθεση και όπως αναφέρεται σχετικώς από τον *Αρ. Χαραλαμπάκη*, Ποινικός Κώδικας, όπ. π., σελ. 841.

[746] Βλ. *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, όπ. π., σελ. 841-843 όπου και ανάλυση των εν λόγω εννοιών.

των εργασιών, καθώς και την κατανομή των διαθέσιμων πόρων. Το λειτουργικό σύστημα παρέχει ένα θεμέλιο, ένα μεσολαβητικό επίπεδο λογικής διασύνδεσης μεταξύ λογισμικού και υλικού, διαμέσου του οποίου οι εφαρμογές αντιλαμβάνονται εμμέσως τον υπολογιστή. Μια από τις κεντρικές αρμοδιότητες του λειτουργικού συστήματος είναι η διαχείριση του υλικού, απαλλάσσοντας έτσι το λογισμικό του χρήστη από τον άμεσο και επίπονο χειρισμό του υπολογιστή και καθιστώντας ευκολότερο τον προγραμματισμό τους. Στην προκειμένη, δηλαδή, περίπτωση, στο βαθμό που οι τηλεπικοινωνίες (όπως περιορίστηκε η εφαρμογή της διάταξης ανωτέρω) παρέχονται και ασκείται η όποια διαχείρισή τους μέσω ηλεκτρονικών προγραμμάτων (π.χ. το γνωστό πρόγραμμα "skype"), τότε πράγματι μιλούμε για ηλεκτρονικές πληροφορίες των οποίων η προστασία καλύπτεται από τη διάταξη του ά. 292Α ΠΚ.

Επομένως, επί της ουσίας, η εν λόγω περίπτωση είναι αυτή κατά την οποία μπορούμε να διαπιστώσουμε φαινομενική συρροή της διάταξης του ά. 292Α παρ. 1 εδ. α' ΠΚ με τη διάταξη του ά. 370Γ παρ. 2 ΠΚ. Το έννομο αγαθό που προστατεύεται από το ά. 292Α είναι το υπερατομικό έννομο αγαθό του απορρήτου των επικοινωνιών, σύμφωνα με την αιτιολογική έκθεση[747] - από την άλλη πλευρά, η προβληματική για το προστατευόμενο έννομο αγαθό από την διάταξη της δεύτερης παραγράφου του ά. 370Γ αναπτύχθηκε ήδη σε παραπάνω κεφάλαιο[748]. Σε κάθε περίπτωση, όμως, πρέπει να λάβουμε υπόψιν μας ότι για την ίδια πράξη (ακριβώς αυτήν της χωρίς δικαίωμα πρόσβασης) δεν επιτρέπεται να τιμωρείται ο δράστης από δύο διατάξεις. Επομένως, σε περίπτωση πρόσβασης σε λογισμικό παροχής υπηρεσιών τηλεφωνίας θα εφαρμοστεί το ά. 292Α παρ. 1 εδ. α' ΠΚ ως ειδικότερη της διάταξης του ά. 370Γ παρ. 2 ΠΚ (αρχή της ειδικότητας) – στις υπόλοιπες περιπτώσεις (π.χ. σε λογισμικό που δεν χρησιμοποιείται από πάροχο τηλεφωνικών υπηρεσιών για την παροχή των υπηρεσιών αυτών) εφαρμογής τυγχάνει το ά. 370Γ παρ. 2. Σε κάθε περίπτωση, όμως, τυγχάνει εφαρμογής το ά. 370Γ παρ. 2 ακόμη και σε περίπτωση λογισμικού παροχής υπηρεσιών τηλεφωνίας αν θεωρηθεί ότι δεν προέκυψε ο κίνδυνος ο οποίος τίθεται ως προϋπόθεση από το ά. 292Α ΠΚ.

Η ανίχνευση της σχέσης του ά. 292Α ΠΚ και 370Α ΠΚ είναι ίσως πιο περίπλοκη. Και οι δύο διατάξεις αναφέρονται σε σύστημα υλικού ή λογισμικού μέσω του οποίου

[747] Βλ. *Αρ. Χαραλαμπάκης*, Ποινικός Κώδικας, όπ. π., σελ. 853.

[748] Βλ. ανωτέρω παράγραφο 5.1.2 του παρόντος πονήματος.

παρέχονται υπηρεσίες τηλεφωνίας. Στη μεν διάταξη, όμως, του ά. 292Α ΠΚ αναφέρεται η απόκτηση χωρίς δικαίωμα πρόσβασης και η με τον τρόπο αυτόν θέση σε κίνδυνο της ασφάλειας των τηλεφωνικών επικοινωνιών – στη δε διάταξη του ά. 370Α απαιτείται παγίδευση ή με οποιονδήποτε άλλον τρόπο παρέμβαση. Άρα, σε περίπτωση χωρίς δικαίωμα πρόσβασης κατά την οποία προέκυψε κίνδυνος θα εφαρμοστεί η διάταξη του 292Α ΠΚ. Σε κάθε περίπτωση, θεωρώ ότι σε περίπτωση χωρίς δικαίωμα πρόσβασης, αυτή δεν μπορεί να θεωρηθεί παρέμβαση κατά τη γραμματική διατύπωση της διάταξης του ά. 370Α ΠΚ και άρα θα εφαρμοστεί η διάταξη του ά. 292Α ΠΚ ως ειδικότερη (εφόσον βεβαια πληρούνται και οι λοιποί όροι που τίθενται στην εν λόγω διάταξη). Σε περίπτωση, όμως, «παγίδευσης» ή «παρέμβασης» με σκοπό κάποιος να πληροφορηθεί το περιεχόμενο της τηλεφωνικής συνδιάλεξης, ενδεχομένως να μπορεί να υποστηριχθεί ακόμη και η περίπτωση αληθινής πραγματικής συρροής των δύο διατάξεων, αν για την παγίδευση αυτή έλαβε χώρα και χωρίς δικαίωμα πρόσβαση.

5.3 Ο νόμος 3917/2011 και οι ποινικές κυρώσεις του

5.3.1 Ο νόμος 3917/2011 και η ενσωμάτωση της Οδηγίας 2006/24/ΕΚ

Ο νόμος 3917/2011 ενσωμάτωσε στο ελληνικό δίκαιο την Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[749] για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ. Η νομοθετική αυτή ρύθμιση αποβλέπει στην εναρμόνιση των διατάξεων των κρατών - μελών, ούτως ώστε να διατηρούνται για ορισμένο διάστημα δεδομένα που παράγονται ή τυγχάνουν επεξεργασίας από τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών

[749] Η οδηγία διαθέσιμη στο url: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/RELATIVELAW/%CE%9F%CE%94%CE%97%CE%93%CE%8A%CE%912006-24-%CE%95%CE%9A.PDF.

επικοινωνιών ή δημοσίων δικτύων, με σκοπό τη διακρίβωση, διερεύνηση και δίωξη σοβαρών εγκλημάτων (άρθρο 1 παρ. 1 της Οδηγίας).

Όπως αναφέρεται και στην αιτιολογική έκθεση, «*το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο, οδηγήθηκαν στη έκδοση της Οδηγίας 2006/24/ΕΚ, με την οποία εισάγεται η υποχρέωση διατήρησης δεδομένων συνδρομητών και εγγεγραμμένων χρηστών στο πλαίσιο ηλεκτρονικών επικοινωνιών, θεωρώντας ότι η επεξεργασία των σχετικών στοιχείων από τις αρμόδιες αρχές μπορεί να αποτελέσει ένα πολύτιμο εργαλείο στη μάχη κατά της τρομοκρατίας και της οργανωμένης εγκληματικότητας. Κατόπιν αυτού, με την εν λόγω Οδηγία η προαναφερθείσα ευχέρεια των κρατών - μελών να επιβάλλουν στους παρόχους την υποχρέωση προληπτικής διατήρησης ορισμένων δεδομένων της επικοινωνίας, έχει μετατραπεί σε υποχρέωση των κρατών - μελών*»[750].

Σύμφωνα και με τις επιταγές της οδηγίας, τα διατηρούμενα δεδομένα δεν αφορούν στο περιεχόμενο της επικοινωνίας. Επιπρόσθετα, και πάλι σύμφωνα με την αιτιολογική έκθεση, η διατήρηση των δεδομένων της επικοινωνίας δεν συνιστά ανακριτική πράξη, αφού τα δεδομένα της επικοινωνίας παραμένουν στα αρχεία του παρόχου, δεν τυγχάνουν επεξεργασίας και γνωστοποιούνται στις αρμόδιες αρχές, μόνον υπό τις προϋποθέσεις και τις διαδικασίες του εκτελεστικού νόμου του άρθρου 19 παρ. 1 του Συντάγματος, ήτοι της άρσης απορρήτου των επικοινωνιών κατ' ά. 4 ν. 2225/1994 σε συνδυασμό με το άρθρο 253Α παρ. 1 εδ. γ' του Κώδικα Ποινικής Δικονομίας (ΚΠΔ)[751] [752]. Άρα, διευκρινίζεται ότι δεν επιτρέπεται προληπτική επεξεργασία των διατηρούμενων δεδομένων, η οποία θα προσέκρουε στο άρθρο 19 του Συντάγματος και την αρχή της αναλογικότητας

Ο νόμος 3917/2011 στο ά. 5 ορίζει σαφώς ποια είναι αυτά τα δεδομένα που πρέπει να διατηρούνται για διάστημα 12 μηνών (ά. 6 ν. 3917/2011) από τον πάροχο ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών προκειμένου να είναι

---

[750] Η αιτιολογική έκθεση του ν. 3917/2011 είναι διαθέσιμη στο url: http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=In68q5jjdW0%3D&tabid=132.

[751] Πρβλ. *Β. Σωτηρόπουλου*, Εσφαλμένη και η τρίτη γνωμοδότηση Εισαγγελίας Αρείου Πάγου για την ανωνυμία, ιστολόγιο "e-lawyer", url: http://elawyer.blogspot.gr/2011/05/blog-post_31.html, όπου αναλύεται το ζήτημα της άρσης του απορρήτου των επικοινωνιών κατ' ά. 4 ν. 2225/1994 μετά και την ψήφιση του ν. 3917/2011 σε συνάρτηση με σχετικές γνωμοδοτήσεις τις Εισαγγελίας του Αρείου Πάγου.

[752] Πρβλ. για το θέμα *Γ. Νούσκαλη*, Η επεξεργασία των εξωτερικών τηλεπικοινωνιακών δεδομένων θέσης και κίνησης ως ανακριτική πράξη έρευνας κατά το Ν. 3917/2011, ΠοινΧρ ΞΒ/ 2012, σελ. 246 επ.

διαθέσιμα στις αρχές[753]. Είναι, δε, προφανές και από τα διδάγματα της κοινής πείρας ότι τα εν λόγω δεδομένα τηρούνται πλέον σε ηλεκτρονικά συστήματα ή σε λογισμικά και έχουν μορφή ηλεκτρονικής πληροφορίας.

---

[753] Άρθρο 6 ν. 3917.2911:

«*1) Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας:*

α. όσον αφορά την τηλεφωνία σταθερού δικτύου και την κινητή τηλεφωνία:

αα) ο τηλεφωνικός αριθμός του καλούντος,

ββ) το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή του εγγεγραμμένου χρήστη

β. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) ο αποδοθείς κωδικός ταυτότητας χρήστη,

ββ) ο κωδικός ταυτότητας χρήστη και ο τηλεφωνικός αριθμός που δίνονται σε κάθε επικοινωνία που εισέρχεται στο δημόσιο τηλεφωνικό δίκτυο,

γγ) το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου1

2) δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας:

α. όσον αφορά την τηλεφωνία σταθερού δικτύου και την κινητή τηλεφωνία:

αα) ο καλούμενος αριθμός ή αριθμοί (ο αριθμός ή οι αριθμοί τηλεφώνου που κλήθηκαν), στις δε περιπτώσεις όπου υπεισέρχονται συμπληρωματικές υπηρεσίες όπως προώθηση/εκτροπή κλήσης, ο αριθμός ή οι αριθμοί τηλεφώνου προς τους οποίους προωθήθηκε η κλήση,

ββ) τα ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή εγγεγραμμένων χρηστών

β. όσον αφορά τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας,

ββ) ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης

3) δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας:

α. όσον αφορά την τηλεφωνία σταθερού δικτύου και την κινητή τηλεφωνία, η ημερομηνία και η ώρα έναρξης και λήξης της επικοινωνίας

β. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη,

ββ) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου, με βάση συγκεκριμένη ωριαία ζώνη

4) δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας:

α. όσον αφορά την τηλεφωνία σταθερού δικτύου και την κινητή τηλεφωνία: η χρησιμοποιηθείσα τηλεφωνική υπηρεσία

β. όσον αφορά τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου: η χρησιμοποιηθείσα διαδικτυακή υπηρεσία

5.3.2 Οι ποινικές κυρώσεις του ά. 11 ν. 3917/2011

Με το ά. 11 ν. 3917/2011 τιμωρείται η περιέλευση σε γνώση ή οποιαδήποτε επεξεργασία των εν λόγω δεδομένων[754]. Ειπώθηκε, ήδη, πάντως, ότι στην

---

5) δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή του φερομένου ως εξοπλισμού επικοινωνίας τους:

α. όσον αφορά την τηλεφωνία σταθερού δικτύου, οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου

β. όσον αφορά την κινητή τηλεφωνία:

αα) οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου,

ββ) η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI) του καλούντος,

γγ) η διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI) του καλούντος,

δδ) η IMSI του καλουμένου, εε) η IMEI του καλουμένου, στστ) στην περίπτωση προπληρωμένων ανώνυμων υπηρεσιών, η ημερομηνία και ώρα της αρχικής ενεργοποίησης της υπηρεσίας και ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) από την οποία πραγματοποιήθηκε η ενεργοποίηση

γ. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) ο τηλεφωνικός αριθμός καλούντος για την πρόσβαση μέσω τηλεφώνου,

ββ) η ψηφιακή συνδρομητική γραμμή (DSL) ή άλλη απόληξη της πηγής της επικοινωνίας

6) δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας:

α. ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) κατά την έναρξη και λήξη της επικοινωνίας

β. δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών βάσει των κωδικών θέσης (κωδικών ταυτότητας κυψέλης), κατά το χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών.»

[754] Άρθρο 11:

«*1. Όποιος, κατά παράβαση των διατάξεων του παρόντος κεφαλαίου, λαμβάνει γνώση των δεδομένων που διατηρούνται από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών, τα συλλέγει, αποθηκεύει, αντιγράφει, αφαιρεί, μεταφέρει, αλλοιώνει, βλάπτει, καταστρέφει, μεταδίδει, ανακοινώνει ή με άλλο τρόπο τα επεξεργάζεται, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με κάθειρξη μέχρι δέκα ετών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.*

2. Αν ο δράστης των πράξεων της παραγράφου 1 είναι νόμιμος εκπρόσωπος ή μέλος της διοίκησης ή υπεύθυνος ασφάλειας δεδομένων ή εργαζόμενος ή συνεργάτης του παρόχου ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε σε οικονομικό ή άλλο αντάλλαγμα, τιμωρείται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από 55.000 μέχρι 200.000 ευρώ.

3. Αν από τις πράξεις των παραγράφων 1 και 2 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή από 55.000 μέχρι 300.000 ευρώ.

πραγματικότητα δεν μπορεί να γίνει διάκριση ανάμεσα στην απλή απόκτηση πρόσβασης σε στοιχεία σε ξένο ηλεκτρονικό υπολογιστή και στην λήψη γνώσης των στοιχείων αυτών[755]. Είναι πιθανές, επομένως, και οι ενδεχόμενες αποδεικτικές δυσχέρειες[756] για τη συγκεκριμένη αξιόποινη πράξη σε ό,τι αφορά το στοιχείο της γνώσης.

Το περιγραφόμενο έγκλημα είναι κοινό (η διατύπωση της αντικειμενικής υπόστασης ξεκινάει με τη λέξη «όποιος») και μονοπρόσωπο. Είναι, επίσης, έγκλημα ενέργειας και συμπεριφοράς.

Στη δεύτερη παράγραφο του εν λόγω άρθρου περιγράφεται διακεκριμένη περίπτωση του εγκλήματος της πρώτης παραγράφου ως *μη γνήσιο ιδιαίτερο* έγκλημα καθώς η ιδιότητα του δράστη ως νομίμου εκπροσώπου ή μέλους της διοίκησης ή υπεύθυνου ασφάλειας δεδομένων ή εργαζομένου ή συνεργάτη του παρόχου επαυξάνει το αξιόποινο καθώς προστίθεται στην μέχρι δέκα ετών κάθειρξη (ποινή για το έγκλημα της παραγράφου 1) και η δυνατότητα επιβολής χρηματικής ποινής. Επίσης, στην παράγραφο 2 τυποποιείται και έγκλημα υπερχειλούς υποκειμενικής υποστάσεως καθώς προβλέπεται και εναλλακτικά η περίπτωση τέλεσης του εγκλήματος της παραγράφου 1 κατ' επάγγελμα ή κατά συνήθεια[757].

Στην υποκειμενική υπόσταση των παραγράφων 1 και 2 αρκεί ενδεχόμενος δόλος, ο οποίος πρέπει αντιστοίχως να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

Στην παράγραφο 3 του εν λόγω άρθρου τυποποιείται έγκλημα αφηρημένης διακινδύνευσης σε περίπτωση πρόκλησης κινδύνου για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή την εθνική ασφάλεια με επαύξηση του αξιοποίνου σε κάθειρξη και χρηματική ποινή από 55.000 € μέχρι 300.000 €. Για το έγκλημα της παραγράφου 3 αρκεί ενδεχόμενος δόλος, ο οποίος πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

---

4. Αν οι πράξεις των παραγράφων 1 και 2 έχουν τελεστεί από αμέλεια, επιβάλλεται φυλάκιση τουλάχιστον δύο ετών.»

[755] Όπως αναπτύχθηκε σχετικώς ανωτέρω στην παράγραφο 5.1.3.2 του παρόντος πονήματος.

[756] Πρβλ. και *Δ. Αγγελόπουλου* και *Ιωάν. Πάσχου*, Κατάσχεση – ανάλυση ψηφιακών πειστηρίων, ΠοινΔικ 4/2003, σελ. 438 επ.

[757] Υποκειμενικά στοιχεία του αδίκου (subjective Unrechtselemente - έτσι π.χ. ο *Christian Mueller-Gugenberger* (Hg), Wirtschaftsstrafrecht. Eine Gesamtdarstellung des deutschen Wirtschaftsstraf- und Ordnungswidrikeitenrechts, 2η έκδ., Muenster, 1992 σελ. 239).

Τέλος, στην παράγραφο 4 προβλέπεται η τιμώρηση των πράξεων της παραγράφου 1 και 2 και από αμέλεια – η εν λόγω περίπτωση τυποποιείται σε πλημμεληματική μορφή.

5.3.3 Συσχέτιση ά. 11 ν. 3917/2011 με ά. 370Γ παρ. 2 και ά. 292Α ΠΚ

Εν προκειμένω, η αντικειμενική υπόσταση των εν λόγω εγκλημάτων δεν αναφέρεται σε απλή πρόσβαση αλλά σε γνώση των εν λόγω δεδομένων και βεβαίως σε περαιτέρω επεξεργασία, καταστροφή τους κ.λπ. Από πλευράς λοιπόν συσχέτισης της διάταξης με αυτήν του ά. 370Γ παρ. 2 ΠΚ, μπορεί να υποστηριχθεί ότι η διάταξη του ά. 11 ν. 3917/2011 συρρέει αληθώς και πραγματικώς με τη διάταξη του ά. 370Γ παρ. 2. Τούτο διότι ο δράστης δύναται χωρίς δικαίωμα να αποκτήσει πρόσβαση στα δεδομένα (πράξη η οποία ολοκληρώνει την αντικειμενική και υποκειμενική υπόσταση του εγκλήματος της δεύτερης παραγράφου του ά. 370Γ ΠΚ) και έπειτα με ακόλουθη πράξη έρχεται σε γνώση ή επεξεργάζεται τα δεδομένα στα οποία αφορά η διάταξη του ά. 11 ν. 3917/2011. Σε περίπτωση, όμως, πρόσβασης χωρίς δικαίωμα σε αυτά τα δεδομένα χωρίς, ωστόσο, να αποκτηθεί γνώση αυτών, δεν πληρούται η αντικειμενική υπόσταση του ά. 11 ν. 3917/2011 και, άρα, μπορεί να υποστηριχθεί βάσιμα ότι τυγχάνει εφαρμογής μόνον η διάταξη του ά. 370Γ παρ. 2 ΠΚ.

Στην αντικειμενική υπόσταση του εν λόγω άρθρου αναφέρεται, επίσης, η περίπτωση κατά την οποία ο δράστης «*καθιστά προσιτά σε μη δικαιούμενα πρόσωπα*» τα προστατευόμενα δεδομένα. Επομένως, αυτός ο οποίος π.χ. αποκαλύπτει κωδικούς πρόσβασης σε τρίτο ή ξεκλειδώνει κάποιο πρόγραμμα για λογαριασμό τρίτου (το οποίο, βέβαια, αφορά στα προστατευόμενα από τον ν. 3917/2011 δεδομένα), προκειμένου ο τελευταίος να αποκτήσει χωρίς δικαίωμα πρόσβαση σε δεδομένα, θα τιμωρηθεί με την εν λόγω διάταξη. Ο, δε, αποκτών τη χωρίς δικαίωμα πρόσβαση, αν δεν λάβει γνώση (σύμφωνα και με την ανωτέρω παράγραφο) θα τιμωρηθεί κατ' ά. 370Γ παρ. 2. Σε δικαιοπολιτικό επίπεδο βλέπουμε επομένως δύο συμμέτοχους στην ίδια ή παρεμφερή πράξη να τιμωρούνται με δύο διαφορετικές ποινικές διατάξεις, ο μεν σε βαθμό κακουργήματος, ο δε σε βαθμό πλημμελήματος.

Αναφορικά με τη συσχέτιση του ά. 292Α ΠΚ με το ά. 11 του ν. 3917/2011, φαίνεται ότι αναφέρονται σε διαφορετικά ηλεκτρονικά δεδομένα (το μεν ά. 292Α ΠΚ σε λογισμικό και δεδομένα που στην ουσία χρησιμοποιούνται για την παροχή τηλεφωνικών υπηρεσιών, το δε ά. 11 του ν. 3917/2011 σε στοιχεία επικοινωνίας) οπότε αλληλοαποκλείεται η εφαρμογή τους. Επισημαίνεται, επίσης, πως κατά το ά. 292Α πρέπει να τεθεί σε κίνδυνο η ασφάλεια των τηλεφωνικών επικοινωνιών. Πάντως, σε περίπτωση φαινομενικής κατ' ιδέαν συρροής – αν π.χ. ο δράστης έλθει σε επαφή με δεδομένα που προστατεύει το ά. 11 ν. 3917/2011 δια λογισμικού το οποίο προστατεύεται από το ά. 292Α ΠΚ – τότε θα πρέπει να εφαρμοστεί η διάταξη του ά. 11 ν. 3917/2011 και να αποκλειστεί η εφαρμογή του ά. 292Α ΠΚ δυνάμει της αρχής της ειδικότητας. Δυνατή φαίνεται, πάντως, και η περίπτωση αληθινής κατ' ιδέαν συρροής, σε περίπτωση που ο δράστης ήλθε σε επαφή με τα ως άνω δεδομένα και παράλληλα έχει αποκτήσει πρόσβαση σε προστατευόμενο λογισμικό από το ά. 292Α ΠΚ, έχοντας βέβαια θέσει και σε κινδυνο την παροχή τηλεφωνικών υπηρεσιών, όπως απαιτείται από τη διάταξη αυτή.

Σε κάθε περίπτωση, είναι παραπάνω από εμφανή τα σημεία τριβής των διατάξεων μεταξύ τους και, συνεπώς, επιβάλλεται η συστημική θεώρηση και αναμόρφωση όλων των προστατευτικών των ηλεκτρονικών πληροφοριών ή συστημάτων πληροφοριών διατάξεων.

5.4 Ο νόμος 3471/2006 και οι ποινικές διατάξεις του

5.4.1 Ο νόμος 3471/2006 και η ενσωμάτωση της Οδηγίας 2002/58/ΕΚ

Ο ν. 3471/2006 ενσωμάτωσε στο ελληνικό δίκαιο την Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της

ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[758]. Στην εν λόγω Οδηγία, παρά το γεγονός ότι αυτή δεν αναφέρεται συγκεκριμένα σε πρόσβαση χωρίς δικαίωμα/εξουσιοδότηση σε συστήματα πληροφοριών, υπάρχει στη σκέψη 25 του προοιμίου αυτής μια πολύ ενδιαφέρουσα ανάπτυξη σχετικά με λογισμικά, τα οποία μπορούν να εξασφαλίσουν πρόσβαση σε πληροφορίες και να συνδράμουν στην αποθήκευση αθέατων πληροφοριών ή στην ανίχνευση των δραστηριοτήτων του χρήστη (π.χ. γνωστά ως "cookies"). Σύμφωνα με την οδηγία «*... η χρησιμοποίησή τους θα πρέπει να επιτρέπεται υπό τον όρον ότι παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ για τον προορισμό των "cookies" ή τυχόν ανάλογων διατάξεων, ώστε να εξασφαλίζεται ότι είναι εν γνώσει του χρήστη οι πληροφορίες που αποθηκεύονται στον τερματικό εξοπλισμό που χρησιμοποιεί. Οι χρήστες θα πρέπει να έχουν την ευκαιρία να αρνηθούν την αποθήκευση "cookies" ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. ... Οι τρόποι της παροχής πληροφοριών, της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν προσιτότεροι για τον χρήστη. Για την πρόσβαση σε συγκεκριμένο περιεχόμενο ιστοσελίδων επιτρέπεται πάντως να τίθεται ως όρος η ενημερωμένη αποδοχή "cookies" ή παρόμοιων διατάξεων, εφόσον χρησιμοποιούνται για σύννομο σκοπό*».

Εν προκειμένω, με τον ν. 3471/2006 ρυθμίζεται η επεξεργασία των δεδομένων κίνησης και θέσης στην επικοινωνία. Αναφορικά με την πρόσβαση στα προστατευόμενα από το εν λόγω νομοθέτημα δεδομένα η μοναδική αναφορά στον νόμο υπάρχει στην παράγραφο 5 του ά. 4 αυτού (όπως αυτή αντικαταστάθηκε με το ά. 170 του ν. 4070/2012)[759] κατά την οποία «*5. Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό*

[758] Η Οδηγία διαθέσιμη στο url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF.

[759] Η αρχική και αντικατασταθείσα διάταξη αναφερόταν σε απαγόρευση πρόσβασης και είχε ως εξής: «*5. Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες, σύμφωνα με το άρθρο 11 του ν. 2472/1997, όπως ισχύει, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών, παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης.*»

συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης.»

Η εν λόγω διάταξη είναι απαγορευτική, επομένως, για κάθε πρόσβαση χωρίς συγκατάθεση και σε δεδομένα οποιασδήποτε διασυνδεδεμένης συσκευής [καθώς οι λέξεις «συνδρομητής» και «χρήστης» (ά. 2 στοιχ. 1 και 2 αντίστοιχα ν. 3471/2006) παραπέμπουν εκ των ορισμών τους κατά το ά. 2 του παρόντος νόμου σε λειτουργίες διαδικτύου (στην περίπτωση του χρήστη ακόμη και σε περιπτώσεις ελεύθερης σύνδεσης διαδικτύου)]. Εξάλλου, δεν είναι τυχαίο ότι στον ορισμό των «δεδομένων κίνησης» (ά. 2 στοιχ. 3 ν. 3471/2006) περιλαμβάνονται και οι «κωδικοί πρόσβασης»[760]. Άρα, είναι σαφείς οι προθέσεις και του ευρωπαίου αλλά και του εθνικού νομοθέτη στη ρύθμιση του πλασίου αναφορικά με την πρόσβαση σε δεδομένα αποθηκευμένα σε συστήματα πληροφοριών.

5.4.2 Οι ποινικές κυρώσεις του ά. 15 ν. 3471/2006

Παρά την ως άνω κατ' ουσίαν απαγόρευση της χωρίς συγκατάθεση πρόσβασης, στις ποινικές διατάξεις των παραγράφων 1 και 3 του ά. 15 του νόμου[761] δεν τιμωρείται η

[760] Αναφορικά με τον κωδικό πρόσβασης πρβλ. σχετικώς *Εμμ. Μεταξάκη*, Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου, ΠοινΧρ ΞΔ/ 2014, σελ. 11.

[761] Άρθρο 15 – «Ποινικές κυρώσεις»:

> «*1. Όποιος, κατά παράβαση του παρόντος νόμου, χρησιμοποιεί, συλλέγει, αποθηκεύει, λαμβάνει γνώση, αφαιρεί, αλλοιώνει, καταστρέφει, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, ή τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα*

πρόσβαση στα προστατευόμενα αυτά δεδομένα. Η διάταξη προσομοιάζει με την ως άνω αναλυθείσα (και μεταγενέστερη χρονικά) διάταξη του ά. 11 ν. 3917/2011.

Με την παράγραφο 1 του ά. 15 ν. 3471/2006 τιμωρείται και εδώ η περιέλευση σε γνώση[762] ή οποιαδήποτε επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα. Το περιγραφόμενο έγκλημα είναι κοινό (η διατύπωση της αντικειμενικής υπόστασης ξεκινάει με τη λέξη «όποιος») και μονοπρόσωπο. Είναι, επίσης, έγκλημα ενέργειας και συμπεριφοράς.

Για την πλήρωση της υποκειμενικής υπόστασης της ως άνω διάταξης αρκεί ενδεχόμενος δόλος, ο οποίος πρέπει αντιστοίχως να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

Στο α' εδάφιο της παραγράφου 3 του εν λόγω άρθρου εισάγεται αρχικά ως υποκειμενικό στοιχείο του αδίκου ο σκοπός προσπορισμού παράνομου περιουσιακού οφέλους ή η βλάβη τρίτου και στην περίπτωση αυτή επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000) μέχρι και εκατόν πενήντα χιλιάδων ευρώ (150.000). Στο δεύτερο εδάφιο της παραγράφου 3 τυποποιείται έγκλημα συγκεκριμένης διακινδύνευσης σε περίπτωση πρόκλησης κινδύνου για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή την εθνική ασφάλεια με επαύξηση του αξιοποίνου σε κάθειρξη και χρηματική ποινή από πενήντα χιλιάδες ευρώ (50.000 €) μέχρι τριακόσιες πενήντα χιλιάδες ευρώ (350.000 €). Για το έγκλημα της παραγράφου 3 αρκεί ενδεχόμενος δόλος, ο οποίος πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων ευρώ (10.000) μέχρι και εκατό χιλιάδων ευρώ (100.000), αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

2. ...

3. Εφόσον ο δράστης των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτο, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000) μέχρι και εκατόν πενήντα χιλιάδων ευρώ (150.000). Αν προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή πενήντα χιλιάδων ευρώ (50.000) μέχρι και τριακοσίων πενήντα χιλιάδων ευρώ (350.000).

4. Εφόσον οι πράξεις των παραγράφων 1 και 2 του παρόντος άρθρου τελεσθούν από αμέλεια, επιβάλλεται φυλάκιση μέχρι δεκαοκτώ (18) μηνών και χρηματική ποινή μέχρι και δέκα χιλιάδων ευρώ (10.000).»

[762] Για την προβληματική της περιελεύσεως σε γνώση βλ. και ανωτέρω στην παράγραφο 5.1.3.2 του παρόντος πονήματος.

Τέλος, στην παράγραφο 4 προβλέπεται η τιμώρηση της ως άνω πράξης και από αμέλεια σε βαθμό πλημμελήματος.

5.4.3 Συσχέτιση ά. 15 ν. 3471/2006 με το ά. 11 ν. 3917/2011 και το ά. 370Γ παρ. 2

Η ανάλυση της συσχέτισης της διάταξης της παραγράφου 1 του ά. 15 ν. 3471/2006 με τη διάταξη του ά. 370Γ παρ. 2 ΠΚ δεν μπορεί να είναι διαφορετική από την ανωτέρω ανάλυση αναφορικά με τη σχέση ά. 11 ν. 3917/2011 και ά. 370Γ παρ. 2 ΠΚ[763]. Και σε αυτήν την περίπτωση, η αντικειμενική υπόσταση των εν λόγω εγκλημάτων δεν αναφέρεται σε απλή πρόσβαση δεδομένων. Άρα και σε αυτήν την περίπτωση μπορεί να υποστηριχθεί ότι η διάταξη της παραγράφου 1 του ά. 15 ν. 3471/2006 συρρέει αληθώς και πραγματικώς με τη διάταξη του ά. 370Γ παρ. 2 (βλ. και ανωτέρω στην παράγραφο 5.3.3).

Ίδιος προβληματισμός με την ανωτέρω ανάλυση της παραγράφου 5.3.3 υπάρχει και στην περίπτωση κατά την οποία ο δράστης «*καθιστά προσιτά σε μη δικαιούμενα πρόσωπα*» τα προστατευόμενα δεδομένα.

Αναφορικά με τη σχέση της διάταξης του ά. 11 ν. 3917/2011 και του ά. 15 ν. 3471/2006, είναι προφανές ότι οι δύο αυτές διατάξεις προστατεύουν δεδομένα τα οποία ορίζονται διαφορετικά στον νόμο. Είναι, δηλαδή, η φύση των δεδομένων αυτή που θα καθορίσει ποια από τις δύο διατάξεις θα τύχει εφαρμογής. Σε περίπτωση που αυτά τα δεδομένα ταυτίζονται, τότε φαίνεται ότι έχουμε φαινομένη συρροή και πιθανόν θα εφαρμοστεί ως ειδικότερη η διάταξη του ά. 11 ν. 3917/2011.

5.5 Νομολογιακή αντιμετώπιση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα από τα ελληνικά δικαστήρια

[763] Βλ. ανωτέρω παράγραφο 5.3.3.

Η μόνη από τις ανωτέρω διατάξεις η οποία έχει τύχει εφαρμογής από τα ελληνικά δικαστήρια – μετά από ενδελεχή έρευνα σε επίπεδο δημοσιευμένων αποφάσεων σε νομικά περιοδικά και βάσεις δεδομένων – είναι αυτή του ά. 370Γ παρ. 2 ΠΚ. Καμία από τις υπόλοιπες διατάξεις οι οποίες αναλύονται ανωτέρω δεν φαίνεται (τουλάχιστον στον νομικό τύπο) να έχει εφαρμοστεί.

Η εφαρμογή της διάταξης του άρθρου 370Γ παρ. 2 ΠΚ από τη νομολογία περιορίζεται αποκλειστικά και μόνο στη με αριθμό ***530/2003*** απόφαση του Ναυτοδικείου Πειραιά[764], με την οποία καταδικάστηκε κελευστής για παράνομη χρησιμοποίηση προγράμματος υπολογιστή.

Συγκεκριμένα, ο κατηγορούμενος κελευστής, ενώ δεν περιελαμβάνετο στο εξουσιοδοτημένο προσωπικό, εισήλθε στο γραφείο του Κυβερνήτη του πλοίου στο οποίο υπηρετούσε, έθεσε σε λειτουργία τον ηλεκτρονικό υπολογιστή και χρησιμοποιώντας εγκατεστημένο πρόγραμμα προέβη σε εκτύπωση ορισμένων εγγράφων.

Με την ως άνω απόφαση υιοθετείται η παραδοχή ότι η φράση «χωρίς δικαίωμα», η οποία αποτελεί στοιχείο της αντικειμενικής υπόστασης του εγκλήματος του ά. 370Γ παρ. 2 ΠΚ, σημαίνει αφενός την απουσία οποιασδήποτε μορφής συναίνεσης εκ μέρους του νόμιμου κατόχου των στοιχείων, αφετέρου τη μη ύπαρξη σχετικού δικαιώματος εκ του νόμου (ή από σύμβαση). Αναφορικά προς την πρώτη έννοιά της είναι βέβαιον ότι πρόκειται για συγκατάθεση, η οποία αποκλείει την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος και δεν αίρει απλώς τον άδικο χαρακτήρα της πράξεως, αφού, όταν αυτή συντρέχει, δεν υφίσταται καν προσβολή του εννόμου αγαθού. Συμπληρώνει δε ότι *«η χρησιμοποίηση προγραμμάτων που ανήκουν σε άλλους τιμωρείται σε κάθε περίπτωση που λαμβάνει χώρα, χωρίς σχετικό δικαίωμα, γεγονός που διευρύνει υπερβολικά το αξιόποινο και οδηγεί στο συμπέρασμα ότι με τη διάταξη αυτή δεν κολάζονται μόνο οι σοβαρές προσβολές (π.χ. δημόσια εκτέλεση ενός προγράμματος) αλλά και οι πλέον μηδαμινές (π.χ. χρησιμοποίηση του προσωπικού υπολογιστή συναδέλφου που απουσιάζει, του υπολογιστή τσέπης άλλου κ.λπ.)»*. Ωστόσο, όπως ήδη αναφέρθηκε, οι όποιες τυχόν δυσμενείς συνέπειες της διεύρυνσης του αξιοποίνου σαφώς περιορίζονται από το γεγονός ότι το έγκλημα διώκεται κατ'

[764] Βλ. απόφ. Ναυτ. Πειρ. 530/2003, ΠοινΧρ ΝΔ/2004, σελ. 75.

έγκληση, η οποία πρέπει να υποβληθεί από τον παθόντα εντός τριών μηνών, όπως προβλέπεται στην τελευταία παράγραφο του άρθρου 370Γ παρ. 2 ΠΚ.

Είναι, άρα, προφανές ότι αυτή η μία και μοναδική δημοσιευμένη απόφαση (και άρα η έλλειψη σχετικής νομολογίας)[765] ισοδυναμεί με κατ' ουσίαν μη εφαρμογή της διάταξης του ά. 370Γ παρ. 2 ΠΚ. Αν ληφθεί, δε, υπόψη ότι η εν λόγω απόφαση αφορά σε έγκλημα τελεσθέν όχι μέσω διαδικτύου αλλά μέσω απλού εγκατεστημένου προγράμματος ηλεκτρονικού υπολογιστή, η αχρησία της διάταξης του άρθρου 370Γ παρ. 2 ΠΚ για περιπτώσεις hacking στο διαδίκτυο είναι δεδομένη.

5.6 Κριτική επισκόπηση και προτάσεις de lege ferenda αναφορικά με την ποινική αντιμετώπιση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking

Μετά την επισκόπηση των διατάξεων της ελληνικής ποινικής νομοθεσίας αναφορικά με την τιμώρηση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και σε σχετικές πράξεις, βασικό συμπέρασμα το οποίο προκύπτει είναι ότι οι νομοθετικές πρωτοβουλίες που έχουν αναληφθεί έχουν αποσπασματικό χαρακτήρα και ότι δεν έχουν ενταχθεί στην ελληνική νομοθεσία ως συστημικά διασυνδεδεμένες μεταξύ τους.

Καταρχάς, είκοσι έξι χρόνια μετά την ψήφιση του ν. 1805/1988, οι ισχύουσες νομοθετικές ρυθμίσεις κρίνονται εκ των πραγμάτων ανίσχυρες και αλυσιτελείς – λόγω και της περιορισμένης νομολογιακά εφαρμογής τους – αναφορικά με το να ανταποκριθούν στην εμφανιζόμενη πολυπλοκότητα και ιδιαιτερότητα των νέων μορφών ηλεκτρονικής εγκληματικότητας. Βέβαια, ο νομοθέτης του ν. 1805/1988 δεν ήταν σε θέση να γνωρίζει και να προβλέψει τα νέα δεδομένα που θα επέρχοντο και τελικά δημιουργήθηκαν από την αλματώδη εξέλιξη της πληροφορικής και τη διαρκώς

[765] Κατά μία έννοια σχετική με πληροφορικό έγκλημα είναι και η απόφαση ΑΠ 121/2003 (ΠοινΧρ ΝΓ/2003, σελ. 910 επ. με παρατηρήσεις *Αγγ. Κωνσταντινίδη*) στην οποία εφαρμόστηκε το ά. 370Β ΠΚ σε περίπτωση αντιγραφής προγράμματος ηλεκτρονικού υπολογιστή το οποίο εμπίπτει στο επαγγελματικό απόρρητο. Κατά τα πραγματικά περιστατικά, ωστόσο, της ως άνω απόφασης, δεν έλαβε χώρα «χωρίς δικαίωμα» πρόσβαση αλλά αθέμιτη αντιγραφή προγράμματος ηλεκτρονικού υπολογιστή το οποίο κρίθηκε ότι ενέπιπτε στο επαγγελματικό απόρρητο, σύμφωνα και με την αντικειμενική υπόσταση της διάταξης του άρθρου 370Β ΠΚ.

αυξανόμενη χρήση και εξάπλωση του διαδικτύου. Λόγω των νέων αυτών δεδομένων της τεχνολογικής εξέλιξης, η σύγχρονη κοινωνία αποτελεί πλέον «κοινωνία της πληροφορίας»[766], στο χώρο της οποίας διαμορφώνεται το αγαθό της πληροφορίας, η οποία ρέει πλέον ταχύτατα στο χωρίς σύνορα διαδίκτυο.

Από εκεί και πέρα, οι προσπάθειες του νομοθέτη να διαφυλάξει το λογισμικό τηλεφωνικών εταιρειών για την αποτροπή παρακολουθήσεων των τηλεφωνικών κλήσεων καθώς και των δεδομένων, τα οποία μπορούν να είναι πολύτιμα για την αντιμετώπιση της τρομοκρατίας ή του οργανωμένου εγκλήματος είναι προφανώς αποσπασματικές. Καλύπτουν μόνο ένα μικρό μέρος ηλεκτρονικών δεδομένων και η αφορμή για την θέσπισή τους ήταν είτε κάποιο σημαντικό γεγονός (όπως οι υποκλοπές τηλεφωνικών συνδιαλέξεων μελών της Κυβέρνησης), το οποίο οδήγησε σε σπασμωδικές νομοθετικές αντιδράσεις, είτε η εσπευσμένη ανάγκη για ενσωμάτωση ευρωπαϊκών νομικών κειμένων. Για όλες τις υπόλοιπες πράξεις χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και συνεπώς για δεδομένα που δεν εντάσσονται στις αντικειμενικές υποστάσεις των ά. 292Α ΠΚ, ά. 15 ν. 3471/2006 και 11 ν. 3917/2011 αντιστοίχως, όπως αναλύονται ανωτέρω, εφαρμόζεται ακόμη η διάταξη της παραγράφου 2 του ά. 370Γ ΠΚ.

Άρα, βασικό μέλημα του έλληνα ποινικού νομοθέτη πρέπει να είναι η κωδικοποίηση των ανωτέρω διατάξεων. Ενδεχομένως, ο έλληνας νομοθέτης πρέπει να προβεί στην κατάρτιση μίας διάταξης η οποία θα καλύπτει όλες τις επιθυμητές περιπτώσεις (σε συνδυασμό και με την κύρωση της Σύμβασης της Βουδαπέστης[767])[768], προκειμένου να αποφευχθεί η πολυνομία και η σύγχυση μεταξύ περισσότερων ποινικών νόμων – οι οποίοι μάλιστα έχουν ενίοτε και μεγάλες αποκλίσεις στα πλαίσια ποινής που προβλέπουν – γεγονός το οποίο ενδεχομένως να λειτουργεί αρνητικά αναφορικά με την εφαρμογή των εν λόγω κανόνων δικαίου[769]. Η διάταξη αυτή θα πρέπει να είναι

[766] Βλ. χαρακτηριστικά *Λίλιαν Μήτρου,* Το δίκαιο στην κοινωνία της πληροφορίας, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002.

[767] Βλ. κατωτέρω παράγραφο 6.2.2.

[768] Για τις σύγχρονες τάσεις στην αναμόρφωση του ποινικού δικαίου αναφορικά με την εγκληματικότητα στον Κυβερνοχώρο βλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 284 επ.

[769] … με αποτέλεσμα οι εν λόγω διατάξεις να αποτελούν περισσότερο law in books παρά law in action (πρβλ. σχετικώς τη διάκριση από τον *R. Pound*, Law in Books and Law in Action, εις: American Law Review, 1910, 118 επ., 398 επ., 510 επ. όπως παραπέμπεται από τον *Ν. Κουράκη* καθώς και όλη την εύστοχη ανάπτυξη του τελευταίου στο άρθρο του: Ποινικές διατάξεις που μένουν ανεφάρμοστες – Ένα κρίσιμο πρόβλημα της αντεγκληματικής πολιτικής, εις: *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π. σελ. 149 επ.).

στραμμένη στην προστασία των συστημάτων πληροφοριών[770] (ανεξαρτήτως περιεχομένου αυτών και αν μέσω αυτών παρέχονται τηλεφωνικές υπηρεσίες) και να έχει ως προστατευόμενο έννομο αγαθό την ασφάλεια των συστημάτων πληροφοριών [όπως αναλύεται ανωτέρω και ορίζεται διαζευκτικά και όχι σωρευτικά σε εμπιστευτικότητα (confidentiality) – (άλλως το απόρρητο των πληροφοριών που ενσωματώνουν), ακεραιότητα (integrity) και διαθεσιμότητα (availability) των στοιχείων]. Η διάταξη θα πρέπει να προβλέπει την τιμώρηση όχι μόνο για τη χωρίς δικαίωμα πρόσβαση αλλά και για τον αποκλεισμό της πρόσβασης και για κάθε άλλη πράξη η οποία προσβάλλει τα ως άνω στοιχεία της ασφάλειας των δεδομένων. Η ασφάλεια των συστημάτων πληροφοριών πρέπει να προστατεύεται και στις τρεις ανωτέρω εκφάνσεις της, όχι σωρευτικά αλλά ακόμη και στην περίπτωση κατά την οποία πληγεί μία εξ αυτών (π.χ. μια DDoS επίθεση μπορεί να μην πλήττει την εμπιστευτικότητα και την ακεραιότητα, πλήττει, όμως, τη διαθεσιμότητα των στοιχείων) Επίσης, η αναφορά σε συστήματα πληροφοριών (σύμφωνα και με τις σύγχρονες νομοθετικές εξελίξεις σε ευρωπαϊκό επίπεδο) θα παράσχει προστασία σε στοιχεία και δεδομένα τα οποία είναι αποθηκευμένα ή αφορούν νέου τύπου συσκευές με δυνατότητα διασύνδεσης (π.χ. κινητά τηλέφωνα – smart phones), για τα οποία δήμερα δεν υπάρχει σχετική πρόβλεψη[771]. Πρέπει, στη συνέχεια, να καταβληθεί προσπάθεια ώστε η διάταξη αυτή να έχει τέτοιο εύρος και ελαστικότητα διατύπωσης (τηρώντας βέβαια την αρχή nullum crimen nulla poena sine lege σε όλες τις εκφάνσεις της[772]) προκειμένου να μπορεί να ρυθμίσει και μελλοντικές μορφές πρόσβασης σε στοιχεία, οι οποίες κατά το χρόνο θέσπισης θα είναι εκ των πραγμάτων

[770] Στην πλέον πρόσφατη Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών ως σύστημα πληροφοριών ορίζεται «*η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους*» (βλ. και παράγραφο 6.3.13 του παρόντος πονήματος). Ο ορισμός αυτός ανταποκρίνεται στη σύγχρονη πραγματικότητα όπου έχουμε δει ότι παντός είδους συσκευές διασυνδέονται πλέον στο διαδίκτυο (παράγραφος 5.1.3.1 του παρόντος πονήματος).

[771] Βλ. ανωτέρω έννοια «στοιχείων» στην ανάλυση του ά. 370Γ παρ. 2. Η, δε, διάταξη του ά. 15 ν. 3471/2006 αναφέρεται αφενός σε δεδομένα προσωπικού χαρακτήρα, αφετέρου δεν αναφέρεται σε χωρίς δικαίωμα πρόσβαση αλλά σε άλλες ενέργειες.

[772] ... και σύμφωνα και με το ά. 7 του Συντάγματος (βλ. ενδεικτικά σχετικές ερμηνευτικές αναλύσεις του *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 93 επ. καθώς και *Ιακ. Φαρσεδάκη & Χρ. Σατλάνη*, Βαθμίδες, κριτήρια και μέθοδοι ερμηνείας και περαιτέρω διάπλασης του Ουσιαστικού Ποινικού Δικαίου, ΠοινΔικ 12/2012, σελ. 1118 επ.).

παντελώς άγνωστες στον νομοθέτη. Έτσι, θεωρώ ότι θα αποφευχθεί και η διαπίστωση νομοθετικού κενού σε σύντομο χρονικό διάστημα.

Η προσοχή του νομοθέτη πρέπει να επικεντρωθεί στο σύστημα πληροφοριών αυτό καθεαυτό. Σήμερα, ο νομοθέτης δίνει ιδιαίτερη σημασία στα «κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή του ιδιωτικού τομέα» (λαμβάνοντας υπόψιν το πολύ αυστηρότερο πλαίσιο ποινής του ά. 370Β σε σχέση με το ά. 370Γ παρ. 2). Η ειδική αυτή προστασία είναι προφανώς μονομερής καθώς, κατά πρώτον, υπάρχει περίπτωση εντός ενός συστήματος πληροφοριών να ανευρίσκονται δεδομένα με διαφορετικά χαρακτηριστικά (από επαγγελματικά έως μόνο προσωπικά) αλλά και, κατά δεύτερον, το ηλεκτρονικό σύστημα πληροφοριών στο οποίο μπορεί να αποκτηθεί χωρίς δικαίωμα πρόσβαση ενδέχεται να αποτελέσει τη «γέφυρα» μέσω διασύνδεσης για επαφή με δεδομένα αποθηκευμένα σε διασυνδεδεμένο σύστημα πληροφοριών. Με μια ενιαία ρύθμιση θα υπερβούμε εντελώς κάθε συζήτηση αναφορικά με τη σχέση του ά. 370Γ παρ. 2 και του ά. 370Β ΠΚ (η οποία, ούτως η άλλως, θεωρώ ότι έχει σε επίπεδο νομικής θεωρίας διασαφηνιστεί πλήρως από τις αναπτύξεις του Κιούπη[773]) και θα λυθούν οι αντινομίες που υπάρχουν σήμερα μεταξύ του ά. 370Β και 370Γ παρ. 2 αναφορικά με το πλαίσιο ποινής, το οποίο είναι εντελώς διαφορετικό σε αυτές τις δύο διατάξεις.

Η ενιαία διάταξη αυτή πρέπει, επιπλέον, να λάβει υπόψη της δύο ακόμα στοιχεία:

Κατά πρώτον, φαίνεται να είναι απαραίτητη η συμπερίληψη στην ισχύουσα διάταξη επιβαρυντικής περίστασης του βασικού εγκλήματος της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα σε περίπτωση που ο δράστης είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον (περιουσιακό) όφελος ή να προξενήσει βλάβη στο σύστημα πληροφοριών του θύματος. Τούτο φαίνεται αναγκαίο λόγω της τεράστιας οικονομικής αξίας της ηλεκτρονικής πληροφορίας[774].

Κατά δεύτερον, ενδεχομένως να πρέπει να επεξεργαστούμε τη μη τιμώρηση πρόσβασης σε ηλεκτρονικά δεδομένα σε περίπτωση μη παραβίασης μέτρου ασφαλείας[775] σύμφωνα και με το ά. 3[776] της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού

[773] Βλ. *Δημ. Κιούπη*, Ποινικό Δίκαιο και Internet, όπ. π., σελ. 133.

[774] Βλ. ανωτέρω αναπτύξεις στην παράγραφο 1.2 του παρόντος πονήματος καθώς και κατωτέρω παραγράφους 8.2 και 8.3 σχετικά με τον σχολιασμό των αποτελεσμάτων της έρευνας που ακολουθεί.

[775] Βλ. σχετικά ά. 2 της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Σύμβαση της Βουδαπέστης), όπως αναλύεται κατωτέρω στην παράγραφο 6.2.2 του παρόντος πονήματος.

Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου[777]. Αυτή η προσέγγιση ίσως βοηθήσει στην εκτόνωση της δράσης των hackers που θέλουν να εξελίξουν τις δυνατότητές τους εξερευνώντας τα συστήματα πληροφοριών. Πέραν τούτου, όμως, δεν φαίνεται να είναι και αναγκαία η τιμώρηση σε περίπτωση μη παραβίασης μέτρου ασφαλείας. Η χρήση (τουλάχιστον) ενός προσωπικού κωδικού αριθμού αποτελεί μια απλή αλλά και σαφή δήλωση ότι ο νόμιμος κάτοχος των ηλεκτρονικών δεδομένων και διαχειριστής του συστηματος πληροφοριών επιθυμεί να ελέγξει και να περιορίσει την πρόσβαση στα δεδομένα. Σε περίπτωση ανυπαρξίας κάποιου μέτρου ασφαλείας, ο νόμιμος κάτοχος των δεδομένων δεν έχει ο ίδιος δείξει ενδιαφέρον για τα δεδομένα του – επομένως, μια διάταξη η οποία θα τιμωρεί για πράξη για την οποία το ίδιο το θύμα δεν έκανε τίποτε για να αποτρέψει θα αποτελεί έκφραση ενός άκρως προστατευτικού ποινικού δικαίου, το οποίο τουλάχιστον θα υπονομεύει την κουλτούρα της πρόληψης των εγκλημάτων. Βέβαια, είναι γεγονός ότι σήμερα η χωρίς δικαίωμα πρόσβαση κατ' ά. 370Γ παρ. 2 είναι κατ' έγκληση διωκόμενο έγκλημα και η δίωξη αυτού καταλείπεται, ουσιαστικά, στην επιμέλεια του παθόντος ή του αμέσως ζημιωθέντος. Υπάρχει, όμως, περίπτωση κάποιος να υποβάλλει έγκληση για χωρίς δικαίωμα πρόσβαση σε δεδομένα του χωρίς να έχει ο ίδιος λάβει κανένα μέτρο προστασίας αυτών. Είναι αυτή η αντινομία η οποία θεωρείται πως είναι σκόπιμο να λυθεί.

Πιθανός αντίλογος σε αυτή την τελευταία θέση μπορεί, ίσως, να αρθρωθεί. Αρχικά, ο αντίλογος μπορεί να έχει ως βάση μια ενδεχόμενη «παραβίαση οικιακής ειρήνης» στον χώρο του διαδικτύου, στην οποία αναφέρεται εύστοχα ο Κιούπης[778]. Πιστεύω ότι για τα συστήματα πληροφοριών σε περίπτωση μη λήψεως μέτρου ασφαλείας δεν τίθεται θέμα «οικιακής ειρήνης» διότι φαίνεται ο hacker να «παραβιάζει ανοιχτές θύρες». Ακόμη και π.χ. σε μια οικία χωρίς πόρτα είναι αλήθεια ότι το έννομο αγαθό προβάλλει εξασθενημένο, πολλώ δε μάλλον στα συστήματα πληροφοριών και στο διαδίκτυο.

---

[776] Άρθρο 3: ***Παράνομη πρόσβαση σε συστήματα πληροφοριών***

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

[777] Βλ. κατωτέρω παράγραφο 6.3.13 του παρόντος πονήματος.

[778] *Δημήτρης Κιούπης*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, όπ. π., σελ. 970.

Επιπρόσθετα, θα μπορούσε να υποστηριχθεί ότι κατά την πρόσβαση σε επίπεδο πνευματικής ιδιοκτησίας θίγεται το ηθικό δικαίωμα του δημιουργού[779] του ηλεκτρονικού προγράμματος[780], το οποίο κάποιος hacker δύναται να εξερευνήσει (σε περίπτωση αντιγραφής πιστεύω ότι μπορεί να υποστηριχθεί ότι θίγεται στον πυρήνα του το περιουσιακό δικαίωμα του δημιουργού και άρα η πράξη έχει μεγαλύτερη απαξία). Κάποιος προγραμματιστής πρέπει να αφήσει κενά ασφαλείας σε κάποιο πρόγραμμα τα οποία, ωστόσο, και αυτά δύνανται να προστατεύονται ή να ελέγχεται η πρόσβαση σε αυτά από κάποιο μέτρο ασφαλείας, το οποίο μπορεί να θέσει ο ίδιος. Η χρήση μέτρου ασφαλείας είναι μάλλον η πλέον εύκολη σε τεχνικό επίπεδο για κάποιον που επιθυμεί να προστατεύσει ηλεκτρονικά του δεδομένα, ιδίως αν είναι προγραμματιστής συστημάτων πληροφοριών. Επομένως, καταλείπεται αρχικά στον διαχειριστή των ηλεκτρονικών δεδομένων η επιλογή ή όχι της προστασίας – εκ των υστέρων, ο ποινικός νόμος, ως «έσχατο καταφύγιο» μπορεί να κληθεί να τιμωρήσει όσους παραβίασαν ήδη τεθειμένα όχι μόνο ηθικά αλλά και πραγματικά όρια.

Περαιτέρω, υπάρχουν και δύο πραγματιστικοί προβληματισμοί αναφορικά με την ανωτέρω θέση: κατά πρώτον, υπάρχει η δυνατότητα απομακρυσμένης χωρίς δικαίωμα πρόσβασης (π.χ. μέσω διαδικτύου) χωρίς την παραβίαση κάποιου μέτρου ασφαλείας; Δεν μπορεί να εικάζεται ότι σε αυτήν την περίπτωση, αφού δεν έχει τεθεί μέτρο ασφαλείας, η πρόσβαση δεν λαμβάνει χώρα χωρίς δικαίωμα; Εκτιμώ ότι μπορεί να λάβει χώρα απομακρυσμένη χωρίς δικαίωμα πρόσβαση χωρίς παραβίαση μέτρου ασφαλείας. Ενδεικτικά, υπάρχουν στο διαδίκτυο ιστότοποι που χρησιμοποιούνται πολλές φορές για τη διαχείριση άλλων ιστοσελίδων (π.χ. cms – content manager system), οι οποίοι δεν δημοσιοποιούν την διεύθυνσή τους (url) και δεν είναι μάλιστα εντοπίσιμοι μέσω των μηχανών αναζήτησης του διαδικτύου. Η, δε, ύπαρξη ή μη δικαιώματος για πρόσβαση, όπως είδαμε ανωτέρω, δύναται να

[779] Για την πνευματική ιδιοκτησία πρβλ. ενδεικτικά *Δ. Καλλινίκου*, Πνευματική ιδιοκτησία και συγγενικά δικαιώματα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000 και *Δ. Μαλακάση*, Η πνευματική ιδιοκτησία, 2η εκδ. Αθήνα, 2002. Ενδεικτικά για την πνευματική ιδιοκτησία στο διαδίκτυο πρβλ. *Έλσας Δεληγιάννη*, Πνευματική ιδιοκτησία και επικοινωνία την εποχή του διαδικτύου: νομικό πλαίσιο και προοπτικές για την διαδικτυακή ανταλλαγή μουσικών αρχείων, ΔιΜΕΕ 4/2007, σελ. 480 επ., *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 426-427 και κυρίως *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 238 επ.

[780] Βλ. συγκεκριμένα *Δημ. Απρογέρακας*, Ποινική προστασία προγραμμάτων Η/Υ, Πρακτικά ημερίδας για την «Πειρατεία Λογισμικού: Οικονομικές και Νομικές Επιπτώσεις», ΑΣΟΕΕ, 24.05.1999, σελ. 33-41, *Ηλίας Βολονάσης*, Ποινική προστασία προγραμμάτων Η/Υ, Πρακτικά ημερίδας της Ένωσης Δικαστών και Εισαγγελέων για την «Προστασία προγραμμάτων ηλεκτρονικών υπολογιστών», ΑΣΟΕΕ, 19.02.1999, σελ. 29-35 και *Μιχαήλ – Θεόδωρος Μαρίνος*, Λογισμικό (software). Νομική προστασία και συμβάσεις, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1992.

συνάγεται από τις περιστάσεις. Είναι δυνατόν να θεωρηθεί ότι, από τη στιγμή που κάποιος χρήστης δεν έχει δημοσιοποιήσει την ηλεκτρονική διεύθυνση (url) μιας τέτοιας ιστοσελίδας (η οποία, μάλιστα, είναι με τέτοιο τρόπο κατασκευασμένη ώστε να μην ανευρίσκεται στις μηχανές αναζήτησης), ο αποκτών πρόσβαση με πρόθεση σε αυτήν πράττει χωρίς δικαίωμα (σε περίπτωση που ο hacker αποκτήσει χωρίς δικαίωμα πρόσβαση σε μια τέτοια ιστοσελίδα από αμέλεια δεν τιμωρείται, καθώς, όπως είδαμε, κατά τη διάταξη του ά. 370Γ παρ. 2 η πράξη δεν τιμωρείται όταν τελείται εξ αμελείας). Υπάρχει, λοιπόν, περίπτωση ο hacker να αποκτήσει χωρίς δικαίωμα πρόσβαση σε μια τέτοια σελίδα χωρίς να παραβιάσει κάποιον κωδικό, αν δεν έχει τεθεί κωδικός για την πρόσβαση σε αυτή τη σελίδα. Η τιμώρηση μόνο σε περιπτώσεις παραβίασης μέτρου ασφαλείας θα λύσει, παρά τα παραπάνω, τις δυσχέρειες της υπάρξης ή μη δικαιώματος (συναγομένης εκ των περιστάσεων), θα προκαλέσει τους διαχειριστές ιστοσελίδων στο να προστατεύουν πληρέστερα τα δεδομένα τους, θα συμβάλλει στη δημιουργία «κουλτούρας ασφαλείας»[781] και, γενικότερα, θα διασαφηνιστεί και θα καθορισθεί ακριβώς ποια είναι η παράνομη και ποια η νόμιμη δραστηριότητα.

Κατά δεύτερον, είναι πλέον προφανής η πρακτική σχεδόν όλων των χρηστών ψηφιακών συσκευών (π.χ. "smart phones") να εισέρχονται σε σύστημα πληροφοριών με κωδικό και να επιλέγουν η συγκεκριμένη ψηφιακή συσκευή να μην τους ζητήσει ξανά τον κωδικό για εισαγωγή τους στο συγκεκριμένο σύστημα πληροφοριών. Μπορεί επομένως κάποιος να αποκτήσει χωρίς δικαίωμα πρόσβαση σε δεδομένα εισερχόμενος σε σύστημα πληροφοριών του θύματος μέσω π.χ. του κινητού τηλεφώνου ή του tablet του θύματος τη στιγμή που το θύμα δεν είναι παρόν, χωρίς να παραβιάσει κανένα μέτρο ασφαλείας (αφού οι κωδικοί έχουν ήδη δοθεί στο σύστημα από το θύμα). Είναι λογικό ότι δεν μπορούμε να μην προβλέψουμε αυτήν την εξαίρεση σε μια de lege ferenda ρύθμιση. Άρα, η νέα αυτή ρύθμιση θα πρέπει να προβλέπει ως χωρίς δικαίωμα πρόσβαση, πέρα απο την παραβίαση μέτρου ασφαλείας, και την απόκτηση φυσικής πρόσβασης σε σύστημα πληροφοριών από συσκευή του θύματος ή χωρίς τη συγκατάθεση του θύματος (και σε κάθε περίπτωση, βέβαια, τη διάθεση κωδικών πρόσβασης που μπορούν να επιτρέπουν την πρόσβαση,

[781] Βλ. και κατωτέρω παραγράφους 8.4. και 9.2.

σύμφωνα και με το ά. 7 περ. β' της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου)[782].

Τέλος, de lege ferenda θα πρέπει να ληφθεί υπόψιν και η χρήση επιβλαβών προγραμμάτων τα οποία ενδεχομένως δύναται να δημιουργηθούν και να χρησιμοποιηθούν για παρακολούθηση ενός συστήματος πληροφοριών[783], καθώς βάσιμα μπορεί να εκτιμηθεί ότι η τεχνολογία μπορεί να στραφεί στο μέλλον στη δημιουργία προγραμμάτων τα οποία θα εγκαθίστανται σε κάποιο σύστημα πληροφοριών (ίσως ακόμη και χωρίς να παραβιαστεί κάποιο μέτρο ασφαλείας) και θα λειτουργούν στην ουσία ως προγράμματα παρακολούθησης των δραστηριοτήτων του χρήστη στο σύστημα πληροφοριών.

[782] Βλ. την ανάλυση της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12.08.2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου στην παράγραφο 6.3.13 κατωτέρω.

[783] Βλ. και ά. 7 περ. β' της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12.08.2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (βλ. κατωτέρω παράγραφο 6.3.13).

6. ΤΟ HACKING ΣΤΑ ΔΙΕΘΝΗ ΚΑΙ ΕΥΡΩΠΑΪΚΑ - ΚΟΙΝΟΤΙΚΑ ΚΕΙΜΕΝΑ

6.1 Εισαγωγή

Αυτό που έγινε ιδιαίτερα αντιληπτό τα τελευταία χρόνια, με την τεράστια ανάπτυξη του διαδικτύου και κινητοποίησε τη διεθνή κοινότητα είναι ότι οι συνέπειες εγκληματικών συμπεριφορών που στρέφονται κατά συστημάτων πληροφοριών ή δεδομένων μπορεί να έχουν ευρύτατη επέκταση χωρίς να γνωρίζουν γεωγραφικά ή εθνικά όρια[784].

Η ευρωπαϊκή και διεθνής εναρμόνιση των πράξεων που θα πρέπει να θεωρούνται αξιόποινες αποτελεί το πρώτο βήμα για να σχεδιαστούν από εκεί και πέρα εναρμονισμένες παρεμβάσεις στο πεδίο του δικονομικού δικαίου αλλά και να διευκολυνθεί η δικαστική συνεργασία μεταξύ των κρατών με λήψη πρόσφορων μέτρων[785]. Είναι προφανές ότι, όταν το ενδιαφέρον εστιάζεται στην ποινική προστασία των συστημάτων πληροφοριών και των δεδομένων τους από επιθέσεις που στρέφονται κατά αυτών, οι επιλογές, οι πολιτικές και οι δράσεις αντεγκληματικής

[784] Πρβλ. σχετικώς για τις σύγχρονες εξελίξεις στο ευρωπαϊκό ποινικό δίκαιο *Μ. Καϊάφα – Γκμπάντι*, Ευρωπαϊκό ποινικό δίκαιο και Συνθήκη της Λισσαβώνας, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2011.

[785] Σε επίπεδο υπερκρατικών οργανισμών, η Ευρωπαϊκή Ένωση διεκδικεί να δημιουργήσει για τα κράτη μέλη της έναν ενιαίο χώρο ελευθερίας, ασφάλειας και δικαιοσύνης (ά. 3 παρ. 2 ΣΕΕ και ά. 67 ιδίως παρ. 1 και 3 ΣΛΕΕ) και να αντιμετωπίσει την ιδιαίτερα σοβαρή εγκληματικότητα με διακρατική διάσταση, την οποία εμφανίζει και το ηλεκτρονικό έγκλημα.

Πρβλ. και το πολύ ενδιαφέρον άρθρο της *Estella Baker*, Governing through crime – the case of the European Union, European Journal of Criminology, vol. 7, n. 3, May 2010, pp. 187 f. όπου ως συμπέρασμα αναφέρεται στη στρατηγική της ΕΕ "governing through security" καθώς και το εξίσου ενδιαφέρον άρθρο του *Γ. Νικολόπουλου*, «Ελευθερία, Ασφάλεια, Δικαιοσύνη»: Οι προβληματικές οριοθετήσεις του Ευρωπαϊκού Κοινωνικού Ελέγχου, εις: *Χ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 73 επ.

πολιτικής του διεθνούς και ενωσιακού θεσμικού πλαισίου[786], οι οποίες συγκαθορίζουν και τις αποφάσεις των εθνικών νομοθετών, έρχονται αναγκαστικά στο προσκήνιο[787].

6.2 *Το hacking και η χωρίς δικαίωμα πρόσβαση σε δεδομένα στο πλαίσιο του Συμβουλίου της Ευρώπης*

6.2.1 Συστάσεις του Συμβουλίου της Ευρώπης για τα πληροφορικά εγκλήματα

Το Συμβούλιο της Ευρώπης έχει ιδιαίτερα ασχοληθεί με το ηλεκτρονικό έγκλημα εντός αλλά και εκτός κυβερνοχώρου ήδη από το λυκαυγές της ευρείας χρήσης των υπολογιστών και του διαδικτύου. Ειδικότερα, έχουν εκδοθεί δύο σχετικές με το θέμα Συστάσεις: πρώτον, η Σύσταση No R (89) 9 της 13.09.1989 σχετικά με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή[788] [789] και, δεύτερον, η Σύσταση No R (95) 13 της 11.09.1995 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών[790]. Η σπουδαιότητα της τελευταίας Σύστασης είναι πολύ μεγάλη διότι καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων[791].

---

[786] Αναφορικά με την αντεγκληματική πολιτική στον ευρωπαϊκό χώρο πρβλ. το αναλυτικό πόνημα του *Γ. Νικολόπουλου*, Η Ευρωπαϊκή Ένωση ως φορέας αντεγκληματικής πολιτικής, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2008.

[787] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ ΞΑ/2011, σελ. 490.

[788] Recommendation No R (89) 9 on Computer related crime. Το πλήρες κείμενο της Σύστασης ανευρίσκεται στο url: http://www.oas.org/juridico/english/89-9&final%20Report.pdf.

[789] Βλ. *Τάσος Ν. Μαρίνος*, Σύμβουλος Επικρατείας, Οι ηλεκτρονικοί υπολογιστές και το δίκαιο, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1991, σελ. 144.

[790] Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology. Το πλήρες κείμενο της Σύστασης ανευρίσκεται στο url: http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp.

[791] Βλ. *Ιωάννης Εμμ. Αγγελής*, Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime – Internet Crime), ΠοινΧρ Ν/2000, σελ. 680.

6.2.2 Η Σύμβαση του Συμβουλίου της Ευρώπης της 23.11.2001 για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on cyber-crime)

Σε διεθνές πεδίο κεντρική θέση στον τομέα αντιμετώπισης της ηλεκτρονικής εγκληματικότητας κατέχει η Σύμβαση του Συμβουλίου της Ευρώπης *«για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο»*[792]. Η αλματώδης ανάπτυξη του διαδικτύου κινητοποίησε τη διεθνή κοινότητα, η οποία αντιλήφθηκε ότι οι συνέπειες των εγκληματικών συμπεριφορών που στρέφονται κατά των συστημάτων πληροφοριών ή των δεδομένων έχουν ευρύτατη επέκταση, χωρίς να γνωρίζουν εθνικά σύνορα. Συγκεκριμένα, το Συμβούλιο της Ευρώπης, συνειδητοποιώντας τις ριζικές αλλαγές και τις εξελίξεις στην ψηφιακή κοινωνία, αναγνώρισε ότι η αποτελεσματική αντιμετώπιση της αυξανόμενης εγκληματικότητας στον κυβερνοχώρο μπορεί να γίνει μόνο με αναπτυγμένη, γρήγορη και καλά εφαρμοσμένη διεθνή συνεργασία σε ποινικά θέματα[793]. Συνεπώς, με τη σύναψη της συνθήκης αυτής επιχειρήθηκε η κοινή χάραξη πολιτικής και η υιοθέτηση από τα συμβαλλόμενα κράτη νομοθετικών μέτρων προκειμένου να αντιμετωπισθούν από κοινού και με κοινό τρόπο τα εγκλήματα που τελούνται στο διαδικτυακό περιβάλλον[794].

Στη Βουδαπέστη, στις 23 Νοεμβρίου 2001, καταρτίσθηκε στο πλαίσιο του Συμβουλίου της Ευρώπης η ως άνω Σύμβαση. Η Σύμβαση τέθηκε σε ισχύ ήδη στα τέλη Φεβρουαρίου του 2002, σύμφωνα με το ά. 36 παρ. 2 αυτής. Τα περισσότερα από τα κράτη-μέλη της ΕΕ την έχουν, μάλιστα, ήδη κυρώσει, η Ελλάδα, ωστόσο, δεν συγκαταλέγεται ακόμη σε αυτά[795]. Επίσης, την έχουν υπογράψει και 4 χώρες ως

---

[792] Βλ. Η Σύμβαση αυτή έχει δημοσιευθεί στην ηλεκτρονική διεύθυνσηhttp://conventions.coe.int/Treaty/en/Treaties/html/185.htm. Το κείμενο έχει δημοσιευθεί με τον τίτλο "European Committee on Crime Problems (CDPC), Committee of Experts on Crime in Cyber – Space (PC-CY), Draft Convention on Cyber – crime (Draft No 22 REV.2)".

[793] Βλ. *Ιωάννης Εμμ. Αγγελής*, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 12/2001, σελ. 1218. Σημαντική χαρακτηρίζει τη Σύμβαση και η Τσήτσουρα (*Αγ. Τσήτσουρα*, Εγκληματικότητα και αντεγκληματική πολιτική στην εποχή της παγκοσμιοποίησης, εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ ΙΙ, σελ. 1418).

[794] Βλ. *Νικόλαος Δ. Φαραντούρης*, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 196.

[795] Την ανάγκη για κύρωση της Συμβασης και από την Ελλάδα έχουν επισημάνει ήδη από το 2003 και οι *Δ. Αγγελόπουλος* και *Ιωάν. Πάσχος*, Κατάσχεση – ανάλυση ψηφιακών πειστηρίων, ΠοινΔικ 4/2003,

παρατηρητές (Καναδάς, Ιαπωνία, Νότιος Αφρική και Ηνωμένες Πολιτείες Αμερικής). Χαρακτηριστικό είναι ότι η Ευρωπαϊκή Επιτροπή ενθαρρύνει με επίταση τα κράτη μέλη της Ένωσης που δεν έχουν ακόμη κυρώσει τη Σύμβαση να το πράξουν το συντομότερο δυνατό. Ωστόσο, η ίδια η Ευρωπαϊκή Ένωση δεν αποτελεί συμβαλλόμενο μέρος της[796].

Η Σύμβαση αυτή, γνωστή και ως Σύμβαση της Βουδαπέστης[797], αποσκοπεί στην καθιέρωση χάραξης κοινής αντεγκληματικής πολιτικής. Αναφορικά με το περιεχόμενό της, η Σύμβαση θέτει τις βάσεις για την εναρμόνιση των εσωτερικών ποινικών νομοθεσιών στον τομέα της εγκληματικότητας στον κυβερνοχώρο[798] με τη θέσπιση εσωτερικών δικονομικών διατάξεων για την έρευνα, τη δίωξη και την εκδίκαση των εγκλημάτων του κυβερνοχώρου καθώς και με τη θέσπιση κανόνων αναφορικά με τη διεθνή συνεργασία.

Στη Σύμβαση αυτή προβλέφθηκε ότι τα κράτη πρέπει να ποινικοποιήσουν όχι μόνο συμπεριφορές που στρέφονται κατά των συστημάτων πληροφοριών και των δεδομένων τους, δηλαδή τα λεγόμενα γνήσια πληροφορικά εγκλήματα[799], αλλά και συμπεριφορές που προσβάλλουν διάφορα άλλα έννομα αγαθά και τελούνται μέσω ηλεκτρονικού υπολογιστή (π.χ. απάτη) ή συμπεριφορές που πρέπει να αναχθούν σε εγκλήματα λόγω του περιεχομένου που διακινείται από τα συστήματα πληροφοριών (π.χ. πορνογραφία ανηλίκων). Με αυτή την έννοια, αλλά και ενόψει των αναλυτικών της προβλέψεων για παρεμβάσεις στον τομέα του δικονομικού δικαίου και της δικαστικής συνεργασίας, έχει υποστηριχθεί ότι η Σύμβαση του Συμβουλίου της Ευρώπης εμφανίζεται ως το πληρέστερο σχετικό διεθνές εργαλείο[800].

Συγκεκριμένα, η διάρθρωση του περιεχομένου της Σύμβασης πραγματοποιείται σε τρεις βασικές κατηγορίες διατάξεων: διατάξεις ουσιαστικού ποινικού δικαίου,

---

σελ. 442 επισημαίνοντας ότι θα συνδράμει και στο έργο των διωκτικών αρχών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

[796] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 491.

[797] Βλ. και το άρθρο του *Mike Keyser*, The Council of Europe Convention of Cybercrime, Journal of Transnational Law & Policy, 12 J. Transnat'l L. & Pol'y 287, Spring, 2003, lexisnexis database.

[798] Ωστόσο, η Σύμβαση δεν περιλαμβάνει ορισμό για το κυβερνοέγκλημα εν γένει (έτσι *Ιακ. Φαρσεδάκης*, Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π.).

[799] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, όπ. π., σελ. 1062.

[800] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 490.

διατάξεις ποινικού δικονομικού δικαίου και διατάξεις της διεθνούς δικαστικής συνεργασίας.

Οι διατάξεις του ουσιαστικού ποινικού δικαίου, οι οποίες αφορούν την παρούσα μελέτη, διακρίνονται σε:

(α) διατάξεις που αναφέρονται σε εγκλήματα κατά της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και διαθεσιμότητας (availability) των δεδομένων και συστημάτων[801] [802]*,*

(β) διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές (computer related offences),

(γ) διατάξεις για εγκλήματα σχετιζόμενα με το περιεχόμενο και

(δ) διατάξεις για εγκλήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων (offences related to infringement of copyright and related rights).

Αρχικά, στο πρώτο κεφάλαιο της Σύμβασης δίνονται οι ορισμοί εννοιών όπως αυτή του συστήματος υπολογιστή (computer system), των δεδομένων υπολογιστών (computer data) και του παρόχου πρόσβασης (service provider), προκειμένου να καθιερωθεί μια κοινά αποδεκτή ορολογία για ορισμένες βασικές τεχνικές και δύσκολα κατανοητές έννοιες και να διασφαλιστεί με τον τρόπο αυτό η ομοιογενής εννοιολογική προσέγγιση των όρων αυτών από τις εθνικές έννομες τάξεις.

Εν συνεχεία, στο πρώτο μέρος του δευτέρου κεφαλαίου της Σύμβασης, αναφέρονται τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο. Η Σύμβαση προβλέπει ρητά ότι κάθε μέλος που την αποδέχεται αναλαμβάνει την υποχρέωση να ποινικοποιήσει τις αναφερόμενες σε αυτή συμπεριφορές στο διαδίκτυο.

---

[801] Βλ. και *Ιωάννης Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 12/2001 (Έτος 4ο) σελ. 1295, όπου: *Εμπιστευτικότητα (confidentiality)* των στοιχείων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος. *Ακεραιότητα (integrity)* των στοιχείων είναι η ιδιότητά τους να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας. *Διαθεσιμότητα (availability)* των στοιχείων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμα σε κάθε εξουσιοδοτημένο χρήστη του συστήματος. Με αυτόν τον τρόπο προστατεύονται σφαιρικά τα ηλεκτρονικά στοιχεία.

[802] Όπως είναι προφανές, το Συμβούλιο της Ευρώπης στην εν λόγω Σύμβαση προκρίνει την ασφάλεια των πληροφοριών στο διαδίκτυο σύμφωνα με τον τεχνικό ορισμό της ασφάλειας όπως παρουσιάζεται στο παρόν πόνημα στην παράγραφο 1.3 αλλά και όπως αναπτύσσεται επίσης στις αναπτύξεις του κεφαλαίου 5 του παρόντος για το προστατευόμενο έννομο αγαθό.

Κατά το άρθρο 2 της Σύμβασης, κάθε κράτος μέλος υποχρεούται να λάβει νομοθετικά μέτρα για τη θεμελίωση της ειδικής υπόστασης του *εγκλήματος της παράνομης πρόσβασης σε σύστημα πληροφοριών (illegal access)* στις περιπτώσεις της εκ προθέσεως και χωρίς δικαίωμα πρόσβασης στο σύνολο ή σε τμήμα συστήματος πληροφοριών. Προβλέπεται η δυνατότητα των κρατών μελών να περιορίσουν το αξιόποινο, ορίζοντας ότι η χωρίς δικαίωμα πρόσβαση σε μέρος συστήματος πληροφοριών ή στο σύνολό του τιμωρείται *μόνο όταν το αδίκημα διαπράττεται κατά παράβαση μέτρου ασφαλείας ή σε σχέση με ένα πληροφορικό σύστημα που είναι συνδεδεμένο με άλλα ή όταν συντρέχουν επιπρόσθετα υποκειμενικά στοιχεία του αδίκου, όπως η τέλεση της πράξης με σκοπό απόκτησης ηλεκτρονικών δεδομένων ή με σκοπό τέλεσης άλλης παράνομης πράξης*. Με αυτόν τον τρόπο η Σύμβαση θέλησε να υπερκεράσει την κριτική ενός ευρύτατου αξιοποίνου, το οποίο σε περίπτωση που δεν αναγνωριστούν οι ως άνω εξαιρέσεις από τα κράτη μέλη, μπορεί να καταλαμβάνει ακόμη και συμπεριφορές από τις οποίες δεν δημιουργείται κανένας κίνδυνος με την παράνομη πρόσβαση σε σύστημα πληροφοριών[803].

Ουσιαστικός σκοπός αυτής της διάταξης είναι να ποινικοποιήσει το hacking στη βασικότερη εκδοχή του, δηλαδή τη διείσδυση και την απόκτηση χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα. Η δικαιολογητική βάση της ποινικοποίησης της παράνομης πρόσβασης συνίσταται στο γεγονός ότι κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος τα άτομα τα οποία μπορούν να έχουν πρόσβαση ή εξουσία χρήσης του συστήματος πληροφοριών. Στις περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνονται διατάξεις σχετικές με την παράνομη πρόσβαση σε σύστημα πληροφοριών. Στην ελληνική έννομη τάξη, όπως αναλύθηκε ήδη, το εν λόγω έγκλημα τυποποιείται στη διάταξη του ά. 370Γ παρ. 2 ΠΚ και σε ειδικότερες διατάξεις.

Σύμφωνα με το άρθρο 3 της Σύμβασης τα κράτη μέλη καλούνται να ποινικοποιήσουν την *υποκλοπή δεδομένων ηλεκτρονικών υπολογιστών (illegal interception)* από, προς ή εντός ενός συστήματος υπολογιστών (συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών που μεταφέρει τέτοια στοιχεία), η οποία γίνεται με τεχνικά μέσα από μη δημόσια εκπομπή. Μια μερική σχετική προστασία

[803] *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 492.

προβλέπουν οι ποινικές διατάξεις του ά. 292Α ΠΚ και του ν. 3917/2011, όπως αναλύθηκαν ανωτέρω, χωρίς ωστόσο να καλύπτουν πλήρως την υποχρέωση του απορρέει για τη χώρα μας από το εν λόγω άρθρο της Σύμβασης (αναφέρονται σε δεδομένα που αφορούν τηλεφωνικές επικοινωνίες ή που διατηρούνται από παρόχους τηλεπικοινωνιακών υπηρεσιών).

Με βάση το άρθρο 4 της Σύμβασης κάθε κράτος μέλος δεσμεύεται να λάβει τα απαραίτητα νομοθετικά μέτρα, προκειμένου να καθιερώσει ως ποινικό αδίκημα την *επέμβαση* σε *ηλεκτρονικά δεδομένα (data interference)*, η οποία αναλύεται στην άνευ δικαιώματος καταστροφή (damaging), διαγραφή (deletion), φθορά (deterioration). μεταβολή (alteration) ή απόκρυψη (suppression) δεδομένων[804]. Ο σκοπός της διάταξης αυτής είναι να προστατεύσει τα δεδομένα και τα προγράμματα των ηλεκτρονικών υπολογιστών από κάθε εξωτερική επέμβαση (interference) στον υλικό φορέα τους. Προστατεύεται, δηλαδή, η υλική ακεραιότητα και η λειτουργία των δεδομένων και των ηλεκτρονικών προγραμμάτων. Παραπλήσιο έγκλημα με αυτό που περιγράφεται εν προκειμένω είναι αυτό της φθοράς της ξένης ιδιοκτησίας του άρθρου 381 του ελληνικού Ποινικού Κώδικα. Ωστόσο, όπως αναφέρθηκε ήδη, δεν υπάρχει στην ελληνική έννομη τάξη αντίστοιχο αδίκημα, παρά το γεγονός ότι η χώρα μας έχει υπογράψει τη σύμβαση[805].

Στη συνέχεια της Σύμβασης και συγκεκριμένα στο άρθρο 5 υπαγορεύεται η ποινικοποίηση της *επέμβασης* σε *σύστημα (system interference)*[806], η οποία τελείται με την εκ προθέσεως και άνευ δικαιώματος παρακώλυση της λειτουργίας ενός συστήματος υπολογιστών μέσω της εισαγωγής (inputting), μεταφοράς (transmitting), καταστροφής (damaging), διαγραφής (deleting), φθοράς (deterioration), μεταβολής (alteration) ή απόκρυψης (suppression) ηλεκτρονικών δεδομένων. Με τη διάταξη αυτή ποινικοποιείται το κοινώς λεγόμενο computer sabotage (δολιοφθορά ηλεκτρονικού υπολογιστή). Συμπεριφορές που μπορούν να υπαχθούν σε αυτή τη

[804] Σύμφωνα με το ά. 1 περίπτ. β΄ της Σύμβασης ως δεδομένο νοείται «*η οιανδήποτε αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή πρόσφορη προς επεξεργασία σε ηλεκτρονικό σύστημα, συμπεριλαμβανομένου και ενός κατάλληλου προγράμματος για την εκτέλεση μιας λειτουργίας*».

[805] Βλ. για το εν λόγω ζήτημα *Δημ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 422-423 και *Δημ. Κιούπη*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, Υπερ. / 2000, σελ. 960 επ.

[806] Σύστημα ηλεκτρονικού υπολογιστή σημαίνει «*κάθε συσκευή ή ομάδα συσκευών που είναι εσωτερικά συνδεδεμένες μεταξύ τους ή με άλλες συσκευές, οι οποίες επεξεργάζονται κατά τρόπο αυτόματο δεδομένα*» (άρθρο 1 περίπτ. α΄ της Σύμβασης).

νομοτυπική μορφή είναι, ενδεικτικά, το «mail bombing», δηλαδή η αποστολή τεράστιου όγκου ηλεκτρονικών μηνυμάτων με σκοπό να υπερφορτωθεί το σύστημα και να καταρρεύσει καθώς και οι επιθέσεις τύπου DDoS. Στην ελληνική ποινική νομοθεσία δεν υπάρχει ανάλογη διάταξη με αυτή του άρθρου 5 της Σύμβασης. Κατά συνέπεια, θα πρέπει, προς συμμόρφωση στη Σύμβαση, να θεσπιστεί μία νέα ποινική διάταξη, η οποία να καλύπτει τις ως άνω μορφές αξιόποινης συμπεριφοράς.

Στο άρθρο 6 της Σύμβασης κάθε κράτος μέλος αναλαμβάνει την υποχρέωση να ποινικοποιήσει την *κατάχρηση των υπηρεσιών του διαδικτύου (misuse of devices),* εννοώντας την εκ προθέσεως και χωρίς δικαίωμα παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιοδήποτε τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου και προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί με σκοπό τη διάπραξη οποιουδήποτε αδικήματος των άρθρων 2 έως 5 της Σύμβασης. Σημειώνεται ότι στην ελληνική έννομη τάξη το άρθρο αυτό αντιστοιχεί στο ά. 292Α παρ. 6, το οποίο όμως αναφέρεται, όπως ήδη είδαμε, μόνο σε περιπτώσεις λογισμικού παρόχων τηλεπικοινωνιών[807].

Επιπλέον, τα κράτη καλούνται με την υπογραφή της Σύμβασης να θεσπίσουν ειδικές ποινικές διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές (computer related offences) και συγκεκριμένα αυτά της πλαστογραφίας και της απάτης. Ιδιαίτερη μνεία γίνεται για τα εγκλήματα που σχετίζονται με το περιεχόμενο που διακινείται μέσω διαδικτύου και ειδικά σχετικά με την παιδική πορνογραφία. Παράλληλα, στη Σύμβαση συμπεριλαμβάνονται διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων (offences related to infringement of Copyright and related rights). Επίσης, περιλαμβάνονται και διατάξεις για την απόπειρα, τη συμμετοχή και την ευθύνη των νομικών προσώπων.

Στο δεύτερο *μέρος του δευτέρου κεφαλαίου* της Σύμβασης βρίσκονται οι διατάξεις του ποινικού δικονομικού δικαίου. Αναφέρονται σε θέματα ταχείας διαφύλαξης αποθηκευμένων δεδομένων σε ηλεκτρονικό υπολογιστή (expedited preservation of stored computer data), ταχείας διαφύλαξης και γνωστοποίησης διακινούμενων αρχείων (expedited preservation and disclosure of traffic data), εντολής παροχής πληροφοριών (production order) έρευνας και κατάσχεσης αποθηκευμένων σε ηλεκτρονικό υπολογιστή στοιχείων (search and seizure of stored computer data),

[807] Βλ. παράγραφο 5.2.2 του παρόντος πονήματος.

πραγματικού χρόνου συλλογής διακινούμενων δεδομένων (real-time collection of traffic data), καθώς και παγίδευσης – υποκλοπής περιεχομένου δεδομένων (intervention of content data)[808].

Τέλος, στο *τρίτο* κεφάλαιο η Σύμβαση περιλαμβάνει διατάξεις διεθνούς δικαστικής συνεργασίας που αναφέρονται στην έκδοση, σε γενικές αρχές σχετικά με την αμοιβαία συνδρομή, σε παροχή αυτοματοποιημένων πληροφοριών, στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε υπολογιστή και στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων.

Αξίζει να σημειωθεί ότι στις 28 Ιανουαρίου 2003 υπεγράφη στο Στρασβούργο Πρόσθετο Πρωτόκολλο, ως συμπληρωματικό της Σύμβασης, στο οποίο ποινικοποιούνται πράξεις ρατσισμού και ξενοφοβίας που διαπράττονται μέσω του διαδικτύου.

6.3 Ευρωπαϊκό ενωσιακό θεσμικό πλαίσιο[809] και ψηφίσματα για το hacking και τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα

Η Ευρωπαϊκή Ένωση έχει δείξει ιδιαίτερο ενδιαφέρον σε ό,τι αφορά τα συστήματα πληροφοριών και τους χρήστες τους. Νομικά κείμενα που παρήχθησαν έχουν επηρεάσει την νομική σκέψη αναφορικά με το κυβερνοέγκλημα όχι μόνο σε ενωσιακό αλλά και σε διεθνές επίπεδο. Χαρακτηριστικό παράδειγμα αποτελεί η απόφαση-πλαίσιο της 28.05.2001 για την καταπολέμηση της απάτης και της πλαστογραφίας όσον αφορά τα μέσα πληρωμών[810], η οποία είχε υπογραφεί και

[808] Βλ. *Ιωάννης Εμμ. Αγγελής*, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, όπ. π., σελ. 1219.

[809] Για την εναρμόνιση του ουσιαστικού ποινικού δικαίου στην Ευρωπαϊκή ένωση και την εξέλιξή της μέσα στον χρόνο από την περίοδο πριν τη Συνθήκη του Μάαστριχτ μέχρι τη Συνθήκη της Λισαβόνας πρβλ. *Σπ. Καρανικόλα*, Η επίδραση του ευρωπαϊκού ποινικού δικαίου στην ελληνική ποινική έννομη τάξη, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2012, σελ. 128 επ.

[810] Όλο το κείμενο διαθέσιμο στο url: http://europa.eu/legislation_summaries/fight_against_fraud/fight_against_counterfeiting/l24212_el.htm .

κυρωθεί και από μη κράτη μέλη, όπως οι ΗΠΑ, ο Καναδάς και η Ιαπωνία[811]. Παρακάτω εκτίθενται το σύνολο των νομικών πρωτοβουλιών, ανακοινώσεων και θέσεων της ΕΕ με χρονολογική σειρά, προκειμένου να δοθεί η δυνατότητα στον αναγνώστη να καταγράψει, πέρα από τη δραστηριότητα της ΕΕ σε επίπεδο πραστασίας των συστημάτων πληροφοριών, και η εξέλιξη της νομικής σκέψης και των εννοιών που διαλαμβάνονται στα σχετικά κείμενα και έχουν επηρεάσει τα σύγχρονα νομοθετικά κείμενα.

6.3.1 Η Απόφαση του Συμβουλίου της 31.03.1992 στον Τομέα της Ασφάλειας Συστημάτων Πληροφοριών

Η Ευρωπαϊκή Ένωση δεν έχει μείνει αδιάφορη απέναντι στην ηλεκτρονική εγκληματικότητα. Ήδη στις 31 Μαρτίου 1992 το Συμβούλιο των Ευρωπαϊκών Κοινοτήτων εξέδωσε την Απόφαση 92/242/ΕΟΚ στον τομέα της ασφάλειας των συστημάτων πληροφοριών[812]. Στόχος του σχεδίου δράσης της εν λόγω Απόφασης υπήρξε η ανάπτυξη συνολικών στρατηγικών για την παροχή στους χρήστες και παραγωγούς της ενδεδειγμένης προστασίας των συστημάτων πληροφοριών έναντι τυχαίων ή σκόπιμων απειλών. Παράλληλα, η ασφάλεια των συστημάτων πληροφοριών αναγνωρίστηκε από την Κοινότητα ως μια ευρέως διαδεδομένη ανάγκη στη σύγχρονη κοινωνία. Το ως άνω σχέδιο δράσης περιελάμβανε έξι βασικές κατευθύνσεις: 1. ανάπτυξη στρατηγικού πλαισίου για την ασφάλεια των συστημάτων πληροφοριών - 2. προσδιορισμό των αναγκών των χρηστών και των παρεχόντων υπηρεσίες σε θέματα ασφάλειας των συστημάτων πληροφοριών – 3. λύσεις για άμεσες και προσωρινές ανάγκες των χρηστών, των προμηθευτών και των παρεχόντων υπηρεσίες – 4. κατάρτιση προδιαγραφών, προτύπων, αξιολόγηση και πιστοποίηση σε θέματα ασφάλειας των συστημάτων πληροφοριών – 5. τεχνολογικές εξελίξεις σε θέματα ασφάλειας των συστημάτων πληροφοριών – 6. κατοχύρωση της ασφάλειας των συστημάτων πληροφοριών. Το σχέδιο δράσης εφαρμόστηκε από την Επιτροπή

[811] *Hans Graux*, "New Directive on Attacks against Information Systems", 16.10.2013, url: http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems.

[812] Δημοσιευμένη στην Επίσημη Εφημερίδα με αρ. L 123 της 08/05/1992 σελ. 0019 – 0025 και κείμενο διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:31992D0242&from=EL.

σε στενό συσχετισμό με συναφείς δράσεις στα κράτη μέλη και σε συνδυασμό με πρωτοβουλίες έρευνας και ανάπτυξης.

Με την Απόφαση αυτή ουσιαστικά εκφράστηκε η ανάγκη θέσπισης κοινοτικού πλαισίου για την ασφάλεια των συστημάτων πληροφοριών, το οποίο να συμβιβάζει τους κοινωνικούς, οικονομικούς και πολιτικούς στόχους με τις τεχνικές, λειτουργικές και νομικές επιλογές της Κοινότητας σε διεθνές πλαίσιο. Η λεπτή ισορροπία ανάμεσα στα διαφορετικά συμφέροντα, στόχους και περιορισμούς αναζητήθηκε μέσω της συνεργασίας των κρατών μελών για την επεξεργασία πλαισίου κοινής αντίληψης και στρατηγικής.

6.3.2 Η Σύσταση του Συμβουλίου της 07.04.1995 για τα κοινά κριτήρια ασφάλειας της τεχνολογίας πληροφοριών

Στις 7 Απριλίου 1995 το Συμβούλιο της Ευρωπαϊκής Ένωσης προέβη στην έκδοση της Σύστασης για κοινά κριτήρια ασφαλείας της τεχνολογίας πληροφοριών (95/144/ΕΚ)[813]. Με την εν λόγω Σύσταση εκτιμήθηκε ότι η πολυπλοκότητα της ασφαλείας των συστημάτων πληροφορικής απαιτεί την ανάπτυξη στρατηγικών που επιτρέπουν την ελεύθερη κυκλοφορία των πληροφοριών μέσα στην ενιαία αγορά και συγχρόνως διασφαλίζουν την ασφάλεια των εν λόγω συστημάτων. Η χρήση κοινών κριτηρίων ασφαλείας των συστημάτων πληροφοριών τέθηκε ως βασική προϋπόθεση για τη δημιουργία πανευρωπαϊκών ασφαλών εφαρμογών και υπηρεσιών, η οποία κρίθηκε ότι δεν δύναται να επιτευχθεί εάν στα επιμέρους κράτη μέλη και οικονομικούς κλάδους υπάρχουν διαφορετικά κριτήρια. Η Σύσταση αυτή είναι σημαντική διότι καταδεικνύει πως ήδη από το 1995 η άναρχη εξέλιξη της πληροφορικής και της τεχνολογίας θεωρήθηκε ότι έθετε σε κίνδυνο την ασφάλεια των ηλεκτρονικών πληροφοριών και μια «τεχνολογική εναρμόνιση» τέθηκε στο επίκεντρο της πολιτικής της ευρωπαϊκής κοινότητας.

[813] Δημοσιευμένη στην Επίσημη Εφημερίδα με αρ. L 093 της 26/04/1995 σελ. 0027 – 0028 και κείμενο διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:31995H0144&from=EN.

6.3.3 Το Ψήφισμα του Συμβουλίου της 17.02.1997 για το παράνομο και επιβλαβές περιεχόμενο του Διαδικτύου

Στις 17 Φεβρουαρίου 1997 το Συμβούλιο της Ευρωπαϊκής Ένωσης και οι αντιπρόσωποι των κυβερνήσεων των κρατών μελών προχώρησαν στην έκδοση του No 97/C70/01 Ψηφίσματος για το παράνομο και επιβλαβές περιεχόμενο του διαδικτύου. Κύριο χαρακτηριστικό του Ψηφίσματος αυτού είναι ότι αναγνωρίζονται τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητες στους πολίτες, μειώνοντας τα εμπόδια ως προς τη δημιουργία και τη διανομή περιεχομένου και προσφέροντας ευρεία πρόσβαση σε όλο και πλουσιότερες πηγές ψηφιακών πληροφοριών. Επίσης, αναγνωρίζεται η ανάγκη καταπολέμησης της παράνομης χρήσης των τεχνικών δυνατοτήτων του κυβερνοχώρου, ιδιαίτερα για αξιόποινες πράξεις κατά των παιδιών.

Σημαντικό χαρακτηριστικό του ψηφίσματος αυτού είναι ότι η Ευρωπαϊκή Ένωση χαρακτηρίζει τμήμα του περιεχομένου του διαδικτύου παράνομο και επιβλαβές[814]. Ωστόσο, το σχετικό Ψήφισμα δεν καθορίζει ακριβώς τί σημαίνει παράνομο και επιβλαβές περιεχόμενο[815]. Οι έννοιες αυτές αφέθηκαν προς προσδιορισμό από τον εθνικό νομοθέτη σε περίπτωση που ψηφιστεί σχετικός νόμος που θα ρυθμίζει την συμπεριφορά όσων «κινούνται» στον χώρο του διαδικτύου. Η αντιμετώπιση αυτή είναι αδιαμφισβήτητα δεκτική κριτικής. Καταρχάς, η περίπτωση του διαφορετικού ορισμού του παράνομου και επιβλαβούς περιεχομένου από τις εθνικές νομοθεσίες μπορεί να οδηγήσει σε αντινομίες και σημαντικές διαφοροποιήσεις. Επιπλέον, έχει διατυπωθεί και η άποψη ότι οι «εσωτερικές νομοθεσίες» δεν επαρκούν αυτοτελώς να αντιμετωπίσουν αποτελεσματικά τις επιβλαβείς πράξεις στον κυβερνοχώρο, λόγω της φύσεως του εγκλήματος και του ιδιαίτερου τρόπου τελέσεως τους – εξάλλου, για αυτόν τον λόγο είναι απαραίτητες οι πολυμερείς διεθνείς συμβάσεις[816].

---

[814] Βλ. *Ιωάννης Εμμ. Αγγελής*, Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime – Internet Crime), όπ. π., σελ. 680.

[815] Αναλυτικά για την έννοια και παραδείγματα παράνομου και επιβλαβούς περιεχομένου στο διαδίκτυο πρβλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 25 επ.

[816] Βλ. *Cornelius Prittwitz*, Περίγραμμα του Ποινικού Δικαίου και της αντεγκληματικής πολιτικής στην εποχή της παγκοσμιοποίησης, Υπερ/2000, σελ. 215.

6.3.4 Το Ψήφισμα του Συμβουλίου της 28.01.2002 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων

Με γνώμονα το ότι η ασφάλεια των δικτύων και των συστημάτων πληροφοριών αποτελεί συνεχώς διογκούμενο δημόσιο συμφέρον, το Συμβούλιο της Ευρωπαϊκής Ένωσης εξέδωσε στις 28.01.2002 το Ψήφισμα (2002/C 43/02) για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων[817].

Με το εν λόγω Ψήφισμα ζητήθηκε από τα κράτη μέλη να δρομολογήσουν, μέχρι τα τέλη του 2002, ενημερωτικές και εκπαιδευτικές εκστρατείες για μεγαλύτερη ευαισθητοποίηση όσον αφορά την ασφάλεια των δικτύων και των πληροφοριών, να απευθύνουν ειδικά τις δράσεις αυτές στις επιχειρήσεις, τους ιδιώτες χρήστες και τις δημόσιες διοικήσεις, να προβάλουν βέλτιστες πρακτικές – ενδεχομένως βάσει διεθνώς αναγνωρισμένων προτύπων – στη διαχείριση της ασφάλειας των πληροφοριών και να εξετάσουν την αποτελεσματικότητα των εθνικών ρυθμίσεων όσον αφορά την αντιμετώπιση έκτακτης ανάγκης στον ηλεκτρονικό τομέα.

Επίσης, μεταξύ άλλων, τονίστηκε η ανάγκη να προβληθεί από τα κράτη μέλη η χρήση κοινών κριτηρίων ως προτύπου (ISO-15408) και να διευκολυνθεί η αμοιβαία αναγνώριση των σχετικών πιστοποιητικών. Ιδιαίτερο βάρος, επιπλέον, δόθηκε στη σημασία της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και της Επιτροπής, όσον αφορά θέματα σε ασφάλειας των δικτύων και των πληροφοριών, για τη διευκόλυνση της κοινοτικής και της διεθνούς συνεργασίας.

6.3.5 Το Ψήφισμα του Συμβουλίου της 18.02.2003 για την ευρωπαϊκή αντίληψη για την ασφάλεια των δικτύων και των πληροφοριών

[817] Δημοσιευμένο στην Επίσημη Εφημερίδα με αρ. C 043 της 16/02/2002 σελ. 0002 – 0004.

Σε συνέχεια του προηγούμενου Ψηφίσματος της 28.01.2002, το Συμβούλιο της Ευρωπαϊκής Ένωσης προέβη στις 18.02.2003 στην έκδοση του Ψηφίσματος (2003/C 48/01) για την ευρωπαϊκή αντίληψη για την ασφάλεια των δικτύων και των πληροφοριών[818].

Εν προκειμένω, τα κράτη μέλη κλήθηκαν να προωθήσουν την ασφάλεια των δικτύων και των πληροφοριών ως ουσιαστικό στοιχείο της διακυβέρνησης σε δημόσιο και ιδιωτικό επίπεδο. Επιπλέον, το Συμβούλιο προέτρεψε τα κράτη μέση μέσω του παρόντος Ψηφίσματος να φροντίσουν για την κατάλληλη γενική και επαγγελματική εκπαίδευση αλλά και την ευαισθητοποίηση, ιδίως των νέων, σε θέματα ασφάλειας καθώς και να λάβουν τα απαραίτητα μέτρα για την πρόληψη και την αντιμετώπιση συμβάντων ασφαλείας. Τέτοιου είδους μέτρα είναι η συνεχής βελτίωση του εντοπισμού και της αξιολόγησης των προβλημάτων ασφάλειας και η διεξαγωγή των δεόντων ελέγχων, ο καθορισμός αποτελεσματικών τρόπων προκειμένου να καταστεί γνωστή σε όλους τους ενδιαφερομένους η ανάγκη για δράση καθώς και η ανταλλαγή πληροφοριών σε ευρωπαϊκό και εθνικό επίπεδο και, αν χρειάζεται, σε διεθνές επίπεδο.

Επίσης, το Συμβούλιο απευθύνθηκε αφενός στη βιομηχανία, καλώντας την να ενσωματώσει τη διαχείριση των κινδύνων ασφάλειας στον κύριο κορμό της διοικητικής σκέψης και του σχεδιασμού των επιχειρήσεων, αφετέρου στους χρήστες προκειμένου να αποκτήσουν οι ίδιοι συνολική άποψη για τους κινδύνους που συνδέονται με τα συστήματα πληροφοριών και να μελετήσουν τις απειλές που προέρχονται από φυσικά γεγονότα, από ανθρώπινα λάθη καθώς και από τεχνολογικές αδυναμίες και εσκεμμένες επιθέσεις. Ταυτόχρονα, βιομηχανία και χρήστες εκλήθησαν να ανοίξουν διάλογο με τις κυβερνήσεις τους, ενόψει της διάπλασης μιας κοινής ευρωπαϊκής αντίληψης για την ασφάλεια των δικτύων και των πληροφοριών.

6.3.6 Ο Κανονισμός 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών

[818] Δημοσιευμένο στην Επίσημη Εφημερίδα με αρ. C 048 της 28/02/2003 σελ. 0001 – 0002.

Το ζήτημα της ασφάλειας των δικτύων υπολογιστών θεωρήθηκε τόσο σημαντικό για την Ευρωπαϊκή Ένωση ώστε οδήγησε στην ψήφιση του Κανονισμού 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10.03.2004 για τη δημιουργία του «Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών»[819]. Ο εν λόγω Οργανισμός ("ENISA": "European Union Agency for Network and Information Security") δημιουργήθηκε προκειμένου να εξασφαλισθεί υψηλό και ουσιαστικό επίπεδο ασφάλειας δικτύων και πληροφοριών εντός της Κοινότητας και να αναπτυχθεί η αντίληψη της ασφάλειας δικτύων και πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα της Ευρωπαϊκής Ένωσης, συμβάλλοντας έτσι στην ομαλή λειτουργία της εσωτερικής αγοράς (άρθρο 1).

Στο δεύτερο άρθρο του Κανονισμού θεσπίζονται οι τέσσερις βασικοί στόχοι του παρόντος Οργανισμού:

πρώτον, η ενίσχυση της ικανότητας της Κοινότητας, των κρατών μελών και, ως εκ τούτου, της επιχειρηματικής κοινότητας, να προλαμβάνουν, να αντιμετωπίζουν και να ανταποκρίνονται στα προβλήματα ασφάλειας δικτύων και πληροφοριών·

δεύτερον, η παροχή συνδρομής και συμβουλών στην Επιτροπή και στα κράτη μέλη σχετικά με θέματα που αφορούν την ασφάλεια δικτύων και πληροφοριών, τα οποία εμπίπτουν στις αρμοδιότητές του·

τρίτον η ανάπτυξη υψηλού επιπέδου ειδικών γνώσεων για την προώθηση ευρείας συνεργασίας μεταξύ παραγόντων του δημόσιου και του ιδιωτικού τομέα και,

τέταρτον, η συνδρομή στην Επιτροπή, όταν αυτή του ζητείται, σχετικά με τις τεχνικές προπαρασκευαστικές εργασίες ενημέρωσης και ανάπτυξης της κοινοτικής νομοθεσίας στον τομέα της ασφάλειας δικτύων και πληροφοριών (άρθρο 2)[820].

Πρόκειται, δηλαδή, για ένα σημαντικό ευρωπαϊκό γνωμοδοτικό όργανο σε θέματα δικτύων πληροφορικής[821]. Αξίζει δε να σημειωθεί ότι στο ά. 4 του Κανονισμού

[819] Δημοσιευμένος στην Επίσημη Εφημερίδα L 77 της 13.03.2004, σελ. 1 και τροποποιηθείς από τον Κανονισμό (ΕΚ) 1007/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Σεπτεμβρίου 2008, δημοσιευμένος στην Επίσημη Εφημερίδα L 293 1 31.10.2008 σελ. 1.

[820] Βλ. url: http://www.enisa.europa.eu.

[821] Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών – "European Union Agency for Network and Information Security" (ENISA) εδρεύει από 01/09/2004 στο Ηράκλειο της Κρήτης στην Ελλάδα.

δίνονται αξιόλογοι ορισμοί εννοιών σχετικών με την ασφάλεια δικτύων και πληροφοριών[822].

6.3.7 Η Απόφαση Πλαίσιο της 24.02.2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών

[822] «Άρθρο 4: Ορισμοί. Για τους σκοπούς του παρόντος κανονισμού, νοούνται ως:

α) **«δίκτυο»**: τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών·

β) **«σύστημα πληροφοριών»**: οι ηλεκτρονικοί υπολογιστές και τα δίκτυα ηλεκτρονικών επικοινωνιών, καθώς επίσης και τα ηλεκτρονικά δεδομένα τα οποία έχουν αποθηκευθεί, έχουν αποτελέσει αντικείμενο επεξεργασίας, έχουν ανακτηθεί ή έχουν μεταδοθεί μέσω των εν λόγω δικτύων με σκοπό τη λειτουργία τους, τη χρήση, την προστασία και τη συντήρησή τους·

γ) **«ασφάλεια δικτύων και πληροφοριών»:** η δυνατότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε συγκεκριμένο επίπεδο εμπιστοσύνης, σε ατυχήματα ή σε παράνομες ή κακόβουλες δράσεις, οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και την εμπιστευτικότητα όσον αφορά τα δεδομένα που έχουν αποθηκευθεί ή μεταδίδονται καθώς και οι σχετικές υπηρεσίες που προσφέρονται από τα εν λόγω δίκτυα ή συστήματα ή είναι προσβάσιμες μέσω αυτών·

δ) **«διαθεσιμότητα»**: το γεγονός ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργικές·

ε) «**αυθεντικοποίηση»**: η επιβεβαίωση της δηλούμενης ταυτότητας οντοτήτων ή χρηστών·

στ) «**ακεραιότητα δεδομένων**»: η επιβεβαίωση ότι τα δεδομένα τα οποία έχουν σταλεί, έχουν παραληφθεί ή έχουν αποθηκευθεί είναι πλήρη και αμετάβλητα·

ζ) **«εμπιστευτικότητα δεδομένων»**: η προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα πρόσωπα·

η) **«κίνδυνος»**: η εκδήλωση της πιθανότητας τα τρωτά σημεία του συστήματος να επηρεάσουν την αυθεντικοποίηση, τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων τα οποία αποτελούν αντικείμενο επεξεργασίας ή μεταδίδονται, καθώς και η σοβαρότητα των εν λόγω επιπτώσεων, ως συνέπεια της σκόπιμης ή μη αξιοποίησης των συγκεκριμένων τρωτών σημείων·

θ) «**εκτίμηση κινδύνου**»: η επιστημονική διαδικασία η οποία βασίζεται στην τεχνολογία και συνίσταται σε τέσσερις φάσεις: στον εντοπισμό της απειλής, στο χαρακτηρισμό της απειλής, στην αξιολόγηση της έκθεσης στην απειλή και στο χαρακτηρισμό του κινδύνου·

ι) **«διαχείριση κινδύνου»**: η διαδικασία, διακριτή από την εκτίμηση κινδύνου, κατά την οποία σταθμίζονται οι εναλλακτικές πολιτικές έπειτα από διαβούλευση με τα ενδιαφερόμενα μέρη, λαμβάνεται υπόψη η εκτίμηση του κινδύνου και άλλων εύλογων παραγόντων και, εφόσον χρειασθεί, επιλέγονται οι κατάλληλες λύσεις πρόληψης και ελέγχου·

ια) «**αντίληψη για την ασφάλεια δικτύων και πληροφοριών**»: η ίδια έννοια με εκείνη που ορίζεται στις κατευθυντήριες γραμμές του ΟΟΣΑ, της 25ης Ιουλίου 2002, για την ασφάλεια δικτύων και πληροφοριών, και στο ψήφισμα του Συμβουλίου, της 18ης Φεβρουαρίου 2003, για την ευρωπαϊκή αντίληψη για την ασφάλεια δικτύων και πληροφοριών».

Στο Ευρωπαϊκό Συμβούλιο στο Τάμπερε τον Οκτώβριο του 1999 αναγνωρίστηκε η αναγκαιότητα μιας προσέγγισης των εθνικών νομοθεσιών σχετικά με τα αδικήματα και τις ποινές στον τομέα της εγκληματικότητας στον κυβερνοχώρο, η οποία επιβεβαιώθηκε στην ανακοίνωση με τίτλο «Δημιουργία μιας ασφαλέστερης κοινωνίας της πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής»[823]. Η Ευρωπαϊκή Ένωση, ενόψει της διαφοράς των ποινικών συστημάτων των κρατών μελών, επεδίωξε, δηλαδή, την εξεύρεση ελάχιστων σημείων συμφωνίας μεταξύ τους, τα οποία στη συνέχεια μετέτρεψε σε ελάχιστα σημεία υποχρεώσεων των κρατών για εναρμόνιση στις εθνικές τους έννομες τάξεις και έτσι προέκυψε μία δυναμική επανακαθορισμού των εθνικών ποινικών συστημάτων[824].

Προς αυτήν την κατεύθυνση εκδόθηκε η Απόφαση Πλαίσιο 2005/222/ΔΕΥ της 24.02.2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών[825] [826], η οποία ενετάσσετο στο ευρύτερο πλαίσιο και του σχεδίου δράσης eEurope για την κοινωνία της πληροφορίας και στόχευσε στην υλοποίηση μιας ασφαλέστερης κοινωνίας της πληροφορίας και ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, σύμφωνα και με τον βασικό στόχο της Πρότασης Απόφασης Πλαίσιο της 27.08.2002 για τις επιθέσεις κατά των συστημάτων πληροφοριών, όπως αυτή τροποποιήθηκε από το Ευρωπαϊκό Κοινοβούλιο την 4.11.2002[827], δυνάμει της οποίας η πρώτη εκδόθηκε[828]. Αυτή η Απόφαση Πλαίσιο έχει, επίσης, ως στόχο τη συμπλήρωση και ανάπτυξη των δραστηριοτήτων που πραγματοποιούνται σε διεθνές επίπεδο, όπως οι εργασίες της

---

[823] Το κείμενο της ανακοίνωσης διαθέσιμο στο url: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm.

[824] Βλ. *Μαρία Καϊάφα-Γκμπάντι*, Προς μία νέα οριοθέτηση του αξιοποίνου του οργανωμένου εγκλήματος στην Ε.Ε. –Η σημασία της για την εθνική μας έννομη τάξη, ΠοινΔικ 12/2005 (Έτος 8ο), σελ. 1436.

[825] Δημοσιευμένη στην Επίσημη Εφημερίδα L 069 της 16/03/2005 σελ. 0067 – 0071.

[826] Το κείμενο της Απόφασης Πλαίσιο διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:32005F0222.

[827] COM/2002/0173 τελικό - CNS 2002/0086, δημοσιευμένη στην Επίσημη Εφημερίδα με αρ. 203 Ε της 27/08/2002, σελ. 0109 – 0113 και στα Επίκαιρα Νομοθετήματα, ΠοινΔικ 2/2003 (Έτος 6ο) σελ. 115.

[828] Υποστηρίχθηκε τότε η άποψη ότι η εν λόγω πρόταση υιοθετούσε ευρεία ποινικοποίηση συμπεριφορών η οποία κατευθυνόταν στον υπερακοντισμό ακόμη και της Σύμβασης του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα (cybercrime), ενόψει του μεγέθους του κινδύνου από τις επιθέσεις σε συστήματα πληροφοριών των δικτύων επικοινωνιών αλλά και του ηλεκτρονικού εμπορίου (παράγραφος 1.1 της Αιτιολογικής Έκθεσης της Πρότασης) [Βλ. σχετικά *Γεώργιος Νούσκαλης*, Απάτη με Ηλεκτρονικό Υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και της Ευρωπαϊκής Ένωσης, ΠοινΔικ 2/2003 (Έτος 6ο) σελ. 190].

G8 και η Σύμβαση του Συμβουλίου της Ευρώπης σχετικά με την εγκληματικότητα στον κυβερνοχώρο[829].

Ήδη από την Πρόταση της εν λόγω Απόφασης Πλαίσιο κατέστη σαφής η προσέγγιση περί σύγκλισης των εγκλημάτων που τελούνται με ηλεκτρονικό υπολογιστή και των εγκλημάτων που τελούνται στον κυβερνοχώρο σε μία ενιαία κατηγορία των εγκλημάτων που στρέφονται εναντίον συστημάτων πληροφοριών. Συγκεκριμένα, κατά τους ορισμούς στο άρθρο 2 της Πρότασης[830] στο «σύστημα πληροφοριών» εντάσσονται το λογισμικό και το «υλικό του συστήματος» (hardware) οποιουδήποτε δικτύου επικοινωνίας, είτε αυτόνομου είτε διασυνδεδεμένου, ξεπερνώντας τους ορισμούς που περιέχονται στις διεθνείς συμβάσεις του ΟΟΣΑ το 1992, τους οποίους όμως η πρόταση χρησιμοποιεί ως σημείο εκκίνησης. Στον ανωτέρω ορισμό δεν συμπεριλαμβάνεται, πάντως, το περιεχόμενο της πληροφορίας, την οποία διακινούν τα συστήματα. Η διευκρίνιση αυτή είναι αναγκαία, ενόψει του ότι τα εγκλήματα που αφορούν το περιεχόμενο της πληροφορίας θεωρούνται ότι δεν συνιστούν επιθέσεις εναντίον των «συστημάτων πληροφοριών», αλλά πράξεις που εντάσσονται στις

---

[829] Βλ. *Στέφανος Παύλου,* Αποφάσεις - Πλαίσια/Διεθνή και Ευρωπαϊκά Κείμενα Ποινικού Δικαίου, Τεύχος ΙΙ, εκδ. Δίκαιο και Οικονομία, Π. Ν. Σάκκουλας Αθήνα 2005, σελ. 41-24.

[830] «Άρθρο 2 – **Ορισμοί**. Για τους σκοπούς της παρούσας απόφασης πλαισίου, νοείται ως:

(α) "**Δίκτυο ηλεκτρονικών επικοινωνιών**": τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής και δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων με χρήση καλωδίου, ραδιοκυμάτων, οπτικών ή άλλων ηλεκτρομαγνητικών μέσων, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (κυκλωμάτων μεταγωγής δεδομένων και πακετομεταγωγής) και κινητών επίγειων δικτύων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές καθώς και των δικτύων καλωδιακής τηλεόρασης ανεξάρτητα από το είδος των μεταδιδόμενων πληροφοριών.

(β) **"Ηλεκτρονικός υπολογιστής":** οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, την αυτόματη επεξεργασία ηλεκτρονικών δεδομένων.

(γ) **"Ηλεκτρονικά δεδομένα**": οποιαδήποτε παρουσίαση γεγονότων, πληροφοριών ή εννοιών δημιουργείται ή λαμβάνει μορφή που επιτρέπει την επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία.

(δ) "**Σύστημα πληροφοριών**": οι ηλεκτρονικοί υπολογιστές και τα ηλεκτρονικά δίκτυα επικοινωνιών, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τους υπολογιστές με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους.

(ε) **"Νομικό πρόσωπο**": κάθε οντότητα στην οποία το ισχύον δίκαιο αναγνωρίζει αυτό το καθεστώς, εξαιρουμένων των κρατών ή άλλων δημόσιων οργάνων κατά την άσκηση κριτικής εξουσίας και των δημόσιων διεθνών οργανισμών.

(στ) "**Εξουσιοδοτημένο άτομο**": οποιοδήποτε φυσικό ή νομικό πρόσωπο που έχει το δικαίωμα, δυνάμει σύμβασης ή νόμου, ή τη νόμιμη εξουσιοδότηση, να χρησιμοποιεί, να διαχειρίζεται, να ελέγχει, να δοκιμάζει, να πραγματοποιεί νόμιμες επιστημονικές έρευνες ή να λειτουργεί σύστημα πληροφοριών και το οποίο δρα σύμφωνα με αυτό το δικαίωμα ή την εξουσιοδότηση.

(ζ) "**Χωρίς δικαίωμα**": αποκλείει τις πράξεις των εξουσιοδοτημένων ατόμων ή άλλες πράξεις των οποίων ο νόμιμος χαρακτήρας αναγνωρίζεται από το εθνικό δίκαιο.»

αντικειμενικές υποστάσεις παραδοσιακών εγκλημάτων. Για τις πράξεις αυτές, η Πρόταση θεωρεί ότι είναι επαρκής η νομοθεσία των κρατών μερών, όπως π.χ. για την πνευματική ιδιοκτησία[831], το απόρρητο των επικοινωνιών, τα προσωπικά δεδομένα (παράγραφος 1.4 της Αιτιολογικής Έκθεσης). Θα μπορούσε να ισχυριστεί κανείς ότι η εν λόγω Πρόταση ενοποιεί σε μία κατηγορία τις πράξεις που ενέταξε σε δύο κατηγορίες η Σύμβαση του Συμβουλίου της Ευρώπης, δηλαδή των προσβολών κατά των συστημάτων ηλεκτρονικών υπολογιστών και εκείνων που σχετίζονται με ηλεκτρονικούς υπολογιστές, με σκοπό να τις διακρίνει από εκείνες που αφορούν σε προσβολή παραδοσιακών εννόμων αγαθών με τη χρήση του ηλεκτρονικού υπολογιστή και του internet[832].

Στόχος της παρούσας, δηλαδή, Απόφασης Πλαίσιο υπήρξε η καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο και η προώθηση της ασφάλειας της πληροφορίας. Απέναντι σε αυτή τη νέα μορφή διεθνικής εγκληματικότητας, πρωταρχικός σκοπός της Απόφασης Πλαίσιο υπήρξε η ενίσχυση της συνεργασίας μεταξύ των δικαστικών αρχών και των λοιπών αρμόδιων αρχών, χάρη σε μια προσέγγιση των ποινικών κανόνων τους όσον αφορά στην παράνομη πρόσβαση σε συστήματα πληροφοριών (ά. 2)[833], στην προσβολή κατά της ακεραιότητας ενός συστήματος (ά. 3)[834] και στην προσβολή κατά της ακεραιότητας των δεδομένων (ά. 4)[835]. Η προτροπή, η υποβοήθηση, η συνενοχή ή η απόπειρα διάπραξης μιας ή

---

[831] Αναφορικά με την πνευματική ιδιοκτησία στο διαδίκτυο πρβλ. ενδεικτικά *Έλσας Δεληγιάννη*, Πνευματική ιδιοκτησία και επικοινωνία την εποχή του διαδικτύου: νομικό πλαίσιο και προοπτικές για την διαδικτυακή ανταλλαγή μουσικών αρχείων, ΔιΜΕΕ 4/2007, σελ. 480 επ.

[832] Βλ. *Γεώργιος Νούσκαλης*, Απάτη με Ηλεκτρονικό Υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και της Ευρωπαϊκής Ένωσης, όπ. π., σελ. 190.

[833] «Άρθρο 2: ***Παράνομη πρόσβαση σε σύστημα πληροφοριών***

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως πρόσβαση, χωρίς δικαίωμα, στο σύνολο ή σε μέρος συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

2. Κάθε κράτος μέλος μπορεί να αποφασίσει ότι η αναφερόμενη στην παράγραφο 1 πράξη ποινικοποιείται μόνον όταν το αδίκημα διαπράττεται κατά παράβαση μέτρου ασφαλείας.»

[834] «Άρθρο 3: ***Παράνομη παρεμβολή σε σύστημα***

Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή, μετάδοση, ζημία, διαγραφή, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

[835] «Άρθρο 4: ***Παράνομη παρεμβολή σε δεδομένα***

Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως διαγραφή, ζημία, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό

περισσοτέρων μεταξύ των προαναφερομένων πράξεων καταγράφονται, επίσης, ως κολάσιμες (ά. 5). Επίσης, ορίζεται ότι τα κράτη μέλη θα πρέπει να προβλέψουν τη δυνατότητα τιμώρησης των προαναφερομένων πράξεων με ποινικές κυρώσεις αποτελεσματικές, ανάλογες και αποτρεπτικές (άρθρ 6). Θα θεωρείται, δε, επιβαρυντική περίσταση η διάπραξη της αξιόποινης πράξης στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της κοινής δράσης 98/733/ΔΕΥ καθώς επίσης και η πρόκληση σοβαρής ζημίας και προσβολής ουσιαστικών συμφερόντων (ά. 7).

Επιπλέον, η Απόφαση Πλαίσιο προτείνει κριτήρια για τον καθορισμό της ευθύνης του νομικού προσώπου και τις ενδεχόμενες κυρώσεις που θα μπορούν να επιβάλλονται σε περίπτωση που δηλώνεται η ευθύνη αυτού του νομικού προσώπου, όπως παραδείγματος χάριν προσωρινή ή οριστική απαγόρευση άσκησης εμπορικής δραστηριότητας, δικαστική εντολή διάλυσης, απώλεια των δημοσίων ωφελημάτων κ.λπ. (ά. 8 και 9). Αντίστοιχα, τα ζητήματα δικαιοδοσίας και ανταλλαγής πληροφοριών ρυθμίζονται στα άρθρα 10 και 11 αντίστοιχα.

Αναλυτικότερα, η ως άνω Απόφαση Πλαίσιο προβλέπει στο δεύτερο άρθρο της ότι ως ποινικό αδίκημα τιμωρείται η εκ προθέσεως και χωρίς δικαίωμα πρόσβαση σε σύστημα πληροφοριών, τουλάχιστον όταν δεν πρόκειται για περιπτώσεις ήσσονος σημασίας. Ταυτόχρονα δίνει τη δυνατότητα στα κράτη μέλη να προβλέψουν την πράξη αυτή ως αξιόποινη μόνο στην περίπτωση παράβασης μέτρου ασφαλείας. Παρατηρείται ότι η νομοθετική πρόβλεψη εξαίρεσης των περιπτώσεων ήσσονος σημασίας επήλθε σταδιακά μέσα από τα ευρωπαϊκά και διεθνή κείμενα. Συγκεκριμένα, στη Σύμβαση της Βουδαπέστης δεν προβλεπόταν τίποτα σχετικό ενώ στην Πρόταση Απόφασης Πλαίσιο του 2002 η εν λόγω εξαίρεση προβλέφθηκε ως ιδιαίτερη περίσταση που επισύρει ηπιότερη ποινή, η κρίση περί της οποίας επαφίεται στην αρμόδια δικαστική αρχή. Στην παρούσα Απόφαση Πλαίσιο, όμως, οι περιπτώσεις ήσσονος σημασίας εξαιρούνται από την ίδια την ίδια την αντικειμενική υπόσταση του εγκλήματος της παράνομης πρόσβασης σε συστήματα πληροφοριών. Είναι συνεπώς εμφανής η πρόθεση του Συμβουλίου της Ευρωπαϊκής Ένωσης να αποφύγει την υπερβολική ποινικοποίηση του σχετικού εγκλήματος ή με άλλα λόγια

αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

να αποποινικοποιήσει την περίπτωση της απλής πρόσβασης στα συστήματα πληροφοριών. Ωστόσο, το δύσκολο ζήτημα του προσδιορισμού των ορίων της απλής πρόσβασης και του καθορισμού, δηλαδή, των περιπτώσεων ήσσονος σημασίας, επαφίεται στην κρίση του εθνικού νομοθέτη.

Επιτυχείς κρίνονται και οι ορισμοί των εννοιών του συστήματος πληροφοριών, των ηλεκτρονικών δεδομένων και του «χωρίς δικαίωμα», όπως αυτοί αποτυπώνονται στο ά. 1 της Απόφασης Πλαίσιο[836]. Όσον αφορά στα προστατευόμενα στοιχεία, ο ορισμός εν προκειμένω είναι ευρύτερος αφού δεν χρησιμοποιείται πλέον η λέξη «ηλεκτρονικός υπολογιστής» αλλά «σύστημα πληροφοριών», έννοια η οποία μάλιστα ορίζεται με αρκετή ευρύτητα σε σχέση με άλλες διεθνείς συμβάσεις. Στην έννοια του συστήματος περιλαμβάνεται το λογισμικό και τα ηλεκτρονικά υλικά μέρη του συστήματος (hardware) οποιασδήποτε ηλεκτρονικής συσκευής ή δικτύου επικοινωνίας. Με αυτόν τον τρόπο υπάγονται στην προστασία των διατάξεων όχι μόνο οι ηλεκτρονικοί υπολογιστές αλλά κάθε συσκευή ή σύστημα με αντίστοιχες λειτουργίες με αυτές του ηλεκτρονικού υπολογιστή και με δυνατότητα επεξεργασίας δεδομένων (π.χ. σύγχρονα κινητά τηλέφωνα – "smart phones" – με δυνατότητα σύνδεσης στο διαδίκτυο).

Αλλά και η έννοια «δεδομένα» ορίζεται με αρκετά ευρύ τρόπο ώστε να περιλαμβάνονται και τα προγράμματα ηλεκτρονικού υπολογιστή (λογισμικό – software) τα οποία επιτρέπουν στον τελευταίο να λειτουργεί. Επίσης, ο ορισμός της έννοιας της χωρίς δικαίωμα πρόσβασης ή παρεμβολής είναι αρκετά επιτυχημένος, καθώς η εξουσιοδότηση δεν αναφέρεται μόνο σε νομοθετικές διατάξεις ή στην εξουσιοδότηση του κυρίου αλλά και στην εξουσιοδότηση οποιουδήποτε δικαιούχου

---

[836] «Άρθρο 1: *Ορισμοί. Για τους σκοπούς της παρούσας απόφασης-πλαίσιο, νοείται ως:*

*α) **"Σύστημα πληροφοριών"**: οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τους υπολογιστές με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους.*

*β) **"Ηλεκτρονικά δεδομένα"**: οποιαδήποτε παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου ενός προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία.*

*γ) **"Νομικό πρόσωπο"**: κάθε οντότητα που έχει αυτό το καθεστώς βάσει του ισχύοντος δικαίου, εκτός των κρατών ή άλλων δημόσιων οργάνων κατά την άσκηση κρατικής εξουσίας και των δημόσιων διεθνών οργανισμών.*

*δ) **"Χωρίς δικαίωμα"**: πρόσβαση ή παρεμβολή μη εξουσιοδοτημένη από τον ιδιοκτήτη ή άλλο δικαιούχο του συστήματος ή μέρους του, ή μη επιτρεπόμενη δυνάμει της εθνικής νομοθεσίας.*»

του συστήματος ή μέρους του. Ωστόσο, ορθότερη μάλλον θα ήταν η αναφορά στον δικαιούχο των δεδομένων και όχι στον δικαιούχο του συστήματος.

Τέλος, αξιοσημείωτη είναι η σχετική Έκθεση της Επιτροπής COM(2008)448 της 14.07.2008 στο Συμβούλιο βάσει του άρθρου 12 της Απόφασης Πλαίσιο και σχετικά με αυτήν. Στην Έκθεση αυτή η Επιτροπή διαπιστώνει ότι η Απόφαση Πλαίσιο βρίσκεται ακόμη στο στάδιο μεταφοράς στα κράτη μέλη και παρατηρείται ήδη αξιοσημείωτη πρόοδος στα είκοσι κράτη μέλη που αξιολογήθηκαν. Παρά τη μεγάλη ποικιλομορφία των λεπτομερειών εφαρμογής, ο βαθμός εφαρμογής είναι σχετικά ικανοποιητικός. Ταυτόχρονα η Επιτροπή κάλεσε τα επτά κράτη μέλη (Μάλτα, Πολωνία, Σλοβακία, Ισπανία, Ιρλανδία, Ελλάδα και Ηνωμένο Βασίλειο) που δεν είχαν ακόμη κοινοποιήσει, στις αρχές Ιουλίου 2008, τα μέτρα μεταφοράς της Απόφασης Πλαίσιο στο εθνικό τους δίκαιο, να επιληφθούν αυτού του ζητήματος το συντομότερο δυνατόν.

Επίσης, απέναντι στην ανάπτυξη της εγκληματικότητας στον κυβερνοχώρο, η Επιτροπή τονίζει στην ως άνω Έκθεση ότι σκοπεύει να λάβει νέα μέτρα μετά την υιοθέτηση της Απόφασης Πλαίσιο για την καταπολέμηση της χρήσης «botnets» με εγκληματικούς σκοπούς. Συγκεκριμένα, οι επιθέσεις μέσω δικτύων προγραμμάτων ρομπότ BOTNETS αναγνωρίζονται ως ιδιαιτέρως σοβαρή απειλή κατά των συστημάτων πληροφοριών. Τονίστηκε, επομένως, η ανάγκη για αντιμετώπιση των εν λόγω επιθέσεων και επισημάνθηκε ότι η Επιτροπή πρέπει να μελετήσει μέτρα που αποβλέπουν στην εξεύρεση καλύτερων απαντήσεων στις απειλές που προκαλούνται από τα δίκτυα προγραμμάτων ρομπότ και να προωθήσει τη χρήση των ίδιων σημείων επαφής με αυτά που χρησιμοποιούνται από το Συμβούλιο της Ευρώπης και την G8 για την άμεση αντιμετώπιση των απειλών που συνδέονται με τεχνολογίες αιχμής.

6.3.8 Η Ανακοίνωση της Επιτροπής της 15.11.2006 σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού

Η Επιτροπή με την Ανακοίνωση της 15.11.2006 COM(2006)688[837] πραγματεύτηκε την αντιμετώπιση των ανεπίκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα (spam) καθώς και απειλών όπως το κατασκοπευτικό και το κακόβουλο λογισμικό. Δεδομένου ότι οι εν λόγω απειλές υπονομεύουν την εμπιστοσύνη και την ασφάλεια στην κοινωνία της πληροφορίας, με συνεπαγόμενο παράλληλα σημαντικό οικονομικό αντίκτυπο, η Επιτροπή, αξιοποιώντας το ρόλο της ως μεσάζουσας, συνέβαλε στην επίτευξη μεγαλύτερης ευαισθητοποίησης σχετικά με την ανάγκη ανάληψης ευρύτερης πολιτικής δέσμευσης για την αντιμετώπιση αυτών των απειλών.

Όσον αφορά στις παγκόσμιες διαστάσεις του φαινομένου των αυτόκλητων μηνυμάτων, του κατασκοπευτικού και κακόβουλου λογισμικού, η Επιτροπή τόνισε ότι τα κράτη μέλη οφείλουν να αναγνωρίσουν ότι η αποτελεσματική διασυνοριακή συνεργασία συνιστά ουσιώδη παράγοντα στην αντιμετώπισή του. Για τον σκοπό αυτό, η Επιτροπή για τα θέματα των ανεπίκλητων μηνυμάτων, του κατασκοπευτικού και κακόβουλου λογισμικού έδειξε την πρόθεσή της για ενίσχυση του διαλόγου και της συνεργασίας με τρίτες χώρες (επιδιώκοντας σύναψη συμφωνιών) και για εξέταση της δυνατότητας υποβολής νέων νομοθετικών προτάσεων και ανάληψης δράσεων έρευνας για την περαιτέρω ενίσχυση της προστασίας της ιδιωτικής ζωής και της ασφάλειας στον τομέα των ηλεκτρονικών επικοινωνιών.

6.3.9 Η Ανακοίνωση της Επιτροπής της 22.05.2007 προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Η Ανακοίνωση της Επιτροπής της 22.05.2007 [COM(2007) 267 τελικό] σχετικά με την πολιτική για το έγκλημα στον κυβερνοχώρο[838] ουσιαστικά παγιώνει και αναπτύσσει την προηγούμενη Ανακοίνωση της Επιτροπής της 26.01.2001 "για μια ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας των

[837] Το πλήρες κείμενο της ανακοίνωσης διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52006DC0688&from=EN.

[838] Το πλήρες κείμενο διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52007DC0267&from=EL.

υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής"[839]. Η Ανακοίνωση του 2001 πρότεινε κατάλληλες ουσιαστικές και διαδικαστικές νομοθετικές διατάξεις για την αντιμετώπιση τόσο των εγχώριων όσο και των διεθνικών αξιόποινων ενεργειών ενώ είχε ως επακόλουθο πολλές σημαντικές προτάσεις, μεταξύ των οποίων, ιδίως, αυτές οι οποίες περιλάμβαναν την πρόταση που οδήγησε στην Απόφαση Πλαίσιο 2005/222/ΔΕΥ για τις επιθέσεις κατά των συστημάτων πληροφοριών.

Ο στόχος της παρούσας Ανακοίνωσης μπορεί να υποδιαιρεθεί σε τρεις κύριες λειτουργικές πτυχές, οι οποίες συνοψίζονται ως εξής:

πρώτον, στη βελτίωση και διευκόλυνση του συντονισμού και της συνεργασίας μεταξύ των μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο, άλλων αρμόδιων αρχών και άλλων εμπειρογνωμόνων στην Ευρωπαϊκή Ένωση·

δεύτερον, στη συνεργασία με τα κράτη μέλη, με τους αρμόδιους ευρωπαϊκούς και διεθνείς οργανισμούς και με άλλα ενδιαφερόμενα μέρη με σκοπό ένα συνεκτικό πλαίσιο πολιτικών της Ευρωπαϊκής Ένωσης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και

τρίτον, ευαισθητοποίηση σχετικά με το κόστος και τους κινδύνους που συνεπάγεται το έγκλημα στον κυβερνοχώρο.

Επίσης, στην Ανακοίνωση τονίζεται ότι η κατ' ουσίαν διασυνοριακή φύση του εγκλήματος στον κυβερνοχώρο εντείνει τις απειλές, οι οποίες μπορούν πλέον να αντιμετωπιστούν μόνο στο πλαίσιο μιας πρωτοβουλίας γενικής πολιτικής, που να αποσκοπεί στη βελτίωση του συντονισμού της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε ευρωπαϊκό και διεθνές επίπεδο.

Ωστόσο, λόγω των περιορισμένων εξουσιών της Επιτροπής στον τομέα του ποινικού δικαίου, η πολιτική αυτή μπορεί μόνο να αποτελέσει συμπλήρωμα των μέτρων που λαμβάνονται από τα κράτη μέλη και από άλλους φορείς. Μακροπρόθεσμα, η ως άνω γενική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο μπορεί να περιλαμβάνει βελτιωμένη επιχειρησιακή συνεργασία μεταξύ των αρχών επιβολής του νόμου, βελτιωμένη πολιτική συνεργασία και συντονισμό μεταξύ των κρατών μελών,

[839] COM(2000) 890 τελικό.

πολιτική και νομική συνεργασία με τρίτες χώρες, ευαισθητοποίηση, κατάρτιση, έρευνα, ενισχυμένο διάλογο με τις επιχειρήσεις και ενδεχομένως νομοθετικά μέτρα.

6.3.10 Το Ψήφισμα του Συμβουλίου της 18.12.2009 για μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών

Η «Ευρωπαϊκή Συνεργατική Προσέγγιση για την Ασφάλεια των Δικτύων και των Πληροφοριών» εγκρίθηκε με το Ψήφισμα 2009/C 321/01 του Συμβουλίου Υπουργών Τηλεπικοινωνιών της Ευρωπαϊκής Ένωσης στις 18.12.2009 στις Βρυξέλλες[840]. Συγκεκριμένα, το εν λόγω Ψήφισμα αναφέρεται στην αποστολή του Ευρωπαϊκού Οργανισμού για την Ασφάλεια των Δικτύων και των Πληροφοριών (ENISA) και ζητά από την Ευρωπαϊκή Επιτροπή να καταθέσει τις νομοθετικές της προτάσεις για το μέλλον του Οργανισμού, αναγνωρίζοντας το ρόλο, τις δυνατότητες και τις εργασίες του στον τομέα της ασφάλειας δικτύων και πληροφοριών, καθώς και την ανάγκη για περαιτέρω ανάπτυξη του ENISA, ώστε να καταστεί μια αποτελεσματική υπηρεσία με σαφή πλεονεκτήματα για τον τομέα της ευρωπαϊκής ασφάλειας δικτύων και πληροφοριών. Υπογραμμίζεται, επίσης, η ανάγκη να εκσυγχρονιστεί και να ενισχυθεί ο Οργανισμός προκειμένου να υποστηρίξει την Ευρωπαϊκή Επιτροπή και τα κράτη μέλη στη γεφύρωση του χάσματος μεταξύ τεχνολογίας και πολιτικής, χρησιμεύοντας ως κέντρο εμπειρογνωμοσύνης της Ευρωπαϊκής Ένωσης σε θέματα που αφορούν την Ασφάλεια Δικτύων και Πληροφοριών. Μεταξύ άλλων, το Συμβούλιο καλεί την Επιτροπή, σε συνεργασία με τον ENISA, να αρχίσει εκστρατεία ευαισθητοποίησης μεταξύ των δημόσιων και ιδιωτικών ευρωπαϊκών φορέων όσον αφορά στη σπουδαιότητα της κατάλληλης διαχείρισης του κινδύνου για την ασφάλεια δικτύων και πληροφοριών. Παράλληλα, σημειώνεται ότι οι νέοι τρόποι χρήσης, όπως τα νεφελοειδή υπολογιστικά συστήματα (cloud computing) ως υπηρεσία, τονίζουν έτι περαιτέρω τη σημασία της ασφάλειας δικτύων και πληροφοριών. Μία διευρυμένη και

[840] Το πλήρες κείμενο του ψηφίσματος διαθέσιμο στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32009G1229(01)&from=EN.

ολιστική ευρωπαϊκή στρατηγική για την ασφάλεια δικτύων και πληροφοριών[841], με σαφώς καθορισμένους ρόλους της Ευρωπαϊκής Επιτροπής, των κρατών μελών και του ENISA, είναι σύμφωνα με το ψήφισμα αυτό ζωτικής σημασίας για την αντιμετώπιση των τρεχουσών και των μελλοντικών αυτών προκλήσεων.

6.3.11 Η Ανακοίνωση της Επιτροπής της 22.11.2010 για τη «στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη»

6.3.11.1 Το περιεχόμενο της ανακοίνωσης για την πρόληψη του κυβερνοεγκλήματος

Η Ανακοίνωση αυτή της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο [COM(2010) 673 τελικό][842] στον στόχο υπ' αρ. 3 έχει προτάξει την αύξηση των επιπέδων ασφάλειας των πολιτών και των επιχειρήσεων στον κυβερνοχώρο. Όπως αρχίζει το σκεπτικό της, «*η ασφάλεια των δικτύων πληροφορικής αποτελεί ουσιαστική προϋπόθεση για την εύρυθμη λειτουργία της κοινωνίας της πληροφορίας*». Στο πλαίσιο, λοιπόν, της περαιτέρω δράσης του τμήματος δίωξης εγκλήματος υψηλής τεχνολογίας της Europol ανακοινώθηκε η δημιουργία έως το 2013 κέντρου για το έγκλημα στον κυβερνοχώρο, μέσω του οποίου τα κράτη μέλη και τα όργανα της ΕΕ θα είναι σε θέση να δημιουργούν επιχειρησιακές και αναλυτικές ικανότητες για τη διενέργεια ερευνών και για τη συνεργασία με τους διεθνείς εταίρους. Σκοπό για τη δημιουργία του κέντρου αυτού απετέλεσε η βελτίωση της αξιολόγησης και της παρακολούθησης των υφιστάμενων προληπτικών και ερευνητικών μέτρων, η υποστήριξη και ανάπτυξη προγραμμάτων κατάρτισης και ευαισθητοποίησης για τις αρχές επιβολής του νόμου και τις δικαστικές αρχές, η

[841] Πρβλ. σχετικά με το ευρωπαϊκό νομοθετικό πλαίσιο για το κυβερνοέργκλημα και την ενσωμάτωσή του το ενδιαφέρον άρθρο του *Francesco Calderoni*, The European legal framework on cybercrime: striving for an effective implementation, Crime Law Soc Change, 2010, 54, pp.: 339–357.

[842] Το πλήρες κείμενο της ανακοίνωσης διαθέσιμο στο url: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0673_/com_com(2010)0673_el.pdf.

καθιέρωση συνεργασίας με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) κ.ά.

Επιπρόσθετα, στη συγκεκριμένη ανακοίνωση τα κράτη μέλη καλούνται, σε συνεργασία με την CEPOL[843], την Eurojust και την Europol[844], να αναπτύξουν έως το 2013 τις εθνικές τους δομές για την ευαισθητοποίηση και την κατάρτιση σχετικά με το ηλεκτρονικό έγκλημα και να δημιουργήσουν κέντρα αριστείας σε εθνικό επίπεδο ή σε εταιρική σχέση με άλλα κράτη μέλη. Ειδικότερα, τα κράτη μέλη καλούνται να προβλέψουν εύκολη διαδικασία καταγγελίας εγκλημάτων στον κυβερνοχώρο και να λάβουν μέτρα για να διευκολύνουν την παροχή οδηγιών στους πολίτες σχετικά με τις απειλές στον κυβερνοχώρο και με τα μέτρα προφύλαξης που πρέπει να λαμβάνουν. Επίσης, έως το 2012 όλα τα κράτη μέλη, καθώς και τα ίδια τα θεσμικά όργανα της ΕΕ, πρέπει να διαθέτουν μια ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT – Computer Emergency Response Team)[845] – οι ομάδες αυτές πρέπει, έπειτα, να συνεργάζονται μεταξύ τους ιδίως προκειμένου να αναπτυχθεί, με την υποστήριξη της Επιτροπής και του ENISA, έως το 2012 το ευρωπαϊκό σύστημα συναγερμού και ανταλλαγής πληροφοριών (EISAS) και να δημιουργηθεί δίκτυο σημείων επαφής μεταξύ των αρμόδιων φορέων και των κρατών μελών. Τέλος, ανακοινώθηκε ότι τα κράτη μέλη μαζί με τον ENISA πρέπει να καταρτίσουν εθνικά σχέδια έκτακτης ανάγκης και να πραγματοποιούν τακτικά ασκήσεις σε εθνικό και ευρωπαϊκό επίπεδο για την αντιμετώπιση τέτοιων περιστατικών και για την αποκατάσταση σε προτέρα κατάσταση μετά από «ψηφιακές καταστροφές»[846].

6.3.11.2 Η δημιουργία του ευρωπαϊκού κέντρου για τα εγκλήματα στον κυβερνοχώρο (EC3)

[843] Ευρωπαϊκή αστυνομική ακαδημία (CEPOL – European Police Colege). Βλ. σχετικά στο url: https://www.cepol.europa.eu/el.

[844] Για τη δημιουργία των Europol και Eurojust πρβλ. *Μ. Καϊάφα – Γκμπάντι*, Συντονιστικά όργανα για την καταπολέμηση του οργανωμένου εγκλήματος στην ΕΕ: Από τον αστυνομικό (Europol) στον δικαστικό (Eurojust) συντονισμό – Η προοπτική της προστασίας των θεμελιωδών δικαιωμάτων, ΠοινΔικ 2/2003, σελ. 165 επ.

[845] Για τις ομάδες CERT βλ. και *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 296.

[846] Αναφορικά με εθνικές στρατηγικές και σχέδια δράσης αρκετών χωρών για την ενίσχυση της ασφάλειας των συστημάτων πληροφοριών βλ. url: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

Σύμφωνα με τις επιταγές της ανωτέρω ανακοίνωσης, το ευρωπαϊκό κέντρο για τα εγκλήματα στον κυβερνοχώρο (EC3) εγκαινιάστηκε στις 11 Ιανουαρίου 2013 στις εγκαταστάσεις του στα γραφεία της Ευρωπαϊκής Αστυνομικής Υπηρεσίας, στην έδρα της Europol, στη Χάγη της Ολλανδίας[847]. Σύμφωνα και με τις εξαγγελίες της Επιτροπής, το κέντρο θα εστιάσει σε παράνομες δραστηριότητες στο διαδίκτυο που αναπτύσσονται από ομάδες οργανωμένου εγκλήματος και ιδίως σε επιθέσεις σε τραπεζικές τηλεσυναλλαγές, στη σεξουαλική εκμετάλλευση παιδιών και στα εγκλήματα που θίγουν ζωτικής σημασίας πληροφορίες και υποδομές στην ΕΕ. Επίσης, σκοπός του Κέντρου είναι να διευκολύνει την έρευνα και να αναπτύξει την ενημέρωση των εφαρμοστών του νόμου, να συλλέγει και να επεξεργάζεται δεδομένα σχετικά με τα εγκλήματα στον κυβερνοχώρο και να παρέχει στις μονάδες αρχών επιβολής του νόμου στις χώρες της ΕΕ υπηρεσίες υποστήριξης (help desk) για εγκλήματα στον κυβερνοχώρο.

6.3.12 Ο Κανονισμός υπ' αρ. 526/2013[848] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21.05.2013 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αρ. 460/2004

Ο νέος αυτός κανονισμός αναδιοργανώνει και εξελίσσει τη λειτουργία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[849], καταργώντας σχετικές διατάξεις του μέχρι τότε ισχύοντος Κανονισμού για τη λειτουργία του ENISA. Σύμφωνα και με δηλώσεις του εκτελεστικού διευθυντή του ENISA Καθηγητή Udo Helmbrecht[850], αναγνωρίζει και διαφυλάσσει τα μέχρι

[847] Βλ. σχετικό δελτίο τύπου Ευρωπαϊκής Επιτροπής στο url: http://europa.eu/rapid/press-release_IP-13-13_el.htm.

[848] Το πλήρες κείμενο του κανονισμού στο url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32013R0526&qid=1403976176105&from=EN.

[849] Για τον ENISA βλ. και *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 297.

[850] … όπως διαλαμβάνονται στο από 18.06.2013 δελτίο τύπου του ENISA (url: https://www.enisa.europa.eu/media/press-releases/neos-kanonismos-gia-ton-organismo-gia-ten-asphaleia-diktuon-kai-plerophorion-enisa-tes-ee-me-nea-kathekonta).

σήμερα επιτεύγματα του ENISA σε τομείς όπως οι ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT – Computer Emergency Response Team)[851] στα κράτη-μέλη και οι σημαντικού κύρους ασκήσεις ασφάλειας στον κυβερνοχώρο, όπως η Cyber Europe 2012 με 600 συμμετέχοντες από όλη την Ευρώπη[852]. Βασικά σημεία του νέου κανονισμού αποτελούν τα εξής: κατά πρώτον, ο ENISA αποκτά διασύνδεση με το ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο (EC3) της Europol και κατά δεύτερον, παγιώνεται ο συμβουλευτικός και υποστηρικτικός ρόλος του στις χώρες της ΕΕ και στα όργανα της Ένωσης.

6.3.13 Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12.08.2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου[853]

Η εν λόγω Οδηγία είναι σημαντική για τις έννομες τάξεις, όπως η ελληνική, που ανήκουν τόσο στο Συμβούλιο της Ευρώπης όσο και στην Ευρωπαϊκή Ένωση, λόγω της αυξημένης δεσμευτικότητας που αναπτύσσουν τα νομικά εργαλεία που προβλέπονται σε αυτήν και για το πεδίο του ποινικού δικαίου, ιδίως μετά τη θέση σε ισχύ της Συνθήκης της Λισσαβόνας[854] [855]. Στόχος ήδη της πρότασης της εν λόγω

[851] Για τις ομάδες CERT του ENISA βλ. url: https://www.enisa.europa.eu/activities/cert.

[852] Για την άσκηση ασφαλείας του διαδικτύου cyber Europe 2012 βλ. url: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_EL_TRA.pdf.

[853] Το κείμενο της Οδηγίας διαθέσιμο στο url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EL:PDF.

[854] Η Οδηγία εκδόθηκε βάσει του ά. 83 (1) (α) [8] της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), το οποίο αναφέρει ότι το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο μπορούν να θεσπίζουν ελάχιστους κανόνες για τον ορισμό των ποινικών αδικημάτων και των κυρώσεων σε τομείς ιδιαιτέρως σοβαρής εγκληματικότητας με διασυνοριακή διάσταση, όταν υπάρχει ανάγκη τα εγκλήματα αυτά να καταπολεμούνται σε κοινή βάση. Βάσει του ά. 83 παρ. 1 της Συνθήκης της Λισσαβόνας, για την έκδοση Οδηγίας για τον ορισμό ελάχιστων κανόνων ως προς τα στοιχεία των εγκλημάτων και τις ποινές μεταξύ άλλων σε τομείς ιδιαίτερα σοβαρής εγκληματικότητας με διασυνοριακή διάσταση δεν χρειάζεται πλέον η ομόφωνη έγκριση από το Ευρωπαϊκό Συμβούλιο των Υπουργών αλλά η πλειοψηφία των κρατών μελών στο Συμβούλιο μαζί με το Ευρωπαϊκό Κοινοβούλιο.

[855] Για την πλεον σύγχρονη προσέγγιση του ποινικού δικαίου στον ευρωπαϊκό χώρο μετά τη συνθήκη της Λισαβόνας πρβλ. το αναλυτικό πόνημα των *Δ. Κιούπη, Ρ. Παπαδοπούλου και Δ. Μουζάκη*, Το Ποινικό Δίκαιο μετά τη συνθήκη της Λισαβόνας, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011 και ιδίως αναπτύξεις του Κιούπη στις σελίδες 75 επ. σχετικά με τις οδηγίες και τη μεταφορά τους στις εθνικές

Οδηγίας [COM(2010)517 (30.09.2010)] υπήρξε η αντικατάσταση της Απόφασης-Πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών. Σύμφωνα, άλλωστε, με τα συμπεράσματα της από 14.07.2008 Έκθεσης της Επιτροπής σχετικά με την εφαρμογή της ανωτέρω απόφασης πλαίσιο, είχε συντελεστεί σημαντική πρόοδος στα περισσότερα κράτη μέλη, ωστόσο η εφαρμογή δεν είχε ακόμη ολοκληρωθεί σε ορισμένα από αυτά. Επίσης, στην Έκθεση επισημαινόταν ότι οι *«πρόσφατες επιθέσεις στην Ευρώπη μετά την έκδοση της απόφασης-πλαίσιο, τόνισαν την ύπαρξη διαφόρων απειλών όπως η εμφάνιση μαζικών ταυτόχρονων επιθέσεων κατά συστημάτων πληροφοριών και η αυξημένη εγκληματική χρήση του καλούμενου δικτύου προγραμμάτων ρομπότ (botnet)»*. Οι επιθέσεις τύπου botnet δεν βρίσκονταν στο επίκεντρο της προσοχής την εποχή που είχε εκδοθεί η Απόφαση-Πλαίσιο. Τα στοιχεία αυτά οδήγησαν την Επιτροπή να εξετάσει δράσεις σχεδιασμού καλύτερων τρόπων αντιμετώπισης της συγκεκριμένης απειλής[856].

Οι μεγάλης κλίμακας επιθέσεις, η ευκολότερη παραγωγή και χρήση κακόβουλου λογισμικού, οι νέες μέθοδοι διάπραξης εγκλημάτων με χρήση botnet και η ανάγκη καταπολέμησης του οργανωμένου εγκλήματος και της τρομοκρατίας και άρσης των εμποδίων στη διερεύνηση και δίωξη των εγκλημάτων σε διασυνοριακές υποθέσεις καλά συντονισμένων και ευρείας κλίμακας άμεσων επιθέσεων κατά των υποδομών ζωτικής σημασίας ενός κράτους, κατέστησαν αναγκαία την κατάργηση της Απόφασης Πλαίσιο και την επικαιροποίηση αυτής[857]. Επιπρόσθετα, ήδη από την πρόταση ακόμη της οδηγίας ελήφθη υπόψη η Σύμβαση της Βουδαπέστης για το κυβερνοέγκλημα, την οποία η Επιτροπή θεωρεί μάλιστα τόσο σπουδαία, ώστε να ενθαρρύνει τα κράτη μέλη που δεν την κύρωσαν ακόμη να πράξουν σχετικώς.

Ειδικότερα και όσον αφορά στο έγκλημα της παράνομης πρόσβασης σε συστήματα πληροφοριών (ά. 3), η τυποποίησή του είναι η ίδια με εκείνη της Απόφασης Πλαίσιο. Κατά την πρόταση της Οδηγίας, είχε εξαλειφθεί η πρόβλεψη της δυνατότητας των κρατών μελών να ποινικοποιήσουν το αδίκημα μόνο σε περιπτώσεις παράβασης μέτρου ασφαλείας. Η εν λόγω εξάλειψη συνιστούσε στην ουσία διεύρυνση του

νομοθεσίες καθώς και *Χρ. Μυλωνόπουλου*, Το Ευρωπαϊκό Ποινικό Δίκαιο μετά τη Συνθήκη της Λισαβόνας, ΠοινΧρ ΞΑ/2011, σελ. 81 επ.

[856] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π. σελ. 491.

[857] Βλ. *Γρηγόρης Τσόλιας*, Η πρόταση Οδηγίας του ΕΚ και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών, 2ο Πανελλήνιο Συνέδριο e ΘΕΜΙΣ, www.ethemis.gr.

αξιοποίνου για το συγκεκριμένο έγκλημα σε σύγκριση με την Απόφαση Πλαίσιο αλλά και με τη Σύμβαση για το κυβερνοέγκλημα. Η εξάλειψη του ως άνω περιορισμού του αξιοποίνου, ωστόσο, δεν ανταποκρινόταν στο θεμελιώδες αίτημα της χρήσης του ποινικού δικαίου ως έσχατης λύσης (ultima ratio), αφού η λήψη αποτελεσματικών μέτρων ασφαλείας για τα συστήματα πληροφοριών δύναται να εξασφαλίσει στην πράξη αποτελεσματικότερα την εμπιστευτικότητά τους από ό,τι μία ευρεία ποινικοποίηση[858]. Γι' αυτό και μάλλον κρίνεται ως θετική η πρόταση της Προεδρίας της Ένωσης προς το Συμβούλιο, η οποία, αποτυπώνοντας μία προσωρινή συμφωνία ορισμένων κρατών μελών, επανεισήγαγε ως προϋπόθεση του συγκεκριμένου εγκλήματος την κατά παράβαση μέτρων ασφαλείας απόκτηση πρόσβασης σε συστήματα πληροφοριών[859], η οποία φαίνεται ότι επηρέασε το νομοπαρασκευαστικό αποτέλεσμα και τελικώς στο ά. 3 της Οδηγίας συμπεριελήφθη πάλι ως προϋπόθεση η παραβίαση μέτρου ασφαλείας. Η πρόβλεψη των περιπτώσεων ήσσονος σημασίας διατηρήθηκε και αυτή στο κείμενο της διάταξης του ά. 3 της Οδηγίας ως περιορισμός του αξιοποίνου προκειμένου να καλύψει την ανάγκη παροχής στους εθνικούς νομοθέτες μιας δυνατότητας κάποιων περιορισμών του αξιοποίνου. Κρίθηκε, δε, σημαντική νομική έννοια με δεδομένο ότι διατηρήθηκε στα άρθρα στα οποία υπήρχε ήδη από την Απόφαση-Πλαίσιο. Η Καϊάφα Γκμπάντι επεσήμανε, πάντως, ότι το μη οριζόμενο, έστω με τη μορφή κατεύθυνσης, περιεχόμενο των «περιπτώσεων ήσσονος σημασίας»[860], οι οποίες εξαιρούνται από το

---

[858] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 493.

[859] Βλ. το με αρ. 8795/8.4.2011 έγγραφο της Προεδρίας προς το Συμβούλιο της Ένωσης.

[860] Κατά την παράγραφο 11 του Προοιμίου της Οδηγίας: «*...Τα κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές. Η περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης*». Επιπρόσθετα, στην αιτιολογική έκθεση της Πρότασης για την Οδηγία, οι περιπτώσεις ήσσονος σημασίας αποτελούν "*στοιχείο ευελιξίας που σκοπό έχει να επιτρέψει στα κράτη μέλη να μην καλύπτουν περιπτώσεις οι οποίες θεωρητικά θα υπάγονταν στο βασικό ορισμό, αλλά θεωρείται ότι δεν ζημιώνουν τα προστατευόμενα νομικά συμφέροντα, όπως παραδείγματος χάριν οι ενέργειες νέων που προσπαθούν να αποδείξουν τις γνώσεις τους στην τεχνολογία των πληροφοριών. Ωστόσο, αυτή η δυνατότητα περιορισμού του πεδίου της ποινικοποίησης δεν θα πρέπει να οδηγεί στην εισαγωγή πρόσθετων στοιχείων ως προς την αντικειμενική υπόσταση των αδικημάτων πέραν αυτών που ήδη περιλαμβάνει η οδηγία, διότι αυτό θα μπορούσε να οδηγήσει στην κάλυψη μόνο των αδικημάτων που διαπράττονται με επιβαρυντικές περιστάσεις. Κατά τη διαδικασία μεταφοράς στην εθνική νομοθεσία, τα κράτη μέλη πρέπει να αποφεύγουν ιδίως την εισαγωγή πρόσθετων στοιχείων ως προς την αντικειμενική υπόσταση των βασικών αδικημάτων, όπως π.χ. ειδική πρόθεση είσπραξης παράνομων εσόδων από εγκληματική δραστηριότητα ή παρουσία ειδικού αποτελέσματος όπως πρόκληση σημαντικής ζημίας*".

επιβαλλόμενο στα κράτη μέλη αξιόποινο, δεν συνάδει με όσα απαιτεί η αρχή της νομιμότητας σε ευρωπαϊκό περιβάλλον[861].

Για πρώτη φορά επιχειρείται να οριστεί δεσμευτικά το ελάχιστο περιεχόμενο δύο νέων αυτοτελών αξιόποινων πράξεων, της παράνομης υποκλοπής (ά. 6)[862] και της χρήσης των εργαλείων – π.χ. χρήση κακόβουλου λογισμικού, χρήση botnets – με τα οποία διαπράττονται τα σχετικά αδικήματα (ά. 7 περ. α')[863] καθώς και της διάθεσης συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών (ά. 7 περ. β')[864]. Ως θετικό στοιχείο πρέπει να επισημανθεί η μη πρόβλεψη αξιοποίνου στην περίπτωση της απόπειρας (ά. 8 παρ. 2) στα εγκλήματα του ά. 3 και 6 και 7 της Οδηγίας[865].

Όσον αφορά στις κυρώσεις, η Οδηγία προβλέπει στο άρθρο 9 ευρύτερο αξιόποινο για τα σχετικά εγκλήματα σε σχέση με την Απόφαση Πλαίσιο, ξεπερνώντας κατά πολύ τη γενική απαίτηση για τιμώρηση με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις. Ειδικότερα, σε περιπτώσεις επιθέσεων από εγκληματική

---

[861] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 493.

[862] «Άρθρο 6: ***Παράνομη υποκλοπή***.

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

[863] «Άρθρο 7: ***Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων.***

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις:

α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6·

β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών.»

[864] Βλ. και *Mark Turner, Nick Pantlin, Loretta Pugh & Christine Young*, EU Cyber Crime Directive takes a tougher stance against attacks on information systems, 17.10.2013, url: http://cn.lexology.com/library/detail.aspx?g=d3863b21-3c3b-419e-8a8f-2b007acb3a10.

[865] Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., σελ. 494 αναφορικά με το αδίκημα της παρ. 7.

οργάνωση, σε περιπτώσεις πρόκλησης σημαντικής ζημίας και ιδίως σε περιπτώσεις επηρεασμού συστήματος πληροφοριών υποδομής ζωτικής σημασίας προβλέπεται στερητική της ελευθερίας ποινή άνω των πέντε ετών. Επίσης, για τη χρήση των δικτύων προγραμμάτων ρομπότ (botnet) προβλέπεται ελάχιστη στερητική της ελευθερίας ποινή τριών ετών, εφόσον προκληθεί οικονομική ζημία ή απώλεια δεδομένων προσωπικού χαρακτήρα. Τέλος, η οδηγία εισάγει την απόδοση ευθύνης και σε εταιρείες που παραβαίνουν τις υποχρεώσεις της εποπτείας και ελέγχου και με αυτόν τον τρόπο επιτρέπουν σε πρόσωπο υπό τη δικαιοδοσία τους να διαπράξει οποιοδήποτε από τα αδικήματα που απαριθμούνται στην οδηγία[866].

Αναφορικά με τη διαδικασία ανταλλαγής πληροφοριών, η Οδηγία, έχουσα ως σκοπό τη βελτίωση της ευρωπαϊκής δικαστικής συνεργασίας σε ποινικές υποθέσεις, προβαίνει σε ισχυροποίηση της ήδη υφιστάμενης υποδομής σημείων επαφής πληροφόρησης σε εικοσιτετράωρη και εβδομαδιαία βάση καθώς και στη θέσπιση υποχρέωσης απάντησης των κρατών μελών σε αίτημα συνδρομής σε χρονικό διάστημα μόλις οκτώ ωρών σε επείγουσες περιπτώσεις. Καινοτομία της Οδηγίας συνιστά η θέσπιση υποχρέωσης των κρατών μελών να παρακολουθούν, να καταγράφουν και να συλλέγουν τα στατιστικά στοιχεία για τα σχετικά εγκλήματα.

Η εν λόγω Οδηγία εξακολουθεί να περιέχει σημεία τα οποία πρέπει να διασαφηνιστούν, όπως η μη σαφής αναφορά του αριθμού των συστημάτων πληροφοριών που απαιτούνται προκειμένου να θεωρηθεί ότι πρόκειται για περίπτωση "botnet" [(το κείμενο της Οδηγίας αναφέρεται σε «σημαντικό αριθμό υπολογιστών» (ά. 5 προοιμίου)] καθώς και η αναφορά σε δικαιούχους ταυτότητας (ά. 9 παρ. 5 της Οδηγίας).

Η Οδηγία αυτή πρέπει να ενσωματωθεί από τα κράτη-μέλη στις έννομες τάξεις τους έως τις 04.09.2015. Η ανάγκη για εναρμόνιση των δικαίων των κρατών-μελών καλύπτεται σε μεγάλο βαθμό και ως προς και αυτήν τη διάσταση η Οδηγία φαίνεται να βρίσκεται σε σωστή κατεύθυνση. Ωστόσο, στο πλαίσιο έντονης κριτικής αποτίμησης των επιλογών της Ευρωπαϊκής Ένωσης για το αξιόποινο των επιθέσεων κατά συστημάτων πληροφοριών, υποστηρίζεται ότι η Ένωση ανανεώνοντας το θεσμικό της πλαίσιο για την ποινική προστασία των συστημάτων πληροφοριών δεν ασχολήθηκε όσο θα έπρεπε με το θεμελιώδες αίτημα για τη *χρήση του ποινικού*

[866] *Brid – Aine Parnell*, EU crackdown will see tougher sentences for stupid cyber-badhats, The Register, 05.07.2013, url: http://www.theregister.co.uk/2013/07/05/eu_tougher_sentences_for_hackers.

δικαίου ως ultima ratio, ιδίως σ' έναν τομέα όπου η θέσπιση αξιοποίνου μπορεί να αντιμάχεται την τεχνολογική εξέλιξη ή την ελεύθερη ροή της πληροφορίας[867]. Εξάλλου, η θέση για χρήση του ποινικού δικαίου ως έσχατη λύση προκύπτει, όπως είναι γνωστό, από την ίδια την αρχή της αναλογικότητας, η οποία είναι κατοχυρωμένη και στο ευρωπαϊκό δίκαιο[868] και τυγχάνει γενικότερης αναγνώρισης.

[867] Κριτική της Μ. Καϊάφα-Γκμπάντι ήδη κατά την περίοδο πρότασης της εν λόγω Οδηγίας, όπου επισημαίνεται για την περίοδο εκείνη ότι πρέπει να γίνει συνείδηση ότι έχει τεράστια σημασία η ενεργός εμπλοκή των εθνικών αντιπροσωπειών και των ίδιων των κοινοβουλίων στη φάση της συζήτησης της Πρότασης Οδηγίας, διότι με τη συμβολή τους αυξάνονται οι πιθανότητες όχι μόνο να αποφευχθούν σοβαρά προβλήματα προσβολής θεμελιωδών αρχών του ποινικού δικαίου αλλά και οι πιθανότητες να επιτύχει η Ευρωπαϊκή Ένωση τον διακηρυγμένο στόχο της, που θέλει τον άνθρωπο στο επίκεντρο της δράσης της. Βλ. *Μ. Καϊάφα-Γκμπάντι*, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, όπ. π., ιδιώς σελ. 496 και 500.

[868] Βλ. *Χρ. Μυλωνόπουλος*, Κοινοτικό ποινικό δίκαιο και γενικές αρχές κοινοτικού δικαίου, ΠοινΧρ 2010, σελ. 161.

7. ΈΡΕΥΝΑ ΣΕ ΝΟΜΙΚΟΥΣ, ΕΠΙΣΤΗΜΟΝΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ (ΔΙΑΧΕΙΡΙΣΤΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΕΔΟΜΕΝΩΝ) ΚΑΙ HACKERS

7.1 Ο στόχος της έρευνας

Όπως είδαμε ανωτέρω, τα τελευταία χρόνια, μαζί με την ανάπτυξη του διαδικτύου και την ψηφιοποίηση του μεγαλύτερου μέρους των πληροφοριών που αφορούν σήμερα την ιδιωτική και δημόσια ζωή, αναπτύχθηκε και σχετική νομοθεσία σε εθνικό και ευρωπαϊκό επίπεδο για την προστασία των συστημάτων πληροφοριών και κυρίως για τον έλεγχο της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα[869]. Η πολυνομία και οι αλληλεπικαλύψεις των κείμενων διατάξεων, η «αποξενωμένη» σε κάποιες περιπτώσεις διατύπωση νομικών κανόνων από τις τεχνολογικές εξελίξεις και η άκρως περιορισμένη εφαρμογή αυτών των κανόνων[870] τελικά δημιουργούν ζητήματα προς διερεύνηση[871].

Συγκεκριμένα, στόχος της εν λόγω έρευνας[872] είναι η καταγραφή της άποψης για το hacking και τους hackers ειδημόνων που θα κληθούν να διαχειριστούν σε νομικό και

[869] Βλ. ανωτέρω κεφάλαια 4, 5, και 6.

[870] Βλ. χαρακτηριστικά την μία και μοναδική (δημοσιευμένη) ποινική απόφαση απόφαση αναφορικά με το ά. 370Γ παρ. 2 ΠΚ, ως ανωτέρω στην παράγραφο 5.5.

[871] Πρβλ. *Soumyo D. Moitra*, Analysis and modeling of cybercrime: Prospects and potential, Max Planck Intitute for foreign and international criminal law, για την σύγχρονη προβληματική και τις προτάσεις που αναπτύσσονται σε ό,τι αφορά έρευνες αναφορικά με το κυβερνοέγκλημα.

[872] Ο Gery Rose προτείνει το μοντέλο ABCDE για τη διεξαγωγή μιας έρευνας ως εξής:

Α) Θεωρία: αιτιολόγηση για κάποιο κοινωνικό φαινόμενο

Β) Θεωρητικές προτάσεις: συγκεκριμένες υποθέσεις προς διερεύνηση στη συγκεκριμένη μελέτη

C) Ζητήματα διενέργειας (operationalisation): αποφάσεις για την εμπειρική διεξαγωγή τις έρευνας - τεχνική συλλογής δεδομένων - δειγματοληψία - έννοιες και δείκτες – μεταβλητές - μονάδες

D) Πεδίο εργασίας: η συλλογή δεδομένων, πρακτικά προβλήματα εφαρμογής των αποφάσεων στο στάδιο C

Ε) Αποτελέσματα: η ανάλυση των δεδομένων οδηγεί σε διαπιστώσεις – η ερμηνεία δίνει υλικό σε μορφή ανατροφοδότησης στα στάδια C, Β και Α.

τεχνικό επίπεδο ζητήματα ασφάλειας ηλεκτρονικών πληροφοριών (δηλαδή νομικών και επιστημόνων πληροφορικής) αλλά και των ίδιων των hackers, η αξιολόγηση της αποτελεσματικότητας της ισχύουσας ποινικής νομοθεσίας[873] σε επίπεδο γενικής πρόληψης[874], οι απόψεις για ενδεχόμενη ανάγκη τροποποίησης και επικαιροποίησής της και η διατύπωση και προώθηση προτάσεων συναφούς αντεγκληματικής πολιτικής[875].

7.2 Οι υποθέσεις της έρευνας

7.2.1 Η σύγχρονη έννοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking

Όπως έχει αναλυθεί ανωτέρω, η αθέμιτη ή/και χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα λαμβάνει χώρα από hackers (ως βασικό συστατικό στοιχείο, τις περισσότερες φορές, των συμπεριφορών τους) των οποίων όμως ο σκοπός, η δράση και τα κίνητρα ποικίλλουν. Επιπρόσθετα, πέραν της χωρίς δικαίωμα πρόσβασης, στην έννοια του hacking περιλαμβάνονται και πράξεις οι οποίες ενδεχομένως μόνο «εκλεκτικές συγγένειες» έχουν με τη χωρίς δικαίωμα πρόσβαση

(έτσι στον πίνακα 2.1 στο πόνημα του *Gerry Rose,* Deciphering Sociological Research εις: *Anthony Giddens* (ed.), Contemporary Social Theory, London School of Economics and Political Science, M 1982, σελ. 14).

Ακριβώς ίδιο μοντέλο για τα στάδια εμπειρικών μελετών προτείνει και η Σπινέλλη (έτσι *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 94).

Στην προκειμένη περίπτωση το βήμα Α έχει συντελεστεί στο κεφάλαιο 3 του παρόντος πονήματος. Οι υποθέσεις της έρευνας οι οποίες παρουσιάζονται στην παράγραφο 7.2 αποτελούν το βήμα Β, τα βήματα C και D παρουσιάζονται διεξοδικά κατωτέρω στο κεφάλαιο 7 της παρούσας και τα αποτελέσματα και η ερμηνεία αυτών αναλύονται στα κεφάλαια 7 και 8 του παρόντος πονήματος.

[873] Η αξιολόγηση νομοθετικών ρυθμίσεων αποτελεί βασικό αντικείμενο της μεθοδολογίας της εγκληματολογίας (βλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 83). Αναφορικά με την αξιολόγηση της αποτελεσματικότητας των ποινικών κυρώσεων βλ. *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 220 επ.

[874] Για την έννοια της γενικής πρόληψης πρβλ. ενδεικτικώς *Ν. Ανδρουλάκη,* Ποινικό Δίκαιο – Γενικό Μέρος – Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα 2000, σελ. 41 επ. και *Ν. Κουράκη*, Εισαγωγή στη Θεωρία της ποινής, όπ. π., σελ. 29 επ.

[875] Βασικό αντικείμενο της μεθοδολογίας της εγκληματολογίας είναι και «*η διερεύνηση αντιλήψεων του κοινού σχετικά με το έγκλημα, τις ποινές, το σύστημα ποινικής δικαιοσύνης, τον φόβο του εγκλήματος ή τη θυματοποίηση των πολιτών*» (*Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 83-84).

σε ηλεκτρονικά δεδομένα. Άρα, λαμβανομένου υπόψιν ότι ο όρος hacking είναι πολύ και ενίοτε υπέρ του δέοντος χρησιμοποιημένος[876] και με σημασίες οι οποίες αναφέρονται σε διάφορες πράξεις, είναι σκόπιμο να καταγραφεί το σύγχρονο περιεχόμενο της έννοιας του hacking, σύμφωνα και με τις πλέον σύγχρονες πρακτικές, οι οποίες ενδεχομένως να μην έχουν ακόμη αναλυθεί στη σχετική βιβλιογραφία.

Εξάλλου, ο διαχωρισμός των hackers με κριτήριο το κίνητρο και τη δράση τους σε hacking και cracking δεν φαίνεται να είναι απολύτως αποτελεσματικός καθώς υπάρχει σύγχυση των όρων[877]. Οι ειδικοί οι οποίοι θα κληθούν να χαράξουν αντεγκληματική ή/και εγκληματοπροληπτική πολιτική είναι οι νομικοί και οι επιστήμονες πληροφορικής - από τις απαντήσεις τους και τον ορισμό που δίνουν στο hacking θα καταγραφεί αν η εν λόγω σύγχυση υφίσταται και σε αυτές τις δύο ομάδες ειδημόνων. Μέσω της περιγραφικής έρευνας που ακολουθεί θα διαπιστωθεί, δηλαδή, αν οι ειδικοί για την ενίσχυση της ασφάλειας των ηλεκτρονικών πληροφοριών «μιλούν την ίδια γλώσσα». Περαιτέρω, στο πλαίσιο σύγκρισης των απαντήσεων των ανωτέρω με τις απόψεις των ίδιων των hackers θα ελεγχθεί αν οι hackers και οι ειδικοί που ασχολούνται με την ενίσχυση της ασφάλειας των ηλεκτρονικών πληροφοριών αναφέρονται στις ίδιες συμπεριφορές (προκειμένου να υπάρχει μια κοινή βάση συζήτησης για τις πολιτικές ασφάλειας δεδομένων και συστημάτων πληροφοριών που θα πρέπει να ακολουθηθούν).

Συνεπώς, θα προσπαθήσουμε να προσδιορίσουμε κατά το δυνατόν ακριβέστερα το σύγχρονο περιεχόμενο της έννοιας του hacking, σύμφωνα και με τους προβληματισμούς που αναφέρονται ανωτέρω.

7.2.2 Ιδεολογία ή οικονομικό όφελος/ οικονομική ζημία;

[876] *Chuck Easttom and Det. Jeff Taylor*, Computer Crime, Investigation and the Law, Course Technology PTR, A part of Cengage Learning, 2011, pp. 10.

[877] Βλ. *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 9 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) κατά τους οποίους η επινόηση του όρου "cracker" 'ελαβε χώρα γιατί υπήρχε υπερβολική χρήση του όρου "hacker" κυρίως από δημοσιογράφους σε περιπτώσεις βλάβης ηλεκτρονικών συστημάτων.

Όπως διατυπώθηκε ανωτέρω, βασικός λόγος ανάπτυξης της δραστηριότητας του hacking και, άρα, της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικα δεδομένα ως κύρια έκφανση αυτής, φέρεται να είναι η ιδεολογία των hackers[878]. Επιπρόσθετα, ο ουσιαστικός διαχωρισμός μεταξύ hacking και cracking προκύπτει από τις επιβλαβείς συνέπειες των ενεργειών cracking στα ηλεκτρονικά δεδομένα (καταστροφή ιστοσελίδας, αποκλεισμός της πρόσβασης σε ιστοσελίδα κ.ά.) οι οποίες έχουν οικονομικό αντίκτυπο[879] [880]. Σε κάθε περίπτωση, ενέργειες που αποδίδονται σε hackers μπορούν να έχουν οικονομική διάσταση (π.χ. botnet herder[881], πώληση exploit kits, πώληση δυνατότητας πρόσβασης σε ηλεκτρονικές πληροφορίες, ακόμη και εξόρυξη ψηφιακών νομισμάτων bitcoins[882] κ.λπ.)[883]. Περαιτέρω, οι εγκληματολογικές θεωρίες, οι οποίες παρουσιάστηκαν ανωτέρω[884], αναφέρονται άλλες σε ιδεολογικές ερμηνείες και εξηγήσεις της προσπάθειας απόκτησης χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα [π.χ. θεωρία ηθικής ουδετεροποίησης, κριτική εγκληματολογία, θεωρία της έντασης, θεωρία ηθικών πεποιθήσεων (moral beliefs and moral judgement theory)], άλλες σε στάθμιση συμφερόντων και ανάλυση κόστους-οφέλους εκ μέρους των hackers (θεωρίες με βάση την ορθολογική επιλογή, οι οποίες μπορούν να συμπεριλάβουν και οικονομικό όφελος αλλά και όφελος που μπορεί να προκύψει από την ελευθερία της

[878] Βλ. ανωτέρω παράγραφο 2.7 του παρόντος πονήματος όπου και ανάλυση αναφορικά με τις συναρτήσεις ιδεολογίας και ηθικής των hackers αλλά και σχετική υποσημείωση για οριοθέτηση της έννοιας της ιδεολογίας αναφορικά με τους hackers (διάσταση από ορισμούς ιδεολογίας π.χ. ενός πολιτικού κόμματος).

[879] Βλ. ανωτέρω παράγραφο 2.3.1.

[880] Βλ. και αποτελέσματα έρευνας των *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 31 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) κατά την οποία το ισχυρότερο κίνητρο του hacking είναι οικονομικοί λόγοι.

[881] ... όπως έχει εξηγηθεί ανωτέρω (παράγραφος 2.2).

[882] Με αφορμή ένα τέτοιο περιστατικό και την φερόμενη «πρόσληψη» των hackers από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, δόθηκε στη δημοσιότητα στις 18 Ιουλίου 2014 ανοικτή επιστολή, η οποία υπογράφεται από 19 Καθηγητές ΑΕΙ και ΤΕΙ, για το «παράνομο» hacking (βλ. url: http://www.koutipandoras.gr/article/118505/anoihti-epistoli-kathigiton-aei-kai-tei-gia-paranomo-hacking). Οι συντάκτες της επιστολής αποδομούν τις προσπάθειες ηρωοποίησης των hackers και απορρίπτουν κάθε επιχείρημα το οποίο αναφέρεται σε περιέργεια ή παιχνίδι, αναφέροντας ότι το hacking είναι μια παράνομη και επικίνδυνη συμπεριφορά. Ωστόσο, θεωρώ ότι στην εν λόγω επιστολή όλες οι ενέργειες hacking μπαίνουν «στο ίδιο τσουβάλι», ανεξαρτήτως σκοπού ή αποτελέσματος. Ο διαχωρισμός τους και η ανάγκη αυτού είναι κεντρικός στόχος της συγκεκριμένης ερώτησης.

[883] Πρβλ. ενδεικτικά το άρθρο των *Woohyun Shim, Luca Allodi & Fabio Massacci*, Crime Pays If You Are Just an Average Hacker, University of Trento, Povo, Italy, url: http://disi.unitn.it/~allodi/shim-12-cybersecurity.pdf.

[884] Βλ. κεφάλαιο 3 του παρόντος πονήματος.

πληροφορίας – π.χ. «κατέβασμα» προγραμμάτων) και άλλες συγκεκριμένα σε οικονομικό όφελος (θεωρία εγκλημάτων λευκού περιλαιμίου). Παρά τα ανωτέρω, στη βασική διάταξη του ά. 370Γ παρ. 2 ΠΚ η οποία τιμωρεί τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα δεν περιλαμβάνεται επιβαρυντική περίσταση σε περίπτωση σκοπού αποκόμισης οικονομικού οφέλους ή πρόκλησης οικονομικής ζημίας από τον δράστη[885].

Λαμβανομένων υπόψιν των ποικίλων ως άνω θεωριών, σκόπιμο είναι να διερευνηθεί ειδικότερα το κίνητρο των hackers και ιδίως αν η ιδεολογία τους ή το οικονομικό όφελος ή η πρόκληση ζημίας προέχει στην απόφασή τους για «πέρασμα στην πράξη» ("passage à l' acte") και σε ποιο βαθμό[886]. Το πόρισμα αυτό θα εξοπλίσει την επιστημονική κοινότητα προκειμένου να λάβει αποφάσεις σχετικά με ενδεχόμενη αυστηρότερη ή όχι τιμώρηση των hackers ανάλογα με το κίνητρο και το αποτέλεσμα της δράσης τους και θα συμβάλει στον σχεδιασμό κατάλληλων εγκληματοπροληπτικών μέτρων.

7.2.3 Έλεγχος γενικοπροληπτικής αποτελεσματικότητας της ελληνικής ποινικής νομοθεσίας και προτάσεις de lege ferenda για τη σύγχρονη νομοθετική αντιμετώπιση του hacking

Οι διατάξεις που αναλύθηκαν ανωτέρω αναφορικά με την χωρίς δικαίωμα πρόσβαση σε δεδομένα εξυπηρετούν και σκοπούς γενικής πρόληψης[887], προκειμένου να ενισχυθεί στο μέγιστο δυνατό βαθμό η ασφάλεια των σύγχρονων ηλεκτρονικών συστημάτων πληροφοριών. Η αρχική εκτίμηση είναι ότι πρόκειται για διατάξεις ανεπαρκείς, κυρίως λόγω της σχεδόν ανύπαρκτης νομολογιακής εφαρμογής τους (η

[885] Βλ. ανωτέρω κεφάλαιο 5 του παρόντος πονήματος.

[886] Το δίπολο «ιδεολογία και οικονομική διάσταση» ως προς το hacking διατυπώνεται κατωτέρω και στο κείμενο το οποίο έστειλε στον γράφοντα εκπρόσωπος της ελληνικής χάκινγκ σκηνής (GHS): «*Σε καμια περίπτωση δεν υποστηρίζεται κανένα είδος οικονομικού hacking, και οτιδήποτε είναι αντίθετο με την ιδεολογία*». Το κείμενο αυτό παρατίθεται αυτούσιο στο Παράρτημα IV της παρούσας.

[887] Για την έννοια της γενικής πρόληψης πρβλ. ενδεικτικώς *Ν. Ανδρουλάκη,* Ποινικό Δίκαιο – Γενικό Μέρος – Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα 2000, σελ. 41 επ. και *Ν. Κουράκη*, Εισαγωγή στη θεωρία της ποινής, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 29 επ. Ειδικότερα για τη γενική πρόληψη και τη σχέση της με την αποτελεσματικότητα των ποινικών νόμων βλ. *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 185 επ.

περιορισμένη, βέβαια, εφαρμογή τους θα μπορούσε ίσως να σημαίνει σε μια αντίθετη θεωρητική ανάγνωση ότι επιτελούν ιδανικά το σκοπό τους αναφορικά με την γενική πρόληψη)[888]. Στην εν λόγω έρευνα θα αξιολογηθεί αν και κατά πόσο οι κείμενες διατάξεις έχουν λειτουργήσει αποτρεπτικά για τους (επίδοξους) παραβιαστές[889] και αν και κατά πόσο έχουν δράσει ενισχυτικά για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων[890], προκειμένου τελικώς να καταδειχθεί αν μια επιεικέστερη ή αυστηρότερη νομοθεσία είναι επιθυμητή. Επιπρόσθετα, σκόπιμο κρίνεται να ερευνηθεί η τάση αποποινικοποίησης[891] της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα. Όλα τα ανωτέρω και οι αναλύσεις που θα ακολουθήσουν έχουν ως στόχο τη διατύπωση προτάσεων για την αναμόρφωση της ποινικής νομοθεσίας ούτως ώστε αυτή να ανταποκρίνεται στις σύγχρονες αντιλήψεις και ανάγκες.

7.2.4 Εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών δεδομένων

Στην παρούσα περιγραφική/επεξηγητική έρευνα θα αναζητηθούν εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών πληροφοριών[892], οι οποίοι δύνανται να λειτουργούν συμπληρωματικά ή παραπληρωματικά με τις ποινικές διατάξεις για την ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων.

Ειδικότερα, η υπόθεση έρευνας επικεντρώνεται εν προκειμένω στο ερώτημα εάν η προαγωγή της ασφάλειας των δεδομένων στο διαδίκτυο εξαντλείται στην ποινική νομοθεσία ή εάν η ανάπτυξη και η προώθηση εναλλακτικών μέτρων και μεθόδων

[888] Από την άλλη πλευρά για ερμηνεία πιθανής αναποτελεσματικότητας των ποινικών νόμων πρβλ. *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 179 επ.

[889] Για την αποτρεπτική λειτουργία και τα συγκρατιτικά αποτελέσματα των (ποινικών) κανόνων δικαίου βλ. την εμπεριστατωμένη ανάλυση του *Λ. Κοτσαλή*, Ποινική δογματική και αντεγκληματική πολιτική: σχέση τριβής; εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. Ι, σελ. 645 επ.

[890] Βλ. σχετική ανάλυση για έρευνες αξιολόγησης ή αποτίμησης εις *Κ. Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 101.

[891] Πρβλ. *Ν. Κουράκη*, Κριτήρια για την (απ)εγκληματοποίηση μιας συμπεριφοράς, εις: *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π., σελ. 86 επ.

[892] ... με παραδείγματα των πρακτικών που υποστηρίζονται και από την «διαχειριστική εγκληματολογία» - βλ. ανωτέρω παράγραφο 3.10.

μπορεί να αποτελέσει σημαντικό εργαλείο για την επίτευξη του στόχου. Η έρευνα στοχεύει στην αναζήτηση πρακτικών που κινούνται εκτός του ποινικού συστήματος και της ποινικής δικαιοσύνης και μπορεί να εφάπτονται σε άλλους κλάδους του δικαίου ή να βρίσκονται εκτός της θέσπισης κανόνων δικαίου[893]: μέτρα όπως ο έλεγχος της πρόσβασης, οι επιτηδευμένες τεχνικές ασφάλειας του συστήματος, η καλή οργάνωση («ευταξία») του «κατόχου» των πληροφοριών (π.χ. επιχείρηση), η κρυπτογραφία, η αξιοποίηση της εμπειρίας και κατάρτισης των hackers, η ενημέρωση από σχετικούς δικτυακούς τόπους, η διαπαιδαγώγηση των χρηστών και η αυτορρύθμιση συνιστούν ουσιαστικά προληπτικά μέτρα, εντασσόμενα στο πλαίσιο μιας επικαιροποιημένης αντεγκληματικής πολιτικής, της οποίας κύριο μέλημα είναι η ασφάλεια των ηλεκτρονικών δεδομένων και πληροφοριών. Θα καταγραφεί σχετικά η άποψη των δειγμάτων και θα ανιχνευθούν προτάσεις (σαν αυτές που ήδη μόλις αναφέρθηκαν ή διαφορετικές) η υιοθέτηση των οποίων, κατά την άποψη και των συμμετεχόντων στην έρευνα, θα ενισχύσει την ασφάλεια των συστημάτων πληροφοριών.

7.3 Η ταυτότητα της έρευνας

Για την αξιολόγησης της ελληνικής ποινικής νομοθεσίας για τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, τη σύγχρονη προσέγγιση της έννοιας του hacking, τη διατύπωση προτάσεων αντεγκληματικής πολιτικής και της ανίχνευσης της βαρύτητας του οικονομικού ή ιδεολογικού κινήτρου των hackers, όπως διατυπώνονται ανωτέρω ως υποθέσεις της έρευνας[894], ακολουθεί κατωτέρω σχετική έρευνα[895].

[893] Ήδη ο *Ulrich Sieber* στο βασικό αναφορικά με το ποινικό δίκαιο του διαδικτύου πόνημά του Legal aspects of computer-related crime in the Information society, January 1998, prepared for the European Commission αναφέρεται στο ότι στο μέλλον πρέπει να προωθηθούν εξωδικαιικές λύσεις όπως η εκπαίδευση και η αυτορρύθμιση.

[894] Βλ. παράγραφο 7.2 του παρόντος πονήματος αναφορικά με τις υποθέσεις της έρευνας.

[895] Για τα σύγχρονα ζητήματα της έρευνας πρβλ. *Β. Βλάχου*, Εγκληματολογική έρευνα: προκλήσεις, δυσχέρειες, προοπτικές, εις: *Ν. Κουράκη, Χρ. Ζαραφωνίτου, Χρ. Τσουραμάνη, Ε. Χαϊνά (επιστ. επιμ.)*, Εγκληματολογία: Διδασκαλία και Έρευνα στην Ελλάδα, Πρακτικά Επιστημονικού Συνεδρίου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2011, σελ. 69-80.

Η έρευνα είναι συνδυαστική (ποσοτική και ποιοτική)[896]. Ως προς τον σκοπό της εντάσσεται στις κατηγορίες[897] της διερευνητικής[898] / περιγραφικής[899] / επεξηγητικής έρευνας[900] και της έρευνας αξιολόγησης / αποτίμησης[901]. Διενεργήθηκε σε πρωτογενή δεδομένα[902] τα οποία συνελέγησαν κυρίως με την τεχνική του ερωτηματολογίου[903] σε δείγματα σκοπιμότητας[904]. Αξιοποιήθηκε, επίσης, η τεχνική της συνέντευξης καθώς και δευτερογενή δεδομένα[905].

Η έρευνα έλαβε χώρα σε δείγμα 158 νομικών[906] στο διάστημα από 07.07.2013 έως 31.07.2013, 104 επιστημόνων πληροφορικής[907] στο διάστημα από 05.11.2013 έως 30.11.2013 και 48 hackers[908] στο διάστημα από 04.07.2013 έως 31.01.2014.

7.3.1 Μορφές και φύση της έρευνας

7.3.1.1 Διερευνητική έρευνα

Διερευνητικές έρευνες[909] είναι εκείνες που στοχεύουν στην εξοικείωση με ένα νέο, αδιερεύνητο θέμα και στο εντοπισμό μηχανισμών ή συσχετίσεων[910]. Δεν απαιτούν

[896] Βλ. παράγραφο 7.3.2.1 του παρόντος πονήματος.

[897] Βλ. την κατηγοριοποίηση των *A. Binder & G. Geis*, Methods of Research in Criminology and Criminal Justice, New York, 1983, σελ. 119 επ και της *Καλλιόπης Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, Δεύτερη ανανεωμένη έκδοση, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 2005, σελ. 97 επ.

[898] Βλ. παράγραφο 7.3.1.1 του παρόντος πονήματος.

[899] Βλ. παράγραφο 7.3.1.2 του παρόντος.

[900] Βλ. παράγραφο 7.3.1.3 του παρόντος.

[901]Βλ. παράγραφο 7.3.1.4 του παρόντος.

[902] Βλ. παράγραφο 7.3.1.6 του παρόντος.

[903] Βλ. παράγραφο 7.3.2.2 του παρόντος.

[904] Βλ. παράγραφο 7.3.1.5 του παρόντος.

[905] Βλ. παράγραφο 7.3.2.2.

[906] Βλ. παράγραφο 7.5.3 του παρόντος. Όλες οι απαντήσεις των νομικων περιλαμβάνονται στο Παράρτημα Ι του πονήματος.

[907] Βλ. παράγραφο 7.5.4 του παρόντος. Όλες οι απαντήσεις των επιστημόνων πληροφορικής περιλαμβάνονται στο Παράρτημα ΙΙ του πονήματος.

[908] Βλ. παράγραφο 7.5.5 του παρόντος. Όλες οι απαντήσεις των hackers περιλαμβάνονται στο Παράρτημα ΙΙΙ του πονήματος.

[909] Αναφορικά με τις διερευνητικές έρευνες βλ. ενδεικτικά *Β. Φίλια (γεν. εποπτ.)*, Εισαγωγή στη μεθοδολογία και τις τεχνικές κοινωνικών ερευνών, 2η εκδ., εκδ. Gutenberg, Αθήνα, 1996, σελ. 28 επ.

ιδιαίτερο σχεδιασμό και μεγάλα κονδύλια ενώ διεξάγονται σε ένα μικρό δείγμα με τη μέθοδο της παρατήρησης ή με ερωτηματολόγιο[911]. Στην προκειμένη περίπτωση, η πρωτοτυπία των διερευνώμενων θεμάτων (όπως αναπτύχθηκαν αμέσως ανωτέρω) καθώς και ο συνδυασμός και η συσχέτιση απαντήσεων σε ερωτηματολόγια που ελήφθησαν από τρία διαφορετικά δείγματα[912] παραπέμπει άμεσα στον χαρακτηρισμό της έρευνάς μας ως διερευνητικής.

7.3.1.2 Περιγραφική έρευνα

Η περιγραφική έρευνα (descriptive research)[913] έχει ως σκοπό τον αναλυτικό προσδιορισμό των χαρακτηριστικών μιας δεδομένης κατάστασης ή γεγονότος. Κύριος σκοπός του ερευνητή στη συγκεκριμένη περίπτωση είναι η λεπτομερής περιγραφή του φαινομένου. Βασικό χαρακτηριστικό αυτού του είδους έρευνας είναι ότι δεν στηρίζεται σε «υποθέσεις». Δηλαδή, ο ερευνητής αντί να μελετά συσχετίσεις μεταβλητών, ενδιαφέρεται απλώς να περιγράψει την εγκληματικότητα μιας περιοχής, τους παραβάτες των νόμων, ομάδες ατόμων, συνοικίες, ιδρύματα κράτησης εγκληματιών, αντιλήψεις του κοινού για την ποινή ή για ορισμένους θεσμούς κ.λπ. Οι περιγραφικές έρευνες χρησιμοποιούνται όταν δεν υπάρχει θεωρία στην οποία να μπορεί να προσφύγει ο ερευνητής για την εξέταση του συγκεκριμένου ζητήματος ή όταν δεν υπάρχουν προς το παρόν επαρκείς επιστημονικές γνώσεις για την

---

[910] Έτσι *Κ. Δ. Σπινέλλη,* Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 97 επ.

[911] Κλασικό παράδειγμα καταφυγής σε πολλές ερευνητικές τεχνικές είναι η έρευνα των Shaw και McKay στην περιοχή του Σικάγο, όπου χρησιμοποιήθηκαν στατιστικές του συστήματος ποινικής δικαιοσύνης, παρατήρηση και ιστοριογραφίες προσώπων της ερευνώμενης περιοχής (βλ. *Καλλιόπη Δ. Σπινέλλη*, Εγκληματολογία –Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π, σελ. 97-99).

[912] Χαρακτηριστικό παράδειγμα διερευνητικής έρευνας σε διαφορετικά δείγματα ήταν η έρευνα που πραγματοποιήθηκε σε θύματα ατόμων τρίτης ηλικίας, όπως παρουσιάζεται από την Σπινέλλη. Στο πλαίσιο της έρευνας αυτής χρησιμοποιήθηκε ένα ερωτηματολόγιο απευθυνόμενο σε δείγμα ατόμων τρίτης ηλικίας, ένα δεύτερο ερωτηματολόγιο απευθυνόμενο σε υπηρεσίες νοσοκομείων, ΚΑΠΗ κ.λπ. και παράλληλα ελέγχθηκαν και τα βιβλία συμβάντων στα αστυνομικά τμήματα των περιοχών, όπου διεξήχθη η έρευνα, προκειμένου να εντοπιστούν περιστατικά θυματοποίησης ηλικιωμένων (βλ. σχετικά *Καλλιόπη Δ. Σπινέλλη*, Προσβολές και προστασία της τρίτης ηλικίας – Εγκληματολογική, κοινωνιολογική και ποινική διερεύνηση του φαινομένου της κακοποίησης και παραμέλησης, Ποινικά υπ' αρ. 34, Αθήνα – Κομοτηνή, 1991).

[913] Αναλυτικά αναφορικά με τις περιγραφικές έρευνες βλ. ενδεικτικά *Β. Φίλια (γεν. εποπτ.)*, Εισαγωγή στη μεθοδολογία και τις τεχνικές κοινωνικών ερευνών, όπ. π., σελ. 31 επ.

κατασκευή «υποθέσεων». Οι έρευνες αυτές είναι χρήσιμες αλλά δεν έχουν την ίδια ερευνητική αξία, όπως οι έρευνες με θεωρητικό πλαίσιο και «υποθέσεις»[914] [915].

Στην προκειμένη περίπτωση, η αποτύπωση της σύγχρονης έννοιας του hacking και της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και η καταγραφή πρακτικών πρόληψης είναι θέματα τα οποία δεν βασίζονται στην επαλήθευση μια συγκεκριμένης θεωρητικής υπόθεσης – ωστόσο, τα πορίσματα αυτά μπορούν να αξιολογηθούν με βάση εγκληματολογικές θεωρίες, οι οποίες δύνανται να ερμηνεύσουν και να αιτιολογήσουν το hacking και ιδίως τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Επιπρόσθετα, με αφορμή το ότι ένα από τα δείγματα είναι αυτό στο οποίο συμμετέχουν hackers, η έρευνα αποκτά περιγραφική διάσταση καθώς σε κάποιες από τις ερωτήσεις, οι οποίες θα συμπεριληφθούν στο ερωτηματολόγιο, θα μπορέσουμε να περιγράψουμε και να καταγράψουμε δραστηριότητα και απόψεις των συμμετεχόντων στην έρευνα οι οποίες μέχρι σήμερα μας ήταν άγνωστες (π.χ. το ποσοστό των hackers που χρησιμοποιεί ψευδώνυμο και άλλες τέτοιου τύπου ερωτήσεις).

7.3.1.3 Επεξηγητική έρευνα

Η επεξηγητική έρευνα (explanatory research) σχετίζεται με μελέτες στις οποίες οι ερευνητές προσπαθούν να αναπτύξουν ή να ελέγξουν την εγκυρότητα μιας θεωρίας για κάποιο φαινόμενο, αναζητώντας παράγοντες που επηρεάζουν αιτιακά το φαινόμενο. Βέβαια, συχνά και στις επεξηγητικές έρευνες υπάρχει ένα τμήμα περιγραφικό, αν και αυτές προχωρούν σε μεγαλύτερη έκταση σε γενικεύσεις[916]. Για

[914] Βλ. *Καλλιόπη Δ. Σπινέλλη*, Εγκληματολογία –Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π, σελ. 99.

[915] Χαρακτηριστικό παράδειγμα περιγραφικής έρευνας είναι η διερεύνηση του προβλήματος της από κοινού τέλεσης εγκλημάτων από περισσότερους ανήλικους ή των συμμοριών ανηλίκων μέσα από 3.595 αποφάσεις του Μονομελούς Δικαστηρίου και 176 αποφάσεις του Τριμελούς Δικαστηρίου Ανηλίκων Αθηνών κατά το έτος 2000 (βλ. *Ν. Ε. Κουράκης / Π. Ζαγούρα / Μ. Γαλανού*, "Συμμορίες ανηλίκων στην Ελλάδα – Πορίσματα από τις αποφάσεις του Δικαστηρίου Ανηλίκων Αθηνών", Ποινικός Λόγος 5/2003, σελ. 2205-2218).

[916] Έτσι *Κ. Δ. Σπινέλλη,* Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 100.

τον λόγο αυτό οι κατηγοριοποιήσεις της έρευνας είναι περισσότερο σχηματικές και λιγότερο δεσμευτικές για τους ερευνητές[917] [918].

Στην προκειμένη περίπτωση διατυπώθηκαν ανωτέρω οι υποθέσεις της έρευνας οι οποίες παραπέμπουν σε εγκληματολογικές θεωρίες που μπορούν να υποστηριχθούν για την αιτιολόγηση του φαινομένου του hacking, την ερμηνεία του και την πρόληψή του. Τα αποτελέσματα που θα προκύψουν από την ανάλυση των απαντήσεων των ερωτηματολογίων θα επιβεβαιώσουν ή θα διαψεύσουν μερικώς ή ολικώς τις σχετικές με τις υποθέσεις της έρευνας θεωρίες.

7.3.1.4 Έρευνα αξιολόγησης

Κατά τα τελευταία έτη γίνεται συστηματική χρήση των αποτελεσμάτων των ερευνών αξιολόγησης με βασικό σκοπό την αξιολόγηση οργανισμών, θεσμών (π.χ. της κοινωφελούς εργασίας) κ.ά.[919]

Παραδοσιακά, στις εν λόγω έρευνες αποτιμάται ιδίως η αποτελεσματικότητα, δηλαδή ο βαθμός επίτευξης των επιδιωκόμενων στόχων (π.χ. η μείωση της υποτροπής, η μείωση της εγκληματικότητας, ο βαθμός επανένταξης στην κοινότητα με μία σταθερή εργασία και οικογενειακή ζωή, η ολοκλήρωση της εκπαίδευσης και κατάρτισης, μεταβλητές, δηλαδή, που αποτιμώνται αριθμητικά). Επίσης, λαμβάνεται υπόψη η αποδοτικότητα, δηλαδή η σχέση κόστους (οικονομικού και κοινωνικού) και οφέλους

---

[917] Βλ. *A. Binder & G. Geis*, όπ. π., σελ. 119-120

[918] Αρκετές ελληνικές έρευνες θα μπορούσαν να ενταχθούν στην κατηγορία των επεξηγητικών ερευνών, όπως χαρακτηριστικά η έρευνα για την εγκληματικότητα των μεταναστών αναφορικά με το πώς απεικονίζεται το φαινόμενο σε συγκεκριμένη μερίδα του απογευματινού τύπου τη δεκαετία του 1990 (βλ. *Α. Μοσχοπούλου*, Η εγκληματικότητα των Μεταναστών – Απεικόνιση του φαινομένου στον απογευματινό τύπο, 1990-1999, σειρά Ποινικά αρ. 69, Αθήνα – Κομοτηνή, 2005).

[919] ... ενδεικτικά: προγραμμάτων εσω-ιδρυματικής μεταχείρισης ανηλίκων, θεραπευτικών προγραμμάτων ουσιοεξαρτημένων, προγραμμάτων παρέμβασης σε ευπαθείς ομάδες, προγραμμάτων πρόληψης στην κοινότητα κ.λπ.

Οι έρευνες αποτίμησης της αποτελεσματικότητας εξελίχθηκαν και διαδόθηκαν τα τελευταία χρόνια, εκτός των άλλων, επειδή η Ευρωπαϊκή Ένωση απαιτεί αξιολογήσεις για τις κοινωνικές παρεμβάσεις που έχει συγχρηματοδοτήσει. Εξάλλου, σε πολλά ποινικού περιεχομένου κείμενα της Ένωσης αναφέρονται συχνά οι όροι «βέλτιστες, καλές, πολλά υποσχόμενες πρακτικές» (πρβλ. *Καλλιόπη Δ. Σπινέλλη*, Κρατούμενοι χρήστες ή εξαρτημένοι: προς αναζήτηση των βέλτιστων θεραπευτικών πρακτικών, σε: Τιμητικό Τόμο για τον Ιωάννη Μανωλεδάκη, Δημοκρατία - Ελευθερία – Ασφάλεια, Αθήνα – Θεσσαλονίκη 2005, σελ. 391 επ.), οι οποίες για να χαρακτηριστούν ότι είναι αποτελεσματικές και να αποτελέσουν πρότυπα για άλλα κράτη – μέλη (πολιτική διάχυσης των βέλτιστων πρακτικών) πρέπει να έχουν αξιολογηθεί σύμφωνα με ορισμένα, επιστημονικά καθιερωμένα, κριτήρια.

αλλά και ο βαθμός ικανοποίησης των αποδεκτών των προσφερόμενων υπηρεσιών και προγραμμάτων[920]. Η αξιολόγηση η οποία δύναται να λάβει χώρα μπορεί να είναι εσωτερική[921] και εξωτερική[922].

Στην προκειμένη περίπτωση βασικός κορμός των ερευνητικών μας υποθέσεων είναι η αποτίμηση της αποτελεσματικότητας της κείμενης ελληνικής ποινικής νομοθεσίας[923] στην περίπτωση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα. Ο βαθμός ικανοποίησης νομικών και επιστημόνων πληροφορικής, η αίσθηση (αν)ασφάλειας την οποία νιώθουν για τα ηλεκτρονικά τους δεδομένα, η αυτοομολογούμενη αποχή από εγκληματικές πράξεις στις απαντήσεις των hackers ένεκα της αποτρεπτικής λειτουργίας της ισχύουσας νομοθεσίας καθώς και άλλα στοιχεία τα οποία δύνανται να προκύψουν από τη γενικότερη ενασχόληση με το ζήτημα και μέσω της τεχνικής της παρατήρησης[924] (π.χ. η νομολογιακή εφαρμογή των ποινικών διατάξεων για τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, όπως αναλύθηκε ανωτέρω) θα

---

[920] Βλ. *Καλλιόπη Δ. Σπινέλλη*, Εγκληματολογία –Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π, σελ. 101.

[921] Η εσωτερική αξιολόγηση διεξάγεται από επιστήμονες – εργαζομένους στον ίδιο τον οργανισμό ή το ίδρυμα ή ακόμη και σε ένα συγκεκριμένο πρόγραμμα. Οι επιστήμονες αυτοί διερευνούν, μεταξύ άλλων, τις απόψεις των αποδεκτών των υπηρεσιών και την πρόοδό τους συνεπεία της παρέμβασης προκειμένου να προβούν στην αποτίμηση της αποτελεσματικότητας των προσφερόμενων υπηρεσιών.

Από πλευράς μεθοδολογίας είναι ενδιαφέρουσα η εσωτερική αξιολόγηση μιας παρέμβασης πρωτογενούς πρόληψης σε ένα σχολικό συγκρότημα περιοχής Αθηνών με κύριο στόχο παιδιά ηλικίας 6-12 ετών, που υλοποιήθηκε από το Κέντρο Θεραπείας Εξαρτημένων Ατόμων (ΚΕΘΕΑ). Το εν λόγω πρόγραμμα περιελάμβανε παρεμβάσεις σε όλες τις υπο-ομάδες του σχολείου (μαθητές, δασκάλους, γονείς) καθώς και παρεμβάσεις στο ίδιο το σχολείο, το οποίο είναι ενταγμένο σε μία ευρύτερη κοινότητα. Η στρατηγική εσωτερικής αξιολόγησης που σχεδιάστηκε περιελάμβανε σε όλες τις επιμέρους φάσεις του προγράμματος αποτιμήσεις με ατομικά ερωτηματολόγια σε μαθητές, δασκάλους και γονείς, παρατήρηση τάξης (συζητήσεις, παιχνίδια ρόλων, εργασίες ομάδων μαθητών) και εστιασμένες συνεντεύξεις σε ομάδες δασκάλων και γονέων (βλ. *Ι. Κυρίτση και Σ. Τσιώτρα*, "Ένα μοντέλο ολιστικής προσέγγισης πρωτογενούς πρόληψης στην πρωτοβάθμια εκπαίδευση", Περιοδικό Εξαρτήσεις 2004, σελ. 29-30).

[922] Η εξωτερική αξιολόγηση ανατίθεται σε εξωτερικούς, αντικειμενικούς αξιολογητές, όπως ένα ερευνητικό πανεπιστημιακό κέντρο ή μια ομάδα έγκριτων επιστημόνων. Πιο συγκεκριμένα, η εξωτερική αξιολόγηση συνίσταται στην κριτική-αναλυτική εξέταση των αποτελεσμάτων της εσωτερικής αξιολόγησης. Σκοπός της είναι η διαπίστωση της πληρότητας, της διαφάνειας και της αντικειμενικότητας της εσωτερικής αξιολόγησης και των τεκμηριωτικών της δεδομένων και η διατύπωση ουδέτερης αντικειμενικής γνώμης (βλ. σχετικά την υπ' αρ. 65 υποσημείωση της *Καλλιόπης Δ. Σπινέλλη*, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π, σελ. 103, όπου ως παράδειγμα εξωτερικής αξιολόγησης αναφέρεται η αξιολόγηση προγράμματος μεθαδόνης, η οποία ανατέθηκε σε τρεις εξωτερικούς κριτές, τον Κώστα Στεφανη, την Καλλιόπη Σπινέλλη και τη Μαριέττα Γιαννάκου - Κουτσίκου, οι οποίοι υπέγραψαν την «Έκθεση τριμελούς επιτροπής αξιολόγησης των προγραμμάτων υποκαταστάτων»).

[923] Για την αποτελεσματικότητα των ποινών στην πρόληψη των εγκλημάτων πρβλ. και τα αποτελέσματα σχετικής έρευνας των *Α. Μαγγανά, Μ. Ζάννη, Στ. Παπαμιχαήλ και Γ. Λάζου*, Εγκλήματα, ποινές και ελληνική κοινή γνώμη, ΠοινΔικ 8-9/2002, σελ. 943 επ.

[924] Όσον αφορά τις μεθόδους και τις τεχνικές που χρησιμοποιούνται στο πλαίσιο της έρευνας αξιολόγησης, αυτές ποικίλουν. Συνήθως, οι τεχνικές που χρησιμοποιούνται είναι τα ερωτηματολόγια, οι συνεντεύξεις και η παρατήρηση.

αποτελέσουν χαρακτηριστικά στοιχεία αξιολόγησης της κείμενης νομοθεσίας. Με την σειρά της, η αξιολόγηση αυτή θα καταδείξει την ανάγκη ή όχι και σε ποιο βαθμό και ύφος de lege ferenda παρεμβάσεων. Σύμφωνα με αυτά, η παρούσα έρευνα είναι στον πυρήνα της αξιολογική.

7.3.1.5 Έρευνα σε δείγμα σκοπιμότητας

Η έρευνα μπορεί, αντί να μελετά το «σύνολο» ή ολόκληρο τον «πληθυσμό», να μελετά ένα δείγμα. Η τεχνική δειγματοληψίας ως διαδικασία είναι αρκετά πολύπλοκη ενώ διακρίνεται σε δύο γενικές κατηγορίες, το τυχαίο δείγμα ή δείγμα πιθανοτήτων (simple random sampling)[925] και το μη–τυχαίο δείγμα ή δείγμα σκοπιμότητας (purposive sample)[926].

Μη τυχαίο δείγμα ή δείγμα σκοπιμότητας είναι εκείνο για το οποίο ο ερευνητής έχει ανάγκη να επικεντρώσει την έρευνά του σε ορισμένες μεταβλητές[927]. Σε αυτή την περίπτωση ο ερευνητής συλλέγει ένα δείγμα τα μέλη του οποίου θεωρεί ότι είναι περισσότερο σημαντικά για τη συγκεκριμένη έρευνα - υπάρχει δηλαδή σκοπιμότητα για την επιλογή του κάθε μέλους στο δείγμα. Ο πληθυσμός υποδιαιρείται σε υπο–

[925] Τυχαίο είναι το δείγμα όταν κάθε ένα από τα άτομα ή τις μελετώμενες μονάδες έχει την ίδια πιθανότητα να είναι αυτό ή αυτή που θα επιλεγεί και έχει μηδέν πιθανότητα να μην επιλεγεί (αμερόληπτη επιλογή). Παραδείγματος χάριν, αν έχουμε ένα πληθυσμό 100 ατόμων, κάθε μέλος έχει 1% πιθανότητα επιλογής. Όταν ένα μέλος επιλεγεί δεν έχει δεύτερη δυνατότητα επιλογής (διαγράφεται από το αρχείο) ενώ κάθε νέα επιλογή δεν επηρεάζεται από τις προηγούμενες επιλογές Η μέθοδος αυτή είναι παρόμοια με την μέθοδο της κληρωτίδας, με τη διαφορά ότι για την επιλογή δεν χρησιμοποιούμε κλήρους με ονόματα, αλλά πίνακες τυχαίων αριθμών. Βλ. αναλυτικότερα για την έννοια του δείγματος τις αναπτύξεις του *Χρήστου Κελπερή* εις *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 280 επ.

[926] *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 124-125.

[927] Στην επιστήμη γίνεται λόγος για ανεξάρτητες μεταβλητές ή μεταβλητές πρόβλεψης και για εξαρτημένες μεταβλητές. Ανεξάρτητες μεταβλητές είναι έννοιες, όπως η ηλικία, το φύλο, η φυλή, ο τόπος γέννησης ή κατοικίας, το θρήσκευμα, το εισόδημα κ.λπ. ενώ εξαρτημένη μεταβλητή σε μία σχέση που περιλαμβάνει δύο ή περισσότερες μεταβλητές είναι η μεταβλητή που έπεται της ανεξάρτητης, είναι δηλαδή το αποτέλεσμα, το αιτιατό. Λόγου χάρη η παράβαση των νόμων, η εγκληματικότητα, η υποτροπή κ.λπ.

Αναλυτικότερα για την έννοια της μεταβλητής στις κοινωνικές έρευνες βλ. ενδεικτικά *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 112 επ. και *Αθ. Κατσής, Γ. Σιδερίδης και Αν. Εμβαλωτής*, Στατιστικές μέθοδοι στις κοινωνικές επιστήμες, εκδ. Τόπος, Αθήνα, 2010, σελ. 11 επ.

σύνολα ή στρώματα ανάλογα με τα χαρακτηριστικά που ενδιαφέρουν τον ερευνητή (π.χ. θρήσκευμα)[928].

Στην προκειμένη περίπτωση επελέγη δείγμα σκοπιμότητας και από τις τεχνικές επιλογής δείγματος σκοπιμότητας[929] προκρίθηκε η τεχνική του ειδήμονα και η

[928] Βλ. *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 285 επ.

[929] Στο πλαίσιο της έρευνας σε δείγμα σκοπιμότητας, ο ερευνητής δύναται να επιλέξει μία από τις παρακάτω τεχνικές:

α) **Τεχνική της διαμέσου (median)**

Με αυτή την τεχνική ο ερευνητής επιλέγει άτομα που θεωρούνται ότι είναι αντιπροσωπευτικά του *τυπικού* μέλους του πληθυσμού που τον ενδιαφέρει (π.χ. ο μέσος καταναλωτής κ.λπ). Κατά μία έννοια ο ερευνητής προσπαθεί να επιλέξει αυτούς που βρίσκονται γύρω από τη διάμεσο της κατανομής συγκεκριμένων χαρακτηριστικών του πληθυσμού και να αποφύγει τις ακραίες περιπτώσεις. Το μειονέκτημα είναι ότι θα πρέπει εκ των προτέρων να γνωρίζει ο ερευνητής ποιά είναι στην πραγματικότητα αυτά τα χαρακτηριστικά. Για το σκοπό αυτό μπορεί να ζητήσει την άποψη ειδικών.

β) **Τεχνική του ειδήμονα ή της ομοιογένειας**

Σε αυτή την περίπτωση ο ερευνητής επιθυμεί να συμπεριλάβει στο δείγμα του άτομα που θεωρούνται ειδήμονες σε κάποιο ζήτημα ή άτομα με ειδικά χαρακτηριστικά (π.χ. άτομα με συγκεκριμένο σεξουαλικό προσανατολισμό, ειδικούς σε ένα θέμα, άτομα με κάποια συγκεκριμένη ασθένεια κ.λπ).

γ) **Τεχνική quota (μεριδίου)**

Το δείγμα περιλαμβάνει κάποιο *μερίδιο* του ερευνητικού πληθυσμού, το οποίο ο ερευνητής αποφασίζει εκ των προτέρων. *Αναλογική τεχνική quota:* ο ερευνητής κάνει κάποιες αυθαίρετες υποθέσεις σχετικά με την κατανομή των χαρακτηριστικών που τον ενδιαφέρουν στον πληθυσμό. Στη συνέχεια συλλέγει ένα δείγμα το οποίο θα αντιπροσωπεύει τα χαρακτηριστικά αυτά στις προαποφασισμένες από τον ερευνητή αναλογίες. Π.χ. σε έναν πληθυσμό 1000 φοιτητών ο ερευνητής επιθυμεί να συλλέξει ένα δείγμα 100 ατόμων. Δεν έχει στη διάθεσή του άλλα στοιχεία. Αποφασίζει αυθαίρετα ότι το 50% είναι άνδρες και το άλλο 50% γυναίκες και τηρώντας την αναλογία αυτή περιλαμβάνει στο δείγμα 50 άνδρες και 50 γυναίκες. *Μη αναλογική τεχνική quota:* ο ερευνητής θεωρεί ότι ο πληθυσμός περιλαμβάνει κάποιες υπο-ομάδες που τον ενδιαφέρουν, και επιθυμεί το δείγμα να περιλαμβάνει έναν ελάχιστο αριθμό ατόμων από την κάθε μία υπο-ομάδα. Ο στόχος είναι να διασφαλιστεί η αντιπροσώπευση όλων των υπο-ομάδων του ενδιαφέροντος. Π.χ. σε μία έρευνα σχετική με τους μετανάστες, επιλέγει 50 Αλβανούς, 50 Νιγηριανούς, 50 Πακιστανούς, 50 Ινδούς και 50 Κινέζους. Η μέθοδος αυτή αποτελεί κατά μία έννοια την μη τυχαία εκδοχή της τυχαίας δειγματοληψίας κατά στρώματα.

δ) **Τεχνική της ετερογένειας**

Αντίθετα από την τεχνική της διαμέσου, σε αυτόν τον τύπο δειγματοληψίας ο ερευνητής επιθυμεί να συλλέξει ένα δείγμα το οποίο να περιλαμβάνει ένα ευρύ φάσμα των τιμών του υπό μελέτη χαρακτηριστικού / χαρακτηριστικών. Δηλαδή, ο ερευνητής προσπαθεί να διασφαλίζεται μία ικανοποιητική κάλυψη της κατανομής των τιμών στο υπό μελέτη χαρακτηριστικό. Π.χ. σε μία μελέτη που αφορά το εισόδημα των συμμετεχόντων, είναι σημαντικό να αντιπροσωπεύονται ικανοποιητικά όλες οι εισοδηματικές ομάδες, από τα χαμηλότερα εισοδήματα μέχρι τα υψηλότερα εισοδήματα (ανεξάρτητα από την αριθμητική αντιπροσώπευσή τους στον πληθυσμό).

ε) **Δειγματοληψία χιονοστιβάδας**

Αυτή η τεχνική είναι ιδιαίτερα χρήσιμη για τη μελέτη περιθωριοποιημένων ομάδων ή ομάδων στις οποίες υπάρχει δυσκολία πρόσβασης (π.χ. ομοφυλόφιλοι άνδρες 20-45 ετών που ζουν στο Ρέθυμνο). Σε αυτή την περίπτωση εντοπίζονται αρχικά όσο το δυνατόν περισσότερα μέλη της ομάδας αυτής, τα οποία δέχονται να λάβουν μέρος στην έρευνα. Στη συνέχεια, τα άτομα αυτά έρχονται σε επαφή με άλλα άτομα της ομάδας τα οποία και τα «στρατολογούν» στην έρευνα. Π.χ. μπορεί να τους δώσουν ερωτηματολόγια προς συμπλήρωση ή να τους φέρουν σε επαφή με τον ίδιο τον ερευνητή. Αυτά τα νέα μέλη θα «στρατολογήσουν» επιπλέον συμμετέχοντες κ.ο.κ., μέχρις ώτου να συμπληρωθεί ένα ικανοποιητικό μέγεθος δείγματος.

(Βλ. ειδικότερα *Θ. Ιωσηφίδης*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 58 επ. και *Αν. Σταλίκας*, Μέθοδοι έρευνας στην ψυχολογία, εκδ. Ελληνικά Γράμματα, Αθήνα, 2005).

δειγματοληψία χιονοστιβάδας σε περίπτωση δείγματος αυτοομολογούμενης παραβατικότητας[930]. Συγκεκριμένα, κρίθηκε ότι ένα αντιπροσωπευτικό δείγμα νομικών που διαθέτουν δεδομένα στο διαδίκτυο έχει το αισθητήριο να αξιολογήσει επαρκώς τις ισχύουσες διατάξεις, να διατυπώσει απόψεις και να προτείνει λύσεις για την προαγωγή της ασφάλειας των δεδομένων και των συστημάτων πληροφοριών και σε κάθε περίπτωση να απαντήσει σε ερωτήσεις με τη μικρότερη δυνατή φόρτιση που ενδεχομένως δημιουργεί ο ηθικός πανικός[931] από περιστατικά hacking (τεχνική του ειδήμονα)[932]. Στην ίδια κατεύθυνση ένα άλλο αντιπροσωπευτικό δείγμα διαχειριστών ηλεκτρονικών δεδομένων (π.χ. διαχειριστές ιστοσελίδων, υπεύθυνοι ηλεκτρονικών δικτύων κ.λπ.) αλλά και επιστημόνων πληροφορικής (π.χ. προγραμματιστές κ.ά.) κρίθηκε ότι έχει την εμπειρία να συμβάλει στην καταγραφή της χωρίς δικαίωμα

---

[930] Αναφορικά με τις έρευνες αυτοομολογούμενης παραβατικότητας βλ. *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 44 επ., κεφάλαιο 1 παρ. 1.3 με τίτλο «Οι έρευνες (αυτο)ομολογούμενης ενοχής».

[931] Δεν πρέπει να διαφεύγουν της προσοχής μας οι «ηθικοί πανικοί», οι οποίοι ενδεχομένως δημιουργούνται από τα ΜΜΕ αναφορικά με το hacking. Ως **ηθικός πανικός** ορίζεται «*...Μια κατάσταση, ένα επεισόδιο, ένα άτομο ή ομάδα ατόμων προσδιορίζονται ως απειλές για το κοινωνικό αξιακό πλαίσιο. Κάποιες φορές το αντικείμενο του πανικού είναι νέο· κάποιες άλλες απλά προϋπάρχει κι εμφανίζεται ξαφνικά με μια συγκεκριμένη, διακριτή μορφή· Τα ΜΜΕ προσδίδουν μια στερεοτυπική φύση στις οντότητες αυτές, ενώ στο έργο της ηθικής οχύρωσης της κοινωνίας συντελούν εκδότες, πολιτικοί, αλλά και άλλοι «ορθά» σκεπτόμενοι άνθρωποι, όπως πάσης φύσεως κοινωνικά αναγνωρισμένοι ειδικοί, προτείνοντας διάγνωση και λύση στο πρόβλημα.* (η εμφάνιση του πανικού) *Μερικές φορές έχει πιο σοβαρές και μακροπρόθεσμες επιπτώσεις και μπορεί να προκαλέσει μεταβολές στο νομικό σύστημα και την κοινωνική πολιτική, ή ακόμα και στον τρόπο με τον οποίο αντιλαμβάνεται μια κοινωνία τον εαυτό της*» (βλ. *Αφρ. Κουκουτσάκη*, Νεολαία και «Ηθικοί Πανικοί», url: http://crimevssocialcontrol.blogspot.com/2009/10/blog-post_17.html όπως παραπέμπει στον *S. Cohen*) Η Κουκουτσάκη επισημαίνει επίσης «*...ως προσδιοριστικό στοιχείο του ηθικού πανικού, το στοιχείο της υπερβολής και της αναντιστοιχίας ανάμεσα σ' αυτό που ορίζεται ως κοινωνική απειλή και τις προκαλούμενες αντιδράσεις, κυρίως μέσα από το λόγο θεσμικών φορέων*».

Κατά την Ζαραφωνίτου, τα ΜΜΕ αποτελούν την κυριότερη πηγή πληροφόρησης για το έγκλημα και την ποινική δικαιοσύνη και παρουσιάζουν τις σχετικές ειδήσεις με τρόπο δραματοποιημένο, επιφανειακό και επαναλαμβανόμενο – ενέχονται, επομένως, για τη δημιουργία «ηθικού πανικού» και για την ενίσχυση έντονων τιμωρητικών τάσεων (έτσι *Χ. Ζαραφωνίτου*, Όψεις και διαστάσεις του κοινωνικού φαινομένου της ανασφάλειας, εις: *Χ. Ζαραφωνίτου,* (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 45). Βλ. και σχετικά με την κατασκευή της κοινωνικής πραγματικότητας από τα ΜΜΕ το πόνημα της *Έφης Λαμπροπούλου*, Η κατασκευή της κοινωνικής πραγματικότητας και τα Μέσα Μαζικής Επικοινωνίας – Η περίπτωση της βίας και της εγκληματικότητας, εκδ. Εκλληνικά Γράμματα, Αθήνα, 1999.

Ο Taylor εξηγεί ότι οι περιπτώσεις hacking επιδέχονται υπερβολών στην αντιμετώπισή τους από τα ΜΜΕ διότι προκαλούν εξίσου φόβο και εντυπωσιασμό ως άμεσα συνδεδεμένες με την τεχνολογία σε συνδυασμό με την ανωνυμία, η οποία αποτελεί χαρακτηριστικό των ψηφιακών εγκλημάτων (έτσι *Paul A. Taylor*, Hackers: Crime in the Digital Sublime, Routledge, 1999, url: http://www.google.gr/books?hl=el&lr=&id=V9VkmdYlvK4C&oi=fnd&pg=PP1&dq=Psychological+Theories+of+Crime+and+%E2%80%9CHacking&ots=1mWfjiP22v&sig=e98naWli9K0H0FTeYMwmVMqg4u8&redir_esc=y#v=onepage&q=Psychological%20Theories%20of%20Crime%20and%20%E2%80%9CHacking&f=false, pp. ix-x). Για τον σχετικό ρόλο των ΜΜΕ πρβλ. και *Έφη Λαμπροπούλου,* Η κατασκευή της κοινωνικής πραγματικότητας και τα μέσα μαζικής επικοινωνίας : η περίπτωση της βίας και της εγκληματικότητας, εκδ. Ελληνικά γράμματα, Αθήνα, 1999.

[932] Αναφορικά με το δείγμα νομικών βλ. παράγραφο 7.5.3 καθώς και παράγραφο 7.6 αναφορικά με τους περιορισμούς της έρευνας.

πρόσβασης σε δεδομένα, να αξιολογήσει την εγκληματοπροληπτική λειτουργία της ισχύουσας νομοθεσίας και να προτείνει τεχνικές και όχι μόνο λύσεις[933] αφού οι συμμετέχοντες σε αυτό γνωρίζουν το πρόβλημα της ασφάλειας των συστημάτων πληροφοριών εκ των έσω. Τέλος, αποφασίστηκε να γίνει η φιλόδοξη προσπάθεια να ανευρεθούν hackers, οι οποίοι με ερωτήσεις αυτοομολογούμενης παραβατικότητας θα δώσουν την δική τους οπτική για τη σχέση τους με τον νόμο και την ασφάλεια των ηλεκτρονικών δεδομένων – για τον εντοπισμό των hackers, λόγω της δυσκολίας πρόσβασης που υπάρχει σε αυτούς, χρησιμοποιήθηκε η τεχνική της χιονοστιβάδας[934].

7.3.1.6 Έρευνα με πρωτογενή δεδομένα

Γενικότερα, οι έρευνες ανάλογα με την επιλεγόμενη στρατηγική συλλογής δεδομένων διακρίνονται σε έρευνες πρωτογενείς και δευτερογενείς. Έρευνα με πρωτογενή δεδομένα είναι εκείνη της οποίας τα στοιχεία συλλέγει ο ερευνητής μόνος του, με δικές του μεθόδους και για το σκοπό της δικής του διερεύνησης[935]. Χαρακτηριστικό παράδειγμα τέτοιου είδους έρευνας είναι η έρευνα με δεδομένα προερχόμενα από ερευνητικά ερωτηματολόγια. Τα πρωτογενή δεδομένα (raw data) δεν έχουν υποστεί το φιλτράρισμα μιας θεωρίας, μιας ιδεολογίας ή μιας σκοπιμότητας ή έστω τούτο έχει λάβει χώρα με τρόπο και σε βαθμό που είναι γνωστός και αξιολογήσιμος. Για την επιστημονική κοινότητα η ύπαρξη των πρωτογενών δεδομένων είναι απολύτως απαραίτητη για την συζήτηση οποιαδήποτε ερευνητικού αποτελέσματος. Τα πρωτογενή δεδομένα (raw data) καθιστούν δυνατό τον έλεγχο και την επιβεβαίωση μιας θεωρίας, ενός πειραματικού αποτελέσματος ή ενός συμπεράσματος. Αντίθετα, έρευνες με δευτερογενή δεδομένα είναι εκείνες που αντλούν δεδομένα από στοιχεία τα οποία έχουν συλλέξει τρίτοι σε διαφορετικό χρονικό διάστημα και για σκοπούς άλλους από αυτούς που τα χρησιμοποιεί στον παρόντα χρόνο ο ερευνητής (π.χ.

[933] Εξάλλου, οι *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, όπ. π., σελ. 13 αναφέρονται σε "επιτιθέμενους" ("attackers") και «προστατευτές» ("protectors"), όπου «επιτιθέμενοι» κατά των συστημάτων πληροφοριών οι hackers απέναντι στους επαγγελματίες ("secutity professionals"), οι οποίοι σχεδιάζουν και υλοποιούν τις πρακτικές ασφαλείας των συστημάτων πληροφοριών.

[934] Βλ. ανωτέρω σχετική υποσημείωση για τις τεχνικές επιλογής δείγματος σκοπιμότητας και κατωτέρω για τον εντοπισμό του δείγματος hackers.

[935] *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 106.

αρχεία δικαστηρίων)[936]. Οι έρευνες αυτές μπορούν να διεξάγονται και με τη συγκέντρωση και αξιολόγηση στοιχείων που έχουν ήδη συλλεχθεί στο πλαίσιο προηγούμενης πρωτογενούς έρευνας.

Στην προκειμένη περίπτωση οι καταγραφείσες ανωτέρω υποθέσεις έρευνας σε επίπεδο αξιολόγησης της κείμενης νομοθεσίας, της αποκρυστάλλωσης της σύγχρονης έννοιας του hacking, της ανίχνευσης προτάσεων αντεγκληματικής πολιτικής και γενικότερα της καταγραφής της άποψης των ειδημόνων αλλά και των hackers μπορούν να καλυφθούν επιστημονικά μόνο με έρευνα σε πρωτογενή στοιχεία. Εξάλλου, πλην των αποφάσεων των ελληνικών δικαστηρίων (αναφορικά με την εφαρμογή της ελληνικής ποινικής νομοθεσίας), οι οποίες μπορούν να ανευρεθούν σε πηγές όπως τα επιστημονικά περιοδικά, δεν υπήρχε δυνατότητα και περίπτωση εύρεσης στοιχείων από δευτερογενείς πηγές, τα οποία να καλύπτουν τις ανωτέρω υποθέσεις έρευνας. Τέλος, η προσπάθεια για πρωτοτυπία της έρευνας επιτάσσει τη συλλογή πρωτογενών δεδομένων, τα οποία με τη σειρά τους θα οδηγήσουν στη διατύπωση πρωτογενών συμπερασμάτων, ιδίως σχετικά με τα ερευνητικά δεδομένα που θα προκύψουν από το δείγμα των hackers καθώς είναι ίσως η πρώτη εγκληματολογική έρευνα στην Ελλάδα σε δείγμα hackers.

7.3.2 Μέθοδος και τεχνική της έρευνας[937]

Η εγκληματολογία δεν απολαμβάνει την «ηρεμία του αξιώματος» - αυτή είναι και η μέγιστη ίσως πρόκληση που έχει να αντιμετωπίσει. Διαθέτει, ωστόσο, την «ηρεμία» της μεθόδου, η οποία έρχεται σε εμάς ήδη από τις σκέψεις του Αριστοτέλη[938] [939] [940].

---

[936] Βλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 106.

[937] Σημειώνεται ότι οι έννοιες «μέθοδοι» και «τεχνικές», αν και συχνά χρησιμοποιούνται εναλλακτικά, δεν είναι ταυτόσημες. Μέθοδος είναι ο τρόπος προσέγγισης της πραγματικότητας με σκοπό τη διάγνωση, την αιτιολόγηση ή την ερμηνεία ενός φαινομένου (πειραματική μέθοδος). Τεχνική είναι η τυποποιημένη εφαρμογή της μεθόδου (π.χ. τεχνική του ερωτηματολογίου) (έτσι *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 81).

[938] Βλ. *Ι. Φαρσεδάκης*, Η κοινωνική αντίδραση στο έγκλημα και τα όριά της. Μερικές ιστορικές, συγκριτικές και θεωρητικές επισημάνσεις, εκδ. Νομική Βιβλιοθήκη, Αθήνα 1991, σελ. 16.

[939] Πρβλ. *Η. Π. Νικολούδης (εισαγωγή και μετάφραση)*, ΑΡΙΣΤΟΤΕΛΗΣ – Άπαντα, τομ. 25ος, Όργανον 3, ΤΟΠΙΚΩΝ Ζ, Η, θ – Περί των σοφιστικών ελέγχων, Αρχαία ελληνική γραμματεία – οι Έλληνες, No 214, εκδ. Κάκτος.

[940] Πρβλ. αναφορικά με σύγχρονες εκφάνσεις της επιρροής του Αριστοτέλη στην εγκληματολογική σκέψη και *Β. Βλάχου*, Η ιστορική προσέγγιση της εγκληματικής προσωπικότητας υπό το πρίσμα της

Θα μπορούσε να ειπωθεί ότι υπάρχει ένας συνεχής κατανοητικός, εξηγητικός και ερμηνευτικός κύκλος που περιλαμβάνει, τόσο το φαινόμενο προς έρευνα, τη μέθοδο και τα ερευνητικά εργαλεία όσο και την ίδια την οπτική του ερευνητή.

7.3.2.1 Συνδυασμός ποιοτικής και ποσοτικής έρευνας

Η επιλογή των μεθόδων και η σωστή χρήση τους αποτελούν *αδιαμφισβήτητο κριτήριο για την επιστημονική εγκυρότητα μιας έρευνας*[941]. Ως προς τη στρατηγική συλλογής και ανάλυσης δεδομένων, προκρίθηκε ο *συνδυασμός*[942] *ποσοτικής*[943] *και ποιοτικής*[944] *έρευνας*[945]. Ενδεικτικά, η μεν ποσοτική ανάλυση θα μας βοηθήσει να καταλήξουμε σε συμπεράσματα, τα οποία αφού έχουν υποστεί στατιστική ενσωμάτωση θα είναι κατά το πλέον εύληπτα και κατανοητά. Η, δε, ποιοτική ανάλυση θα προσφέρει την ουσιαστικότερη καταγραφή απαντήσεων και τη λήψη υπόψιν του πραγματικού νοήματος αυτών. Ο συνδυασμός αυτος έρχεται σε συμφωνία με τον πλουραλισμό των μεθόδων που προκρίνεται για την προσέγγιση του αντικειμένου της εγκληματολογίας[946] και τη μίξη/σύνθεση αυτών (mixed research methods)[947] στο

αριστοτέλειας «συλλογιστικής»: Η μετουσίωση της αρχαιοελληνικής εγκληματολογικής σκέψης στη σύγχρονη κοινωνία, Εγκληματολογία, τευχ. 1, 2011, εκδ. Νομική Βιβλιοθήκη, σελ. 112-115.

[941] Βλ. σχετικά *Ν. Κυριαζή*, Η κοινωνιολογική έρευνα: Κριτική επισκόπηση των μεθόδων και τεχνικών, εκδ. Ελληνικά Γράμματα, Αθήνα 2005, σελ. 28.

[942] Κατά τον Παπάνη, οι δύο αυτές μέθοδοι θεωρούνται συμπληρωματικές. Βλ. *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 44 επ. όπου και ανάλυσή του για τη χρήση των μεθόδων έρευνας στο διαδίκτυο.

[943] Για τις ποσοτικές εγκληματολογικές έρευνες βλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 107.

[944] Για τις ποιοτικές εγκληματολογικές έρευνες βλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 108, *Γρ. Λάζο*, Το πρόβλημα της ποιοτικής έρευνας στις κοινωνικές επιστήμες – θεωρία και πράξη, εκδ. Παπαζήση, Αθήνα, 1998, *Jennifer Mason*, Η διεξαγωγή της ποιοτικής έρευνας, μετάφραση: *Ελένη Δημητριάδου*, επιστημονική επιμέλεια: *Νότα Κυριαζή*, εκδ. Ελληνικά Γράμματα, Αθήνα, 2010 καθώς και *Άννα Λυδάκη*, Ποιοτικές μέθοδοι της κοινωνικής έρευνας, εκδ. Καστανιώτη, Αθήνα, 2001. Για την ποιοτική έρευνα στο διαδίκτυο βλ. *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 80 επ.

[945] Για τη διαφορά μεταξύ ποσοτικών και ποιοτικών μεθόδων βλ. *Αν. Σταλίκα*, Μέθοδοι έρευνας στην ψυχολογία, όπ. π., σελ. 185 επ.

[946] Ο πλουραλισμός αυτός κατ' ουσίαν αναγνωρίζει την ύπαρξη μιας «πολυπαραδειγματικής» κατάστασης στον χώρο γενικότερα των κοινωνικών επιστημών, σε αντίθεση με την παλαιότερη κυριαρχία του ενός παραδείγματος. Επιπλέον, η σχέση μεταξύ αυτών των πολλών και διαφορετικών τάσεων δεν προσλαμβάνεται πάντοτε ως αντιθετική αλλά και ως συμπληρωματική (βλ. σχετικά *Ιωάννα Λαμπίρη – Δημάκη*, Η Κοινωνιολογία και η Μεθοδολογία της, Τόμος Α΄, Έβδομη συμπληρωμένη έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2003, σελ. 49-50). Σύμφωνα,

πλαίσιο «πολυμεθοδικών» προσεγγίσεων με σκοπό την αποτελεσματικότερη αντιμετώπιση των αδυναμιών της κάθε μεμονωμένης μεθοδολογίας, την πληρέστερη απάντηση των ερευνητικών ερωτημάτων, την αύξηση της εγκυρότητας των αποτελεσμάτων και την ευρύτητα και σφαιρικότητα στα ερευνητικά αποτελέσματα[948] [949]. Επιπρόσθετα, σημαντικός είναι ο συνδυασμός μεθόδων και για την επιβεβαίωση των αποτελεσμάτων και ερευνητικών ευρημάτων μέσα από τη χρήση πολλαπλών μεθόδων (*τριγωνισμός*). Ο συνδυασμός και η συμπληρωματικότητα διαφορετικών μεθοδολογικών προσεγγίσεων σε διαφορετικά στάδια της ίδιας ερευνητικής διαδικασίας συνδράμει, επίσης, και στη μεθοδολογική ανάπτυξη (με σκοπό την αρτιότερη κατάρτιση τεχνικής σε επόμενο στάδιο)[950] και παραπέμπει σε «υβριδικό μοντέλο»[951] έρευνας.

δε, με τον Φαρσεδάκη, υποχρέωση του ερευνητή είναι να επιλέξει, λαμβάνοντας υπόψη το διττό αντικείμενο της εγκληματολογίας (πέρασμα στην πράξη – κοινωνική αντίδραση) και τη διάκριση της έρευνας σε βασική και εφαρμοσμένη την κατάλληλη κάθε φορά μέθοδο, ανάλογα με τη θεματική της έρευνάς του και το επίπεδο ερμηνείας στο οποίο επιθυμεί να επικεντρωθεί (έτσι *Ι. Φαρσεδάκης*, Στοιχεία Εγκληματολογίας, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 1996, σελ. 138).

[947] Αναφορικά με τις συνδυασμένες ερευνητικές μεθόδους βλ. *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 27 επ.

[948] Για τον υπερκερασμό των προβλημάτων που προκύπτουν από τη χρήση μίας μόνο μεθοδολογικής προσέγγισης όσο και για την ενίσχυση της επικύρωσης των ερευνητικών πορισμάτων έχει επιχειρηθεί η μίξη ή η σύνθεση διαφορετικών μεθόδων έρευνας (mixed research methods). Βασικά επιχειρήματα που τάσσονται υπέρ αυτής της προσέγγισης είναι ότι αυξάνεται η εγκυρότητα των αποτελεσμάτων, εφόσον προκύπτουν παρόμοια συμπεράσματα από διαφορετικά μεθοδολογικά εργαλεία (π.χ. ερωτηματολόγια, συνεντεύξεις, συμμετοχική παρατήρηση) ενώ παράλληλα διευκολύνεται η προσέγγιση διαφορετικών οπτικών θέασης με συνέπεια να αυξάνεται η αναλυτική πυκνότητα που αφορά την απάντηση στο εκάστοτε ερευνητικό ερώτημα με περιορισμό των μειονεκτημάτων κάθε μεμονωμένης μεθόδου [βλ. αναλυτικά *Αναστασία Χαλκιά*, Σκέψεις για τη δόμηση και τη μελέτη των αντικειμένων έρευνας στην Εγκληματολογία, ΠοινΔικ & Εγκληματολογία 1/2010 (Έτος 2ο), σελ. 44].

[949] Βέβαια, κατά τον *Feyerabend* «*όλες οι μεθοδολογίες, ακόμα και οι πιο ευνόητες έχουν τα όριά τους*» (βλ. *P. Feyerabend*, Ενάντια στη μέθοδο. Για μία αναρχική θεωρία της γνώσης, Μετάφραση; *Γ. Καυκαλάς & Γ. Γκουνταρούλης*, Εκδόσεις Σύγχρονα Θέματα, Αθήνα 1991, σελ. 64).

[950] Βλ. κεφάλαιο με τίτλο «Πολυμεθοδολογικές προσεγγίσεις και τριγωνισμός» στο πόνημα του *Θ. Ιωσηφίδη,* Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 274 επ.

[951] Οι μικτές ερευνητικές μέθοδοι μπορούν να ταξινομηθούν σε αυτές που υιοθετούν «διαδοχικούς σχεδιασμούς» (sequential designs) και σε «υβριδικά μοντέλα» (hybrid models). Σύμφωνα με την πρώτη ταξινόμηση, στην αρχή διεξάγεται ποιοτική και μετά ποσοτική έρευνα ή το αντίστροφο. Κατά βάση οι μέθοδοι «διαδοχικού σχεδιασμού» συνιστούν δύο μελέτες με κοινό ερευνητικό ερώτημα. Το μοντέλο αυτό εντάσσεται περισσότερο στη διαδικασία της τριγωνοποίησης (triangulation). Τα είδη τριγωνοποίησης διακρίνονται σε τριγωνοποίηση δεδομένων (τεχνικές δειγματοληψίας), ερευνητών (χρήση περισσότερων του ενός ερευνητών στη συλλογή και κατανόηση των δεδομένων), μεθοδολογίας (χρήση περισσότερων της μιας μεθόδου) και θεωρητικού πλαισίου (χρήση περισσότερων της μιας θεωρητικών θέσεων για την κατανόηση των δεδομένων). Από την άλλη πλευρά, τα «υβριδικά μοντέλα» θεωρούνται περισσότερο συνθετικά και αφορούν συνδυασμό διαφορετικών μεθοδολογικών προσεγγίσεων σε διαφορετικά στάδια της ίδιας ερευνητικής διαδικασίας [βλ. *S. Maruna*, Mixed method research in Criminology: Why not go both ways σε: *A. Piquero & D. Weisburd* (Επιμ.), Handbook of Quantitative Criminology, London: Springer 2010, σελ. 126-127].

7.3.2.2 Τεχνικές της έρευνας (ερωτηματολόγιο και επικουρικά συνέντευξη με hackers, ανάλυση περιεχομένου και δευτερογενών δεδομένων)

Ως βασική τεχνική για τη διενέργεια της έρευνας επελέγη η *τεχνική του ερευνητικού ερωτηματολογίου*[952] (ως μεθοδολογικό εργαλείο της έρευνας με πρωτογενή δεδομένα)[953]. Το ερωτηματολόγιο[954] στην πράξη αποτελεί δύσκολο ερευνητικό εγχείρημα[955] καθώς η κατάρτισή του απαιτεί προσοχή και εξειδικευμένες επιστημονικές γνώσεις[956].

Εν προκειμένω, καταρτίστηκαν τρία διαφορετικά ερωτηματολόγια (ένα για κάθε δείγμα – νομικοί, επιστήμονες πληροφορικής και hackers) με συνδυασμό «ανοικτών» ερωτήσεων[957], οι οποίες αφήνουν περιθώριο στον ερωτώμενο για μία προσωπική απάντηση και «κλειστών» ερωτήσεων, οι οποίες περιέχουν εναλλακτικές απαντήσεις προκειμένου ο ερωτώμενος να δυναται να επιλέξει. Μολονότι αναγνωρίζεται ότι η κωδικοποίηση των απαντήσεων σε ανοικτές ερωτήσεις είναι έργο δύσκολο και επίπονο και γι' αυτό σε πολλές έρευνες διατυπώνονται μόνον κλειστές ερωτήσεις[958], η συμπερίληψη στα ερωτηματολόγια και ανοιχτών ερωτήσεων προκρίθηκε ως αναγκαία προκειμένου να καταστεί πληρέστερη η ποιοτική ανάλυση των ερευνητικών δεδομένων και να εξαχθούν πιο βάσιμα και αξιοποιήσιμα συμπεράσματα. Στις περιπτώσεις των ανοικτών ερωτήσεων, λοιπόν, η κωδικοποίηση

---

[952] Αναφορικά με την τεχνική του ερωτηματολογίου πρβλ. *David Nachmias & Chava Nachmias*, Research Methods in the Social Sciences, St. Martin's Press, New York, 1987, 3rd ed., pp. 253-283 και τις αναπτύξεις του *Χρήστου Κελπερή* εις *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 299 επ.

[953] Βλ. *Καλλιόπη Δ. Σπινέλλη*, Εγκληματολογία –Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π, σελ. 106.

[954] Αναλυτικά για το περιεχόμενο, τη μορφή, την κατασκευή του ερωτηματολογίου κ.λπ. βλ. *Β. Φίλια (γεν. εποπτ.)*, Εισαγωγή στη μεθοδολογία και τις τεχνικές κοινωνικών ερευνών, όπ. π., σελ. 145 επ.

[955] *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 125.

[956] Έχουν γραφτεί σημαντικά πονήματα σχετικά με τον τρόπο (ή την «τέχνη») με τον οποίο πρέπει να διατυπώνονται οι ερωτήσεις (the art of asking questions). Εντελώς τηλεγραφικά επισημαίνεται ότι οι ανόητες ερωτήσεις εκμαιεύουν ανόητες απαντήσεις (!) ενώ οι αποκαλούμενες «καθοδηγητικές» ερωτήσεις (leading questions, π.χ. είστε κατά της θανατικής ποινής;) πρέπει απαραιτήτως να αποφεύγονται προκειμένου να διασφαλίζεται η εγκυρότητα των απαντήσεων, κυρίως με το να εκφράζεται μέσα από αυτές η όσο το δυνατόν περισσότερο ανεπηρέαστη γνώμη ή στάση του ερευνώμενου. Βλ. για περισσότερα *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1995, σελ. 299 επ.

[957] Για τις «ανοιχτές» και «κλειστές» ερωτήσεις και τα πλεονεκτήματα και τα μειονεκτήματά τους βλ. τις αναπτύξεις του *Χρήστου Κελπερή* εις *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 301 επ.

[958] Βλ. αναλυτικά *Ιωάννα Λαμπίρη – Δημάκη*, Η Κοινωνιολογία και η Μεθοδολογία της, όπ. π. 124-125.

των απαντήσεων πραγματοποιείται μετά το πέρας της συμπλήρωσης και κατά το στάδιο της επεξεργασίας των ερωτηματολογίων (σε αντίθεση με τις κλειστές ερωτήσεις που η κωδικοποίηση αυτή λαμβάνει χώρα εξαρχής), με βάση τις ποικίλες απαντήσεις που θα δοθούν, τις οποίες ο ερευνητής κατατάσσει σε κατηγορίες ομοειδών απαντήσεων.

Κατά την κατάρτιση των ερωτηματολογίων ελήφθη, βέβαια, υπόψιν η δυνατότητα να υπάρχει σύγκριση των απαντήσεων και των τριών μερών για την εξαγωγή ερευνητικών συμπερασμάτων. Για αυτόν τον λόγο, εξάλλου, οι περισσότερες ερωτήσεις στα δείγματα νομικών και επιστημόνων πληροφορικής είναι κοινές[959].

Επιπρόσθετα, στο πλαίσιο της ποιοτικής διάστασης της έρευνας χρησιμοποιήθηκε επικουρικά η τεχνική της μη δομημένης («ανοιχτής)[960] συνέντευξης[961] με hackers (μέλη της ομάδας hackerspace.gr – βλ. κατωτέρω), η ανάλυση περιεχομένου[962] στα μηνύματα της ηλεκτρονικής επικοινωνίας με τους hackers καθώς και η αναζήτηση και ανάλυση δευτερογενών δεδομένων (όπως η επισκόπηση της νομολογίας των ελληνικών ποινικών δικαστηρίων για την χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα[963]).

[959] Βλ. κατωτέρω παράγραφο 7.7.3.

[960] Αναφορικά με την μη δομημένη συνέντευξη στην ποιοτική έρευνα βλ. *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 112. Ο Λάζος αναφέρεται εν προκειμένω σε «ανοιχτή» συνέντευξη (βλ. *Γρ. Λάζο*, Το πρόβλημα της ποιοτικής έρευνας στις κοινωνικές επιστήμες – θεωρία και πράξη, εκδ. Παπαζήση, Αθήνα, 1998, σελ. 293 επ.).

[961] Αναφορικά με τη συνέντευξη βάθους πρβλ. *Άννα Λυδάκη*, Ποιοτικές μέθοδοι της κοινωνικής έρευνας, εκδ. Καστανιώτη, Αθήνα, 2001, σελ. 256 επ. Επίσης, βλ. για την τεχνική της συνέντευξης το άρθρο της Καθηγήτριας και συμβούλου εκπαίδευσης ενηλίκων στο ΕΑΠ (Ελληνικό Ανοικτό Πανεπιστήμιο) *Κατερίνας Κεδρακά*, Μεθοδολογία λήψης συνέντευξης, url: https://docs.google.com/document/d/1Ns81KOslEHm0PKruMXSgV-xe9gtye6Npp-x2KgROlBs/edit?hl=en καθώς και *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 126, *Jennifer Mason*, Η διεξαγωγή της ποιοτικής έρευνας, μετάφραση: *Ελένη Δημητριάδου*, επιστημονική επιμέλεια: *Νότα Κυριαζή*, εκδ. Ελληνικά Γράμματα, Αθήνα, 2010, σελ. 83 επ. και *Αν. Σταλίκα*, Μέθοδοι έρευνας στην ψυχολογία, εκδ. Ελληνικά γράμματα, Αθήνα, 2005, σελ. 207 επ.

[962] Για την ανάλυση περιεχομένου πρβλ. ενδεικτικά *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 147 (και ιδίως λεπτομερή πίνακα αναφορικά με τα πλεονεκτήματα και τα μειονεκτήματα της ανάλυσης περιεχομένου στη σελ. 148) και το αναλυτικό πόνημα της *Ιωάννας Τσίγκανου*, Ανάλυση περιεχομένου, Εθνικό Κέντρο Κοινωνικών Ερευνών καθώς και *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 134.

[963] Πρβλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 132 επ. και συγκεκριμένα το κεφάλαιο «Έρευνες σε αρχεία, σε έγγραφα και σε άλλα κείμενα».

7.4 Η ερευνητική ομάδα

Η ερευνητική ομάδα[964] συγκροτήθηκε από μέλη του Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών (Διευθυντής: Καθηγητής Νέστωρ Κουράκης) και του Σπουδαστηρίου Κοινωνικών Μελετών του ΑΤΕΙ Δυτικής Ελλάδος (Διευθυντής: Καθηγητής Χρήστος Τσουραμάνης) τον Ιούνιο του 2013 με συντονιστή τον γράφοντα.

Στην ερευνητική ομάδα συμμετείχαν οι: *Ευαγγελία Ανδρουλάκη* (δικηγόρος – υπ. ΜΔΕ Εγκληματολογίας Παντείου Πανεπιστημίου), *Καλλιόπη Πιτερού* (δικηγόρος – ποινικολόγος – ΜΔΕ Παντείου Πανεπιστημίου), *Φώτης Δασκαλάκης* (τεχνικός ασφαλείας δικτύων – διαχειριστής ηλεκτρονικών δεδομένων) και *Ιωάννα Καρναχωρίτη* (φοιτήτρια Νομικής Αθηνών).

Ειδικός επιστημονικός σύμβουλος της έρευνας σε θέματα τεχνολογίας και ασφάλειας ηλεκτρονικών δεδομένων υπήρξε ο *Ηλίας Πολυχρονιάδης* (επιστήμονας πληροφορικής, τεχνικός ασφαλείας δικτύων - MSc)[965].

Η ερευνητική ομάδα και ο ειδικός σύμβουλος συμμετείχαν στην κατάρτιση των ερωτηματολογίων, στην τεχνική επεξεργασία και αποστολή και στην επεξεργασία των αποτελεσμάτων καθώς και επικουρικά στην αναζήτηση βιβλιογραφίας.

7.5 Ο εντοπισμός του δείγματος της έρευνας

7.5.1 Κατάρτιση, κοινοποίηση και συμπλήρωση των ερωτηματολογίων

[964] Αναφορικά με τη συγκρότηση ερευνητικών ομάδων ως ερευνητικό υποκείμενο βλ. *Γρ. Λάζο*, Το πρόβλημα της ποιοτικής έρευνας στις κοινωνικές επιστήμες – θεωρία και πράξη, εκδ. Παπαζήση, Αθήνα, 1998, σελ. 343 επ.

[965] Και από τη θέση αυτή τους ευχαριστώ όλους από καρδιάς για την πολύτιμη βοήθειά τους!

Για τη διεξαγωγή της έρευνας καταρτίστηκαν τρία διαφορετικά διαδικτυακά ερωτηματολόγια[966] (ένα για κάθε δείγμα), κοινοποιήθηκαν αυτά αντιστοίχως στους συμμετέχοντες από κάθε δείγμα μέσω διαδικτύου και υπεβλήθησαν συμπληρωμένα και πάλι μέσω διαδικτύου, όπως κατωτέρω αναλύεται.

Ειδικότερα, αναφορικά με τον εντοπισμό του δείγματος, όλο το δείγμα προσεγγίστηκε μέσω διαδικτύου[967], προκειμένου αυτοί που απαντούν να έχουν μια έστω τυπική σχέση με ηλεκτρονικά δεδομένα, διαδικτυακή παρουσία και συνεπώς ενδιαφέρον για την ασφάλεια ηλεκτρονικών δεδομένων (π.χ. ένας νομικός χωρίς καμία διαδικτυακή παρουσία και σχέση με το διαδίκτυο σε κάθε περίπτωση πιστεύω ότι θα αδυνατούσε να απαντήσει στο σχετικό ερωτηματολόγιο καθώς το υπό συζήτηση θέμα δεν τον αφορά ή έστω δεν τον έχει απασχολήσει!)[968]. Εξάλλου, κατα τον Παπάνη, η ευρεία χρήση του διαδικτύου διασφαλίζει τις βασικές αρχές αντιπροσωπευτικότητας και τυχαιότητας του δείγματος[969]. Τα ηλεκτρονικά ερωτηματολόγια[970], τα οποία καταρτίστηκαν για τη διενέργεια της έρευνας, και πάλι κοινοποιήθηκαν στο δείγμα μέσω διαδικτύου και οι απαντήσεις καταχωρήθηκαν ανώνυμα μέσω διαδικτύου[971] [972]. Επιπρόσθετα, επιλέχθηκε να μην επιλεγεί ο εύκολος

---

[966] Για τα διαδικτυακά ερωτηματολόγια βλ. *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 63.

[967] Ο Παπάνης αναπτύσσει εύστοχες σκέψεις αναφορικά με την ερμηνεία και τη θέαση του διαδικτύου ως (δημόσιο ή ιδιωτικό) χώρο ή ως κοινότητα και, συνεπώς, τη χρήση διαφορετικών κριτηρίων κάθε φορά εκ μέρους των ερευνητών στις αναλύσεις τους ανάλογα με τη θέση την οποία ασπάζονται (πρβλ. *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 44 επ. και σελ. 54).

[968] Η επιλογή μιας συγκεκριμένης μεθόδου, μιας τεχνικής και γενικότερα του τρόπου σχεδιασμού της έρευνας επηρεάζεται και τελικά (πρέπει να) καθορίζεται από τη φύση του θέματος ή του διερευνώμενου ζητήματος αλλά και από άλλους παράγοντες, όπως είναι τα πλεονεκτήματα και μειονεκτήματα κάθε μεθόδου και τεχνικής, το μέγεθος της ερευνητικής ομάδας, τα ερευνητικά κονδύλια κ.λπ. (βλ. αναλυτικότερα *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 47 επ.).

[969] Βλ. *Ευστράτιο Παπάνη*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 41. Βέβαια, κατά τον *Ιωσηφίδη* η έννοια της αντιπροσωπευτικότητας δεν έχει νόημα σε ό,τι αφορά ποιοτική έρευνα (βλ. σχετική άποψη και δικαιολόγηση αυτής στο πόνημά του: Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 58 επ.).

[970] Πρβλ. σχετικά *Θεόδωρος Χ. Κασκάλης, Αθανάσιος Α. Μαλέτσκος, Κωνσταντίνος Ε. Ευαγγελίδης*, Χρήση και αξιοποίηση ηλεκτρονικών ερωτηματολογίων σε έναν εκπαιδευτικό δικτυακό τόπο, Τμήμα Νηπιαγωγών, Παιδαγωγική Σχολή, Πανεπιστήμιο Δυτικής Μακεδονίας, url: http://www.etpe.eu/new/custom/pdf/etpe43.pdf, σελ. 457.

[971] Για την κατάρτιση, συμπλήρωση και συλλογή των ερωτηματολογίων χρησιμοποιήθηκε η πλατφόρμα googledocs της ιστοσελίδας www.google.com. Εκεί δημιουργήθηκαν τρεις διαφορετικές φόρμες ερωτηματολογίων (για νομικούς, για επιστήμονες πληροφορικής και για hackers). Κάθε φόρμα είχε λάβει ένα διαφορετικό url, το οποίο απεστάλη στο οικείο δείγμα. Ο συμμετέχων στην έρευνα ακολουθούσε το συγκεκριμένο url και απαντούσε ανώνυμα σε όλες τις ερωτήσεις του ερωτηματολογίου. Στο τέλος του ερωτηματολογίου υπήρχε η επιλογή «Υποβολή»/ "Submit" – εφόσον ο ερωτώμενος είχε απαντήσει σε όλες τις ερωτήσεις η επιλογή αυτή ενεργοποιείτο. Με την επιλογή «Υποβολή»/ "Submit" εκ μέρους του συμμετέχοντος στο δείγμα της έρευνας οι απαντήσεις

(!) δρόμος της ανάρτησης σε «κοινή θέα» των ερωτηματολογίων, προκειμένου να αποφευχθεί η περίπτωση να απαντήσουν σε αυτό «άσχετοι» με το δείγμα σκοπιμότητας. Με άλλα λόγια, χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης, το ερωτηματολόγιο εστάλη μόνο σε περιπτώσεις όπου υπήρχε η δυνατότητα, έστω με έναν κατά δήλωση του ερωτώμενου τρόπο, να ελεγχθεί η πραγματική ιδιότητα βάσει της οποίας ο ίδιος απαντάει (βλ. κατωτέρω ειδική ανάλυση και επεξήγηση για κάθε δείγμα[973]).

7.5.2 Η προβληματική της χρήσης του διαδικτύου ως εργαλείου στην έρευνα

Ο Bachmann επισημαίνει προβλήματα τα οποία ενδεχομένως υπάρχουν σε περιπτώσεις έρευνας με εργαλείο το διαδίκτυο και σε περιπτώσεις διαδικτυακής συμπλήρωσης των ερωτηματολογίων[974]. Καταρχάς, οι ερευνητές δεν έχουν άμεση πρόσβαση στο δείγμα – συνεπώς, υπάρχει περίπτωση το δείγμα να παραμένει ασαφές και να υπάρχουν προβλήματα όπως η έλλειψη δυνατότητας εκτίμησης των ποσοστών των αναπάντητων ερωτηματολόγιων (στην περίπτωση ερευνών μέσω Internet τα ποσοστά αυτά φαίνονται υψηλότερα σε σχέση με τις παραδοσιακές μεθόδους). Επιπρόσθετα, το περιβάλλον στο οποίο οι ερωτώμενοι απαντούν στο ερωτηματολόγιο και συμμετέχουν στην έρευνα είναι εντελώς έξω από τον έλεγχο ή την επιρροή του ερευνητή[975]. Επίσης, στη διαδικτυακή έρευνα δεν επιτρέπεται καμία αλληλεπίδραση μεταξύ συμμετεχόντων και ερευνητή, προκειμένου να εξασφαλισθεί η κατανόηση των ερωτηματολογίων εκ μέρους του συμμετέχοντος, η ποιότητα και η σοβαρότητα

καταχωρούνταν αυτόματα στην ήδη δημιουργηθείσα βάση δεδομένων του ερευνητή προς περαιτέρω επεξεργασία και ανάλυση.

[972] Για τα πλεονεκτήματα της διενέργειας ερευνών μέσω διαδικτύου και γενικότερα μέσω νέων τεχνολογιών βλ. το κεφάλαιο «Οι νέες τεχνολογίες στην κοινωνική έρευνα» στο πόνημα *Β. Φίλια (γεν. εποπτ.)*, Εισαγωγή στη μεθοδολογία και τις τεχνικές κοινωνικών ερευνών, όπ. π., σελ. 455 επ.

[973] ... παράγραφοι 7.5.3, 7.5.4 και 7.5.5 του παρόντος πονήματος.

[974] *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 71-72.

[975] Κυρίως προκειμένου να παράσχει εξηγήσεις σε περίπτωση παρερμηνείας των ερωτήσεων – βλ. και κατωτέρω παράγραφο 7.6 αναφορικά με περιορισμούς της έρευνας.

στην απάντηση του ερωτηματολογίου[976]. Παρόλα, βέβαια, τα ανωτέρω, ο ίδιος αποδέχεται ότι η τεχνολογική εξέλιξη καθορίζει σε σημαντικό βαθμό τις δυνατότητες των εργαλείων και την ανάπτυξη πιο σύγχρονων προοπτικών μελέτης του εγκληματικού φαινομένου, επισημαίνοντας ουσιαστικά την πρόκληση που υπάρχει σε περιπτώσεις διαδικτυακών ερευνών.

Από την άλλη, όμως, πλευρά, καταγράφονται και αρκετά θετικά στοιχεία στην χρήση του διαδικτύου ως ερευνητικού εργαλείου. Το διαδίκτυο δύναται να συνδράμει ούτως ώστε να αποφευχθεί η κόπωση των ερωτώμενων, να μειωθεί το κόστος της έρευνας και να καταστεί ευκολότερη η αποθήκευση και επεξεργασία των ερωτηματολογίων[977]. Επιπρόσθετα, αίρονται περιορισμοί όσον αφορά στην απόσταση κατοικίας ή εργασίας των ερωτώμενων, στον χρόνο συλλογής στοιχείων, καθώς και στον αριθμό των συμμετεχόντων στην έρευνα[978] [979].

Τα ανωτέρω ζητήματα ελήφθησαν υπόψιν κατά τον σχεδιασμό της έρευνας προκειμένου να εξασφαλιστεί η κατά το δυνατόν μεγαλύτερη εγκυρότητα των συλλεχθέντων στοιχείων[980]. Οι λύσεις που προκρίθηκαν για την επίτευξη αυτού του στόχου ήταν η απλή και κατανοητή διατύπωση των ερωτήσεων, η συνεκτικότητα κάθε ερωτηματολογίου προκειμένου να προκύπτει σαφώς η γενικότερη στάση του συμμετέχοντος για το hacking, οι ερωτήσεις επαλήθευσης εντός του ερωτηματολογίου (reality testing) [981] [982] καθώς και η ανάδειξη ως ερευνητικού δεδομένου και των «μη σοβαρών» απαντήσεων (εφόσον υπάρξουν τέτοιες).

---

[976] Να σημειωθεί βέβαια ότι αντίστοιχα ζητήματα υπάρχουν σε κάθε περίπτωση αυτοσυμπληρούμενου ερωτηματολογίου το οποίο π.χ. αποστέλλεται ταχυδρομικώς (πρβλ. για το αυτοσυμπληρούμενο ερωτηματολόγιο *Ν. Κυριαζή*, Η κοινωνιολογική έρευνα – Κριτική επισκόπηση των μεθόδων και των τεχνικών, εκδ. Πεδίο, Αθήνα, 2011, σελ. 119 επ.).

[977] *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 75.

[978] Βλ. σχετικά *Θεόδωρος Χ. Κασκάλης, Αθανάσιος Α. Μαλέτσκος, Κωνσταντίνος Ε. Ευαγγελίδης*, Χρήση και αξιοποίηση ηλεκτρονικών ερωτηματολογίων σε έναν εκπαιδευτικό δικτυακό τόπο, Τμήμα Νηπιαγωγών, Παιδαγωγική Σχολή, Πανεπιστήμιο Δυτικής Μακεδονίας, url: http://www.etpe.eu/new/custom/pdf/etpe43.pdf, σελ. 458.

[979] Πρβλ. και *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008 το κεφάλαιο με τίτλο «Ο ρόλος των ηλεκτρονικών υπολογιστών στην ποιοτική ανάλυση», σελ. 192 επ.

[980] Αναφορικά με τις σύγχρονες τάσεις στη διεξαγωγή της έρευνας πρβλ. το ομώνυμο κεφάλαιο στο πόνημα του *Γ. Πανούση*, Εγκληματολογία, εγκληματολογική έρευνα και ΜΜΕ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1999, σελ. 71 επ.

[981] Οι ερωτήσεις ελέγχου διατυπώνονται και στο πλαίσιο της αξιολογικής διάστασης του «αναστοχασμού» των στοιχείων που έχουν συλλεχθεί σχετικά με την εγκυρότητά τους (π.χ. εάν οι ερωτώμενοι είναι αντιπροσωπευτικοί της υπό εξέτασης ομάδας, εάν οι απαντήσεις που δόθηκαν είναι αποτέλεσμα υπερβολής ή ανειλικρίνειας).

7.5.3 Το δείγμα των νομικών

Ο εντοπισμός των ερωτώμενων νομικών και η συμπλήρωση του αντίστοιχου ερωτηματολογίου από μέρους τους υπήρξε αναμφίβολα πιο εύκολο εγχείρημα συγκριτικά με εκείνο των hackers, όπως παρουσιάζεται κατωτέρω. Η ομάδα στην ιστοσελίδα www.facebook.com[983] με την ονομασία «Δικηγόροι», η οποία στις 07.07.2014 απαριθμούσε 3.871 μέλη και στην οποία κατά τεκμήριο γίνονται δεκτοί νομικοί (αποτελεί, δε, μία σημαντική συλλογική προσπάθεια ενημέρωσης και ανταλλαγής απόψεων μεταξύ των νομικών), υπήρξε ο χώρος «υποδοχής» του σχετικού ερωτηματολογίου προς το δείγμα των νομικών. Ειδικότερα, το ερωτηματολόγιο για τους νομικούς κοινοποιήθηκε στην εν λόγω ομάδα στις 07.07.2013 και μέχρι τις 31.07.2013, οπότε και απενεργοποιήθηκε η δυνατότητα υποβολής ερωτηματολογίων, είχαν απαντηθεί 158 ερωτηματολόγια.

Γενικότερα, ο αναστοχασμός, ως άσκηση μιας ειδικής μορφής επιστημολογικής εγρήγορσης, αποτελεί εκείνη τη διαδικασία με την οποία η επιστήμη θέτει τον εαυτό της ως αντικείμενο, χρησιμοποιεί δηλαδή τα ίδια της τα όπλα για να αυτο-κατανοηθεί και να αυτο-ελεγχθεί. Συγκεκριμένα, ο αναστοχασμός έχει πρώτον μία περιγραφική διάσταση αναφορικά με τις αποφάσεις που πρέπει να ληφθούν ως προς την επιλογή του δείγματος και των τεχνικών καταγραφής των δεδομένων και δεύτερον μία αξιολογική διάσταση σχετικά με την πιθανή εγκυρότητα των στοιχείων που έχουν συλλεχθεί, όπως ανωτέρω στην εν λόγω υποσημείωση περιγράφηκε. Στην ευρύτερη προοπτική του, όμως, ο αναστοχασμός αναφέρεται στην κριτική σχετικά με τις δυνατότητες και τα όρια της έρευνας καθώς και της συμμετοχής της έρευνας στην παραγωγή της εγκληματολογικής γνώσης (σχετικά με τον αναστοχασμό βλ. *P. Bourdieu*, Επιστήμη της επιστήμης και αναστοχασμός, Μετάφραση: Θ. Παραδέλλης, Εκδόσεις Πατάκη, Αθήνα 2005, σελ. 199).

[982] Κατά τη Σπινέλλη, ενδείκνυται το ερωτηματολόγιο να περιλαμβάνει μία σχετική ερώτηση σε άλλο σημείο του, ώστε να είναι εφικτό να ελεγχθεί η ειλικρίνεια ή η ορθότητα της απάντησης [π.χ. 1η ερώτηση: *αν μπορούσατε να εκφράσετε τη γνώμη σας για την εφαρμογή του ευρωπαϊκού εντάλματος σύλληψης στην Ελλάδα θα ήσασταν υπέρ ή κατά;* - μετά από αρκετές ερωτήσεις, ο ερωτών επανέρχεται με την ερώτηση «*μήπως γνωρίζετε τι είναι το ευρωπαϊκό ένταλμα σύλληψης;*» (βλ. *Καλλιόπη Δ. Σπινέλλη*, Εγκληματολογία –Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π. σελ. 125-126)].

[983] Πρβλ. αναπτύξεις του Ευστράτιου Παπάνη αναφορικά με ανάλυση περιεχομένου σε 1500 προφίλ της ιστοσελίδας www.facebook.com (*Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 66 επ.).

7.5.4 Το δείγμα των επιστημόνων πληροφορικής (προγραμματιστές, τεχνικοί δικτύων ηλεκτρονικών υπολογιστών και διαχειριστές ηλεκτρονικών δεδομένων)

Για τον εντοπισμό του δείγματος επιστημόνων πληροφορικής χρησιμοποιήθηκε ομοίως η ιστοσελίδα κοινωνικής δικτύωσης www.facebook.com. Συγκεκριμένα, ελλείψει σχετικής ομάδας επαγγελματιών (όπως ανωτέρω η ομάδα «Δικηγόροι), χρησιμοποιήθηκε η λειτουργία «Αναζήτηση» της ως άνω σελίδας και αναζητήθηκαν επιχειρήσεις που διαθέτουν «προφίλ» στην ως άνω ιστοσελίδα στα λήμματα: *Η/Υ, ηλεκτρονικός υπολογιστής, πληροφορική, δίκτυα, λογισμικό, ασφάλεια διαδικτύου, computer service, προγραμματιστής*. Προκειμένου να εξακριβωθεί ότι το συγκεκριμένο προφίλ, στο οποίο εστάλη το ερωτηματολόγιο, ανήκει σε παρέχοντα υπηρεσίες πληροφορικής, έγινε έλεγχος για το αν αναφέρονται στο συγκεκριμένο προφίλ και τα στοιχεία της επιχείρησης όπως έδρα, παρεχόμενες υπηρεσίες κ.λπ. Επομένως, το ερωτηματολόγιο αυτό εστάλη σε σύνολο 245 επιχειρήσεων που πληρούσαν τα ως άνω κριτήρια. Η αποστολή των ερωτηματολογίων άρχισε στις 04.11.2013. Η εφαρμογή υποβολής απαντήσεων έμεινε ανοιχτή από τις 05.11.2013 έως τις 30.11.2013 και υπεβλήθησαν συνολικά 104 ερωτηματολόγια.

7.5.5 Το δείγμα των hackers

7.5.5.1 Οι hackers στην Ελλάδα[984]

Το hacking στην Ελλάδα φαίνεται να εμφανίζεται αρκετά αργότερα σε σχέση με τις πρώτες εκφάνσεις του στο εξωτερικό[985]. Η πρώτη επίθεση από hackers στην Ελλάδα φαίνεται να λαμβάνει χώρα τα Χριστούγεννα του 1993 στο δίκτυο «Αριάδνη» του

[984] Βλ. το αναλυτικό ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy, στο οποίο και παρουσιάζεται η ιστορία του hacking στην Ελλάδα.

[985] Βλ. παράγραφο 2.2 και γενικότερα κεφάλαιο 2 του παρόντος πονήματος.

Ερευνητικού Κέντρου «Δημόκριτος». Έπειτα, υποστηρίζεται ότι περίπου το έτος 1995 η κοινότητα των hackers αποκτά πιο οργανωμένη μορφή και αρχικά αποτελείται από περίπου δέκα φοιτητές σε ακαδημαϊκά ιδρύματα στην Αθήνα, την Πάτρα και τη Βόρεια Ελλάδα. Ο τρόπος επικοινωνίας μεταξύ τους είναι το BBS (Bulletin Board Services), μια μορφή ηλεκτρονικού πίνακα ανακοινώσεων, ιδιαίτερα δημοφιλούς πριν από την εξάπλωση του διαδικτύου. Την εποχή εκείνοι αρκετοι από τους hackers ασχολούνταν και με το "phreaking"[986], την αναζήτηση, δηλαδή, τρόπων για να διενεργούν τηλεφωνικές συνομιλίες χωρίς να χρεώνονται. Επίσης, οι πρακτικές hacking είχαν ως επίκεντρο περισσότερο τις «φάρσες» με την εκμετάλλευση της ψηφιακής τεχνολογίας.

Το 1999 οι Ελληνες hackers εντείνουν τη δράση τους. Αποκτούν ως σημείο αναφοράς την ιστοσελίδα hack.gr[987], στην οποία αναρτούν κείμενο διαμαρτυρίας για τις ακριβές χρεώσεις στις τηλεπικοινωνίες[988], δημοσιεύουν ειδήσεις για δραστηριότητες hacking στο εξωτερικό, ανταλλάσσουν απόψεις και γνώσεις και παρουσιάζουν αναλυτικά τις δράσεις τους (κυρίως τις αλλοιώσεις περιεχομένου ιστοσελίδων – "defacements"). Η δραστηριότητά τους εκείνη την περίοδο περιλαμβάνει και επιθέσεις στο Υπουργείο Εξωτερικών (με αφορμή την υπόθεση Οτσαλάν), στο Υπουργείο Εσωτερικών κ.λπ. Η πιο γνωστή, όμως, επιδρομή ελλήνων hackers φαίνεται ότι συντελέσθη τον Νοέμβριο του 1999, οπότε και απέκτησαν μέσω των servers Πανεπιστημίων της Αθήνας, της Θεσσαλονίκης και της Κρήτης χωρίς δικαίωμα πρόσβαση στη στρατιωτική βάση της Αριζόνα στις ΗΠΑ – οι δράστες της πράξης αυτής δεν εντοπίστηκαν ποτέ. Τον Ιούλιο του 2000 λαμβάνουν χώρα οι πρώτες συλλήψεις hackers στην Ελλάδα[989] [990].

---

[986] Βλ. και ανωτέρω στην παράγραφο 2.4 όπου το "phone-phreaking" περιγράφεται ως δραστηριότητα της δεύτερης γενιάς των hackers, των οποίων τις πρακτικές λογικό είναι ότι υιοθέτησαν οι πρώτοι έλληνες hackers.

[987] Η ιστοσελίδα hack.gr φαίνεται να συνεχίζει τη λειτουργία της μέχρι το 2005. Σήμερα, η νέα γενιά hackers επισκέπτεται αρκετά συχνά την ιστοσελίδα secnews.gr, στην οποία δημοσιοποιούνται περιστατικά αναφορικά με τις δραστηριότητες ελλήνων hackers.

[988] ... σύμφωνα και με το «Μανιφέστο του hacker», ως ανωτέρω.

[989] Έτσι ο *Θ. Παπαθεοδώρου*, Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 207.

[990] Αυτές οι συλλήψεις δεν είχαν να κάνουν με το αδίκημα του ά. 370Γ παρ. 2 ΠΚ ή με κάποια άλλη διάταξη που να τιμωρεί μόνο τη χωρίς δικαίωμα πρόσβαση αλλά με το αδίκημα του ά. 386Α ΠΚ (απάτη με υπολογιστή). Για την απάτη με υπολογιστή βλ. ενδεικτικά *Χρ. Μυλωνόπουλου,* Ποινικό Δίκαιο – Ειδικό μέρος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, όπ. π., σελ. 548 επ. και *Γ. Νούσκαλη*, Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκής Ένωση, ΠοινΔικ 2/2003, σελ. 178 επ.

Σταδιακά, η κοινότητα των ελλήνων hackers διασπάστηκε σε μια κατηγορία που ασχολήθηκε με την ανακάλυψη των ευάλωτων σημείων σε δίκτυα εταιρειών (ευελπιστώντας σε σχετική επαγγελματική τους αποκατάσταση), σε μια κατηγορία, η οποία επιδόθηκε σε εθνικιστικού τύπου επιθέσεις, και σε μία έτερη κατηγορία, η οποία ασχολείται με τον «χακτιβισμό».

7.5.5.2 Η δυσκολία της ανεύρεσης δείγματος hackers

Είναι γεγονός ότι, όπως έχει καταγραφεί και σε σχετική αρθρογραφία, αποτελεί αρκετά δύσκολο εγχείρημα η δειγματοληψία και η εύρεση αντιπροσωπευτικού δείγματος hackers. Η Σπινέλλη αναφέρει ως τεχνική ερευνητική δυσχέρεια το γεγονός ότι όσοι παραβαίνουν τον νόμο δεν είναι δυνατόν να προσεγγιστούν εύκολα, διότι φοβούνται μήπως αποκαλυφθούν ή στιγματισθούν[991]. Ο Παπάνης αναφέρεται ειδικότερα στους χρήστες του διαδικτύου ως δείγμα υποστηρίζοντας ότι «*οι κοινότητες των χρηστών μερικές φορές έχουν τόσο διακριτή κουλτούρα, διάλεκτο, αξιακό σύστημα αυτοκαθορισμούς και ετεροκαθορισμούς σε σχέση με άλλες κοινότητες*[992]*, ώστε η ένταξη του ερευνητή να εκλαμβάνται πολλές φορές ως παραβίαση του ζωτικού-εικονικού χώρου*»[993]. Πέρα, όμως από τα ανωτέρω, είναι και γεγονός ότι οι hackers αποτελούν μάλλον σπάνιο πληθυσμό[994]. Τούτων δοθέντων, η συμμετοχή στο δείγμα 48 hackers κρίνεται ικανοποιητική[995].

---

[991] Έτσι *Κ. Δ. Σπινέλλη,* Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 86.

[992] Τα εν λόγω χαρακτηριστικά υπάρχουν στις ομάδες των hackers – βλ. και ανωτέρω παράγραφο 2.8 για την (υπο)κουλτούρα του hacking.

[993] Έτσι ο *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 23.

[994] *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 70.

[995] Το μέγεθος του δείγματος για κάθε μία από τις ερευνώμενες ομάδες και ιδίως για αυτή των hackers το οποίο τελικώς εξασφαλίστηκε (δεδομένων των δυσκολιών που έχουν αναφερθεί ανωτέρω) φαίνεται να καλύπτει τις ανάγκες και παραδοχές της βιβλιογραφίας σύμφωνα με την οποία «*πολλοί ερευνητές θεωρούν ότι πρέπει να έχουμε ως δείγμα τουλάχιστον τριάντα περιπτώσεις αν θέλουμε να χρησιμοποιήσουμε κάποια μορφή στατιστικής ανάλυσης των δεδομένων μας*» (έτσι *L. Cohen, L. Manion & K. Morrison*, Μεθολολογία εκπαιδευτικής έρευνας, εκδ. Μεταίχμιο, 2007, σελ. 151). Επιπρόσθετα, αναφορικά με το μέγεθος του δείγματος και την αντιπροσωπευτικότητα βλ. *Αν. Σταλίκα*, Μέθοδοι έρευνας στην ψυχολογία, εκδ. Ελληνικά γράμματα, Αθήνα, 2005, σελ. 223 επ.

Βέβαια, πρέπει πάντοτε να λαμβάνουμε υπόψιν μας ότι όσο αντιπροσωπευτικό και αν δύναται να θεωρηθεί το δείγμα, πολλές φορές υπάρχει πρόβλημα στο να αναπαραστήσει πιστά τον πληθυσμό, με αποτέλεσμα να φέρεται να υπάρχει ενίοτε ασυμφωνία ανάμεσα στον στατιστικό δείκτη που προκύπτει

7.5.5.3 Η προσέγγιση ομάδων hackers στην Ελλάδα

Χρησιμοποιώντας, λοιπόν, το διαδίκτυο, όσον αφορά τους hackers, έτσι όπως φαίνεται να έχουν διασπαστεί ανωτέρω[996], μέσω της ιστοσελίδας κοινωνικής δικτύωσης www.facebook.com προσεγγίστηκε κατά πρώτον η *Ελληνική Χάκινγκ Σκηνή (Greek Hacking Scene)*[997] και έπειτα η ομάδα *hackerspace.gr*. Πρόκειται για δύο ομάδες με έντονη διαδικτυακή και όχι μόνο παρουσία και με διαφορετικά χαρακτηριστικά η καθεμιά, όπως παρακάτω θα αναλυθεί. Το εν λόγω σχέδιο δειγματοληψίας εφαρμόστηκε προκειμένου να εξασφαλιστεί στον κατά το δυνατόν μεγαλύτερο βαθμό η αντιπροσωπευτικότητα και ως προς τους "hackers με λευκό καπέλο" (white hat hackers) καθώς και ως προς τους "hackers με μάυρο καπέλο" (black hat hackers)[998] – των δύο, δηλαδή, βασικών διαφορετικών τάσεων του

από το δείγμα και την αντίστοιχη τιμή της παραμέτρου του πληθυσμού και, συνεπώς, ο προκύψας στατιστικός δείκτης να αποτελεί τελικώς μόνο μία εκτίμηση της αντίστοιχης παραμέτρου του πληθυσμού. Η περίπτωση αυτή ονομάζεται «σφάλμα δειγματοληψίας» ("sampling error") και αποτελεί ένα από τα κύρια προβλήματα που καλείται να αντιμετωπίσει ο ερευνητής όταν προσπαθεί να εξάγει γενικά συμπεράσματα για πληθυσμούς (βλ. *Χ. Κατσάνου & Ν. Αβούρη*, Στατιστικές Μέθοδοι Ανάλυσης Πειραματικών Δεδομένων Συνεργασίας, url: http://karagian.users.uth.gr/cscl/22-Katsanos-Avouris.pdf, Πανεπιστήμιο Πατρών, σελ. 4, ειδικά για το σφάλμα δειγματοληψίας αλλά και γενικώς για στατιστικές μεθόδους ανάλυσης).

[996] Βλ. παράγραφο 7.5.5.1.

[997] Βλ. urls: https://www.facebook.com/groups/GreekHackScene/?fref=ts, https://www.facebook.com/pages/Greek-Hacking-Scene-%CE%95%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CE%AE-%CE%A7%CE%AC%CE%BA%CE%B9%CE%BD%CE%B3%CE%BA-%CE%A3%CE%BA%CE%B7%CE%BD%CE%AE/155940007782512, https://www.facebook.com/groups/GreekHackers/?ref=ts&fref=ts, http://www.digitallife.gr/tag/greek-hacking-scene.

[998] Όπως αναφέρθηκε ανωτέρω, οι «hackers με λευκό καπέλο» δεν προβαίνουν σε καταστροφικές για τα ηλεκτρονικά δεδομένα ενέργειες σε αντίθεση με τους «hackers με μάυρο καπέλο», οι οποίοι αναπτύσσουν επιβλαβή δραστηριότητα. Στην προκειμένη περίπτωση, από την καταγραφή του προφίλ και των δραστηριοτήτων αυτών των δύο ομάδων προκύπτουν τα εξής:

- οι συμμετέχοντες στην «Ελληνική Χάκινγκ Σκηνή – Greek Hacking Scene – GHS» μπορούν να θεωρηθούν «hackers με μάυρο καπέλο» αφού έχουν διενεργήσει επιθέσεις καταστροφής ιστοσελίδων και έχουν πλήξει την ασφάλεια ηλεκτρονικών δεδομένων και πληροφοριών (βλ. σχετικά το κείμενο που παρουσιάζει την ιδεολογία, την ίδρυση και τη δράση της GHS – Παράρτημα IV όπως εστάλη από τον ίδιο τον διαχειριστή του λογαριασμού της GHS στο facebook, δημοσιεύματα για τη δράση της GHS όπως παραπέμπονται σε παραπομπές του παρόντος πονήματος καθώς και φωτογραφίες από επιθέσεις της GHS στο url: http://antiparakmi.blogspot.com/search/label/Greek%20Hacking%20Scene).
- από την άλλη πλευρά, οι hackers της ομάδας hackerspace.gr πλησιάζουν περισσότερο στους «hackers με λευκό καπέλο» καθώς (δηλώνουν ότι) ως ομάδα έχουν ως μοναδικό στόχο την καινοτομία και την ανάπτυξη της ασφάλειας για προστασία των ηλεκτρονικών δεδομένων (βλ. το όραμα και τις αξίες της ομάδας hackerspace.gr στον ιστότοπο με url: https://www.hackerspace.gr/wiki/Vision).

hacking. Επιπρόσθετα, θεωρήθηκε πιο αποτελεσματική πρακτική η επαφή με hackers σε συλλογικές δραστηριότητες καθώς στο ερωτηματολόγιο, το οποίο επρόκειτο να αποσταλεί, υπήρχε η δυνατότητα να απαντήσουν οι συντονιστές των ομάδων αυτών αλλά και να προωθήσουν το ερωτηματολόγιο προς απάντηση στα μέλη των ομάδων και σε σε μεμονωμένους hackers[999].

7.5.5.4 Η Ελληνική Χάκινγκ Σκηνή (Greek Hacking Scene) – Ανάλυση περιεχομένου της επικοινωνίας

Η πρώτη επαφή με την «Ελληνική Χάκινγκ Σκηνή» (Greek Hacking Scene – GHS), την μεγαλύτερη και πιο δραστήρια ομάδα hackers στην Ελλάδα[1000], έλαβε χώρα πρώτη φορά με μήνυμα που απεστάλη στον οικείο λογαριασμό της ομάδας τους στην ιστοσελίδα www.facebook.com στις 04/07/2013. Εκεί τους ζητήθηκε η συνδρομή τους στην έρευνα και η απάντηση των ερωτηματολογίων. Η επικοινωνία με τον διαχειριστή του συγκεκριμένου λογαριασμού διήρκεσε έως τις 14/07/2013 (το περιεχόμενο αυτής, όπως παρουσιάζεται κατωτέρω, θεωρώ ότι λειτούργησε βάσιμα και ως έλεγχος αξιοπιστίας αναφορικά με το ότι πράγματι πίσω από τον διαχειριστή του συγκεκριμένου προφίλ βρίσκεται όντως η GHS). Περαιτέρω, μέλη της GHS και γνωστοί hackers (π.χ. ο punker GHS[1001] με τον οποίο μάλιστα υπήρξε και ξεχωριστή

---

[999] Η εν λόγω τεχνική, όπως αναφέρθηκε και ανωτέρω, ονομάζεται ***δειγματοληψία χιονοστιβάδας (snowball Sampling)*** και επιλέγεται από τον ερευνητή όταν αυτός επιθυμεί το δείγμα να έχει κάποια συγκεκριμένα κοινωνικά ή πολιτικά χαρακτηριστικά και όταν το επιθυμητό χαρακτηριστικό του δείγματος είναι πολύ σπάνιο (βλ. ενδεικτικά *Θ. Ιωσηφίδης*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 61, *Επ. Διαμαντόπουλος*, Σημειώσεις στατιστικής, Ξάνθη, Νοέμβριος 2012, url: http://users.sch.gr/epdiaman/images/stories/ergasies/biblia/statistics_with_calc_and_R_project.pdf, σελ. 17, *Ashley Crossman*, Snowball Sample, http://sociology.about.com/od/Types-of-Samples/a/Snowball-Sample.htm και *Έλλη Ιωαννίδη-Καπόλου*, Κοινωνιολογική έρευνα – Μέθοδοι και τεχνικές, www.nsph.gr/Files/006_Koinoniologias/Research_Stages.doc, σελ. 7). Ο Bachmann αναφέρει πως μειονέκτημα της χρήσης της δειγματοληψίας χιονοστιβάδας είναι ότι το δείγμα δεν επιλέγεται από ευρύτερο πλαίσιο δειγματοληψίας και ότι εξαρτάται από τις υποκείμενες δομές του δικτύου των συμμετεχόντων (*Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 70).

[1000] Έτσι σε άρθρο της *Λίνας Γιάνναρου*, Έλληνες... οι πιο καλοί οι μαθητές στο χάκινγκ, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 26 Φεβρουαρίου 2012, url: http://www.kathimerini.gr/451545/article/epikairothta/ellada/ellhnes-oi-pio-kaloi-oi-ma8htes-sto-xakingk, όπου και φιλοξενείται συνέντευξη μέλους της GHS και γίνεται αναφορά σε «επιθέσεις» που έχουν πραγματοποιηθεί από τα μέλη της ή έχουν αποδοθεί σε αυτά.

[1001] Στις 21 Ιανουαρίου 2014 υπήρχε δημοσιευμένο στην ιστοσελίδα www.youtube.com βίντεο με θέμα και τίτλο «Οι 10 καλύτεροι Έλληνες χάκερς» (url: http://www.youtube.com/watch?v=LxPlt1ImDaU) στο οποίο μάλιστα στην κορυφαία θέση «φιγούραρε» ο Punker GHS. Πλέον, στο ως άνω url η εν λόγω

προσωπική επικοινωνία ως μετέπειτα «ηλεκτρονικό φίλο» στην ιστοσελίδα www.facebook.com) φαίνεται εμφανώς στην εν λόγω ιστοσελίδα ότι σχετίζονται με την ελληνική χάκινγκ σκηνή (π.χ. στο ως άνω όνομα υπάρχει το πρόθεμα GHS δηλαδή "Greek Hacking Scene").

Κατά την επικοινωνία με τον εκπρόσωπο της ελληνικής χάκινγκ σκηνής (GHS) ανέκυψαν συζητήσεις με πολύ ενδιαφέρον περιεχόμενο αναφορικά με τη σύγχρονη έννοια του hacking. Καταρχάς, δηλώθηκε από εμένα ως ερευνητή στην πρώτη μου επιστολή η ιδιότητά μου, ο στόχος της έρευνάς μου καθώς και ότι αυτή θα διεξαγόταν ανώνυμα, όπως επιτάσσει η δεοντολογία της έρευνας[1002]. Στην απάντηση του διαχειριστή του λογαριασμού της GHS στην ιστοσελίδα κοινωνικής δικτύωσης facebook.com αναφέρονται τα εξής[1003]:

> «***Ευχαριστούμε πολύ για το μήνυμα σας. Είδαμε το ερωτηματολόγιο και μας αρέσει το θέμα. Σίγουρα θετικές ή αρνητικές, πάντα η αλήθεια μας ενδιαφέρει.***

ιστοσελίδα μας ενημερώνει ότι το βίντεο αυτό δεν είναι πλέον διαθέσιμο – λογικά, δηλαδή, οι διαχειριστές της ιστοσελίδας το «κατέβασαν» λόγω του περιεχομένου του.

[1002] Για τη δεοντολογία στην κοινωνική έρευνα βλ. αρχικώς *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 277 επ. Αναφορικά με την θέσπιση κώδικα δεοντολογίας εγκληματολόγων πρβλ. *Κ. Δ. Σπινέλλη & Μ. Κρανιδιώτη*, Κανόνες δεοντολογίας για τους Έλληνες εγκληματολόγους: Πρόταγμα του 21ου αιώνα; /παράρτημα με σχέδιο κώδικα δεοντολογίας, εις: Εγκληματολογία και Ευρωπαϊκή Αντεγκληματική Πολιτική, Προσφορά Τιμής στην Αγλαΐα Τσήτσουρα, εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2009, σελ. 503-546 καθώς και *Κ. Δ. Σπινέλλη & Μ. Κρανιδιώτη*, Κώδικας Δεοντολογίας Εγκληματολόγων, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 10, Φεβρουάριος 2009, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1237301236. Επιπρόσθετα, βλ. για σχετική με τον κώδικα δεοντολογίας εγκληματολόγων εκδήλωση-συζήτηση το ρεπορτάζ των *Αρ. Παππά, Αρ. Πανεζή & Σ. Παναγιωτοπούλου*, Επιστημονική εκδήλωση με θέμα: «Κώδικας Δεοντολογίας για τους Εγκληματολόγους – Πρόταγμα του 21ου αιώνα;», ηλεκτρονικό περιοδικό www.theartofcrime.gr (όπ. π.), τ. 7 Φεβρουάριος 2008, url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1207652324. Αναφορικά με την σύγχρονη προσέγγιση των ζητημάτων δεοντολογίας των εγκληματολόγων βλ. *Κ. Δ. Σπινέλλη & Μ. Κρανιδιώτη*, Ένας Κώδικας Δεοντολογίας για τους εγκληματολόγους, εις: *Ν. Κουράκη, Χρ. Ζαραφωνίτου, Χρ. Τσουραμάνη & Ευαγ. Χαϊνά (εκδ. επιμ.)*, Εγκληματολογία: Διδασκαλία και έρευνα στην Ελλάδα – Πρακτικά Επιστημονικού Συνεδρίου, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών Νομικής Αθηνών, τόμος υπ' αρ. 22, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2011, σελ. 583 επ. και *Αναστασίας – Ασημίνας Παπαγεωργίου,* Προς μία συστηματικότερη αντιμετώπιση των ζητημάτων δεοντολογίας: εξέταση της αναγκαιότητας θέσπισης Επιτροπών Δεοντολογίας εντός των ελληνικών Πανεπιστημίων – μια ανάλυση βασισμένη στη βρετανική εμπειρία, εις: *Ν. Κουράκη, Χρ. Ζαραφωνίτου, Χρ. Τσουραμάνη & Ευαγ. Χαϊνά (εκδ. επιμ.)*, Εγκληματολογία: Διδασκαλία και έρευνα στην Ελλάδα – Πρακτικά Επιστημονικού Συνεδρίου, όπ. π., σελ. 599 επ. Τέλος, βλ. τον τετράλογο της δεοντολογίας του ερευνητή όπως αναπτύσσεται από την Σπινέλλη (*Κ. Δ. Σπινέλλη,* Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 89).

Ειδικά για τη δεοντολογία της έρευνας μέσω διαδικτύου βλ. *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 41 επ.

[1003] Τα δεδομένα επικοινωνίας δημοσιεύονται μετά από έγκριση του διαχειριστή του λογαριασμού της GHS στην ιστοσελίδα κοινωνικής δικτύωσης www.facebook.com.

Μπορούμε να στείλουμε το ερωτηματολόγιο ως έχει σε διάφορα μέλη της κοινότητας αλλά και παραπέρα. Αυτοί που ασχολούνται εις βάθος, δεν πρόκειτε να απαντήσουν μιας και αρκετοί είναι εποφυλακτικοί επειδή οι ίδιοι ξέρουν τι δυνατότητες υπάρχουν μέσω του διαδικτύου. ...»[1004].

Αρχικώς, είναι σημαντική η αποδοχή του ερωτηματολογίου από τον ερωτώμενο, ιδίως σε έρευνες αυτοομολογούμενης παραβατικότητας, όπως η συγκεκριμένη.

Επιπρόσθετα, θεωρώ ότι χρήζει ιδιαίτερης προσοχής η επισήμανση: «***... η αλήθεια μας ενδιαφέρει.***». Η φράση αυτή αναφέρεται στο «***Σίγουρα θετικές ή αρνητικές...***» με εννοούμενο το "***πλευρές του hacking***" από τη συνέχεια της συζήτησης. Κατά τη γνώμη μου, η φράση αυτή μπορεί να ερμηνευθεί διττά: κατά πρώτον, οι hackers ως επίδοξοι κατακτητές της γνώσης και υπέρμαχοι της ελευθερίας της πληροφορίας ειδικότερα και συνεπώς της ελευθερίας γενικότερα έχουν την αλήθεια πραγματικά σε μεγάλη εκτίμηση και δεν φοβούνται να την αντιμετωπίσουν – κατά δεύτερον, ενδεχομένως να αποζητούν μέσω της συγκεκριμένης έρευνας να δείξουν προς τα έξω την αληθινή τους δράση, έχοντας ήδη υπόψιν τους τα διάφορα δημοσιεύματα που έχουν κατά καιρούς κυκλοφορήσει αναφορικά με τη δράση της GHS[1005] και τα οποία ίσως να έχουν παρουσιάσει μια εικόνα της GHS εν όλω ή εν μέρει διαφορετική από την πραγματική.

Στη συνέχεια, δηλώνεται σαφώς η δυσκολία του εγχειρήματος καθώς η έρευνα θα λάβει χώρα μέσω διαδικτύου - οι hackers γνωρίζουν πολύ καλά την ανασφάλεια τους κινδύνους που διατρέχουν τα ηλεκτρονικά δεδομένα στο διαδίκτυο. Και για αυτόν τον λόγο επισημαίνεται ότι ενδεχομένως να μην επιδείξουν εμπιστοσύνη προκειμένου να συμμετάσχουν στο δείγμα, έτσι όπως έχει ήδη καταγραφεί και από τον Bachmann [1006].

[1004] Η υπογράμμιση δική μου – το κείμενο αυτούσιο όπως εστάλη και χωρίς διορθώσεις.

[1005] Βλ. χαρακτηριστικά και ενδεικτικά το δημοσίευμα της ενημερωτικής ιστοσελίδας newsbomb.gr «Μεγάλη επίθεση οργανώθηκε από την Ελληνική Χάκινγκ Σκηνή GHS!", 30 Ιανουαρίου 2013, url: http://www.newsbomb.gr/politikh/story/275005/megali-epithesi-organothike-apo-tin-elliniki-hakingk-skini-ghs, δημοσίευμα του ενημερωτικού blog atticanea.blogspot.gr "Η Ελληνική Χάκινγκ Σκηνή GHS έχει αποκτήση πλήρης πρόσβαση σε όλα τα Πρωτοδικεία και Εφετεία!", 31 Οκτωβρίου 2012, url: http://attikanea.blogspot.gr/2012/10/ghs.html, δημοσίευμα ενημερωτικής ιστοσελίδας in.gr "Ονοματεπώνυμο σε τρία ακόμα μέλη της Greek Hacking Scene", 5 Μαρτίου 2012, url: http://tech.in.gr/news/article/?aid=1231184730.

[1006] Ο Bachmann αναφέρεται συγκεκριμένα στη δυσκολία να κερδίσει ο ερευνητής την εμπιστοσύνη των hackers: «*Πολλοί hackers είναι γενικώς καχύποπτοι σχετικά με τη γνησιότητα και την αξιοπιστία*

Μετά από διάφορες διαδικαστικές παρατηρήσεις, αυτή η πρώτη απάντηση εκ μέρους της «Ελληνικής Χάκινγκ Σκηνής» κλείνει ως εξής:

> ***«Σας ενημερώνουμε μόνο ότι έχουμε κάνει verify ότι όντως κάνετε αυτό που λέτε (και συγνώμη), και είδαμε ότι ασχολείστε με παρόμοια θέματα σε βάθος χρόνου. Οπότε δεν χρειάζεται κάποια εγγύηση κλπ. νομίζουμε ότι αυτό που κάνετε σας αρέσει και το κάνετε, αυτό είναι ότι καλύτερο και ελπίζουμε σε ότι καλύτερο για εσάς στο μέλλον. Αυτό που θα θέλαμε εφόσον το επιθυμείτε είναι σαν μία από τις πηγές σας να αναγράφετε "Ελληνική Χάκινγκ Σκηνή".»***[1007]

Προκειμένου η έρευνα να λάβει χώρα και με δεδομένο ότι τα μέλη της GHS ικανοποιήθηκαν, όπως δηλώνουν, από την επιλογή και προσέγγιση του θέματος, είναι αξιοσημείωτη η δήλωσή τους ότι ο ίδιος ο ερευνητής κατέστην αντικείμενο ελέγχου. Σε προσωπικό επίπεδο, αυτή η (δικαιολογημένη, ίσως, σε μεγάλο βαθμό) ενέργεια της GHS να διαπιστώσει την ιδιότητά μου και τούτο να μου ανακοινωθεί εκ των υστέρων σε κάθε περίπτωση μου δημιούργησε έντονο αίσθημα μεγαλύτερης υπευθυνότητας για την από εδώ και πέρα διαχείριση και χρήση των δεδομένων μου στο διαδίκτυο (αφού πιστεύω βάσιμα πως οι hackers της GHS χρησιμοποίησαν το διαδίκτυο καθώς και τις ειδικές γνώσεις τους πάνω σε αυτό προκειμένου να επαληθεύσουν την ταυτότητά μου και το επιστημονικό μου ενδιαφέρον)[1008].

Επιπρόσθετα, ο εκπρόσωπος της GHS μου ζήτησε να αναφερθεί η συνεργασία της GHS στη διεξαγωγή της έρευνας. Το γεγονός αυτό θεωρώ ότι είναι μη αναμενόμενο δεδομένης της εκτίμησης ότι δεν επιδιώκουν τη δημοσιότητα φοβούμενοι ότι ίσως μπουν στο στόχαστρο ερευνών κ.λπ. Η εκτίμηση αυτή προκύπτει από το γεγονός ότι

των πληροφοριών που ανακτούν online. Για τον ερευνητή, αυτό σημαίνει ότι το δύσκολο έργο της δημιουργίας αναγκαίας εμπιστοσύνης χωρίς την προσωπική επαφή γίνεται μια κρίσιμη πρόκληση. Η αποτυχία να πεισθούν οι hackers να εμπιστευθούν το ερευνητικό έργο θα προκαλέσει πολλούς δυνητικούς συμμετέχοντες να αρνηθούν να λάβουν μέρος στην έρευνα ή να παράσχουν εκ προθέσεως ψευδή στοιχεία» (βλ. *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 72-73).

[1007] Η υπογράμμιση δική μου – το κείμενο αυτούσιο όπως εστάλη και χωρίς διορθώσεις.

[1008] Βέβαια, είναι πιθανόν να μην έλαβε χώρα κάποια χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά μου δεδομένα καθώς ίσως θα αρκούσε και μια απλή αναζήτηση σε κάποια μηχανή αναζήτησης (π.χ. www.google.com, www.bing.com κ.ά.) προκειμένου να ανευρεθεί η επιστημονική ιδιότητα και τα επιστημονικά ενδιαφέροντα κάποιου ερευνητή με περιορισμένη, έστω, παρουσία.

δηλώθηκε ήδη από τους ίδιους η επιφυλακτικότητα με την οποία μέλη της GHS ενδεχομένως να αντιμετωπίσουν την έρευνα[1009].

Τέλος, ενδεικτικό της ιδεολογίας της GHS και τελικά και του λόγου για τον οποίο η GHS έδειξε ενδιαφέρον για να απαντήσει στα ερωτηματολόγια της έρευνας είναι το εξής μήνυμα στις 04/07/2013:

> ***«... Ας σου πω Φώτη, κάθε μέρα λαμβάνουμε πολλά μηνύματα τύπου "πως να χακάρω το fb του φίλου/ης μου", με άλλα λόγια από όλα που γίνονται στο κόσμο μας, τους περισσότερους το πρόβλημα τους είναι ο διπλανός τους, και από το να προτιμάνε την αλήθεια, εμπιστοσύνη και διάλογο, καταφεύγουν σε μεθόδους που μπορούν να τους βάλουν σε μεγαλύτερους μπελάδες, γιατί εκεί που ψάχνουν για τα δεδομένα του φίλου/ης τους, κινδυνεύουν να γίνουν αντικείμενα εκμετάλευσεις από άλλους κακόβουλους χρήστες. Πχ. όταν κάποιος μπαίνει σε μια τέτοια διαδικασία και θέλει να μάθει τον κωδικό του fb κάποιου άλλου ατόμου, τότε ψάχνει να βρει στο ίντερνετ όποιονδήποτε λέει ότι είναι hacker και να τον/την εμπιστευτεί αρκεί να βρει τον κωδικό που ψάχνει και δυστυχώς πολλοί διατίθεντε να πληρώσουν κιόλας, με αποτέλεσμα να τους έχει ξεγελάσει κάποιος κακόβουλος χρήστης, να τους έχει πάρει λεφτά και άλλα στοιχεία ή να έχει κάνει bot το pc τους και εν τέλη ο χρήστης που μόνος του μπήκε σε τέτοια μπελά, να μην έχει ούτε καν και κάποιο κωδικό που έψαχνε. Εμείς τέτοια μηνύματα είτε τα αγνοούμε, είτε λέμε τους κινδύνους, και παρ'όλα αυτά είναι πολλοί εκείνοι που συνεχίζουν να επιμένουν. Άρα τώρα καταλαβαίνεις ότι <u>είναι μεγαλή χαρά μας να βοηθήσουμε εφόσον μπορούμε όσους έχουν θέληση για να κάνουν τις κοινωνίες μας καλύτερες</u>.»***[1010].

Στο ανωτέρω μήνυμα δηλώνεται το ιδεολογικό υπόβαθρο των πράξεων των hackers, η θέληση και ενίσχυση κάθε πρωτοβουλίας που αυτοί θεωρούν ότι θα κάνει τον κόσμο καλύτερο (π.χ. μια διδακτορική διατριβή). Το πιο σημαντικό, όμως, στοιχείο της ανωτέρω ανάπτυξης θεωρώ ότι είναι η διαπίστωση πως υπάρχουν αρκετοί οι

[1009] Δυνάμει των ανωτέρω, ευχαριστώ ιδιαίτερα τα μέλη της Ελληνικής Χάκινγκ Σκηνής για την εμπιστοσύνη που επέδειξαν σε εμένα και για τη συνεργασία τους στην έρευνα.

[1010] Η υπογράμμιση δική μου – το κείμενο αυτούσιο όπως εστάλη και χωρίς διόρθωση.

οποίοι είναι επίδοξοι ηθικοί αυτουργοί χωρίς δικαίωμα πρόσβασης σε δεδομένα και (ελλείψει τεχνικών γνώσεων των ιδίων) αναζητούν hackers προκειμένου να αποκτήσουν πρόσβαση σε ηλεκτρονικές πληροφορίες.

7.5.5.5 Η ομάδα hackerspace.gr – Ανάλυση περιεχομένου της επικοινωνίας – Ανοιχτή συνέντευξη με δύο μέλη της ομάδας

Έτσι όπως η ομάδα αυτή αυτοπροσδιορίζεται στην οικεία ιστοσελίδα της hackerspace.gr "*Το Hackerspace είναι ένας ανοιχτός χώρος δημιουργικότητας, συνεργασίας, έρευνας, ανάπτυξης και φυσικά μάθησης. Είναι όμως και κάτι περισσότερο από ένας φυσικός χώρος. Είναι μια ενεργή κοινότητα ανθρώπων με ιδέες που πηγάζουν απ' τη φιλοσοφία του Ελεύθερου Λογισμικού.*"[1011]. Η συνεκτική ιδέα της ομάδας αυτής πηγάζει από το ελεύθερο και ανοιχτό λογισμικό (Free / Open-Source Software)[1012] και από την ανάγκη να μοιράζονται τα μέλη με όλους τις εμπειρίες που έχουν αποκτήσει μέσα από την ενασχόληση με το hacking. Αντιστοίχως, το hackerspace.gr λειτουργεί ως χώρος ανάπτυξης ιδεών.

Το hackerspace.gr λειτουργεί νομίμως και επώνυμα – έχει μάλιστα περιβληθεί την νομική μορφή αστικής μη κερδοσκοπικής εταιρείας[1013]. Συντηρείται από τις συνδρομές των μελών του και δωρεές. Σήμερα η ομάδα αριθμεί 24 μέλη τα οποία αναφέρονται στην ιστοσελίδα, τα περισσότερα, μάλιστα, με τα πλήρη ονοματεπώνυμά τους[1014].

Ο χώρος του hackerspace.gr βρίσκεται στην Αθήνα. Η είσοδος είναι ελεύθερη στον καθένα οποτεδήποτε ο χώρος είναι ανοιχτός – στην ιστοσελίδα ανακοινώνονται ώρες λειτουργίας κατά τις οποίες στον χώρο εκτελούνται προγράμματα ή συζητήσεις ή μπορεί κάποιος να χρησιμοποιήσει τη βιβλιοθήκη. Επίσης, στην ιστοσελίδα

[1011] url: http://www.hackerspace.gr/wiki/Main_Page.

[1012] Σχετικά με το ανοικτό λογισμικό βλ. σχετικό λήμμα της ηλεκτρονικής εγκυκλοπαίδειας «Βικιπαιδεία» στο url: http://el.wikipedia.org/wiki/%CE%9B%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C_%CE%B1%CE%BD%CE%BF%CE%B9%CE%BA%CF%84%CE%BF%CF%8D_%CE%BA%CF%8E%CE%B4%CE%B9%CE%BA%CE%B1.

[1013] ... όπως ενημερώθηκα από μέλη του hackerspace.gr σε συνάντησή μας στον χώρο του hackerspace.gr – βλ. κατωτέρω.

[1014] url: http://www.hackerspace.gr/wiki/People.

αναφέρονται οι προϋποθέσεις που πρέπει να πληροί και η διαδικασία που πρέπει να ακολουθήσει κάποιος για να γίνει μέλος.

Οι αξίες που ενστερνίζονται τα μέλη του hackerspace.gr, όπως περιγράφονται και αυτές στην ιστοσελίδα[1015], είναι οι εξής:

> *«**Excellence**: Να είσαι ευγενικός με όλους. Να σέβεσαι όλους τους ανθρώπους που θα συναντήσεις στον χώρο, αλλά και τον ίδιο τον χώρο.*
>
> ***Sharing**: Η βασική αξία λειτουργίας του hackerspace είναι πως μοιραζόμαστε τα projects, τον κώδικα, τις ιδέες που παράγουμε μέσα στον χώρο, σε συνεργασία με άλλους. Το moto είναι, εμπνευσμένο από creative commons, "I love to share".*
>
> ***Consensus**: Όλες οι αποφάσεις είναι αποτέλεσμα συναίνεσης μεταξύ των μελών. Οι αποφάσεις για τη διαχείριση του χώρου λαμβάνονται στις μηνιαίες συναντήσεις, οι οποίες είναι ανοιχτές σε όλους.*
>
> ***Do-ocracy**: Δεν χρειάζεται κάποια άδεια για να εργαστείς πάνω σε κάποιο project. Αν θες να οργανώσεις ένα event ή κάποιο workshop πάνω σε κάποιο Open-Source ή Open-Hardware project, μην περιμένεις να το οργανώσει κάποιος άλλος. Πάρε την πρωτοβουλία και κάντο.»*

Οι εν λόγω αξίες εκφράζουν την κουλτούρα των hackers και όσων ασπάζονται την φιλοσοφία του ελεύθερου λογισμικού. Η πρώτη αρχή στην οποία περιγράφεται ο σεβασμός βρίσκει έρεισμα και στην ιδεολογία των hackers, όπως αναλύθηκε ανωτέρω. Συγκεκριμένα, όπως ήδη αναφέρθηκε, ο hacker θα πρέπει πρωτίστως να μάθει να εκτιμά και να σέβεται την ικανότητα[1016] – πιστεύω ότι, πέρα από τον στοιχειώδη σεβασμό που επιβάλλεται στις ανθρώπινες σχέσεις, ο απαιτούμενος σεβασμός στην προκειμένη περίπτωση εκπορεύεται και από το ότι οι συμμετέχοντες στην ομάδα αυτοπροσδιορίζονται ως hackers και για αυτόν τον λόγο αξιώνουν σεβασμό. Στη συνέχεια, το «μοίρασμα» γνώσεων είναι και αυτό στοιχείο της

[1015] url: http://www.hackerspace.gr/wiki/Vision.

[1016] Βλ. ανωτέρω παράγραφο 2.7.

συνεργατικής κουλτούρας του hacking[1017] και της ελευθερίας της πληροφορίας[1018]. Η αξία της συναίνεσης υπογραμμίζει τη δημοκρατική λειτουργία της ομάδας[1019]. Η λειτουργία αυτή επιβεβαιώνεται και από την τέταρτη αξία με τίτλο "do-ocracy", της οποίας ο τίτλος αποδεικνύει την επιρροή που ασκεί η λέξη "democracy" («δημοκρατία») στα μέλη της ομάδας.

Η πρώτη επαφή με τα μέλη του hackerspace.gr έλαβε χώρα με μήνυμα στο προφίλ της ομάδας στην ιστοσελίδα www.facebook.com στις 07.07.2013[1020] με το οποίο τους ζητήθηκε η συνδρομή και συμμετοχή τους στην έρευνα και η απάντηση των ερωτηματολογίων που είχαν καταρτιστεί και απευθύνονταν σε hackers.

Η απάντηση στις 08.07.2013[1021] από τον διαχειριστή του ως άνω προφίλ επικεντρώθηκε στη διαφορετική ερμηνεία του όρου hacking[1022]:

> *«**κύριε Σπυρόπουλε προωθώ στην λίστα το ερωτηματολόγιο σας.***
>
> ***Προσωπικά ο γραφών ερμηνεύει τον όρο hacking διαφορετικά από εσάς. Με την έννοια ότι πρόκειτε για την δημιουργική εξεύρευση λύσεων τεχνικού (ή μη) χαρακτήρα σε προβλήματα. ...**»*

Στο ανωτέρω επιχείρημα αντέλεξα ότι δεν υπάρχει κανένα θέσφατο στην όποια προσέγγιση της έννοιας του hacking, με δεδομένο, μάλιστα, ότι η πρώτη ερώτηση του ερωτηματολογίου είναι η εξής: «***Τί είναι hacking σύμφωνα με την εμπειρία σας;***». Ωστόσο, η επιμονή στην απάντηση εξακολουθεί:

[1017] Βλ. ανωτέρω σχετική ανάπτυξη για την «ηθική» του hacking καθώς και τη ρήση που αναφέρει ότι «*Ο χάκερ κατακτά την ελευθερία της γνώσης για να χαρίσει σε όλη την κοινωνία τη γνώση της ελευθερίας*» (βλ. *Χρ. Τσουραμάνης*, Ψηφιακή εγκληματικότητα, όπ. π., σελ. 107 επ.).

[1018] Βλ. *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες, όπ. π., σελ. 183.

[1019] Αρκετοί hackers επικαλούνται ότι ενστερνίζονται και υποστηρίζουν έντονα δημοκρατικές αρχές (βλ. και στο Παράρτημα IV το κείμενο της GHS το οποίο αρχίζει με τη φράση «*Η Ελληνική Χάκινγκ Σκηνή είναι Ιδέα για Ελευθερια, Δημοκρατία, Δικαιοσύνη και Παιδεία*» – οι αρχές αυτές διακηρύσσονται ακόμη και σε περιπτώσεις επιθέσεων hacking, όπως π.χ. στις επιθέσεις των "Anonymous" (για την κολεκτίβα των "Anonymous" πρβλ. *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756).

[1020] url: https://www.facebook.com/hackerspacegr?ref=ts&fref=ts

[1021] Κατωτέρω παρατίθενται αυτούσια αποσπάσματα των μηνυμάτων της εν λόγω επικοινωνίας – η υπογράμμιση δική μου.

[1022] Τα δεδομένα της επικοινωνίας δημοσιεύονται μετά από την έγκριση των εκπροσώπων του hackerspace.gr.

*«... νομίζω ότι τουλάχιστον **τα μέλη του hackerspace.gr θεωρούν ότι άλλο πράγμα είναι το hacking και άλλο το cracking και ίσως δεν απαντήσουν όλοι οι ενδιαφερόμενοι**...».*

Τη Δευτέρα 27.01.2014 επισκέφθηκα τον χώρο του hackerspace.gr[1023]. Πρόκειται για ένα ημιυπόγειο σε μια πολυκατοικία επί της οδού Αμπατιέλλου αρ. 11 στην Αθήνα. Μπαίνοντας μέσα υπάρχει ένας μεγάλος ενιαίος χώρος στη μέση του οποίου έχει τοποθετηθεί ένα μεγάλο ορθογώνιο τραπέζι και γύρω από αυτό αρκετές (περίπου 20) καρέκλες. Αριστερά από την είσοδο και πίσω από τη μια μεγάλη πλευρά του τραπεζιού βρίσκονταν δύο μικρές βιβλιοθήκες δίπλα σε δύο παλιές πολυθρόνες – οι βιβλιοθήκες είχαν πάνω βιβλία με θέμα κυρίως τον προγραμματισμό ηλεκτρονικων υπολογιστών. Στον τοίχο πίσω από τη μικρή πλευρά του τραπεζιού υπήρχε κολλημένο το λογότυπο του "hackerspace.gr". Στο μέσα μικρότερο δωμάτιο υπήρχε μια μικρή κουζίνα, η οποία χρησιμοποιούταν και ως χώρος για πειράματα biohacking. Κατά την ώρα της επίσκεψης παρόντες στο χώρο ήταν δύο μέλη του hackerspace.gr, ο Αλέξανδρος και ο Στέφανος. Επιπρόσθετα, στο πλαίσιο του ανοιχτού χώρου που συνιστά το hackerspace.gr παρευρίσκετο εκεί και ένας Βούλγαρος μετανάστης ο οποίος είχε έρθει προκειμένου να συνδεθεί στο διαδίκτυο με τον φορητό υπολογιστή του μέσω του ελεύθερου ασύρματου δικτύου που παρέχεται εκεί (οι κωδικοί σύνδεσης στο διαδίκτυο είναι αναρτημένοι σε ανακοίνωση στον τοίχο).

Στον χώρο αυτό και καθισμένοι σε καρέκλες γύρω από το τραπέζι έγινε μια ανοιχτή συζήτηση με τα παρευρισκόμενα μέλη του hackerspace, τον Στέφανο και τον Αλέξανδρο. Καταρχάς, ο Στέφανος και ο Αλέξανδρος με διαβεβαίωσαν ότι η ομάδα είχε λάβει το ερωτηματολόγιο, ότι αυτό είχε πράγματι προωθηθεί προς απάντηση και ότι κάποια μέλη είχαν απαντήσει. Ωστόσο, δεν υπήρχε εντός της ομάδας καμία δεσμευτικότητα ή κοινή απόφαση για απάντηση ή μη του ερωτηματολογίου, αντιθέτως η συμπλήρωσή του αυτού αφέθηκε στη διακριτική ευχέρεια του καθενός. Οι δύο συνομιλητές δήλωσαν ότι δεν είχαν απαντήσει το ερωτηματολόγιο.

Με τους συνομιλητές έλαβε χώρα μία ανοιχτή συζήτηση αναφορικά με το hacking και τα ενδιαφέροντά τους. Ρωτήθηκαν αν μια περίληψη της συζήτησης, εν είδει συνέντευξης, μπορεί να συμπεριληφθεί και να αναλυθεί στο παρόν πόνημα, ως

[1023] Πρβλ. τις αναπτύξεις της *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 127 επ. και ιδίως το κεφάλαιο «Έρευνες με εγκληματία στο φυσικό του περιβάλλον», ιδίως για τους προβληματισμούς που ανακύπτουν.

ακολούθως, και έδωσαν τη συγκατάθεσή τους. Αναλυτικότερη συζήτηση έγινε με τον Στέφανο. Δήλωσε ότι είναι 22 ετών, φοιτητής πληροφορικής στο ΑΤΕΙ Πειραιά, ο οποίος όμως έχει εγκαταλείψει τις σπουδές του γιατί θεώρησε ότι «*δεν μαθαίνει τίποτα*»[1024]. Σήμερα απασχολείται ως προγραμματιστής και παρέχει τέτοιες υπηρεσίες σε πελάτες στο εξωτερικό μέσω εταιρείας που έχει συστήσει ο ίδιος στην Ελλάδα (με τη μορφή μονοπρόσωπης Ε.Π.Ε.). «*Θέλω να γίνομαι όλο και καλύτερος προγραμματιστής*», δηλώνει. «*Δεν είμαι hacker συνέχεια, είμαι προγραμματιστής. Hacker γίνομαι μονο όταν βρίσκω κάτι καινούριο, μια ιδέα που θα με βοηθήσει στη δουλειά μου.*[1025] *Γι' αυτό ψάχνω "τρύπες" στα προγράμματα και τα συστήματα. Οποιοσδήποτε βρίσκει κάτι καινούριο ή δουλεύει κάτι με παράξενο τρόπο είναι hacker. Για παράδειγμα, υπάρχουν και hackers νομικοί, αυτοί που βλέπουν στον νόμο μια δυνατότητα που κανένας άλλος δεν έχει δει ή που βρίσκουν ένα πρόβλημα που κανένας άλλος δεν έχει βρει. Αν κάνεις καλό διδακτορικό, θα είσαι hacker!*». Ο Στέφανος έδειξε μεγάλο ενδιαφέρον για το ερωτηματολόγιο και δήλωσε ότι ενδεχομένως θα το απαντούσε.

Από την άλλη με τον Αλέξανδρο η συζήτηση περιεστράφη περισσότερο γύρω από τη λειτουργία του χώρου hackerspace.gr, όπως αυτή περιγράφεται παραπάνω. «*Ο χώρος είναι ανοιχτός για όλους. Το να είσαι μέλος δημιουργεί περισσότερες υποχρεώσεις παρά δικαιώματα*». Περαιτέρω, ο Αλέξανδρος ήταν εντελώς αρνητικός αναφορικά με το ερωτηματολόγιο: «*Θεωρώ πως είναι φτιαγμένο σε εντελώς λάθος βάση*», υποστήριξε. «*Λαμβάνεις υπόψη σου το hacking ως εγκληματική ενέργεια*». Παρά το ότι του απάντησα ότι, καλώς ή κακώς, η χωρίς δικαίωμα πρόσβαση σε δεδομένα τιμωρείται από ποινικές διατάξεις, ότι επί της ουσίας αναζητώ το δέον και ότι προς αυτήν την κατεύθυνση πραγματοποιώ έρευνα (γι' αυτό και στην πρώτη ερώτηση ζητάω να οριστεί το hacking από αυτούς που απαντούν το ερωτηματολόγιο) ο Αλέξανδρος συνέχισε να είναι αρνητικός όπως παραπάνω[1026].

[1024] Και στο «Μανιφεστο του hacker» υπάρχει περιπαικτική αναφορά στο σχολείο (*... I' m in junior high or high school. I' ve listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."*) και επομένως μπορεί να υποστηριχθεί ότι οι hackers απορρίπτουν θεσμοθετημένες εκπαιδευτικές δομές.

[1025] Στα ερωτηματολόγια των hackers όπως παρουσιάζονται κατωτέρω υπάρχουν σχετικές απαντήσεις hackers οι οποίοι μάλιστα υποστηρίζουν ότι έχουν βγάλει χρήματα ως προγραμματιστές χάρη στις γνώσεις που έχουν αποκτήσει από τη δραστηριότητά τους στο hacking.

[1026] Βλ. και εδώ *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 72-73 αναφορικά με τη δυσκολία του ερευνητή να κερδίσει την εμπιστοσύνη των hackers.

Στο τέλος της συζήτησης ζήτησα από τον Αλέξανδρο και τον Στέφανο να προωθήσουν πάλι το ερωτηματολόγιο σε μέλη του hackerspace.gr προκειμένου να απαντήσουν περισσότεροι (όσοι δηλαδή δεν έχουν ήδη απαντήσει) και να αυξηθεί το δείγμα. Εκείνοι, όμως, αρνήθηκαν να το κάνουν λέγοντάς μου ότι δεν ήθελαν να "επηρεάσουν" τα μέλη του "hackerspace.gr" καθώς το ερωτηματολόγιο είχε ήδη σταλεί, κάποιοι είχαν ήδη απαντήσει και ότι το e-mail με το οποίο προωθήθηκε το ερωτηματολόγιο χαρακτηρίστηκε, όπως με ενημέρωσαν, "out of topic", το οποίο σήμαινε ότι η συζήτηση γύρω από το θέμα είχε τελειώσει σε επίπεδο ομάδας του hackerspace.gr[1027].

7.6 Οι περιορισμοί της έρευνας

Πέρα από την ανωτέρω ανάλυση σχετικά με την προβληματική της χρήσης του διαδικτύου ως εργαλείου για την έρευνα[1028], όπως αναλύθηκε ανωτέρω, πριν προβούμε στην παρουσίαση και ανάλυση των αποτελεσμάτων, σκόπιμο είναι να διατυπωθούν επιπλέον περιορισμοί αναφορικά με ζητήματα τα οποία έχουν να κάνουν με την πληρότητα, την εγκυρότητα[1029], την ακρίβεια και την αξιοπιστία της έρευνας[1030].

Καταρχάς, η έρευνα, με δεδομένο ότι διενεργήθηκε διαδικτυακά και τα ερωτηματολόγια εστάλησαν στους συμμετέχοντες σε ηλεκτρονική φόρμα[1031], υπόκειται στους μεθοδολογικούς περιορισμούς που επισημαίνονται σε έρευνες που βασίζονται και στην ταχυδρομική αποστολή ερωτηματολογίων, τα οποία συμπληρώνονται από τους παραλήπτες. Βασικός, περιορισμός μπορεί να θεωρηθεί

[1027] Ο Παπάνης αναφέρει ότι αυτή η διοχέτευση ερωτηματολογίων μπορεί να αντιμετωπίζεται ως εισβολή και εναντίωση από στους συμμετέχοντες σε διαδικτυακά κοινωνικά μορφώματα (έτσι *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 65).

[1028] Βλ. ανωτέρω παράγραφο 7.5.2 του παρόντος πονήματος.

[1029] Για τα είδη εγκυρότητας στην ερευνητική διαδικασία βλ. *Αν. Σταλίκα*, Μέθοδοι έρευνας στην ψυχολογία, εκδ. Ελληνικά γράμματα, Αθήνα, 2005, σελ. 73 επ.

[1030] Βλ. σχετικά με τα ζητήματα εγκυρότητας και αξιοπιστίας της έρευνας το αναλυτικό πόνημα του *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008 και ιδίως το κεφάλαιο υπ' αρ. 6 με τίτλο «Κριτήρια ποιότητας στην ποιοτική κοινωνική έρευνα», σελ. 269 επ. Αναφορικά με την αξιοπιστία και την εγκυρότητα της ποιοτικής έρευνας στο διαδίκτυο βλ. *Ευστράτιο Παπάνη*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 84.

[1031] Βλ. ανωτέρω παράγραφο 7.5.1 του παρόντος πονήματος.

ότι αποτελεί το ζήτημα της πλήρους κατανόησης από τους συμμετέχοντες των ερωτήσεων του ερωτηματολογίου - ο αποκρινόμενος μπορεί να αντιληφθεί τις ερωτήσεις πολύ διαφορετικά από ό,τι είχε στο νου του ο ερευνητής[1032]. Η απουσία συνεντευκτή, αν και αποτρέπει την πιθανότητα εκδήλωσης προδιάθεσης και προκατάληψης και εξασφαλίζει την ανωνυμία, αποτελεί μειονέκτημα στην περίπτωση όπου τα υπό εξέταση θέματα του ερωτηματολογίου απαιτούν διευκρινιστικές επισημάνσεις.

Πέρα από την μη κατανόηση της ερώτησης, ο Παπάνης καταγράφει και άλλες περιπτώσεις ανακριβών απαντήσεων και, άρα, ελλείψεως αξιοπιστίας σε έρευνες οι οποίες διενεργούνται μέσω διαδικτύου, όπως οι περιπτώσεις α) συμμετεχόντων που εσκεμμένα παρέχουν ανακριβείς πληροφορίες διακατεχόμενοι από προσωπικά συμφέροντα, β) συμμετεχόντων με ελλιπή προσοχή οι οποίοι εξαιτίας του περιορισμένου χρόνου τους ή της μεγάλης έκτασης του ερωτηματολογίου δίνουν επιφανειακές και βιαστικές απαντήσεις, γ) υπερδραστήριων συμμετεχόντων που για διάφορους λόγους συμμετέχουν σε πολλές έρευνες και συμπληρώνουν αναρίθμητα ερωτηματολόγια και δ) συμμετεχόντων που μέσω της κλασικής εξαρτημένης μάθησης ως απόρροια της προγενέστερης συμμετοχής τους σε έρευνες διαφοροποιούν λόγω εμπειρίας της απαντήσεις τους[1033].

Στην παρούσα έρευνα έγινε προσπάθεια να περιοριστούν τα προβλήματα αυτά καταρχάς με επιστολή η οποία συνόδευε τα ερωτηματολόγια[1034] και στην οποία αναφερόταν ότι ήταν δυνατή η επικοινωνία των παραληπτών με τον επιβλέποντα της διδακτορικής διατριβής χάριν της οποίας λαμβάνει χώρα η εν λόγω έρευνα για παροχή τυχόν εξηγήσεων μέσω ηλεκτρονικής αλληλογραφίας[1035]. Επιπλέον,

---

[1032] *Θεόδωρος Χ. Κασκάλης, Αθανάσιος Α. Μαλέτσκος, Κωνσταντίνος Ε. Ευαγγελίδης*, Χρήση και αξιοποίηση ηλεκτρονικών ερωτηματολογίων σε έναν εκπαιδευτικό δικτυακό τόπο, Τμήμα Νηπιαγωγών, Παιδαγωγική Σχολή, Πανεπιστήμιο Δυτικής Μακεδονίας, url: http://www.etpe.eu/new/custom/pdf/etpe43.pdf, σελ. 457 και *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 63.

[1033] Έτσι ο *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 32-33.

[1034] Βλ. Παράρτημα V του παρόντος πονήματος.

[1035] *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 64.

προκρίθηκε η χρηση όχι μεγάλου ερωτηματολογίου[1036], η προσεκτική διατύπωση των ερωτήσεων και η χρήση ερωτήσεων επαλήθευσης και ελέγχου αξιοπιστίας[1037].

Επιπρόσθετα, οι έρευνες που αφορούν σε αυτομολογούμενη παραβατικότητα παρουσιάζουν σημαντικό εγγενές πρόβλημα αδυναμίας ακριβούς προσδιορισμού του αριθμού του συνόλου αυτών που υιοθετούν τέτοιες συμπεριφορές. Στην προκειμένη περίπτωση, είναι αδύνατο να γνωρίζουμε το σύνολο των hackers που δραστηριοποιούνται στην Ελλάδα ή /και που συνεργάζονται με τις εν λόγω ομάδες οι οποίες συμμετέσχον στο δείγμα[1038]. Η αδυναμία αυτή περιορίζει αναπόφευκτα τη δυνατότητα γενίκευσης των αποτελεσμάτων. Ωστόσο, όπως επισημάθηκε ήδη, το σύνολο του δείγματος επιτρέπει την αναγωγή των συμπερασμάτων στον πληθυσμό με ασφάλεια για ποσοτική και ποιοτική ανάλυση[1039]. Συμπληρωματικά, ως επιπλέον περιορισμός πρέπει να προστεθεί και η αδυναμία σύγκρισης των γενικών χαρακτηριστικών των συμμετεχόντων με αυτούς που δεν συμμετείχαν καθώς και η αδυναμία εκτίμησης της σύνδεσης συγκεκριμένων χαρακτηριστικών με την απόφαση της συμμετοχής ή μη στην έρευνα.

[1036] Βλ. και τις αναπτύξεις του *Χρήστου Κελπερή* εις *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 311 επ. αναφορικά με την έκταση και το μέγεθος του ερωτηματολογίου και την πρότασή του για σύντομο ερωτηματολόγιο.

[1037] Βλ. αναλυτικά παράγραφο 7.7.1 του παρόντος πονήματος. Αναφορικά με τον έλεγχο αξιοπιστίας στη μεθοδολογία της έρευνας πρβλ. *Σοφία Αναστασιάδου*, Στατιστική και Μεθοδολογία έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2012, σελ. 171 επ.

[1038] Το γεγονός ότι δεν (μπορούμε να) γνωρίζουμε πόσοι είναι οι hackers σήμερα στην Ελλάδα καταγράφεται και στο εμπεριστατωμένο ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy. Οι εκπρόσωποι και στις δύο ομάδες (GHS και hackerspace.gr) ρωτήθηκαν για το σύνολο των μελών της καθεμιάς. Κοινή απάντηση ήταν ότι δεν υπάρχει σταθερός αριθμός καθώς οι σχέσεις μεταξύ των μελών είναι αρκετά χαλαρές και πολλές φορές τα μέλη δεν γνωρίζονται καν μεταξύ τους. Ειδικά η ομάδα hackerspace.gr έχει στην ιστοσελίδα της αναρτημένο κατάλογο μελών (url: https://www.hackerspace.gr/wiki/People), ο οποίος, όμως, όπως μου ανέφεραν και οι συνεντευξιασθέντες Στέφανος και Αλέξανδρος (βλ. παράγραφο 7.5.5.5 του παρόντος πονήματος) έχει να κάνει με τους υπεύθυνους του χώρου (χαρακτηριστικά ειπώθηκε ότι «το να είσαι μέλος του hackerspace.gr γεννά υποχρεώσεις») και δεν εκφράζει το σύνολο όσων συμμετέχουν στις δράσεις του hackerspace.gr.

[1039] Αναφέρθηκε ήδη ότι το μέγεθος του δείγματος για κάθε μία από τις ερευνώμενες ομάδες και ιδίως για αυτή των hackers το οποίο τελικώς εξασφαλίστηκε (δεδομένων των δυσκολιών που έχουν αναφερθεί ανωτέρω) φαίνεται να καλύπτει τις ανάγκες και παραδοχές της βιβλιογραφίας σύμφωνα με την οποία «*πολλοί ερευνητές θεωρούν ότι πρέπει να έχουμε ως δείγμα τουλάχιστον τριάντα περιπτώσεις αν θέλουμε να χρησιμοποιήσουμε κάποια μορφή στατιστικής ανάλυσης των δεδομένων μας*» (έτσι *L. Cohen, L. Manion & K. Morrison*, Μεθολολογία εκπαιδευτικής έρευνας, εκδ. Μεταίχμιο, 2007, σελ. 151).

Επίσης, η παρούσα έρευνα – όπως όλες οι έρευνες που στηρίζονται σε ερωτηματολόγια αυτοναφοράς / αυτοδιαχειριζόμενα ερωτηματολόγια[1040] – παρουσιάζει, ενδεχομένως, έστω και μικρές αποκλίσεις από την πραγματικότητα. Τούτο εκτιμώ ότι οφείλεται σε δύο παράγοντες: Κατά πρώτον, έχουν ήδη καταγραφεί ανωτέρω οι προβληματισμοί αναφορικά με την θεώρηση του hacking και της χωρίς δικαίωμα πρόσβασης σε δεδομένα ως εγκληματική συμπεριφορά[1041] - η Σπινέλλη αναφέρεται στις πραγματικές δυσκολίες που προκύπτουν στο να προσπελάσει το υλικό της έρευνάς του καθώς «*έγκλημα δεν είναι (μόνο) ό,τι ο νόμος ορίζει αλλά (και) ό,τι οι εγκληματολόγοι προτείνουν*»[1042] και για αυτόν τον λόγο (όπως προτείνει η και πάλι η Σπινέλλη) διαλαμβάνεται ανωτέρω αναλυτική θεώρηση του hacking ακόμη και από ιστορική άποψη. Συνεπώς, υπάρχει περίπτωση στο ερωτηματολόγιο αυτοομολογούμενης παραβατικότητας να απαντήσουν όσοι θεωρούν τους εαυτούς τους hackers, χωρίς, ωστόσο, να προβαίνουν σε συμπεριφορές οι οποίες (πρέπει να) απασχολούν τον ποινικό νομοθέτη (π.χ. biohacking[1043]). Κατά δεύτερον, αποκκλίσεις μπορεί να οφείλονται στη συνειδητή η μή πρόθεση των συμμετεχόντων να εξωραΐζουν την εικόνα που δίνουν με τις απαντήσεις τους. Ειδικά σε ό,τι έχει να κάνει με την (αν)ακρίβεια των απαντήσεων αναφορικά με έρευνες αυτομολογούμενης παραβατικότητας (εν προκειμένω για το δείγμα των hackers) έχει καταγραφεί η δυσκολία της πλήρους διερεύνησης της έκτασης της διστακτικότητας ή αντίθετα της υπερβολικής προθυμίας των ερωτώμενων να δηλώσουν την παραβατική συμπεριφορά ή την εγκληματική τους δραστηριότητα[1044]. Κατά τον σχεδιασμό του ερωτηματολογίου και την επεξεργασία των απαντήσεων έγινε προσπάθεια με τη διατύπωση και την αλληλουχία των ερωτήσεων να περιοριστεί -κατά το δυνατόν- αυτή η δυνατότητα στους συμμετέχοντες και να αποκρυσταλλωθούν οι απαντήσεις τους[1045].

Σχετικά με το δείγμα, όπως παρουσιάστηκε ανωτέρω, άξιες λόγου είναι οι δύο εξής σκέψεις: κατά πρώτον, σε ό,τι έχει να κάνει με τους hackers επιδιώχθηκε η μεγαλύτερη δυνατή ανιπροσωπευτικότητα των τάσεων του hacking (black hat

[1040] Για τα αυτοδιαχειριζόμενα ερωτηματολόγια βλ. *Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 125.

[1041] Βλ. παράγραφο 2.6 και 2.7 καθώς και παράγραφο 4 του παρόντος πονήματος.

[1042] Βλ. *Κ. Δ. Σπινέλλη,* Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 87.

[1043] Βλ. σχετικώς παράγραφο 2.1 του παρόντος πονήματος.

[1044] Έτσι η *Αγγ. Πιτσελά,* Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002, σελ. 536-537.

[1045] Βλ. αναλυτικά παράγραφο 7.7.1 του παρόντος πονήματος.

hacking και white hat hacking) μέσω της συμμετοχής στην έρευνα hackers από δύο διαφορετικές υποομάδες (Greek Hacking Scene και hackerspace.gr) ως προς τη δράση και λειτουργία τους[1046]. Ωστόσο, στο σύνολο των 48 hackers δεν μπορούμε να γνωρίζουμε πόσοι ανήκουν στη μια και πόσοι στην άλλη ομάδα. Σε κάθε περίπτωση, όμως, όπως αναφέρθηκε ανωτέρω, χρησιμοποιήθηκε η τεχνική της χιονοστιβάδας ενόψει και της δυσκολίας να ανευρεθούν hackers και δεν χρησιμοποιήθηκε η τεχνική quota (μεριδίων)[1047] στη δειγματοληψία της έρευνας. Κατά δεύτερον, έχει ήδη αναφερθεί ότι το δείγμα νομικών επελέγη μέσω των χρηστών της ιστοσελίδας κοινωνικής δικτύωσης facebook.gr έτσι ώστε αυτοί να έχουν ηλεκτρονικά δεδομένα για τους λόγους που αναφέρθηκαν ανωτέρω[1048]. Όμως, οι απαντήσεις δεν αντιπροσωπεύουν το σύνολο των νομικών καθώς για την επιλογή του δείγματος νομικών υπάρχει μία επιπλέον προϋπόθεση πέρα από την ιδιότητά τους ως νομικοί (αυτή της διαχείρισης ηλεκτρονικών δεδομένων στο διαδίκτυο).

Τέλος, θα πρέπει να τονισθεί ότι οι έρευνες αυτού του είδους «φωτογραφίζουν» τα χαρακτηριστικά ενός συγκεκριμένου χρονικού διαστήματος. Με δεδομένο, όμως, ότι η τεχνολογία εξελίσσεται καθημερινά και μαζί με αυτήν τροποποιούνται και οι πρακτικές του hacking, τα χαρακτηριστικά αυτά είναι προφανές ότι δεν αναφέρονται σε κάτι το στατικό ή στάσιμο αλλα τροποποιούνται και αλλάζουν. Υπάρχει και εδώ ένας αέναος μετασχηματισμός του φαινομένου και, επομένως, του αντικειμένου προς έρευνα, δυναμικός και πολλές φορές υπεκφεύγων που για κάποια ευτυχή εγκληματολογική στιγμή ο ερευνητής καταφέρνει να δείξει μερικές από τις ως τώρα άφωτες ή ανεξιχνίαστες πτυχές του (κατά την όμορφη διατύπωση της Χαλκιά)[1049]. Ως εκ τούτου, πιθανώς η παρούσα έρευνα να έχει περιορισμένη χρονικά ισχύ.

7.7 Τα ερωτηματολόγια

[1046] Βλ. παράγραφο 7.5.5 του παρόντος πονήματος.
[1047] Βλ. παράγραφο 7.3.1.5 του παρόντος πονήματος.
[1048] Βλ. παράγραφο 7.5.3 του παρόντος πονήματος.
[1049] Βλ. *Αναστασία Χαλκιά*, όπ. π., σελ. 47.

Για τη διεξαγωγή της έρευνας δομήθηκαν τρία διαφορετικά διαδικτυακά ερωτηματολόγια, ένα για κάθε δείγμα, όπως ειπώθηκε ανωτέρω[1050]. Στα ερωτηματολόγια που αναφέρονται στους επιστήμονες πληροφορικής και τους νομικούς οι περισσότερες ερωτήσεις είναι κοινές ή κοινού προσανατολισμού, προκειμένου να μπορούν να συνδυαστούν και να συγκριθούν μεταξύ τους. Το ερωτηματολόγιο που απευθύνθηκε στους hackers έχει ερωτήσεις προσανατολισμένες σε δείγμα αυτοομολογούμενης παραβατικότητας.

Και τα τρία ερωτηματολόγια είχαν ως πρόλογο ενημερωτική επιστολή για τους σκοπούς και τα στοιχεία της έρευνας[1051] – στην επιστολή αυτή διευκρινίστηκε στους συμμετέχοντες ότι με την υποβολή συμπληρωμένου ερωτηματολογίου δίνουν τη συγκατάθεσή τους για τη συμμετοχή τους στην έρευνα χωρις αμοιβή και για την επεξεργασία των στοιχείων που επρόκειτο να καταχωρήσουν[1052].

7.7.1 Γενικές επισημάνσεις για τη διατύπωση των ερωτήσεων

Η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, όπως καταδείχθηκε ανωτέρω[1053], αποτελεί τη βασική δραστηριότητα των hackers – ωστόσο, η δράση των hackers δεν περιορίζεται μόνο στη χωρίς δικαίωμα πρόσβαση αλλά μπορούν να δράσουν και με τρόπους κατά τους οποίους δεν αποκτούν πρόσβαση σε δεδομένα αλλά δύνανται να αποκλείουν την πρόσβαση σε αυτά. Για τον λόγο αυτόν και με δεδομένο ότι στόχος (πρέπει να) είναι η προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών (βλ. ανωτέρω πρόταση για θεώρηση της ασφάλειας των ηλεκτρονικών δεδομένων ως προστατευόμενο έννομο αγαθό), προκρίθηκε από την ερευνητική ομάδα η διατύπωση των ερωτήσεων να αναφέρεται στο φαινόμενο του hacking εν γένει και όχι μόνο στη χωρίς δικαίωμα πρόσβαση σε

[1050] Βλ. παράγραφο 7.5.1 του παρόντος πονήματος.

[1051] Οι *Θεόδωρος Χ. Κασκάλης, Αθανάσιος Α. Μαλέτσκος, Κωνσταντίνος Ε. Ευαγγελίδης*, Χρήση και αξιοποίηση ηλεκτρονικών ερωτηματολογίων σε έναν εκπαιδευτικό δικτυακό τόπο, Τμήμα Νηπιαγωγών, Παιδαγωγική Σχολή, Πανεπιστήμιο Δυτικής Μακεδονίας, url: http://www.etpe.eu/new/custom/pdf/etpe43.pdf, σελ. 457, αναφέρουν ότι έχουν επισημανθεί από ερευνητές προβλήματα άρνησης συμπλήρωσης ερωτηματολογίου, όταν δεν προηγούνται των ερωτήσεων στοιχεία για τον δημιουργό του ερωτηματολογίου και τον σκοπό του.

[1052] Ολόκληρη η ενημερωτική επιστολή παρατίθεται στο Παράρτημα V του παρόντος πονήματος.

[1053] ... και ιδίως στο κεφάλαιο 2 της παρούσας.

ηλεκτρονικά δεδομένα. Επιπρόσθετα και δυνάμει των ανωτέρω, κρίθηκε ότι θα έπρεπε να καταγραφεί η γενικότερη άποψη αναφορικά με την ασφάλεια των ηλεκτρονικών δεδομένων στο διαδίκτυο. Συνεπώς, αποφασίστηκε η διατύπωση των ερωτήσεων να επικεντρωθεί στην προώθηση της ασφάλειας των ηλεκτρονικών δεδομένων και απορρίφθηκαν διατυπώσεις οι οποίες έχουν να κάνουν με την «πρόληψη του hacking» κ.λπ.[1054] Τούτο και προκειμένου να δοθεί στις ενέργειες hacking μια ουδέτερη διάσταση και να μην υπολαμβάνεται καταρχήν ως δραστηριότητα με αρνητικό περιεχόμενο, λαμβανομένου υπόψιν και το ότι αποτελεί δύσκολο εγχείρημα να κερδίσει κανείς την εμπιστοσύνη των hackers[1055], έτσι ώστε να αποφευχθεί και τυχόν καθοδηγητικός χαρακτήρας των ερωτήσεων[1056].

Περαιτέρω, τα ερωτηματολόγια καταρτίστηκαν με τέτοιο τρόπο ώστε οι ερωτήσεις οι οποίες περιλαμβάνουν να δύνανται να αυτοελεγχθούν για την εγκυρότητα των συλλεχθέντων στοιχείων στο πλασίο του αναστοχασμού και της αξιολογικής διάστασης αυτού[1057]. Συγκεκριμένα, από το σύνολο των ερωτήσεων σε κάθε ερωτηματολόγιο μπορεί να προκύψει η συνέπεια ή ασυνέπεια του συμμετέχοντος στην έρευνα στη στάση του και άποψή του σχετικά με το hacking και να καταγραφούν, μέσω σύγκρισης όλων των απαντήσεων μεταξύ τους, τυχόν αξιολογικές αντινομίες. Δηλαδή, κατεβλήθη προσπάθεια οι ερωτήσεις να διατυπωθούν με τέτοιο τρόπο ώστε κάθε μία από αυτές να μπορεί να λειτουργήσει ελεγκτικά και επαληθευτικά αναφορικά με απάντηση του συμμετέχοντος σε άλλη ερώτηση του ερωτηματολογίου.

7.7.2 Δημογραφικά στοιχεία

[1054] Βλ. και τις αναπτύξεις του *Χρήστου Κελπερή* εις *Ι. Λαμπίρη - Δημάκη*, Κοινωνικές έρευνες με στατιστικές μεθόδους, όπ. π. σελ. 305 επ. αναφορικά με την επιλογή των λέξεων στη διατύπωση των ερωτήσεων.

[1055] *Michael Bachmann*, What makes them click? Applying the rational choice perspective to the hacking undergroung, 2004, όπ. π., σελ. 72-73.

[1056] Αναφορικά με τις καθοδηγητικές ερωτήσεις πρβλ. το άρθρο "Leading questions lead to bad data" (url: http://survey.cvent.com/blog/cvent-survey-blog/leading-questions-lead-to-bad-data).

[1057] Βλ *P. Bourdieu*, Επιστήμη της επιστήμης και αναστοχασμός, Μετάφραση: Θ. Παραδέλλης, Εκδόσεις Πατάκη, Αθήνα 2005, σελ. 199, όπως παραπέμπεται στο παρόν πόνημα και σε ανωτέρω υποσημείωση σχετικά με τις ερωτήσεις ελέγχου.

Οι πρώτες ερωτήσεις κάθε ερωτηματολογίου αναφέρονται σε δημογραφικά στοιχεία και έπειτα ακολουθούν οι υπόλοιπες ερωτήσεις. Τα δημογραφικά στοιχεία που αναζητήθηκαν από τους συμμετέχοντες στο δείγμα είναι η ηλικία τους (επιλογές: 1-20, 21-30, 31-40, 41-50, 51-60, 61+)[1058] και το φύλο τους[1059]. Επίσης, οι συμμετέχοντες κλήθηκαν να δηλώσουν το μορφωτικό τους επίπεδο μεταξύ των εξής επιλογών: α) απόφοιτος δημοτικού, β) απόφοιτος γυμνασίου, γ) απόφοιτος δευτεροβάθμιας εκπαίδευσης (λύκειο κ.ά.), δ) απόφοιτος ΑΕΙ – ΤΕΙ, ε) κάτοχος μεταπτυχιακού διπλώματος και στ) κάτοχος διδακτορικού διπλώματος.

7.7.3 Τα ερωτηματολόγια για το δείγμα νομικών και το δείγμα επιστημόνων πληροφορικής

Όπως διατυπώθηκε ανωτέρω, στα δύο αυτά δείγματα ειδημόνων οι περισσότερες από τις ερωτήσεις που διατυπώθηκαν ήταν κοινές ή κοινού προσανατολισμού προκειμένου να μπορούν να συνδυαστούν και να συγκριθούν μεταξύ τους. Παρακάτω ακολουθούν οι ερωτήσεις που ετέθησαν στα δύο αυτά δείγματα – οι κοινές ερωτήσεις αναφέρονται μία φορά ενώ στις περιπτώσεις κατά τις οποίες η ερώτηση τυχόν διαφοροποιείται ανάλογα με το δείγμα παρατίθενται και οι δύο ερωτήσεις.

1) Τι είναι hacking σύμφωνα με την εμπειρία σας;

(ανοικτού τύπου ερώτηση)

Ο ορισμός της έννοιας του hacking στην ψηφιακή κοινωνία που συνεχώς εξελίσσεται από πλευράς του ερωτώμενου νομικού και επιστήμονα πληροφορικής (υπεύθυνου

[1058] Έτσι όπως προτείνεται και από τον Παπάνη, ο οποίος μιλά για κατηγορίες εύρους στα δημογραφικά στοιχεία (έτσι *Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 62-63).

[1059] Αναφορικά με τον ρόλο της ηλικίας και του φύλου στην εγκληματικότητα βλ. ενδεικτικά τις αναπτύξεις της *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 84 επ. και 82 επ. αντίστοιχα. Πρβλ. επίσης και *Φωτεινή Α. Μηλιώνη*, Το "φύλο" ως ιδιαίτερη παράμετρος στην εγκληματολογική έρευνα, εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 587-594.

ασφαλείας δεδομένων) αντίστοιχα θα αποτελέσει σημαντικό εύρημα για την παρούσα έρευνα. Ο νομικός, με τη σχετική του παιδεία και εμπειρία και δεδομένου ότι η νομική είναι κοινωνική επιστήμη, η οποία προσεγγίζει τις συμπεριφορές έτσι όπως γίνονται και κοινωνικά αντιληπτές, δύναται να αποτυπώσει το περιεχόμενο του υπό έρευνα φαινομένου στη σύγχρονη διάστασή του προκειμένου να επιτευχθεί η προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών. Αντίστοιχα και ο επιστήμονας πληροφορικής (συνήθως ο ίδιος διαχειριστής ηλεκτρονικών δεδομένων) με τη δική του ειδική γνώση και εμπειρία αλλά και τον καίριο ρόλο του στην ασφάλεια των ηλεκτρονικών πληροφοριών (αποτροπή, πρόληψη με τεχνικά μέσα κ.ά.), δύναται και αυτός να προσδώσει στο περιεχόμενο του hacking τη σύγχρονη διάστασή του και να αποτυπώσει την προβληματική που ενδεχομένως δημιουργείται στην ασφάλεια των ηλεκτρονικών δεδομένων. Επίσης, οι συμμετέχοντες και στα δύο δείγματα (νομικοί και επιστήμονες πληροφορικής) είναι αυτοί οι οποίοι θα αξιολογήσουν στην παρούσα έρευνα την αποτελεσματικότητα των νόμων για την ασφάλεια της πληροφορίας και θα προτείνουν επιπλέον μέτρα και πολιτικές – άρα, είναι σκόπιμο να καταγραφεί από την αρχή το αν και κατά πόσο πόσο είναι γνώστες του φαινομένου του hacking. Τέλος, η ίδια ερώτηση έχει τεθεί και στο δείγμα των hackers, με σκοπό να συγκριθούν οι απαντήσεις όλων των δειγμάτων σκοπιμότητας μεταξύ τους και έτσι να διαπιστωθεί αν με τον όρο hacking εννοούνται από όλους οι ίδιες συμπεριφορές προκειμένου να υπάρχει μια κοινή βάση συζήτησης για τις πολιτικές ασφάλειας δεδομένων που θα (ή πρέπει να) ακολουθηθούν.

2) Πιστεύετε ότι οι hackers ενεργούν περισσότερο με βάση ιδεολογικά κίνητρα ή με σκοπό το οικονομικό όφελος;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

Η αναγνώριση των κινήτρων των hackers αποτελεί τη δεύτερη υπόθεση έρευνας, έτσι όπως έχει διατυπωθεί ανωτέρω. Έχει ήδη προηγηθεί, στο δεύτερο κεφάλαιο της παρούσας, αναλυτική ανάπτυξη των καταγραφέντων στη βιβλιογραφία κινήτρων των hackers. Με τη συγκεκριμένη ερώτηση στα δύο δείγματα ειδημόνων μέσα από την

εμπειρία τους προσπαθούμε να ανιχνεύσουμε την άποψη για το ποιος τελικώς είναι ο σκοπός που υπερισχύει (ιδεολογικός ή οικονομικός). Βέβαια, μη παραγνωρίζοντας ότι ως κίνητρο μπορει να καταγραφεί και σκοπός ο οποίος δεν εντάσσεται στις δύο αυτές κατηγορίες (π.χ. διασκέδαση), συμπεριελήφθη στο ηλεκτρονικό ερωτηματολόγιο και η επιλογή «Άλλο» (ούτως ώστε ο συμμετέχων στην έρευνα να έχει τη δυνατότητα να καταγραφεί επακριβώς η άποψή του και με αυτόν τον τρόπο να καταστούν πληρέστερα τα ερευνητικά μας δεδομένα). Το πόρισμα το οποίο θα προκύψει θα μας βοηθήσει στο να προσδιορίσουμε ακριβέστερα ποιες από τις εγκληματολογικές θεωρίες που έχουν παρουσιαστεί στο κεφάλαιο 3 της παρούσας διατριβής βρίσκονται πιο κοντά στην αιτιολόγηση και ερμηνεία των ενεργειών hacking καθώς και να διατυπωθούν de lege ferenda προτάσεις.

3) <u>Ερώτηση σε νομικούς:</u>

Θεωρείτε ότι οι έλληνες νομικοί που ασχολούνται με το δίκαιο της πληροφορικής είναι επαρκώς ενημερωμένοι και εκπαιδευμένοι σε θέματα πληροφορικής και ιδίως hacking;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)

Ο ερωτώμενος νομικός είναι, λόγω της ιδιότητάς του, ο πλέον κατάλληλος να κρίνει το βαθμό κατάρτισης σε θέματα hacking των ελλήνων συναδέλφων του νομικών, οι οποίοι ασχολούνται στην πράξη με το δίκαιο της πληροφορικής. Η συγκεκριμένη ερώτηση θα συνδράμει στον σχηματισμό εικόνας για το επίπεδο γνώσης και ικανότητας των νομικών σε θέματα hacking. Η γνώση του νομικού στην Ελλάδα για την ασφάλεια της πληροφορίας παίζει σημαντικό ρόλο αναφορικά με την ανάπτυξη νομικών θεωριών και απόψεων για το οικείο νομικό πλαίσιο. Επιπρόσθετα, ο βαθμός «ενημέρωσης» ειδικών της νομικής επιστήμης για σχετικά θέματα πληροφορικής και ασφάλειας των ηλεκτρονικών πληροφοριών θα καταδείξει το αν η σύγχρονη νομική αντιμετώπιση ή πρακτικές αντεγκληματικές πολιτικής θα μπορούν να γίνουν κατανοητές από τους έλληνες νομικούς. Οι έλληνες νομικοί, ως συλλειτουργοί στην εφαρμογή ή ακόμη και στην κατάρτιση του δικαίου, μπορούν να λειτουργήσουν καταλυτικά εφόσον έχουν το κατάλληλο γνωσιακό υπόβαθρο στην αποτελεσματική

και απρόσκοπτη λειτουργία σύγχρονων de lege ferenda ρυθμίσεων και προτάσεων αντεγκληματικής πολιτικής.

<u>Ερώτηση σε επιστήμονες πληροφορικής:</u>

Θεωρείτε ότι οι έλληνες επιστήμονες πληροφορικής είναι επαρκώς ενημερωμένοι σε σύγχρονα θέματα ασφάλειας των ηλεκτρονικών δεδομένων;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)

Το ενδιαφέρον εστιάζεται εν προκειμένω στο βαθμό ενημέρωσης των ελλήνων επιστημόνων πληροφορικής σχετικά με τα σύγχρονα θέματα ασφάλειας των ηλεκτρονικών δεδομένων. Αυτός ο βαθμός ενημέρωσης θα συντελέσει καταλυτικά στην προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων καθώς θα μπορέσουμε να διαγνώσουμε την άποψη των συμμετεχόντων στο δείγμα για την κατάρτιση των συναδέλφων τους και, άρα, και τη δυνατότητα τεχνικών λύσεων -πέραν των νομικών- στην πρόληψη των προσβολών των ηλεκτρονικών δεδομένων και κυρίως την ικανότητα των επιστημόνων πληροφορικής να τις υποστηρίξουν.

4) Πιστεύετε ότι οι δράσεις των hackers μπορούν να έχουν θετική συμβολή στην κοινωνία; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Ο ανοικτός τύπος της ερώτησης στοχεύει στην αυθόρμητη απάντηση των ερωτώμενων αναφορικά με τον (θετικό – εφόσον κρίνουν ότι υπάρχει) κοινωνικό αντίκτυπο των συμπεριφορών των hackers στην κοινωνία. Υπάρχει η περίπτωση διατύπωσης θετικών απόψεων και ιδεών αναφορικά με τη χρησιμοποίηση των δεξιοτήτων των hackers προς όφελος του κοινωνικού συνόλου. Οι απαντήσεις αυτές θα συνδράμουν στην παραγωγή ιδεών για πρακτικές αντεγκληματικής πολιτικής, οι οποίες θα αξιοποιούν τις ιδιαίτερες δυνατότητες και γνώσεις των hackers. Τέλος, ειδικά ο επιστήμονας πληροφορικής είναι από την ιδιότητά του σε θέση να γνωρίζει

ώς ένα σημαντικό βαθμό τη φύση των διαφόρων δράσεων των hackers και, συνεπώς, δύναται εκ των πραγμάτων να προβεί σε βάσιμη εκτίμηση περί τυχόν θετικής συμβολής του hacking.

5) Κατά τη γνώμη σας, η ελληνική νομοθεσία είναι αποτελεσματική για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ - Δεν είμαι ενημερωμένος για τις νομικές προβλέψεις)

Αυτή είναι η κεντρική ερώτηση αξιολόγησης της ισχύουσας ελληνικής νομοθεσίας. Οι νομικοί, γνώστες της ελληνικής ποινικής νομοθεσίας και του ποινικού συστήματος, δύνανται φύσει και θέσει να αποφανθούν περί της αποτελεσματικότητας της ελληνικής νομοθεσίας[1060] με τελικό στόχο την ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων. Περαιτέρω, οι διαχειριστές ηλεκτρονικών δεδομένων βρίσκονται αρκετές φορές στο επίκεντρο του προβλήματος ανασφάλειας των ηλεκτρονικών δεδομένων και συνεπώς της ανάγκης εφαρμογής της νομοθεσίας είτε οι ίδιοι ως θύματα είτε, κυριότερα, εκπροσωπώντας σε τεχνικό επίπεδο αυτούς των οποίων τα δεδομένα έχουν παραβιαστεί.

6) Πρέπει να είναι ελεύθερη η πρόσβαση στην πληροφορία στο διαδίκτυο; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Το ερώτημα για την ελευθερία πρόσβασης στην πληροφορία στο διαδίκτυο και τα όρια αυτής άπτεται νομικών παραμέτρων, καθώς οι νομικοί θα κληθούν να ρυθμίσουν τα όρια αυτά. Η ελευθερία στην πρόσβαση της πληροφορίας στο διαδίκτυο αποτελεί τον πυρήνα της ιδεολογίας των hackers και ουσιαστικά το

[1060] Αναφορικά με τους παράγοντες αποτελεσματικότητας των κανόνων δικαίου βλ. *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 205 επ.

«δικαίωμά» τους κατ' αυτούς για πρόσβαση σε ηλεκτρονικά δεδομένα[1061]. Στη συγκεκριμένη ερώτηση καλούνται οι νομικοί, με δεδομένο ότι κατά τεκμήριο έχουν αισθητήριο στάθμισης συγκρουόμενων δικαιωμάτων, να διατυπώσουν άποψη και να θέσουν όρια, δίνοντας έτσι τα άκρα της (δεοντολογικής) νομιμοποίησης ή όχι της ιδεολογίας των hackers.

Το συγκεκριμένο ερώτημα, περαιτέρω, άπτεται και των ενδιαφερόντων και γνώσεων των επιστημόνων πληροφορικής/τεχνικών ασφαλείας ηλεκτρονικών δεδομένων, καθώς είναι αυτοί που στις περισσότερες περιπτώσεις δημιουργούν τις «οχυρώσεις» και τα τεχνικά εμπόδια για περιορισμό της πρόσβασης. Στη συγκεκριμένη ερώτηση καλούνται και οι διαχειριστές ηλεκτρονικών δεδομένων να διατυπώσουν άποψη και να θέσουν όρια, δίνοντας και αυτοί – όπως και οι νομικοί – από τη δική τους πλευρά και με τις δικές τους γνώσεις και εμπειρίες τα άκρα της (δεοντολογικής) νομιμοποίησης ή όχι της ιδεολογίας των hackers.

7) Έχετε να προτείνετε άλλα μέτρα - πέρα από ποινικές διατάξεις - που μπορούν να ληφθούν για την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων; Αν ναι, ποια;

(ανοικτού τύπου ερώτηση)

Η ερώτηση επικεντρώνεται στο να εξετάσει εάν η ανάπτυξη και η προώθηση εναλλακτικών μέτρων (δικαιικών και μη) μπορεί να αποτελέσει σημαντικό εργαλείο για την επίτευξη του στόχου. Η ερώτηση στοχεύει στην αναζήτηση μεθόδων και πρακτικών που να κινούνται εκτός του ποινικού συστήματος και της ποινικής δικαιοσύνης. Η συγκεκριμένη ερώτηση ελέγχει αν και κατά πόσο τα ως άνω ενδεικτικώς αναφερόμενα στη οικεία (τέταρτη) υπόθεση έρευνας μέτρα είναι γνωστά (δια τούτο και η ερώτηση ανοικτού τύπου – προκειμένου να μη δοθούν ήδη ιδέες στους απαντώντες) και αν και κατά πόσο αυτά θεωρούνται πρόσφορα και αποτελεσματικά για την ασφάλεια των δεδομένων. Τέλος, στην ερώτηση αυτή δίνεται η δυνατότητα σε νομικούς και επιστήμονες πληροφορικής να προτείνουν οι ίδιοι μέτρα αντεγκληματικής πολιτικής τα οποία θα μπορούσαν να ενισχύσουν την

[1061] Βλ. σχετικά ανωτέρω αναπτύξεις στο κεφάλαιο 2 του παρόνος πονήματος.

ασφάλεια των ηλεκτρονικών δεδομένων. Οι προτάσεις αυτές μπορούν να καταγραφούν, να ενοποιηθούν και να αποτελέσουν σημαντικό ερευνητικό εύρημα το οποίο θα συνδράμει στην υιοθέτηση συναφών πρακτικών.

8) Πόσο ασφαλής νιώθετε αναφορικά με τα ηλεκτρονικά σας δεδομένα στο διαδίκτυο;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)

Το αίσθημα ασφάλειας[1062] των νομικών και των επιστημόνων πληροφορικής επιδρά και αντικατοπτρίζεται στις απαντήσεις που έχουν αντιστοίχως δοθεί στις ερωτήσεις των ερωτηματολογίων (και ιδίως στην ερώτηση που ακολουθεί σχετικά με την αυστηρότητα της ποινικής νομοθεσίας)[1063]. Επίσης, δεδομένης της διαρκώς αυξανόμενης χρήσης του διαδικτύου και των λειτουργιών του από τον μέσο νομικό (ανάπτυξη νομοπληροφορικής, βάσεις νομικών δεδομένων, ηλεκτρονική υπογραφή, ηλεκτρονική κατάθεση δικογράφων κ.λπ.), η έκθεση σε κίνδυνο σημαντικών ηλεκτρονικών δεδομένων του νομικού είναι αναπόφευκτη. Αντίστοιχα, ο επιστήμονας πληροφορικής, ως υπεύθυνος για ηλεκτρονικά δεδομένα, είναι αυτός που γνωρίζει καλύτερα από όλους τους κινδύνους των ηλεκτρονικών δεδομένων, το πόσο ευάλωτα μπορούν να είναι τα ηλεκτρονικά δεδομένα και συνάμα και οι κάτοχοί τους αναφορικά με ηλεκτρονικές προσβολές και επιθέσεις και μπορεί ουσιαστικά να δώσει με τον πιο εναργή τρόπο τους πραγματικούς δείκτες ανασφάλειας αναφορικά με τα ηλεκτρονικά συστήματα πληροφοριών σήμερα. Τέλος, ο δείκτης αυτός θα παίξει σημαντικό ρόλο στην πρόταση πολιτικών και μέτρων προαγωγής της ασφάλειας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών, καθώς θα πρέπει αυτά να ανταποκρίνονται στο αίσθημα των ερωτώμενων, ιδίως λαμβανομένου υπόψιν ότι μια από τις σημαντικότερες απόρροιες της έννοιας και της κατάστασης της ανασφάλειας είναι η ενίσχυση της τιμωρητικότητας των πολιτών[1064],

[1062] Βλ. ανωτέρω την παράγραφο 1.3 της παρούσας.

[1063] Ο φόβος του εγκληματος στο διαδίκτυο αποτελεί αντικείμενο σύγχρονων ερευνών. Βλ. χαρακτηριστικά τη σημαντική έρευνα της *Χρ. Ζαραφωνίτου και συν.*, Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο, όπ. π.

[1064] Για την έννοια, τις όψεις και τις διαστάσεις της τιμωρητικότητας πρβλ. ενδεικτικά το αναλυτικό πόνημα της *Χρ. Ζαραφωνίτου*, Τιμωρητικότητα: ανασφάλεια και κοσμοθεωρία, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος

η οποία λειτουργεί αποπροσανατολιστικά στη χάραξη αντεγκληματικής πολιτικής με κοινωνικο-προληπτικό χαρακτήρα[1065].

9) Ποια η γνώμη σας: χρειάζεται αυστηροποίηση των ποινικών κυρώσεων, αποποινικοποίηση του hacking ή οι νομικές προβλέψεις να μείνουν ως έχουν;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για τη διατύπωση τυχόν διαφορετικής άποψης)

Στη συγκεκριμένη ερώτηση θα καταγραφεί η άποψη νομικών και επιστημόνων πληροφορικής για το αν οι κείμενες ποινικές διατάξεις για το hacking πρέπει να αλλάξουν και προς ποια κατεύθυνση. Η καταγραφή της τάσης αυτής είναι σημαντική γιατί θα καταδείξει την άποψη της κοινής γνώμης για τη χρήση του δικαίου αναφορικά με την ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών και το προς ποια κατεύθυνση οι ειδήμονες των δειγμάτων επιθυμούν να στραφούν de lege ferenda οι ποινικές διατάξεις για το hacking. Σε ό,τι αφορά στη λειτουργία της ερώτησης ως ερώτηση ελέγχου της αξιοπιστίας, κάθε ερωτηματολόγιο ελέγχεται για τη συνέπεια και τη συνεκτικότητα της άποψης αυτού που απαντά σε συνάρτηση και με τις απαντήσεις του συμμετέχοντος σε παραπάνω ερωτήσεις (π.χ. αν σε κάποιο ερωτηματολόγιο ο συμμετέχων στην ερώτηση υπ' αρ. 6 θεωρεί ότι η πρόσβαση στην πληροφορία στο διαδίκτυο δεν πρέπει να είναι ελεύθερη είναι οξύμωρο να υποστηρίξει στην εν λόγω ερώτηση την αποποινικοποίηση / απεγκληματοποίηση του hacking).

<u>Ερώτηση υπ' αρ. 10 στο ερωτηματολόγιο των νομικών</u>

<u>και υπ' αρ. 12 στο ερωτηματολόγιο των επιστημόνων πληροφορικής:</u>

Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τεύχος 13, Φεβρουάριος 2010, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1263811765. Ενισχυτικοί της τιμωρητικής στάσης μπορεί να είναι και οι δημιουργούμενοι από τα ΜΜΕ «ηθικοί πανικοί» (βλ. *Χ. Ζαραφωνίτου*, Όψεις και διαστάσεις του κοινωνικού φαινομένου της ανασφάλειας, εις: *Χ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, όπ. π., σελ. 45).

[1065] *Χρ. Ζαραφωνίτου*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, Αθήνα-Κομοτηνή, εκδ. Αντ. Ν. Σάκκουλα, 2007, σελ. 55-56.

Όποιος αποκτά χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα στο διαδίκτυο με σκοπό οικονομικό όφελος ή πρόκληση ζημίας πρέπει να έχει την ίδια, ηπιότερη ή αυστηρότερη ποινική μεταχείριση από τον νόμο σε σχέση με αυτόν που δεν έχει σκοπό το οικονομικό όφελος ή την πρόκληση ζημίας;

(κλειστού τύπου ερώτηση: Την ίδια ποινική μεταχείριση – Αυστηρότερη ποινική μεταχείριση – Ηπιότερη ποινική μεταχείριση - Καμία ποινική μεταχείριση για χωρίς δικαίωμα πρόσβαση ανεξαρτήτως σκοπού ή αποτελέσματος)

Η ερώτηση αυτή έρχεται ως συνέχεια και ως διευκρινιστική της προηγούμενης και θέτει υπό έρευνα αν de lege ferenda η ποινική μεταχείριση θα πρέπει να εξαρτάται από το κίνητρο των hackers ή από το αποτέλεσμα της πράξης τους, ιδίως σε περίπτωση που ο σκοπός ή το αποτέλεσμα έχουν οικονομικό αντίκτυπο. Η επιλογή για «καμία ποινική μεταχείριση» έχει τεθεί προκειμένου να μπορούν να εκφράσουν την άποψή τους και οι τυχόν υποστηρικτές της αποποινικοποίησης του hacking και να μην αποκλείεται η άποψή τους από τις δυνατότητες των απαντήσεων.

<u>Επιπλέον ερωτήσεις στο ερωτηματολόγιο των επιστημόνων πληροφορικής</u>

10) Ως τεχνικός ασφαλείας ή διαχειριστής ηλεκτρονικών δεδομένων, έχετε αντιμετωπίσει περιστατικά hacking;

(κλειστού τύπου ερώτηση)

Μέσω του παρόντος ερωτήματος ερευνάται ο βαθμός εμπειρίας του τεχνικού ασφαλείας/επιστήμονα πληροφορικής όσον αφορά στην αντιμετώπιση του hacking αλλά και η συχνότητα θυματοποίησης από πρακτικές hacking, με δεδομένο ότι οι επιστήμονες πληροφορικής ως τεχνικοί ασφάλειας ηλεκτρονικών δεδομένων διαχειρίζονται συστήματα και σύνολα ψηφιακών πληροφοριών.

11) Θα συνεργαζόσασταν ποτέ με έναν hacker προκειμένου να βελτιώσετε μία πρακτική ασφαλείας;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

Η ιδέα της συνεργασίας ενός επιστήμονα πληροφορικής, ο οποίος λειτουργεί ως τεχνικός ασφαλείας ή διαχειριστής ηλεκτρονικών δεδομένων, με έναν hacker, με σκοπό τη βελτίωση πρακτικών ασφαλείας των ηλεκτρονικών δεδομένων, φέρεται να εφαρμόζεται ήδη στην πράξη από πολλές εταιρίες και οργανισμούς[1066]. Στο συγκεκριμένο ερώτημα ιχνηλατείται το κατά πόσον η συνδρομή των hackers είναι ευρύτερα αποδεκτή από τους επιστήμονες πληροφορικής, με δεδομένο ότι ο ρόλος των επιστημόνων πληροφορικής βρίσκεται εξ ορισμού απέναντι σε όσους απειλούν ή πλήττουν την ασφάλεια των ηλεκτρονικών δεδομένων.

7.7.4 Το ερωτηματολόγιο για το δείγμα hackers

1) Τι είναι hacking σύμφωνα με την εμπειρία σας; *(ανοικτού τύπου ερώτηση)*

Στην προσπάθεια περιγραφής της σύγχρονης έννοιας του hacking, όπως διαλαμβάνεται στην πρώτη υπόθεση έρευνας, η αποτύπωση από τους ίδιους τους hackers είναι ίσως το πιο σημαντικό εύρημα, το οποίο, σε συνδυασμό και με τα πορίσματα από τα ανωτέρω ερωτηματολόγια, θα μας δώσει την πληρέστερη δυνατή προσέγγιση. Το δείγμα hackers αποτελεί πρωτογενή πηγή καταγραφής του τρόπου με τον οποίο οι ίδιοι οι επιχειρούμενοι και δρώντες αντιλαμβάνονται την έννοια και τα βασικά χαρακτηριστικά της δραστηριότητας αυτής. Το πόρισμα το οποίο θα προκύψει από τη σύγκριση με τα αποτελέσματα των άλλων δύο δειγμάτων θα συνδράμει στην βαθύτερη κατανόηση του hacking προκειμένου να προταθούν επικαιροποιήμενα μέτρα και δράσεις αντεγκληματικής πολιτικής.

[1066] Βλ. το “ethical hacking”, όπως αναλύθηκε ανωτέρω (παράγραφος 2.9.1).

2) Ποιος ο σκοπός της δράσης σας; Υπάρχει ιδεολογικό υπόβαθρο; Είχατε ποτέ έως τώρα οποιουδήποτε είδους οικονομική ωφέλεια από την ενασχόλησή σας με το hacking; *(ανοικτού τύπου ερώτηση)*

Η ερώτηση αυτή αποτελείται από τρία σκέλη και προσπαθεί να αποσαφηνίσει τους σκοπούς της δράσης των hackers και να ανιχνεύσει ιδεολογικές βάσεις και τυχόν οικονομική ωφέλεια των ενασχολουμένων, σύμφωνα και με την αντίστοιχη υπόθεση έρευνας, όπως έχει διατυπωθεί ανωτέρω.

Η γενική διατύπωση του πρώτου σκέλους της ερώτησης αφήνει ελευθερία στον hacker να προσεγγίσει ο ίδιος τα κίνητρα της δράσης του, προκειμένου έτσι να καταγραφούν αυτά από την έρευνα. Τούτο διότι, παρά το γεγονός ότι στην οικεία υπόθεση έρευνας προσπαθούμε να ανιχνεύσουμε αν η ιδεολογία ή το οικονομικό όφελος υπερτερούν ως βασικό κίνητρο των hackers[1067], δεν πρέπει να διαφύγουν του ερευνητικού μας πορίσματος κίνητρα τα οποία μάλλον δεν εντάσσονται στις δύο αυτές κατηγορίες όπως π.χ. η διασκέδαση ή η εξάσκηση.

Το δεύτερο και το τρίτο σκέλος της ερώτησης λειτουργούν από κοινού προκειμένου να διευκρινίσουν αν υπάρχει επίκληση ιδεολογικού υπόβαθρου ή αν οι hackers του δείγματος στοχεύουν περισσότερο σε οικονομικό όφελος. Το πόρισμα, το οποίο και εδώ θα προκύψει από τις απαντήσεις σε αυτήν την ερώτηση (και βέβαια τη σύγκρισή τους με τις σχετικές απαντήσεις των άλλων δύο δειγμάτων της έρευνας), θα μας οδηγήσει σε συμπεράσματα σχετικά με τις εγκληματολογικές θεωρίες, οι οποίες πλησιάζουν περισσότερο στην αιτιολόγηση και ερμηνεία των ενεργειών hacking, όπως αυτές αναφέρθηκαν στο κεφάλαιο 3 του παρόντος πονήματος και θα κατευθύνει τη σκέψη μας για διατύπωση de lege ferenda προτάσεων.

3) Πόσα χρόνια ασχολείστε με το hacking;

[1067] Οι *Budi Arief & Denis Besnard,* Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, όπ. π., σελ. 12-13 παραπέμπουν στη Denning και στην έρευνα του Chantler (1996) κατά την οποία σε 164 hackers ως κορυφαία κίνητρα αναγνωρίστηκαν η θέληση για γνώση με ποσοστό 49%, η αναγνώριση και ο ενθουσιασμός (για τη διάπραξη παράνομης πράξης) και η φιλία με ποσοστό 24% και το κέρδος και η εκδίκηση με ποσοστό 27%.

(κλειστού τύπου ερώτηση: έως 1 έτος – 1 έως 2 έτη – 2 έως 5 έτη – 5 έως 10 έτη – 10 και άνω έτη)

Η χρονική διάρκεια ενασχόλησης με το hacking αποτελεί ένα πρόσθετο σημαντικό στοιχείο για τον ερευνητή προκειμένου να είναι σε θέση να αξιολογήσει το βαθμό εμπειρίας του ερωτώμενου hacker.

4) Σημαίνει κάτι για εσάς ο όρος "ethical hacking"[1068];

(ανοικτού τύπου ερώτηση)

Ο ρόλος της συγκεκριμένης ερώτησης είναι αρχικά διευκρινιστικός της ερώτησης 2 του ερωτηματολογίου των hackers. Όπως καταδείχθηκε ανωτέρω (βλ. παράγραφο 2.9.1), οι ηθικοί παραβιαστές ανακαλύπτουν κενά ασφαλείας σε ένα σύστημα συνήθως μετά από εντολή των διαχειριστών του (ενδεχομένως και με αμοιβή). Άρα, η ερώτηση έχει τεθεί προκειμένου να συμπεριληφθεί στα αποτελέσματα η περίπτωση των hackers οι οποίοι έχουν αποκομίσει οικονομικό όφελος από το hacking χωρίς όμως να βλάψουν την ασφάλεια συστημάτων υπολογιστών και ηλεκτρονικών πληροφοριών, δεδομένης της συγκατάθεσης των διαχειριστών των υπό εξέταση δεδομένων.

Επιπρόσθετα, ο ρόλος της ερώτησης αυτής είναι και ελεγκτικός της αξιοπιστίας του hacker στην ερώτηση 2. Η άποψή του και η στάση του για το ethical hacking πρέπει να εναρμονίζεται με όσα απάντησε στην ερώτηση 2 αναφορικά με τον σκοπό και το κίνητρο της δράσης του.

5) Η ισχύουσα ελληνική νομοθεσία σας έχει αποτρέψει από την επέκταση της δράσης σας;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)

[1068] Ο όρος "ethical hacking" αναλύθηκε στο κεφάλαιο 2 και συγκεκριμένα στην παράγραφο 2.9.1 του παρόντος πονήματος.

Με την παρούσα ερώτηση διερευνάται η αποτελεσματικότητα των ποινικών διατάξεων σε επίπεδο γενικής πρόληψης[1069] και συγκεκριμένα η αποτρεπτική λειτουργία, η οποία επιτελούν. Τα συμπεράσματα τα οποία θα προκύψουν από αυτήν την έρευνα αυτοομολογούμενης παραβατικότητας θα συγκριθούν και με τις σχετικές απαντήσεις των άλλων δύο ερωτηματολογίων προκειμένου να σχολιαστεί η τρίτη υπόθεση έρευνας (ως ανωτέρω) και να ανιχνευθεί η ανάγκη επεξεργασίας και τροποποίησης των ποινικών διατάξεων που αφορούν στην ασφάλεια των δεδομένων.

6) α. Εσείς έχετε πληροφορίες στο διαδίκτυο στις οποίες δεν θα θέλατε κάποιος να έχει πρόσβαση (π.χ. e-mail, facebook account κ.λπ.);

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

β. Αποδέχεστε την ελεύθερη κυκλοφορία στο διαδίκτυο μίας ταινίας ή ενός βιβλίου 2 ημέρες μετά την πρώτη κυκλοφορία του;

(κλειστού τύπου ερώτηση)

Και οι δύο ως άνω ερωτήσεις αποσκοπούν στο να ελέγξουν τη συνέπεια των θέσεων του ερωτώμενου hacker σχετικά με την ελεύθερη και ακώλυτη διακίνηση της πληροφορίας στο διαδίκτυο καθώς και να καταδείξει την ενδεχόμενη διαφορά όταν η τελευταία αφορά δικά τους δεδομένα ή όταν θίγει δικαιώματα τρίτων. Οι απαντήσεις που θα προκύψουν θα αποκρυσταλλώσουν την πραγματική στάση των hackers αναφορικά με το μέτρο της ελεύθερης πρόσβασης στην πληροφορία στο διαδίκτυο.

7) Πιστεύετε ότι μια αυστηρή νομοθεσία αποτρέπει από ενέργειες hacking;

[1069] Μπορεί βάσιμα να υποστηριχθεί ότι η συγκεκριμένη ερώτηση, συμφωνα και με τη Σπινέλλη, μετατρέπει την ποιοτική έννοια «γενική πρόληψη» σε έννοια ποσοτική. Συγκεκριμένα, η Σπινέλλη αναφέρει ως παράδειγμα την ερώτηση «*Νομίζετε ότι η απειλή της ποινής θα σας απέτρεπε από την τέλεση ενός εγκλήματος: πολύ, αρκετά ή καθόλου;*» (*Κ. Δ. Σπινέλλη*, Εγκληματολογία - Σύγχρονες και παλαιότερες κατευθύνσεις, όπ. π., σελ. 96).

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

Η εν λόγω ερώτηση στοχεύει στο να αναδείξει τη δυνητική αποτελεσματικότητα ή μη των (αυστηρών) νομοθετικών διατάξεων σε επίπεδο γενικής πρόληψης και ιδίως της αποτρεπτικής της λειτουργίας, λαμβάνοντας υπόψιν ότι η θεωρία της γενικής πρόληψης προϋποθέτει έναν homo economicus[1070], ο οποίος προβαίνει σε ανάλυση κόστους οφέλους πριν «περάσει στην πράξη» (σύμφωνα και με τις θεωρίες ορθολογικής επιλογης)[1071]. Ειδικότερα, η ερώτηση αυτή στοχεύει στο να διαπιστωθεί εάν οι hackers θα ομολογούσαν πως κάποιου είδους νομοθεσία θα μπορούσε να τους σταματήσει. Με την ερώτηση αυτή, δηλαδή, επιχειρείται να διαπιστωθεί αν οι hackers "φοβούνται" ή όχι τελικώς τον νομοθέτη, σύμφωνα, βέβαια, με τη δική τους δήλωση.

8) Τι εικόνα νομίζετε ότι έχει ο μέσος έλληνας (γνώστης περί του φαινομένου του hacking) για τους hackers; *(ανοικτού τύπου ερώτηση)*

Οι κοινωνικές αναπαραστάσεις[1072] και αντιδράσεις που βιώνουν οι ίδιοι οι hackers σε κοινωνικό επίπεδο καταγράφονται και ενδεχομένως να μπορέσουν να εξηγήσουν τις συμπεριφορές τους σύμφωνα με τη θεωρία της ετικέτας[1073] και την αρχή της

[1070] Έτσι *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 186.

[1071] Βλ. σχετικά παράγραφο 3.1 του παρόντος πονήματος.

[1072] Πρβλ. *David S. Wall*, Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime, Information, Communication & Society Vol. 11, No. 6, pp. 861–884, ημερ. έκδοσης: 1 September 2008 και *David S. Wall*, Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime, International Review of Law, Computers and Technology, vol. 22, nos. 1-2, pp. 45–63 αναφορικά με την κοινωνική κατασκευή της εικόνας των κυβερνοεγκληματιών (μέσα από βιβλία, ταινίες κ.ά.) καθώς και *Αγγ. Κίτσιου & Χρ. Κουρούτζα*, Μελετώντας το ηλεκτρονικό έγκλημα στο πλαίσιο της κοινωνίας της πληροφορίας. Πιλοτική έρευνα αναπαραστάσεων σε φορείς του νομού Λέσβου, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τομ. Ι, σελ. 322.

[1073] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 3 του παρόντος πονήματος.

αυτοεκπληρούμενης προφητείας[1074] και ενδεχομένως να καταδείξουν τρόπους ενσωμάτωσης της συμπεριφοράς τους στην κυρίαρχη κουλτούρα[1075].

9) Η Πολιτεία πρέπει να θέτει όρια στο hacking;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

Όπως αναφέρθηκε ανωτέρω, κυρίαρχη κουλτούρα στο διαδίκτυο φαίνεται να είναι αυτή της θέσης ορίων στο διαδίκτυο (βλ. ανωτέρω τις αναπτύξεις αναφορικά με την υποκουλτούρα του hacking στην παράγραφο 2.8). Θα κριθεί, επίσης, αν και πόσο έντονη και συμπαγής είναι η κουλτούρα για διαδίκτυο χωρίς κανένα όριο, η οποία εκφράζεται από το hacking, όπως διατυπώνεται ανωτέρω.

Τέλος, ο συνδυασμός της ερώτησης αυτής με τις ανωτέρω υπ' αρ. 5 και 7 ερωτήσεις θα δώσει την εικόνα που έχει τελικώς ο hacker για τη λειτουργία της Πολιτείας σε συνδυασμό με την ισχύουσα νομοθεσία ή την νομοθεσία που θα μπορούσε να τεθεί σε εφαρμογή.

10) Σε γενικές γραμμές, ποια είναι η μέχρι τώρα δράση σας και ποιες τεχνικές χρησιμοποιείτε; *(ανοικτού τύπου ερώτηση)*

Με την παρούσα ερώτηση ο hacker καλείται να γίνει πιο συγκεκριμένος δίνοντας πληροφορίες για το είδος και το αντικείμενο της δραστηριότητάς του και τις βασικές μεθόδους και τεχνικές που χρησιμοποιεί.

[1074] Η αυτοεκπληρούμενη προφητεία είναι μια πρόβλεψη που άμεσα ή έμμεσα μπορεί να γίνει πραγματικότητα με «καταλύτες» τους ίδιους τους όρους της ίδιας της προφητείας, λόγω της θετικής ανάδρασης μεταξύ πίστης και συμπεριφοράς. Ο όρος διατυπώθηκε από τον Robert K. Merton, ο οποίος ορίζει την αυτοεκπληρούμενη προφητεία π.χ. ως εξής: όταν η Roxanna πιστεύει λανθασμένα ο γάμος της θα αποτύχει, οι φόβοι της εν λόγω αστοχίας στην πραγματικότητα θα προκαλέσουν την αποτυχία στο γάμο της (βλ. *Robert Merton*, Social Theory and Social Structure, New York: Free Press, 1968 p. 477.).

[1075] Βλ. παράγραφο 2.8 του παρόντος πονήματος αναφορικά με την (υπο)κουλτούρα του hacking.

Καταρχάς, η προσέγγιση αυτή προτείνεται και από τον Clarke[1076], σύμφωνα με τον οποίο η έρευνα θα πρέπει να εστιάζεται περισσότερο στον τρόπο με τον οποίο διενεργείται η υπό μελέτη συμπεριφορά και τελείται το έγκλημα και λιγότερο στις αιτίες του. Σύμφωνα με τον ίδιο, η κατανόηση των σταδίων στη διαδικασία της διάπραξης του εγκλήματος και των συνθηκών που διευκολύνουν αυτήν θα είναι πολύ χρήσιμη προκειμένου να εντοπίσουμε αποτελεσματικούς τρόπους παρέμβασης, πάντοτε λαμβανομένων υπόψη και των θέσεων των αντίστοιχων θεωριών που επιβεβαιώνονται ή διαψεύδονται από τα πορίσματα (π.χ. η θεωρία δραστηριοτήτων ρουτίνας[1077] κατά την οποία ο δράστης εκμεταλλεύεται την «απουσία κατάλληλου φύλακα»).

Τέλος, η συγκεκριμένη ερώτηση επιτελεί λειτουργίες ελέγχου αξιοπιστίας (reality testing). Αν ο απαντήσας το ερωτηματολόγιο τάχα ως hacker αγνοεί βασικά στοιχεία της τεχνικής ή/και της ιδεολογίας των hackers, υπάρχει δυνατότητα από την απάντησή του στην ερώτηση αυτή να αποκαλυφθεί. Σε αυτήν την περίπτωση θα αποκλειστεί από το δείγμα.

11) Τι συμβουλές θα δίνατε σε έναν χρήστη διαδικτύου ως προς την ασφάλεια των δεδομένων του; *(ανοικτού τύπου ερώτηση)*

Με την απάντησή τους στη συγκεκριμένη ερώτηση οι hackers θα μας δείξουν – ιδίως μέσω των μέτρων που προτείνουν – αρχικώς πώς αντιλαμβάνονται οι ίδιοι την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων στο διαδίκτυο. Επίσης, η απάντηση των hackers στην ως άνω ερώτηση βοηθά στο να ανιχνεύσουμε εναλλακτικά μέτρα προαγωγής της ασφάλειας των δεδομένων, πέρα από ή χωρίς την ύπαρξη ποινικής νομοθεσίας. Επιπρόσθετα, η άποψη του ίδιου του hacker για την ισχύουσα κατάσταση σχετικά με την ασφάλεια στο διαδίκτυο κρίνεται διαφωτιστική για την έρευνα στο βαθμό που θα επιβεβαιώσει ή θα διαψεύσει σχετικές θέσεις και προτάσεις (π.χ. τη σημασία της έλλειψης ενός «ικανού φύλακα» κατά τη θεωρία των

[1076] *Ronald V. Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research 10: 55–63, 2004,Kluwer Academic Publishers, p. 58.

[1077] Βλ. ανωτέρω την ανάπτυξη των εγκληματολογικών θεωριών στο κεφάλαιο 3 του παρόντος πονήματος.

δραστηριοτήτων ρουτίνας ως η τρίτη συνθήκη τέλεσης μίας εγκληματικής πράξης, όπως ήδη αναφέρθηκε).

12) Θεωρείτε τον εαυτό σας χακτιβιστή[1078];

(κλειστού τύπου ερώτηση)

Η απάντηση του ερωτώμενου hacker για το εάν είναι οπαδός του κινήματος του «χακτιβισμού», όπως ορίστηκε ανωτέρω, θα μας δείξει, τελικά, αν η πλειοψηφία των hackers δρα με σκοπό την εξέλιξη και ανάπτυξη των ηλεκτρονικών συστημάτων και των κοινωνικών διεκδικήσεων ή απλώς ενδιαφέρεται για την ικανοποίηση προσωπικών στόχων. Επίσης, η απάντηση κάθε hacker οφείλει να συνάδει με τις προηγούμενες θέσεις του αναφορικά με την ιδεολογία και τη δράση του (reality testing question).

13) Ποια η γνώμη σας για τους "Anonymous"[1079];

(ανοικτού τύπου ερώτηση)

Η άποψη των hackers για τους "Anonymous" συμβάλλει στη διαμόρφωση από πλευράς του ερευνητή μιας πληρέστερης εικόνας για την ιδεολογία τους, τη μεμονωμένη ή ομαδική δράση τους δια και της επικρότησης ομαδικών δράσεων, την ενημέρωσή τους για το σύγχρονο γίγνεσθαι στο hacking και τα κίνητρά τους.

14) Ως hacker χρησιμοποιείτε ψευδώνυμο;

[1078] Σχετικά με τον «χακτιβισμό» βλ. ανωτέρω την παράγραφο 2.9.2 του παρόντος πονήματος.

[1079] Για την κολεκτίβα των "Anonymous" πρβλ. *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756. Επιπρόσθετα, βλ. Παράρτημα IV σχετικά με την άποψη της GHS για τους "Anonymous".

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)

Η χρήση ψευδωνύμων από hackers λαμβάνει χώρα για να αποκρυβεί η ταυτότητά τους και να εκμεταλλευτούν την ανωνυμία στη χρήση του διαδικτύου καθώς και για να παρουσιάσουν μια ειδική και ξεχωριστή εικόνα για τον εαυτό τους[1080] μέσω του επιλεχθέντος και χρησιμοποιούμενου ψευδωνύμου[1081]. Εν προκειμένω, η χρήση ή μη ψευδώνυμου από πλευράς του ερωτώμενου hacker αποτελεί ένα επιπλέον στοιχείο προκειμένου ο ερευνητής να ολοκληρώσει τη σκιαγράφηση του προφίλ και του τρόπου δράσης του hacker[1082]. Ταυτόχρονα, η ως άνω ερώτηση εντάσσεται στο πλαίσιο των ερωτήσεων του reality testing των προηγούμενων απαντήσεων σχετικά με το modus operandi του hacker.

15) Τι σημαίνει για εσάς η αναγνώριση και η αποδοχή σας ως hacker από τους υπόλοιπους hackers;

(ανοικτού τύπου ερώτηση)

Με τη συγκεκριμένη ερώτηση προσπαθούμε να ανιχνεύσουμε αν ισχύει η αντίληψη ότι οι περισσότεροι hackers λειτουργούν σε ομάδες ή κοινότητες με χαλαρούς

[1080] *Suelette Dreyfus*, Computer hackers: Juvenile Deliquents or International Saboteurs?, εισήγηση η οποία παρουσιάστηκε στο συνέδριο "Internet Crime" το οποίο έλαβε χώρα στη Μελβούρνη της Αυστραλίας στις 16-17 Φεβρουαρίου 1998 και διοργανώθηκε από το Australian Institute of Criminology.

[1081] Πρβλ. και ανάλυση σχετικά με την χρήση ψευδωνύμων και την ανωνυμία στο διαδίκτυο στο εγχειρίδιο των *Mary Lou Leary & Mary Rappaport*, Beyond the Beat Ethical Considerations for Community Policing in the digital age, National Center for Victims of Crime, Washington DC, November 2008, pp. 39-40.

[1082] Ωστόσο, κατά τους των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 121-122 η ανάλυση του ψευδωνύμου ενός hacker δεν προσφέρεται για την εξαγωγή συμπερασμάτων για την προσωπικότητά του καθώς σε κάθε περίπτωση καταγράφεται ότι οι hackers διαλέγουν επιβλητικά ονόματα προκειμένου να υπερτονίσουν τις τεχνικές τους δυνατότητες. Επίσης, επισημαίνεται ότι οι hackers δεν χρησιμοποιούν το ίδιο ψευδώνυμο σε άλλες δραστηριότητες πέρα από το hacking. Αυτή η τελευταία άποψη πιστεύω ότι πρέπει να εξειδικευθεί στο πλαίσιο της εικόνας που θέλει ο hacker να δημιουργήσει και όχι μόνο στη δραστηριότητά του ως hacker. Π.χ. ο hacker "Punker GHS" – στον οποίο έχουμε αναφερθεί ανωτέρω – χρησιμοποιεί στο λογαριασμό του στην ιστοσελίδα κοινωνικής δικτύωσης www.facebook.com ως όνομα το ως άνω ψευδώνυμό του το οποίο χρησιμοποιεί και ως hacker. Τούτο διότι αυτό είναι στην ουσία το «hacking προφίλ» του!

δεσμούς[1083]. Επιπρόσθετα, θα διαπιστωθεί αν πράγματι για τις κοινότητες των hackers θεωρείται καλύτερο κάποιος να προσδιορίζεται από τους άλλους ως hacker παρά να αυτοπροσδιορίζεται ως hacker. Η εν λόγω απάντηση του ερωτώμενου hacker συμβάλλει στην κατανόηση του τρόπου με τον οποίον ο hacker θεωρεί τον εαυτό του μέλος μίας κοινότητας, βασισμένης στις ικανότητες και στις ανταλλασσόμενες μεταξύ των μελών ιδέες και τεχνικές. Τέλος, καθώς η ερώτηση είναι ανοικτού τύπου, δύναται να καταγραφεί αν η αναγνώρισή του αυτή ως hacker[1084], η αποδοχή και η ένταξη σε ένα κοινωνικό σύνολο συντελεί στην ανάπτυξη και εξέλιξη της δράσης του.

7.8 Αποτελέσματα της έρευνας

7.8.1 Δείγμα νομικών[1085]

7.8.1.1 Απαντήσεις

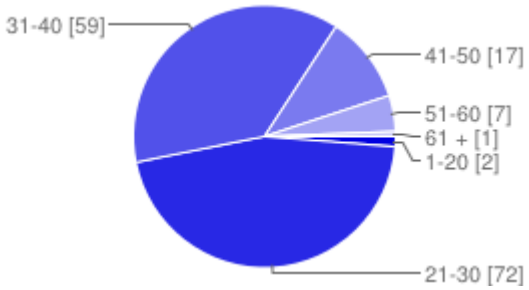
Αρχικώς ζητήθηκε από τους ερωτώμενους η συμπλήρωση δημογραφικών στοιχείων όπως η ηλικία, το φύλο και το επίπεδο σπουδών. Αναφορικά με την ηλικία τα αποτελέσματα ακολουθούν:

Ηλικία

[1083] Βλ. σχετική ανάπτυξη στην παράγραφο 2.8 του παρόντος πονήματος.

[1084] Όπως ειπώθηκε ήδη, οι *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, όπ. π., σελ. 12-13 παραπέμπουν στην Denning και στην έρευνα του Chantler (1996) κατά την οποία σε 164 hackers ως ένα εκ των κορυφαίων κινήτρων αναγνωρίστηκε η θέληση για αναγνώριση με ποσοστό 24%.

[1085] Στη συγκεκριμένη ενότητα όπου αναφέρεται αριθμός ερωτηματολογίου αντιστοιχεί σε αυτόν του Παραρτήματος 1 στο οποίο παρουσιάζονται οι απαντήσεις των νομικών, όπως έχει αναφερθεί ανωτέρω.



1-20	**2**	1%[1086]
21-30	**72**	46%
31-40	**59**	37%
41-50	**17**	11%
51-60	**7**	4%
61 +	**1**	1%

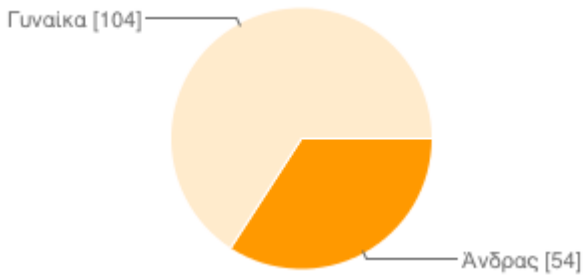
Όπως προκύπτει από τα αποτελέσματα της έρευνας, η συντριπτική πλειοψηφία των συμμετεχόντων – ήτοι το 83% – είναι ηλικίας μεταξύ 21 έως 40 ετών. Το μεγάλο αυτό ποσοστό εξηγείται εύλογα από το γεγονός ότι σε αυτές τις ηλικίες ανήκουν οι

[1086] Δύο από τους ερωτώμενους απάντησαν ότι η ηλικία τους είναι από 1-20. Ωστόσο, σύμφωνα με τα διδάγματα της κοινής πείρας κανείς δεν δύναται να έχει αποκτήσει πτυχίο νομικής προ της ηλικίας των 20 ετών. Εν προκειμένω, τα ερωτηματολόγια στα οποία έχει δοθεί αυτή η οξύμωρη απάντηση είναι τα υπ' αρ. 25 και 70 όπως αριθμούνται στο Παράρτημα Ι. Πρόκειται και στις δύο περιπτώσεις για γυναίκες, οι οποίες έχουν μάλιστα δηλώσει ότι είναι κάτοχοι μεταπτυχιακού διπλώματος. Οι υπόλοιπες απαντήσεις τους φαίνεται να έχουν δοθεί με συναίσθηση των ερωτήσεων. Δυνάμει των ανωτέρω και λαμβανομένου υπόψιν ότι η επιλογή 1-20 σε δείγμα νομικών συνιστά τελικώς μάλλον υπερβολή του ερευνητή, ότι οι υπό συζήτηση απαντήσεις αντιπροσωπεύουν μονάχα το 1,26% των απαντήσεων και ότι η λανθασμένη αυτή απάντηση δεν επηρεάζει τελικώς αρνητικά τα αποτελέσματα της έρευνας, σκόπιμο είναι να μην αποκλειστούν τα δύο αυτά ερωτηματολόγια από την υπόλοιπη έρευνα (μάλλον πρόκειται περί λάθους επιλογής με την γειτονική επιλογή «21-30») - (αναφορικά με τα όρια του στατιστικού λάθους πρβλ. *Volker Blobel*, Statistical and other errors, University of Hamburg, March 2005, url: http://www.desy.de/~blobel/blobel_errors.pdf).

Επισημαίνεται, πάντως, ότι εκτός αυτών των δύο ερωτηματολογίων, όλα τα υπόλοιπα ερωτηματολόγια της έρευνας έχουν συμπληρωθεί σωστά, λόγω και της ομοιογένειας των δειγμάτων αλλά και της εξοικείωσής τους με το διαδίκτυο (βλ. και παράγραγο 7.5.1), σύμφωνα και με την άποψη του Παπάνη (*Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 62).

περισσότεροι χρήστες ηλεκτρονικών υπολογιστών και μέσων κοινωνικής δικτύωσης, ενώ οι μεγαλύτεροι σε ηλικία είναι γεγονός ότι δεν είναι τόσο εξοικειωμένοι με τη χρήση της τεχνολογίας (και μάλλον τελικώς τους αφορά λιγότερο έως καθόλου σε προσωπικό επίπεδο η ασφάλεια των ηλεκτρονικών τους δεδομένων, ως μη χρήστες).

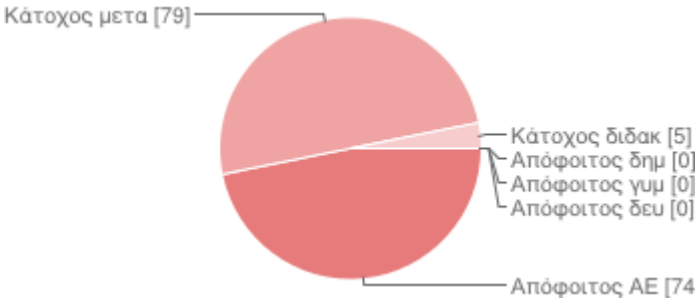
Φύλο



Άνδρας	**54**	34%
Γυναίκα	**104**	66%

Σε επίπεδο φύλου, τα 2/3 (66%) είναι γυναίκες και το υπόλοιπο 1/3 άνδρες.

Επίπεδο Σπουδών



Απόφοιτος δημοτικού	**0**	0%
Απόφοιτος γυμνασίου	**0**	0%

Απόφοιτος δευτεροβάθμιας εκπαίδευσης (λύκειο κ.ά.)	**0**	0%
Απόφοιτος ΑΕΙ - ΑΤΕΙ	**74**	47%
Κάτοχος μεταπτυχιακού διπλώματος	**79**	50%
Κάτοχος διδακτορικού διπλώματος	**5**	3%

Το ακαδημαϊκό επίπεδο των ερωτώμενων, κατά δήλωσή τους, μπορεί να δείξει την επιστημονική επάρκεια του δείγματος. Εν προκειμένω, ακριβώς οι μισοί απαντώντες νομικοί (79) έχουν λάβει μεταπτυχιακό δίπλωμα ειδίκευσης και 5 εξ αυτών (ποσοστό 3%) διδακτορικό δίπλωμα. Οι υπόλοιποι 74 (47%) έχουν λάβει πτυχίο πανεπιστημίου.

<u>Ερώτηση 1</u>: Τι είναι hacking σύμφωνα με την εμπειρία σας;

(ανοικτού τύπου ερώτηση) [1087]

Οι απαντήσεις που κατεγράφησαν σε αυτήν την ερώτηση δείχνουν ότι σε γενικές γραμμές οι ερωτώμενοι νομικοί περιγράφουν το hacking ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, μολονότι είναι γεγονός ότι οι υιοθετούμενες διατυπώσεις ποικίλουν γλωσσολογικά. Η συντριπτική πλειοψηφία των απαντήσεων αναφέρεται σε «παραβίαση», σε «σπάσιμο κωδικών» και γενικότερα σε «αθέμιτη» πρόσβαση σε ηλεκτρονικές πληροφορίες. Επίσης, κάποιες απαντήσεις αναφέρονται στο ότι οι hackers αποκτούν πρόσβαση σε λογισμικά για την προσωπική τους ικανοποίηση αλλά και για να διευρύνουν τις γνώσεις τους. Ωστόσο, αρκετές απαντήσεις συγχέουν το hacking με τη «δολιοφθορά» των ηλεκτρονικών δεδομένων

[1087] Στο πλαίσιο ανοιχτών ερωτήσεων η κωδικοποίηση των απαντήσεων λαμβάνει χώρα κατά την επεξεργασία και παρουσίαση των ερωτηματολογίων, όπως ήδη ανωτέρω ειπώθηκε. Σε αυτό το πνεύμα κατηγοριοποιούνται οι απαντήσεις σε όλες τις ανοικτού τύπου ερωτήσεις που ακολουθούν (βλ. ειδικότερα *Ιωάννα Λαμπίρη – Δημάκη*, Η Κοινωνιολογία και η Μεθοδολογία της, όπ. π. 124-125 και ιδίως για την κωδικοποίηση των ποιοτικών δεδομένων βλ. αναλυτικά *Θ. Ιωσηφίδη*, Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες, εκδ. Κριτική, Αθήνα, 2008, σελ. 179 επ.).

[φαινόμενο το οποίο περιγράφεται ειδικότερα ως cracking (ή crashing)[1088]]. Στον αντίποδα, υπάρχουν απαντήσεις που κάνουν σαφή τη διαφορά χωρίς δικαίωμα πρόσβασης σε δεδομένα και επιζήμιας ενέργειας επί των δεδομένων αυτών. Συμπερασματικά, ωστόσο, είναι γεγονός ότι οι ορισμοί που έχουν δοθεί δεν αναφέρονται με σύγχρονο και εμπεριστατωμένο τρόπο στην παραβίαση της ασφάλειας δεδομένων π.χ. χρησιμοποιώντας ως όρο τα συστήματα πληροφοριών (σύμφωνα και με τις νομικές σε ενωσιακό ευρωπαϊκό επίπεδο εξελίξεις, όπως παραπάνω αναλύθηκαν) ή αναφέροντας επιθέσεις με botnets. Ως αποτέλεσμα μπορεί να υποστηριχθεί ότι στην πλειοψηφία τους οι συμμετέχοντες στο δείγμα δεν γνωρίζουν λεπτομερώς και εμπεριστατωμένως το ζήτημα του hacking σε νομικό επίπεδο και οι περισσότερες απαντήσεις εκπορεύονται περισσότερο από τη γενική αίσθηση του συμμετέχοντος (η οποία επηρεάζεται, βεβαίως, από τις νομικές σπουδές και την επαγγελματική ιδιότητά τους) παρά από την επιστημονική γνώση αυτή καθεαυτή.

Εντός του δείγματος εντοπίζονται απαντήσεις οι οποίες αναφέρουν ότι υπάρχει και νόμιμο αλλά και παράνομο hacking αναφορικά με την πρόσβαση σε ηλεκτρονικά δεδομένα[1089]. Λαμβανομένου υπόψη ότι η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα είναι αξιόποινη[1090], εκτιμάται βάσιμα ότι οι απαντήσεις αυτές έχουν δοθεί όχι με βάση το νομικό «ον» αλλά το «δέον» σύμφωνα με τον κώδικα αξιών του απαντώντος.

Καταγράφεται ότι ένα μεγάλο μέρος των απαντώντων (42 απαντήσεις) χρησιμοποιούν στην απάντησή τους τον όρο «προσωπικά δεδομένα» ως προσβαλλόμενο από συμπεριφορές hacking, μολονότι είναι προφανές ότι τα προσβαλλόμενα ηλεκτρονικά δεδομένα δεν είναι απαραίτητο ότι υπάγονται στο πλέγμα προστασίας που έχει αναπτυχθεί τα τελευταία έτη για τα προσωπικά δεδομένα[1091]. Ωστόσο, πιστεύω ότι η μεγάλη επιστημονική συζήτηση της τελευταίας εικοσαετίας για την προστασία των προσωπικών δεδομένων[1092] έχει γίνει πλέον

[1088] Βλ. την παράγραφο 2.3.1 του παρόντος πονήματος.

[1089] Ενδεικτικώς οι απαντήσεις στα ερωτηματολόγια υπ' αρ. 12, 25 και 27.

[1090] Βλ. κεφάλαια 4 και 5 του παρόντος πονήματος.

[1091] Για την εφαρμογή του ν. 2472/1997 σε σχέση με το ά. 370Γ παρ. 2 και 370Β ΠΚ βλ. *Δημ. Κιούπη,* Ποινικό Δίκαιο και Internet, όπ. π., σελ. 134-135.

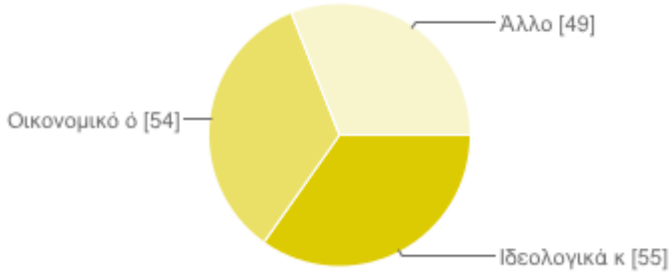
[1092] Σχετικά με την προσέγγιση της προστασίας των προσωπικών δεδομένων στην ελληνική επιστημονική βιβλιογραφίας πρβλ. ενδεικτικά τα εξής δύο σημαντικά πονήματα: *Π. Αρμαμέντος & Β. Σωτηρόπουλος*, Προσωπικά δεδομένα – Ερμηνεία Ν. 2472/1997, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2005 και *Ιωάν. Ιγγλεζάκης*, Ευαίσθητα προσωπικά δεδομένα, εκδ. Π. Ν. Σάκκουλα,

συνείδηση και έχει εμπεδωθεί στο δικαιικό αισθητήριο των νομικών και γι' αυτόν τον λόγο αυτή η έννοια, η οποία έχει απασχολήσει έντονα την νομική επιστήμη τα τελευταία χρόνια, χρησιμοποιείται στην προκειμένη περίπτωση[1093].

Σε ορισμένες απαντήσεις παρατηρείται διάσταση απόψεων αναφορικά με την ύπαρξη ή μη οικονομικών κινήτρων στον hacker[1094] (ακολουθεί, βεβαίως, ειδικότερη ερώτηση επί αυτού του ζητήματος). Επιπρόσθετα, υπήρχαν ελάχιστες απαντήσεις οι οποίες ήταν αρκετά γενικές ή εντελώς άσχετες με την έννοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking γενικότερα[1095].

<u>Ερώτηση 2</u>: Πιστεύετε ότι οι hackers ενεργούν περισσότερο με βάση ιδεολογικά κίνητρα ή με σκοπό το οικονομικό όφελος;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Αθήνα-Θεσσαλονίκη, 2003, σελ. 109 και ειδικότερα για το διαδίκτυο *Ευγενίας Αλεξανδροπούλου – Αιγυπτιάδου*, Η νομική προστασία των προσωπικών δεδομένων κατά την πλοήγηση των ανηλίκων στο Διαδίκτυο, εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 141.

[1093] Πρέπει, βέβαια, να ληφθεί υπόψιν και το ότι «*Οι ερωτώμενοι ενδόμυχα τρέφουν την ελπίδα ότι θα δώσουν τις "σωστές" απαντήσεις. Δεν είναι αυτή, όμως, η επιθυμητή κατάληξη μιας συνέντευξης, γιατί στις συνεντεύξεις δεν γίνονται "λάθη", όσον αφορά στις απαντήσεις των ερωτώμενων. Σκοπός του ερευνητή είναι η προσέγγιση και καταγραφή της αλήθειας, χωρίς αποστέωση και αποχρωμάτιση των απαντήσεων. ...*» (έτσι *Ευφροσύνη-Άλκηστη Παρασκευοπούλου-Κόλλια*, Μεθοδολογία ποιοτικής έρευνας στις κοινωνικές επιστήμες και συνεντεύξεις, Open Education - The Journal for Open and Distance Education and Educational Technology, τεύχος 4, αρ. 1, 2008 / Section one, url: http://openworkshop.pbworks.com/w/file/fetch/64390800/poiotikh-ereyna-ekpaideysh.pdf).

[1094] Ενδεικτικά σε αντιδιαστολή οι απαντήσεις στα ερωτηματολόγια υπ' αρ. 10 και 75.

[1095] ... όπως π.χ. οι απαντήσεις "*παρόμοιο με το trolling*" (ερωτηματολόγιο υπ' αρ. 104), "*Η κατάληψη χώρου στο διαδίκτυο από μη εξουσιοδοτημένα πρόσωπα*" (ερωτηματολόγιο υπ' αρ. 14), "*μορφή ηλεκτρονικού εγκλήματος*" (ερωτηματολόγιο υπ' αρ. 22), "*παραβιαση των κανονων συμπεριφορας κατα τη χρηση του διαδικτυου.*" (ερωτηματολόγιο υπ' αρ. 13).

Ιδεολογικά κίνητρα	**55**	35%
Οικονομικό όφελος	**54**	34%
Άλλο	**49**	31%

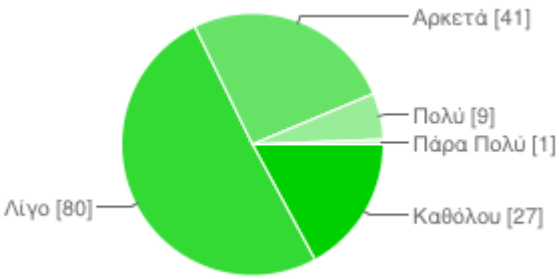
Οι απαντήσεις στην ως άνω ερώτηση φαίνονται μοιρασμένες καθώς το 35% οριακά προκρίνουν την ιδεολογία των hackers ως κίνητρο ενεργειών χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα σε αντίθεση με το 34%, οι οποίοι πιστεύουν ότι τα κίνητρα των hackers συνίστανται περισσότερο στην αποκόμιση οικονομικού οφέλους.

Από την επιλογή «Άλλο», η οποία έλαβε 49 απαντήσεις (31%), στις 36 εξ αυτών (ποσοστό 22,78%) αναφέρεται ότι «Και τα δύο» (δηλαδή ότι οι hackers ενεργούν και με βάση ιδεολογικά κίνητρα αλλά και με σκοπό το οικονομικό όφελος), παρά το ότι η ερώτηση περιλαμβάνει τη λέξη «περισσότερο» αναφορικά με τα ιδεολογικά ή οικονομικά κίνητρα των hackers. Προκύπτει, επομένως, ότι αρκετοί από όσους απάντησαν δεν κάνουν διάκριση ανάμεσα σε ιδεολογία και οικονομικό όφελος. Επίσης, στην επιλογή «Άλλο» απαντήσεις που έχουν δοθεί αναφέρονται επιπλέον στην ικανοποίηση της περιέργειας του hacker αναφορικά με την χωρίς δικαίωμα πρόσβασή του σε ηλεκτρονικά δεδομένα[1096], η άσκηση δραστηριότητας στον ελεύθερο χρόνο (hobby)[1097], η πρόκληση[1098] αλλά κυρίως η επίδειξη ικανοτήτων και γοήτρου εκ μέρους των hackers[1099]. Τέλος, ελήφθησαν δύο απαντήσεις με περιεχόμενο «Δεν γνωρίζω»[1100].

[1096] Στο ερωτηματολόγιο υπ' αρ. 10.
[1097] Στο ερωτηματολόγιο υπ' αρ. 119.
[1098] Στο ερωτηματολόγιο υπ' αρ. 148.
[1099] Στα ερωτηματολόγια υπ' αρ. 25, 43, 142 και 145.
[1100] Στα ερωτηματολόγια υπ' αρ. 89 και 139.

<u>Ερώτηση 3</u>: Θεωρείτε ότι οι έλληνες νομικοί που ασχολούνται με το δίκαιο της πληροφορικής είναι επαρκώς ενημερωμένοι και εκπαιδευμένοι σε θέματα πληροφορικής και ιδίως hacking;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου	**27**	17%
Λίγο	**80**	51%
Αρκετά	**41**	26%
Πολύ	**9**	6%
Πάρα Πολύ	**1**	1%

Οι ίδιοι οι νομικοί αναγνωρίζουν ότι είναι «Λίγο» ενημερωμένοι για τα ζητήματα του hacking (51%) – αν σε αυτό το ποσοστό προστεθεί και το 17% το οποίο απαντά ότι οι έλληνες νομικοί δεν είναι καθόλου ενημερωμένοι σχετικώς προκύπτει ότι το 68% έχει μια αρνητική εικόνα για τη γνώση των ελλήνων νομικών σε θέματα

πληροφορικής και ειδικότερα σε θέματα hacking[1101]. Αυτή η καταγραφείσα άποψη των νομικών είναι σχετική και με τη γενική και όχι εξειδικευμένη και εμπεριστατωμένη προσέγγιση του ορισμού του hacking από το δείγμα των νομικών στην ερώτηση 1 που προηγήθηκε. Τούτο μπορεί να υποστηριχθεί ότι καταδεικνύει πως το έδαφος στο οποίο καλούμαστε να (επανα)σχεδιάσουμε πολιτικές προώθησης της ασφάλειας των ηλεκτρονικών συστημάτων πληροφοριών μάλλον δεν είναι εύφορο και, συνεπώς, η ενημέρωση των εφαρμοστών ή συνδραμόντων στην κατάρτιση κανόνων δικαίου και την εφαρμογή τους αποτελεί sine qua non δράση, η οποία πρέπει να αναληφθεί[1102].

<u>Ερώτηση 4</u>: Πιστεύετε ότι οι δράσεις των hackers μπορούν να έχουν θετική συμβολή στην κοινωνία; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Η ερώτηση αυτή ετέθη στους ερωτώμενους ως ανοικτού τύπου προκειμένου να μπορέσουν χωρίς περιορισμούς να εκφράσουν απόψεις και ιδέες. Προβαίνοντας σε ανάλυση περιεχομένου των απαντήσεων, διαπιστώνεται ότι από το δείγμα των 158 απαντήσεων σε 114 (ποσοστό 72,15%) από αυτές υποστηρίζεται ότι οι hackers μπορούν να έχουν συμβολή με τη δράση τους στην κοινωνία ενώ 40 ερωτώμενοι (ποσοστό 25,31 %) πιστεύουν ότι οι hackers δεν μπορούν να έχουν θετική συμβολή στην κοινωνία. Στις υπόλοιπες 4 απαντήσεις (ποσοστό 2,54 %) δεν διευκρινίζεται η θέση του απαντώντος[1103].

Από τα ερωτηματολόγια στα οποία εντοπίζεται η άποψη ότι οι hackers μπορούν να έχουν θετική συμβολή στην κοινωνία, η διασπορά των απαντήσεων και ιδεών δεν είναι αρκετά μεγάλη, αφού οι πλειοψηφία αυτών ομαδοποιείται στις εξής επιλογές:

[1101] ... μολονότι οι μισοί εξ αυτών έχουν λάβει μεταπτυχιακό δίπλωμα, το οποίο, ακόμη κι αν δεν είναι σχετικό με τις νέες τεχνολογίες, θα αναμενόταν να έχει ως αποτέλεσμα την εντονότερη εγρήγορση αναφορικά με τις τεχνολογικές εξελίξεις.

[1102] Βλ. και σχετικές αναπτύξεις στην παράγραφο 9.2 του παρόντος πονήματος.

[1103] Στα ερωτηματολόγια υπ' αρ. 84, 89, 92 και 95.

α) σε 31 απαντήσεις[1104] (ποσοστό 19,62 % από το γενικό σύνολο και 27,19 % από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers (και συνεπώς οι αποκτώντες χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα) μπορούν να έχουν θετική συμβολή σε περιπτώσεις πρόληψης και καταστολής εγκληματικών πράξεων[1105] (με αρκετές απαντήσεις να δίνουν ιδιαίτερο βάρος σε υποθέσεις παιδικής πορνογραφίας[1106] και ηλεκτρονικών εγκλημάτων γενικότερα)[1107]

β) σε 20 απαντήσεις[1108] (ποσοστό 12,65 % από το γενικό σύνολο και 17,54 % από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers μπορούν να συμβάλουν εντοπίζοντας τα κενά ασφαλείας συστημάτων και προωθώντας με αυτόν τον τρόπο τη δημιουργία ασφαλέστερων προγραμμάτων ηλεκτρονικών υπολογιστών και συστημάτων πληροφοριών

γ) σε 31 απαντήσεις[1109] (ποσοστό 19,62 % από το γενικό σύνολο και 27,19 % από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers μέσω της απόκτησης πρόσβασης ακόμη και χωρίς δικαίωμα σε δεδομένα συμβάλλουν στη σφαιρική ενημέρωση των πολιτών και στην ανάπτυξη της διαφάνειας στη δημόσια ζωή αποκαλύπτοντας σκάνδαλα και πληροφορίες, οι οποίες σκοπίμως αποκρύβονται από τους εκάστοτε κρατούντες.

[1104] Στα ερωτηματολόγια υπ' αρ. 1, 9, 25, 38, 39, 44, 45, 46, 52, 57, 62, 65, 76, 88, 90, 94, 103, 109, 112, 113, 114, 115, 120, 122, 125, 132, 135, 137, 138, 146, 157.

[1105] Η χρήση της τεχνολογίας για πρόληψη και καταστολή εγκληματικών πράξεων αλλά και για την εκτέλεση ποινών απασχολεί έντονα τη σύγχρονη αρθρογραφία – πρβλ. ενδεικτικά *Paul Johnson & Robin Williams*, Internationalizing New Technologies of Crime Control: Forensic DNA Databasing and Datasharing in the European Union, Policing & Society, Vol. 17, No. 2, June 2007, pp. 103-118, *Richard Jones*, Digital rule, Punishment, control and technology, SAGE Publications, London, Thousand Oaks and New Delhi, Vol. 2(1): 5-22, *Αν. Χάιδου*, Εγκληματολογικά κείμενα, Διεθνής αντεγκληματική πολιτική. Αποτελεσματικότητα των κυρώσεων και ανθρώπινα δικαιώματα. Ο ρόλος της σύγχρονης τεχνολογίας, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, σελ. 109 επ.

[1106] Αναφορικά με το ιδιαίτερο σχετικό επιστημονικό ενδιαφέρον πρβλ. *Julia Davidson & Petter Gottschalk*, Characteristics of the Internet for criminal child sexual abuse by online groomers, Criminal Justice Studies, Vol. 24, No. 1, March 2011, 23–36.

[1107] Βλ. σχετικά με τη δυνατότητα συνδρομής των hackers στην πρόληψη ηλεκτρονικών εγκλημάτων το δημοσίευμα της ενημερωτικής ιστοσελίδας «Το κουτί της Πανδώρας» στις 13.07.2014 με τίτλο "Αυτός είναι ο 17χρονος «ταλαντούχος» χάκερ που έγινε συνεργάτης της Δίωξης Ηλεκτρονικού Εγκλήματος" (url: http://www.koutipandoras.gr/article/118088/aytos-einai-o-17hronos-talantoyhos-haker-poy-egine-synergatis-tis-dioxis-ilektronikoy).

[1108] Στα ερωτηματολόγια υπ' αρ. 3, 5, 6, 15, 20, 22, 28, 41, 47, 74, 75, 90, 97, 124, 129, 131, 133, 138, 142, 158.

[1109] Στα ερωτηματολόγια υπ' αρ. 7, 13, 16, 17, 23 (χαρακτηριστικά σε αυτήν την απάντηση υποστηρίζεται η δράση του Julian Assange), 29, 33, 42, 50, 53, 56, 58, 59, 60, 61, 63, 67, 81, 86, 91, 101, 126, 127, 134, 136, 139, 143, 145, 147, 148, 154.

δ) σε 7 απαντήσεις[1110] (ποσοστό 4,43 % από το γενικό σύνολο και 6,14 % από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται ως κεντρική ιδέα η συμβολή των hackers σε ιδεολογική αφύπνιση των πολιτών (με ιδιαίτερο βάρος π.χ. στη δράση των "Anonymous").

Επιπρόσθετα, απαντήσεις άξιες μνείας είναι οι μόνο 3[1111] οι οποίες αναφέρονται στο γεγονός ότι η δράση των hackers μπορεί να συμβάλλει στην ελευθερία της έκφρασης (ενδεχομένως θα περίμενε κάποιος περισσότερες σχετικές απαντήσεις, λαμβανομένου υπόψιν το ότι η ελευθερία της έκφρασης αποτελεί συστατικό στοιχείο της ιδεολογίας των hackers[1112]) καθώς και η απάντηση ότι θα μπορούσε να υπάρξει θετική συμβολή των hackers στην περίπτωση διαγραφής χρεών ιδιωτών σε πιστωτικά ιδρύματα[1113].

Σε μια συνολική θεώρηση των απαντήσεων σύμφωνα με τις οποίες δύναται να υπάρχει κάποιου είδους θετική συμβολή του hacking, πρέπει να λάβουμε υπόψιν ότι αρκετές από αυτές τις απαντήσεις έχουν δοθεί με επιφύλαξη – όπως προκύπτει από τη διατύπωσή τους – αναφορικά με την κατάχρηση της χωρίς δικαίωμα πρόσβασης σε δεδομένα και με όρους αναλογικότητας.

Από την πλευρά των αρνητικών απαντήσεων (ότι δηλαδή οι hackers δεν μπορούν να έχουν θετική συμβολή στην κοινωνία), οι περισσότερες εξ αυτών αρκούνται σε ένα κατηγορηματικό όχι. Σε απαντήσεις στις οποίες αναλύεται η σκέψη του συμμετέχοντος στην έρευνα διαπιστώνουμε την προσήλωση αυτών στη νομιμότητα καθώς θεωρούν το hacking παράνομη δραστηριότητα, η οποία δεν μπορεί με κανέναν τρόπο να νομιμοποιηθεί[1114]. Τέλος, άξιες αναφοράς είναι οι δύο απαντήσεις κατά τις οποίες το hacking μπορεί να έχει θετική συμβολή στην κοινωνία ως παράδειγμα προς αποφυγή[1115].

<u>Ερώτηση 5</u>: Κατά τη γνώμη σας, η ελληνική νομοθεσία είναι αποτελεσματική για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων;

[1110] Στα ερωτηματολόγια υπ' αρ. 34, 51, 66, 68, 72, 73, 85.

[1111] Ερωτηματολόγια υπ' αρ. 82, 104, 139.

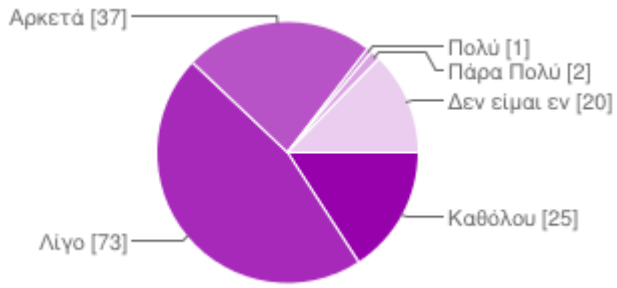
[1112] Βλ. παράγραφο 2.7 του παρόντος πονήματος.

[1113] Στο ερωτηματολόγιο υπ' αρ. 26.

[1114] Βλ. απαντήσεις στα ερωτηματολόγια υπ' αρ. 4, 71, 77 καθώς και στο ερωτηματολόγιο υπ' αρ. 35 στο οποίο αναφέρεται η άποψη για «*καμία νομιμοποίηση της παρανομίας*»!

[1115] Στα ερωτηματολόγια υπ' αρ. 10 και 55.

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ - Δεν είμαι ενημερωμένος για τις νομικές προβλέψεις)



Καθόλου	**25** 16%
Λίγο	**73** 46%
Αρκετά	**37** 23%
Πολύ	**1** 1%
Πάρα Πολύ	**2** 1%
Δεν είμαι ενημερωμένος για τις νομικές προβλέψεις	**20** 13%

Η πλειονότητα των ερωτώμενων νομικών (46%) θεωρεί ότι η ελληνική νομοθεσία είναι *λίγο* αποτελεσματική σε επίπεδο διαφύλαξης της ασφάλειας των ηλεκτρονικών δεδομένων ενώ ένα αξιοσημείωτο ποσοστό του 16% αυτών εκτιμά ότι η σχετική αποτελεσματικότητα της ελληνικής νομοθεσίας είναι μηδενική. Αν προστεθούν αυτά τα δύο ποσοστά διαπιστώνεται ότι το 62% των νομικών θεωρεί ουσιαστικά ανεπαρκείς τις διατάξεις του ελληνικού δικαίου για την ασφάλεια των ηλεκτρονικών δεδομένων. Βέβαια, πρέπει να λάβουμε υπόψιν μας σε κάθε περίπτωση ότι οι νομικοί ενδεχομένως γνωρίζουν την άκρως περιορισμένη νομολογιακή εφαρμογή των

σχετικών διατάξεων και, συνεπώς, οι απαντήσεις τους αυτές μάλλον επηρεάζονται σχετικώς.

Από την άλλη, το 23% των ερωτώμενων νομικών πιστεύει σε μία αρκετά αποτελεσματική προληπτική λειτουργία των ελληνικών ποινικών κυρώσεων που προβλέπονται για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων (άρα και του hacking). Είναι, βέβαια, αξιοσημείωτο ότι το 13% των ερωτηθέντων νομικών δηλώνει ότι δεν έχει ενημέρωση για τις σχετικές νομικές προβλέψεις[1116], ποσοστό σημαντικό αν αναλογιστεί κανείς την εισβολή του διαδικτύου στην καθημερινή επαγγελματική και ατομική δραστηριότητα.

<u>Ερώτηση 6</u>: Πρέπει να είναι ελεύθερη η πρόσβαση στην πληροφορία στο διαδίκτυο; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Προβαίνοντας σε ανάλυση περιεχομένου των απαντήσεων, διαπιστώνεται ότι από το δείγμα των 158 απαντήσεων σε 127 (ποσοστό 80,37%) από αυτές υποστηρίζεται ότι πρέπει η πρόσβαση στην ηλεκτρονική πληροφορία να είναι ελεύθερη, με προϋποθέσεις/ περιορισμούς ή χωρίς. Από αυτές τις 127 απαντήσεις, στις 33 από αυτές (ποσοστό 25,98% από τις θετικές απαντήσεις και 20,88 % από το σύνολο) υποστηρίζεται η ελεύθερη πρόσβαση στην πληροφορία στο διαδίκτυο χωρίς απολύτως καμία προϋπόθεση και περιορισμό[1117]. Επιπρόσθετα, στις απαντήσεις στις οποίες υποστηρίζεται η ελεύθερη πρόσβαση στο διαδίκτυο υπό προϋποθέσεις, ο περιορισμός που τίθεται στις περισσότερες απαντήσεις είναι η προστασία των προσωπικών δεδομένων (προκρίνεται ως προϋπόθεση σε 42 απαντήσεις[1118] [1119] –

[1116] Αναφορικά με την γνώση του δικαίου και τη σημασία της πρβλ. *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 225 επ.

[1117] Στα ερωτηματολόγια υπ' αρ. 7, 8, 13, 17,29,30, 36, 40, 49, 52, 54, 56, 59, 63, 73, 88, 89, 90, 96, 101, 104, 108, 127, 128, 129, 132, 133, 137, 142, 144, 147, 152 και 156.

[1118] Στα ερωτηματολόγια υπ' αρ. 2, 3, 10, 11, 21, 22, 27, 28, 35, 38, 44, 45, 57, 61, 64, 65, 67, 71, 72, 74, 77, 78, 80, 84, 91, 94, 97, 103, 106, 114, 117, 120, 122, 124, 126, 135, 136, 138, 141, 145, 155 και 158.

[1119] Σημειώνεται ότι στην ερώτηση υπ' αρ. 1 ο αριθμός των απαντήσεων αναφορικά με τον ορισμό του hacking οι οποίες περιελάμβαναν τον όρο «προσωπικά δεδομένα» ήταν πάλι 42! Το εύρημα αυτό λειτουργεί αποδεικτικά και ενισχυτικά σε ό,τι αφορά τη συνεκτικότητα της έρευνας.

ποσοστό 33,07% από τις θετικές απαντήσεις και 26,58% στο σύνολο των απαντήσεων). Ένας ακόμη περιορισμός που τίθεται από τους απαντώντες στην ελευθερία της πληροφορίας στο διαδίκτυο είναι η προστασία της ασφάλειας του κράτους, εντοπιζόμενος σε 9 απαντήσεις[1120] (ποσοστό 7,08% από τις θετικές απαντήσεις και 5,69% από το σύνολο). Επιπρόσθετα, ιδιαίτερο βάρος δίνεται σε ορισμένες απαντήσεις αναφορικά με τον περιορισμό της ελεύθερης πρόσβασης στην ηλεκτρονική πληροφορία με σκοπό την προστασία των ανηλίκων (11 απαντήσεις[1121] - ποσοστό 8,66% από τις θετικές απαντήσεις και 6,96% από το σύνολο). Τέλος, σε ορισμένες απαντήσεις προκρίνεται η ελευθερία στην πρόσβαση στην ηλεκτρονική πληροφορία για ερευνητικές και εκπαιδευτικές δραστηριότητες (12 απαντήσεις[1122] - ποσοστό 9,44% από τις θετικές απαντήσεις και 7,59% από το σύνολο).

Μία επιπλέον ομαδοποίηση απαντήσεων εν προκειμένω είναι αυτήν στην οποία η άποψη που εκφράζεται έχει να κάνει με το ότι η πληροφορία πρέπει να είναι ελεύθερη μόνο στην περίπτωση κατά την οποία ο κάτοχός της, ο δημιουργός της ή ο χρήστης της το έχει επιλέξει (12 απαντήσεις[1123] - ποσοστό 9,44% από τις θετικές απαντήσεις και 7,59% από το σύνολο).

Εντελώς αρνητικές αναφορικά με την ελεύθερη πρόσβαση στην πληροφορία καταγράφονται μόλις 6 απαντήσεις (3,79%). Επιπρόσθετα, υπάρχουν 10 απαντήσεις (ποσοστό 6,32%), οι οποίες ουσιαστικά δεν λαμβάνουν θέση υπέρ ή κατά της ελευθερίας της πρόσβασης[1124]. Υπάρχει, επιπρόσθετα, ένα ακόμη ερωτηματολόγιο στο οποίο αναφέρεται ότι η πρόσβαση πρέπει να είναι ελεύθερη μόνο για αποτροπή εγκλημάτων[1125].

Τέλος, σε ένα ερωτηματολόγιο υπάρχει η απάντηση «Δεν απαντώ»[1126] και σε άλλο ένα η απάντηση «Δεν γνωρίζω»[1127].

[1120] Στα ερωτηματολόγια υπ' αρ. 2, 27, 28, 103, 121, 131, 135, 136 και 143.

[1121] Στα ερωτηματολόγια υπ' αρ. 2, 4, 12, 15, 24, 34, 75, 112, 138, 139 και 149.

[1122] Στα ερωτηματολόγια υπ' αρ. 5, 25, 39, 42, 50, 86, 92, 113, 115, 123, 148 και 157.

[1123] Στα ερωτηματολόγια υπ' αρ. 23, 55, 83, 85, 95, 100, 107, 110, 119, 125, 146 και 150.

[1124] Στα ερωτηματολόγια υπ' αρ. 2, 3, 16, 18, 41, 47, 79, 81, 140 και 154.

[1125] «*Μόνο για αποτροπή εγκληματικών ενεργειών και κατόπιν εισαγγελικής παραγγελίας*» στο ερωτηματολόγιο υπ' αρ. 99.

[1126] Στο ερωτηματολόγιο υπ' αρ. 33.

[1127] Στο ερωτηματολόγιο υπ' αρ. 70.

<u>Ερώτηση 7</u>: Έχετε να προτείνετε άλλα μέτρα - πέρα από ποινικές διατάξεις - που μπορούν να ληφθούν για την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων; Αν ναι, ποια;

(ανοικτού τύπου ερώτηση)

Οι απαντήσεις που ελήφθησαν από το δείγμα των νομικών στην ανωτέρω ερώτηση παρουσιάζουν αρκετά μεγάλη ποικιλομορφία. Ωστόσο, είναι προφανές το αίτημα για πληρέστερη ενημέρωση και εκπαίδευση των χρηστών του διαδικτύου αναφορικά με την προστασία των ηλεκτρονικών τους δεδομένων καθώς 45 από τους 158 απαντώντες[1128] (ποσοστό 28,48%) αναφέρονται σε αυτό.

Επιπρόσθετα, σε 18 απαντήσεις[1129] (ποσοστό 11,39 %) οι απαντώντες προτείνουν την έρευνα και τη συνεχή ανανέωση των ηλεκτρονικών προγραμμάτων στα οποία εντοπίζονται τρωτά σημεία και, συνεπώς, την ενίσχυση της ασφάλειας μέσω των ίδιων των ηλεκτρονικών προγραμμάτων. Στο ερωτηματολόγιο υπ' αρ. 25 προτείνεται, επίσης, η πιστοποίηση των ιστοσελίδων αναφορικά με την ασφάλειά τους[1130]. Αντίστοιχες μπορούν να θεωρηθούν οι 8 απαντήσεις[1131] (ποσοστό 5,06%) στις οποίες προτείνονται η χρήση φίλτρων και προγραμμάτων προστασίας από ιούς (antivirus)[1132].

Από την άλλη πλευρά, είναι γεγονός ότι διατυπώνονται και απόψεις οι οποίες στρέφονται προς τον μεγαλύτερο έλεγχο του διαδικτύου. Συγκεκριμένα, πρόταση για μεγαλύτερο έλεγχο εντοπίζεται περιφραστικά αλλά σαφώς σε 16 απαντήσεις[1133] (ποσοστό 10,12%), η οποία ενίοτε εξειδικεύεται σε μεγαλύτερη ευελιξία των αρχών και αμεσότερη άρση του απορρήτου. Προς τούτο διατυπώνεται, επίσης, η άποψη για ενίσχυση των υπηρεσιών ελέγχου του διαδικτύου[1134] ή για τη δημιουργία σχετικής

[1128] Στα ερωτηματολόγια υπ' αρ. 1, 5, 6, 8, 15, 16, 17, 18, 24, 25, 28, 36, 41, 44, 47, 50, 51, 60, 62, 69, 71, 75, 77, 79, 82, 84, 90, 91, 94, 99, 108, 110, 113, 117, 118, 124, 131, 133, 135, 141, 143, 145, 146, 151, 153.

[1129] Στα ερωτηματολόγια υπ' αρ. 2, 4, 5, 21, 24, 25, 34, 40, 63, 69, 74, 78, 80, 99, 117, 118, 121, 122.

[1130] Βλ. σχετικά και παράγραφο 6.3.4 του παρόντος πονήματος όπου και αναφορά στην πιστοποίηση από το Ψήφισμα του Συμβουλίου της 28.01.2002.

[1131] Στα ερωτηματολόγια υπ' αρ. 13, 26, 54, 59, 87, 106, 138, 140.

[1132] Βλ. σχετικές αναπτύξεις στην παράγραφο 9.1.2.

[1133] Στα ερωτηματολόγια υπ' αρ. 12, 27, 38, 43, 53, 55, 58, 64, 76, 80, 92, 107, 115, 136, 141, 152.

[1134] Η Υποδιεύθυνση δίωξης ηλεκτρονικού εγκλήματος της ΕΛ.ΑΣ. έχει γίνει αρκετά γνωστή για τη δράση και την αποτελεσματικότητα της – βλ. χαρακτηριστικά και πρακτικά συνεδρίων «Η ασφαλής

ανεξάρτητης αρχής σε 10 απαντήσεις[1135] (ποσοστό 6,32%). Σε 2, δε, απαντήσεις[1136] (ποσοστό, 1,26%), προτείνεται συγκεκριμένα η ενίσχυση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[1137]. Σε 8 απαντήσεις[1138] (ποσοστό 5,06%), περαιτέρω, προτείνονται διοικητικές ποινές και πρόστιμα[1139] ενώ σε 5 απαντήσεις[1140] (ποσοστό 3,16%) εντοπίζεται η πρόταση για αποκλεισμό της πρόσβασης ως ποινή σε παραβιαστές δεδομένων στο διαδίκτυο. Σε επίπεδο ποινικών νόμων και παρά τη διατύπωση της ερώτησης υπάρχουν 3 απαντήσεις[1141] (ποσοστό 1,89%) στις οποίες προκρίνεται η αυστηροποίηση των ποινικών κυρώσεων ενώ σε 4 απαντήσεις[1142] (ποσοστό 2,53%) ως πρόταση εισφέρεται η γενικότερη καταπολέμηση του ηλεκτρονικού εγκλήματος. Τέλος, με πιο ήπια προσέγγιση υπάρχουν 8 απαντώντες[1143] (ποσοστό 5,06%) οι οποίοι προτείνουν αστικές κυρώσεις και αποζημίωση (χαρακτηριστική η απάντηση στο ερωτηματολόγιο υπ' αρ. 25 στην οποία προτείνεται η δημοσίευση επιστολής συγγνώμης στον τύπο από κάθε hacker ο οποίος εντοπίζεται). Αν ομαδοποιήσουμε τις ανωτέρω απαντήσεις καταλήγουμε στο ότι 49 απαντώντες[1144] (ποσοστό 31,01%) υποστηρίζουν την λήψη αυστηρών μέτρων για την ασφάλεια των συστημάτων πληροφοριών.

Ωστόσο, στα υπό επεξεργασία ερωτηματολόγια ανευρίσκονται και απαντήσεις οι οποίες αναφέρονται στην ευθύνη του ίδιου του χρήστη. Εντύπωση, πιστεύω, προκαλούν οι 4 απαντήσεις[1145] (ποσοστό, 2,53%) στις οποίες υποστηρίζεται η

πλοήγηση είναι υπόθεση όλων μας» (1ο συνέδριο για την ασφαλή πλοήγηση στο διαδίκτυο το έτος 2012 και 2ο συνέδριο το έτος 2013). Αντίστοιχες υπηρεσίες σε χώρες του εξωτερικού είναι το National Infrastructure Protection Center (NIPC) του FBI στις Η.Π.Α., με παραρτήματα σε διάφορες Πολιτείες για την έρευνα των σχετικών εγκλημάτων, το Computer Fraud Squad της Scotland Yard στο Ηνωμένο Βασίλειο και το Royal Canadian Mounted Police Computer Crime Unit στον Καναδά (για τις αρμόδιες υπηρεσίες για την έρευνα του εγκλήματος στον κυβερνοχώρο βλ. και *Ιωάν. Αγγελής*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 12/2001, 1298-1299).

[1135] Στα ερωτηματολόγια υπ' αρ. 14, 33, 34, 60, 65, 102, 110, 123, 126, 150.

[1136] Στα ερωτηματολόγια υπ' αρ. 17 και 30.

[1137] Είναι, βέβαια, γεγονός ότι η ΑΔΑΕ είναι μάλλον αρμόδια για αυτά τα ζητήματα – ωστόσο, μάλλον πρέπει να ληφθεί υπόψιν η «ευαισθησία» στο ζήτημα των προσωπικών δεδομένων, όπως καταδείχθηκε ανωτέρω.

[1138] Στα ερωτηματολόγια υπ' αρ. 22, 39, 57, 76, 83, 103, 134, 135.

[1139] Αναφορικά με τις ποινές σε χρήμα πρβλ. το μνημειώδες έργο του *Ν. Κουράκη*, Ποινική Καταστολή, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2009, 5η εκδ., σελ. 391 επ.

[1140] Στα ερωτηματολόγια υπ' αρ. 9, 31, 39, 73, 93.

[1141] Στα ερωτηματολόγια υπ' αρ. 77, 90, 133.

[1142] Στα ερωτηματολόγια υπ' αρ. 7, 28, 45, 68.

[1143] Στα ερωτηματολόγια υπ' αρ. 19, 52, 61, 73, 77, 86, 88, 109.

[1144] Σε κάποιες απαντήσεις καταγράφονται παραπάνω από μία προτάσεις.

[1145] Στα ερωτηματολόγια υπ' αρ. 10, 75, 82, 97.

ανάρτηση μόνο των απαραίτητων ηλεκτρονικών πληροφοριών (πρόταση, βεβαίως, περιορισμένης εφαρμοσιμότητας λόγω της ψηφιακής λειτουργίας όλων των σύγχρονων συστημάτων) και η χρήση κωδικών εκ μέρους των χρηστών σε 3 απαντήσεις[1146] (ποσοστό 1,89%).

Ως άλλες προτάσεις διατυπώνονται επιπλέον: σε 2 απαντήσεις[1147] (ποσοστό, 1,26%) η δημιουργία ενός είδους ηλεκτρονικής ταυτότητας ή η δήλωση κάθε υπολογιστή που αγοράζεται προκειμένου να μπορεί να προσδιοριστεί ο χρήστης του[1148], η επικαιροποίηση των όρων χρήσης των ιστοσελίδων[1149], η πιο σαφής έκθεση στους όρους των ιστοσελίδων των τρόπων διαφύλαξης του απορρήτου[1150], η θέσπιση ευθύνης των παρόχων σύνδεσης διαδικτύου[1151] [1152], η χρήση ηλεκτρονικών υπογραφών[1153], η δημιουργία ενός κώδικα δεοντολογίας στο διαδίκτυο[1154] μάλλον και σε συνδυασμό με τις 2 απαντήσεις[1155] (ποσοστό 1,26%), οι οποίες προκρίνουν την αυτοοργάνωση των χρηστών του διαδικτύου και την πρόταση για διεθνή συνεργασία[1156] στην πρόληψη παραβιάσεως των ηλεκτρονικών πληροφοριών[1157]. Περαιτέρω, σε 2 απαντήσεις[1158] (ποσοστό 1,26%) υποστηρίζεται ότι είναι αρκετή η εφαρμογή του ισχύοντος νομικού πλαισίου, μάλλον γνωρίζοντας την περιορισμένη εφαρμογή των διατάξεων[1159]. Τέλος, διατυπώνεται η άποψη της αποποινικοποίησης[1160] των πράξεων που προσβάλλουν την ασφάλεια των ηλεκτρονικών δεδομένων και σε άλλη απάντηση αυτή η άποψη μάλλον εξειδικεύεται καθώς υποστηρίζεται ότι ο ίδιος ο σκοπός του διαδικτύου δεν συμβαδίζει ουσιαστικά με την προστασία των δεδομένων[1161]!

[1146] Στα ερωτηματολόγια υπ' αρ. 116, 128, 129.

[1147] Στα ερωτηματολόγια υπ' αρ. 105 και 157.

[1148] ... άποψη η οποία μάλλον σημαίνει ολοκληρωτική άρση του απορρήτου.

[1149] Στο ερωτηματολόγιο υπ' αρ. 139.

[1150] Στο ερωτηματολόγιο υπ' αρ. 158.

[1151] Στο ερωτηματολόγιο υπ' αρ. 149.

[1152] Βλ. σχετικά τις αναπτύξεις στην παράγραφο 4.3.2 ιδίως αναφορικά με το Π.Δ. 131/2003 για την ευθύνη των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας.

[1153] Στο ερωτηματολόγιο υπ' αρ. 42.

[1154] Στο ερωτηματολόγιο υπ' αρ. 149.

[1155] Στα ερωτηματολόγια υπ' αρ. 14 και 60.

[1156] Βλ. και παράγραφο 9.4 του παρόντος πονήματος.

[1157] Στο ερωτηματολόγιο υπ' αρ. 16.

[1158] Στα ερωτηματολόγια υπ' αρ. 49 και 154.

[1159] Βλ. παράγραφο 5.5.

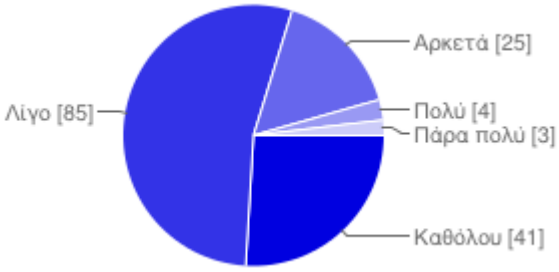
[1160] Στο ερωτηματολόγιο υπ' αρ. 104.

[1161] Στο ερωτηματολόγιο υπ' αρ. 100.

Οι απαντώντες οι οποίοι δεν είχαν να προτείνουν άλλα μέτρα ανήλθαν στους 8[1162] (ποσοστό 5,06%) και όσοι δεν γνώριζαν ή δεν μπορούσαν να προτείνουν κάτι ανήλθαν σε 23[1163] (ποσοστό 14,55%). Κλείνοντας την επεξεργασία της ερώτησης, κατεγράφησαν 3 κενές απαντήσεις[1164].

<u>Ερώτηση 8</u>: Πόσο ασφαλής νιώθετε αναφορικά με τα ηλεκτρονικά σας δεδομένα στο διαδίκτυο;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου	**41**	26%
Λίγο	**85**	54%
Αρκετά	**25**	16%
Πολύ	**4**	3%
Πάρα πολύ	**3**	2%

[1162] Ερωτηματολόγια υπ' αρ. 3, 29, 35, 37, 48, 66, 98 και 114.

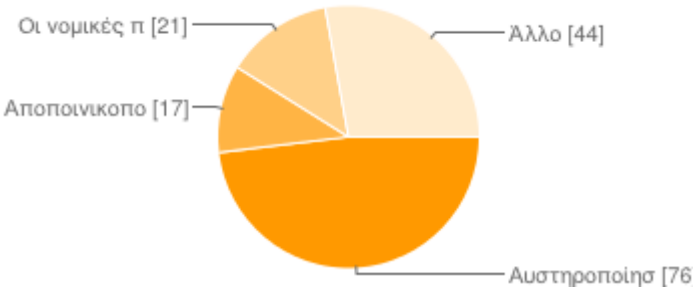
[1163] Στα ερωτηματολόγια υπ' αρ. 11, 32, 46, 56, 67, 70, 72, 81, 85, 95, 96, 101, 111, 112, 119, 120, 125, 127, 130, 137, 147, 148 και 155.

[1164] Στα ερωτηματολόγια υπ' αρ. 20, 142 και 156.

Αναφορικά με το αίσθημα ασφάλειας των νομικών σε ό,τι έχει να κάνει με τις ηλεκτρονικές τους πληροφορίες, η πλειοψηφία των νομικών βιώνει σε μεγάλο βαθμό αίσθημα ανασφάλειας (54% νιώθει λίγο ασφαλής για τις ηλεκτρονικές του πληροφορίες και 26 % δεν νιώθει καμία ασφάλεια – άρα, 80% των ερωτώμενων διάκειται αρνητικά αναφορικά με το αίσθημα ασφάλειας για τις ηλεκτρονικές του πληροφορίες στο διαδίκτυο). Από την άλλη, απολύτως θετικό αίσθημα ασφάλειας βιώνει μοναχά το 5% των ερωτώμενων (3% νιώθει πολύ ασφαλής και 2% πάρα πολύ ασφαλής).

<u>Ερώτηση 9</u>: Ποια η γνώμη σας: χρειάζεται αυστηροποίηση των ποινικών κυρώσεων, αποποινικοποίηση του hacking ή οι νομικές προβλέψεις να μείνουν ως έχουν;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Αυστηροποίηση των ποινικών κυρώσεων	**76**	48%
Αποποινικοποίηση του hacking	**17**	11%
Οι νομικές προβλέψεις να μείνουν ως έχουν	**21**	13%
Άλλο	**44**	28%

Στο ερώτημα για αλλαγές στο ισχύον νομικό πλαίσιο το μεγαλύτερο ποσοστό των ερωτώμενων νομικών (48%) διάκειται υπέρ της αυστηροποίησης των ποινικών κυρώσεων. Ωστόσο, ένα αξιοσημείωτο ποσοστό της τάξης του 11% των ερωτώμενων νομικών εκφράστηκε θετικά απέναντι στο μη αναγκαίο αξιόποινο του hacking και στην αποποινικοποίηση αυτής της δραστηριότητας, ενώ το 13% θεωρεί ότι η ποινική νομοθεσία πρέπει να παραμείνει αμετάβλητη.

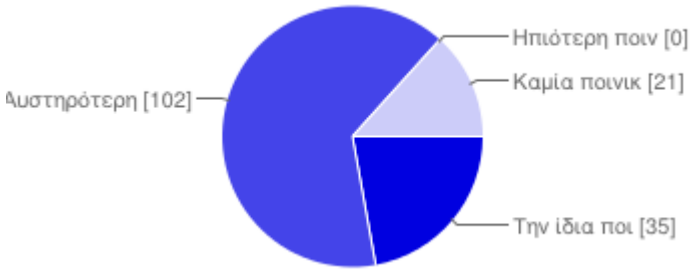
Στη συγκεκριμένη ερώτηση καταγράφεται αρκετά σημαντικό ποσοστό (28%) της επιλογής «*Άλλο*». Σε αυτήν την επιλογή υπάρχει για ακόμη μια φορά μεγάλη ποικιλομορφία απαντήσεων, η οποία δύσκολα ομαδοποιείται. Κυρίαρχες τάσεις μπορεί να υποστηριχθεί ότι συνιστούν η άποψη για όχι αυστηρότερες διατάξεις (4 απαντήσεις[1165]) με εξειδίκευση του hacking στις διατάξεις (2 απαντήσεις[1166]), η υιοθέτηση περισσότερης νομικής ευελιξίας[1167] για σύνθετες και αποτελεσματικές λύσεις[1168] και κατά περίπτωσης ρυθμίσεων (σύμφωνα με την διατύπωση των 4 απαντήσεων[1169]) και γενικότερα εκσυγχρονισμός των νόμων (6 απαντήσεις[1170]). Επιπρόσθετα, υποστηρίζονται και σε αυτήν την απάντηση εξωδικαιικές λύσεις όπως η εντατικοποίηση των μέτρων προστασίας με ειδικά προγράμματα και η βελτίωση συστημάτων αποτροπής προσβολών[1171], η ενίσχυση της προστασίας «στην πηγή της πληροφορίας» (όπου μάλλον εννοείται ο πάροχος της σύνδεσης)[1172] αλλά και γενικότερα η πρόληψη[1173] και η θέσπιση εναλλακτικών μορφών προστασίας[1174]. Επιστρέφοντας στη θεώρηση των ποινών, υποστηρίζεται η αποποινικοποίηση του hacking για ιδεολογικούς λόγους αλλά η αυστηρότερη αντιμετώπιση συμπεριφορών χωρίς δικαίωμα πρόσβασης οι οποίες προκαλούν ζημία[1175], οι οποίες συνδυάζονται με απαντήσεις που αναφέρονται στην λήψη υπόψιν του κινήτρου[1176] με σκοπό την κλιμάκωση των ποινών[1177]. Περαιτέρω, υποστηρίζεται ότι πρόβλημα είναι η μη άρση

[1165] Στα ερωτηματολόγια υπ' αρ. 1, 42, 64 και 106.
[1166] Στα ερωτηματολόγια υπ' αρ. 1 και 139.
[1167] Στα ερωτηματολόγια υπ' αρ. 5 και 122.
[1168] Στα ερωτηματολόγια υπ' αρ. 5 και 58.
[1169] Στα ερωτηματολόγια υπ' αρ. 5, 59, 108 και 134.
[1170] Στα ερωτηματολόγια υπ' αρ. 38, 42, 74, 110, 135, 149.
[1171] Βλ. σχετικώς στα ερωτηματολόγια υπ' αρ. 26, 100 και 154.
[1172] Ερωτηματολόγια υπ' αρ. 64 και 144.
[1173] Ερωτηματολόγιο υπ' αρ. 141.
[1174] Ερωτηματολόγιο υπ' αρ. 14.
[1175] Στα ερωτηματολόγια υπ' αρ. 82 και 138.
[1176] Ερωτηματολόγιο υπ' αρ. 148.
[1177] Ερωτηματολόγιο υπ' αρ. 136.

του απορρήτου[1178] σε περιπτώσεις χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα[1179] και προκρίνεται και εν προκειμένω η αυστηροποίηση των ποινικών διατάξεων[1180] και σε κάθε περίπτωση η μη αποποινικοποίηση[1181]. Τέλος, επισημαίνεται η ανάγκη εφαρμογής των ήδη ισχυόντων νόμων[1182], ο συνδυασμός ποινικών και διοικητικών μέτρων[1183] και, από την άλλη, η απόδοση κινήτρων (για εποικοδομητικές δράσεις) στους «ηθικούς» hackers[1184]. Κλείνοντας, σε 11 ερωτηματολόγια του δείγματος[1185] (ποσοστό 6,96%) εντοπίζεται απάντηση με ουσιαστικό περιεχόμενο «Δεν γνωρίζω».

<u>Ερώτηση 10</u>: Όποιος αποκτά χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα στο διαδίκτυο με σκοπό οικονομικό όφελος ή πρόκληση ζημίας πρέπει να έχει την ίδια, ηπιότερη ή αυστηρότερη ποινική μεταχείριση από τον νόμο σε σχέση με αυτόν που δεν έχει σκοπό το οικονομικό όφελος ή την πρόκληση ζημίας;

(κλειστού τύπου ερώτηση: Την ίδια ποινική μεταχείριση – Αυστηρότερη ποινική μεταχείριση – Ηπιότερη ποινική μεταχείριση – Καμία ποινική μεταχείριση για χωρίς δικαίωμα πρόσβαση ανεξαρτήτως σκοπού ή αποτελέσματος)



[1178] Στα ερωτηματολόγια υπ' αρ. 41 και 65.

[1179] Το ά. 370Γ παρ. 2 ΠΚ δεν περιλαμβάνεται στην numerous clausus αναφορά των εγκλημάτων για τα οποία λαμβάνει χώρα άρση του απορρήτου σύμφωνα με το ά. 4 του ν. 2225/1994.

[1180] Στο ερωτηματολόγιο υπ' αρ. 65.

[1181] Στο ερωτηματολόγιο υπ' αρ. 121.

[1182] Ερωτηματολόγιο υπ' αρ. 126.

[1183] Ερωτηματολόγιο υπ' αρ. 103.

[1184] Ερωτηματολόγιο υπ' αρ. 90.

[1185] Στα ερωτηματολόγια υπ' αρ. 6, 11, 23, 79, 84, 97, 115, 121, 151, 153 και 158.

Την ίδια ποινική μεταχείριση	**35**	22%
Αυστηρότερη ποινική μεταχείριση	**102**	65%
Ηπιότερη ποινική μεταχείριση	**0**	0%
Καμία ποινική μεταχείριση για χωρίς δικαίωμα πρόσβαση ανεξαρτήτως σκοπού ή αποτελέσματος	**21**	13%

Το δείγμα των νομικών φαίνεται να πιστεύει σαφώς ότι ο σκοπός οικονομικού οφέλους ή πρόκλησης ζημίας σε περίπτωση χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα χρήζει αυστηρότερης ποινικής μεταχείρισης, καθώς αυτό υποστηρίζει το 65% των ερωτηθέντων. Το, δε, 22% των ερωτηθέντων πιστεύει ότι το κίνητρο δεν πρέπει να παίζει ρόλο στην ποινική μεταχείριση και, συνεπώς, πρέπει οι «παραβιαστές» να έχουν την ίδια ποινική μεταχείριση ανεξαρτήτως σκοπού. Ούτε ένας από το δείγμα δεν υποστήριξε την ηπιότερη ποινική μεταχείριση σε περίπτωση σκοπού οικονομικού οφέλους ή πρόκλησης ζημίας. Τέλος, το 13% των ερωτηθέντων υποστηρίζει την αποποινικοποίηση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα.

7.8.1.2 Συνολική θεώρηση απαντήσεων δείγματος νομικών

Προβαίνοντας στον άμεσο συσχετισμό και τη σύνοψη των απαντήσεων των νομικών, όπως παρουσιάστηκαν ανωτέρω, διαπιστώνεται στις περισσότερες περιπτώσεις μια λογική συνοχή και ακολουθία σε αυτές.

Το 62% (46% λίγο και 16% καθόλου) των ερωτώμενων νομικών στην ερώτηση 5 που δεν θεωρεί αρκετά αποτελεσματική την ισχύουσα ποινική νομοθεσία για το hacking συμφωνεί με τα στην ερώτηση 9 ποσοστά του 48% των νομικών που τάσσεται υπέρ της αυστηροποίησης των σχετικών ποινών και το 11% αυτών που επιθυμούν την αποποινικοποίηση του hacking (σύνολο 59%). Επιπρόσθετα, σε κάθε περίπτωση το μεγάλο ποσοστό που υποστηρίζει την αυστηροποίηση των ποινικών διατάξεων ως

ανωτέρω δικαιολογείται και εξηγείται από το ότι στην ερώτηση 8 το 26% των νομικών δηλώνει ανασφάλεια για τα δεδομένα του στο διαδίκτυο ενώ το ισχυρό 54% δηλώνει ότι αισθάνεται μόλις λίγο ασφάλεια για τα ηλεκτρονικά δεδομένα (βλ. ανωτέρω τη σχετική ανάπτυξη περί έντασης της τιμωρητικότητας σε περιπτώσεις «ανασφάλειας»[1186]). Ωστόσο, πρέπει να επισημανθεί με επιφύλαξη (όπως εξηγήθηκε στην ανωτέρω ερώτηση 4), ότι μόνο το 25,31% όσων απάντησαν πιστεύουν ότι οι hackers δεν μπορούν να έχουν καμία θετική συμβολή στην κοινωνία (ποσοστό σίγουρα μικρότερο από το 48% το οποίο υποστηρίζει την αυστηροποίηση των ποινικών κυρώσεων).

Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι ενώ το 25% (23% αρκετά, 1% πολύ, 1% πάρα πολύ) των ερωτώμενων νομικών στην ερώτηση 5 θεωρεί αρκετά αποτελεσματική την ελληνική ποινική νομοθεσία για το hacking, μόλις οι μισοί εξ αυτών, το 13% δηλαδή στην ερώτηση 9, πιστεύουν ότι η σχετική νομοθεσία πρέπει να παραμείνει ως έχει.

Στην ερώτηση 9 το 11% των ερωτηθέντων επιθυμεί την αποποινικοποίηση του hacking, ποσοστό παρεμφερές και αντίστοιχο με το 13% της ερώτησης 10 που υποστηρίζει ότι δεν πρέπει να υπάρχει καμία ποινή για την απόκτηση χωρίς δικαίωμα πρόσβασης σε δεδομένα (λαμβανομένου υπόψιν ότι στην ερώτηση 9 υπήρχε και η επιλογή «Άλλο» για τον ερωτώμενο σε αντίθεση με την ερώτηση 10). Ωστόσο, το 20,88% στην ερώτηση 6 δηλώνει ότι επιθυμεί ελεύθερη την πληροφορία στο διαδίκτυο χωρίς κανέναν περιορισμό (συμπεριλαμβανομένων και ποινικών διατάξεων).

Αναφορικά με την πρώτη υπόθεση έρευνας για τη σύγχρονη έννοια του hacking και τη χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, αναφέρθηκε ήδη ότι σε γενικές γραμμές οι ερωτώμενοι νομικοί περιγράφουν, με ποικιλομορφία στη διατύπωση, το hacking ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα αλλά και ότι σε κάποιες περιπτώσεις υπάρχει σύγχυση μεταξύ hacking και cracking καθώς αποδίδονται στον hacker και πράξεις αλλοίωσης των δεδομένων κ.λπ. Είναι γεγονός ότι στις απαντήσεις που αντιστοιχούν στην ερώτηση 1 δεν ανευρέθη κάποια πιο μοντέρνα ή ρηξικέλευθη περιγραφή της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά

[1186] Και *Χρ. Ζαραφωνίτου*, Τιμωρητικότητα: ανασφάλεια και κοσμοθεωρία, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τεύχος 13, Φεβρουάριος 2010, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1263811765.

δεδομένα – ωστόσο, θα μπορούσε να υποστηρίξει κάποιος ότι αυτό είναι λίγο έως πολύ αναμενόμενο καθώς οι νομικοί είναι αυτοί που παρακολουθούν περισσότερο το πεδίο του δικαίου παρά των τεχνολογικών εξελίξεων.

Σε ό,τι έχει να κάνει με την δεύτερη υπόθεση έρευνας, είδαμε ήδη στην ερώτηση 2 ότι οι απόψεις είναι μοιρασμένες αναφορικά με τα κίνητρα των hackers, καθώς το 35% πιστεύει ότι σημαντικότερο κίνητρο για τους hackers είναι η ιδεολογία τους, σε αντίθεση με το 34% που θεωρεί σημαντικότερο κίνητρο για τους hackers την αποκόμιση οικονομικού οφέλους ενώ σε 36 απαντήσεις της επιλογής «Άλλο» (ποσοστό 22,78%) αναφέρονται ως κίνητρα «Και τα δύο» (δηλαδή ότι οι hackers ενεργούν και με βάση ιδεολογικά κίνητρα αλλά και με σκοπό το οικονομικό όφελος). Άρα, ορθολογικές θεωρίες αλλά και κριτική εγκληματολογία φαίνεται να μπορούν να ερμηνεύσουν εξίσου την χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Πάντως, οι νομικοί στέκονται πολύ περισσότερο τιμωρητικοί σε περιπτώσεις οικονομικής ζημίας ή οφέλους, όπως προκύπτει από την ερώτηση 10.

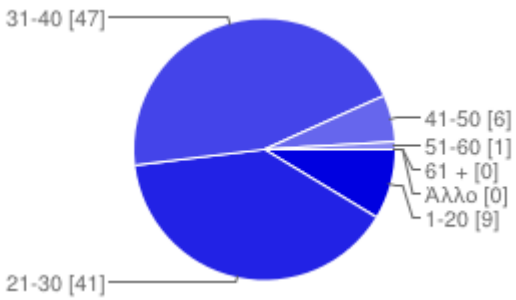
Οι απόψεις των νομικών για την αποτελεσματικότητα της νομοθεσίας, αποσαφηνίζονται στα ευρήματα της ερώτησης 5 με αποτέλεσμα αρνητικό για την ισχύουσα νομοθεσία, όπως διατυπώνεται ο αντίστοιχος προβληματισμός στην οικεία υπόθεση έρευνας, και οι προθέσεις αλλαγής της νομοθεσίας στις ερωτήσεις 9 και 10.

Ως εναλλακτικοί τρόποι προώθησης της ασφάλειας των ηλεκτρονικών δεδομένων διατυπώθηκαν αρκετοί ιδίως στην ερώτηση 7, με την εκπαίδευση να παίζει σημαντικό ρόλο στις προτάσεις αυτές. Η εν λόγω άποψη φαίνεται απαραίτητη καθώς, σύμφωνα με την ερώτηση 3, το 68% των ελλήνων νομικών που ασχολούνται με το δίκαιο της πληροφορικής δεν είναι επαρκώς ενημερωμένοι και εκπαιδευμένοι (καθόλου ή λίγο) σε θέματα πληροφορικής και ιδίως hacking. Είναι, όμως, γεγονός ότι στην ανάλυση των απαντήσεων των νομικών ανευρέθησαν και άλλες ενδιαφέρουσες απαντήσεις, όπως π.χ. οι διοικητικές ποινές και πρόστιμα που μπορούν να έχουν γενικοπροληπτικό αποτέλεσμα. Ωστόσο, οι απόψεις που υποστηρίζουν την αυτοοργάνωση του διαδικτύου με την κατάρτιση π.χ. ενός καταστατικού χάρτη δικαιωμάτων του διαδικτύου (ίσως αναμενόμενες από το δείγμα των νομικών λόγω του επιστημονικού και επαγγελματικού τους υπόβαθρου) ήταν πράγματι ελάχιστες.

7.8.2 Δείγμα επιστημόνων πληροφορικής (τεχνικών ασφαλείας και υπεύθυνων διαχείρισης ηλεκτρονικών δεδομένων)

7.8.2.1 Απαντήσεις

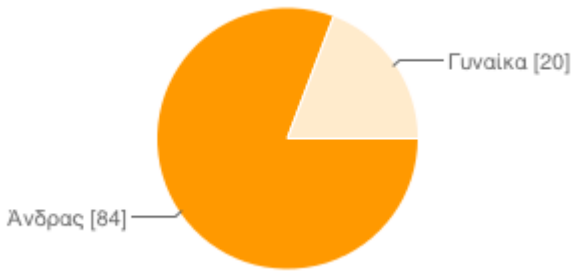
Ηλικία



1-20	**9**	9%
21-30	**41**	39%
31-40	**47**	45%
41-50	**6**	6%
51-60	**1**	1%
61 +	**0**	0%

Η συντριπτική πλειοψηφία των συμμετεχόντων επιστημόνων πληροφορικής στην έρευνα – ήτοι το 84% – είναι ηλικίας μεταξύ 21 έως 40 ετών[1187]. Το μεγάλο αυτό ποσοστό εξηγείται εύλογα από το γεγονός ότι, κατά την κοινή πείρα, σε αυτές τις ηλικίες ανήκουν αυτοί που ενδιαφέρονται περισσότερο για την χρήση των ηλεκτρονικών υπολογιστών. Επιπρόσθετα, αναφορικά με τους επιστήμονες πληροφορικής, είναι γεγονός ότι την τελευταία εικοσαετία λειτουργούν αντίστοιχες πανεπιστημιακές και τεχνικές σχολές, επομένως είναι λογικό να είναι ελάχιστοι εντός του συνόλου αυτοί οι οποίοι είναι σήμερα στην ηλικία των 50 και έχουν αντίστοιχες εξειδικεύσεις. Οι, δε, 9 απαντώντες οι οποίοι έχουν δηλώσει ότι είναι μικρότεροι από 20 ετών προφανώς έχουν λάβει κάποια ειδίκευση σε κάποιο ΙΕΚ ή άλλη σχολή επαγγελματικής κατάρτισης, η οποία ανταποκρίνεται στην ηλικία τους.

Φύλο



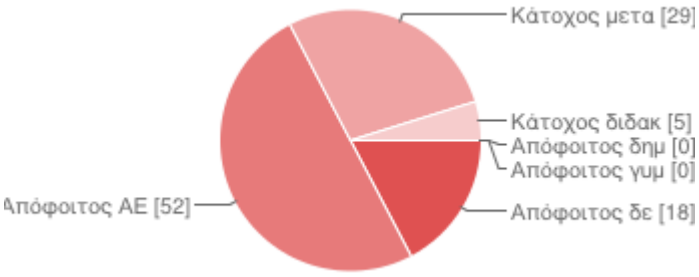
Άνδρας **84** 81%

Γυναίκα **20** 19%

Από το δείγμα το οποίο απάντησε στο ερωτηματολόγιο των επιστημόνων πληροφορικής οι 84 (ποσοστό 81%) είναι άνδρες και οι 20 (ποσοστό 19%) είναι γυναίκες. Η υπεροχή αυτή των ανδρών εξηγείται από τα διδάγματα της κοινής πείρας καθώς οι τεχνικές σπουδές και επαγγέλματα ελκύουν περισσότερο τους άνδρες από τις γυναίκες (σε αντιδιαστολή με το υψηλό ποσοστό γυναικών νομικών 66% που απάντησαν στην έρευνα, αφού είναι γνωστό ότι οι θεωρητικές επιστήμες «τραβούν» περισσότερο το ενδιαφέρον των γυναικών).

[1187] Το ποσοστό είναι αντίστοιχο με το 83% των νομικών που συμμετείχαν στο δείγμα και ήταν μεταξύ 21 και 40 ετών, όπως αναφέρθηκε ανωτέρω.

Επίπεδο Σπουδών



Απόφοιτος δημοτικού	**0**	0%
Απόφοιτος γυμνασίου	**0**	0%
Απόφοιτος δευτεροβάθμιας εκπαίδευσης (λύκειο κ.ά.)	**18**	17%
Απόφοιτος ΑΕΙ - ΑΤΕΙ	**52**	50%
Κάτοχος μεταπτυχιακού διπλώματος	**29**	28%
Κάτοχος διδακτορικού διπλώματος	**5**	5%

Σε αντίθεση με το δείγμα των νομικών στο οποίο ακριβώς οι μισοί απαντώντες (79) έχουν λάβει μεταπτυχιακό δίπλωμα ειδίκευσης, εν προκειμένω ακριβώς οι μισοί (52) είναι απόφοιτοι ΑΕΙ ή ΑΤΕΙ και μεταπτυχιακό δίπλωμα ειδίκευσης έχουν λάβει 29 (ποσοστό 28%). Διδακτορικό δίπλωμα έχουν λάβει 5 εξ αυτών που απάντησαν (ποσοστό 5%). Τέλος, οι υπόλοιποι 18 (17%) είναι απόφοιτοι δευτεροβάθμιας εκπαίδευσης και προφανώς ασχολούνται με την ασφάλεια ηλεκτρονικών δεδομένων έχοντας μάλλον λάβει κάποια ειδίκευση στο πλαίσιο επαγγελματικού λυκείου, ΙΕΚ κ.ά. Μεταξύ των επιλογών είχαν τεθεί και απαντήσεις οι οποίες δεν θα ήταν δυνατόν να ανταποκρίνονται σε κάποιον επιστήμονα πληροφορικής (π.χ. «απόφοιτος δημοτικού»), ωστόσο δίνουν το πλήρες πλέγμα των δημογραφικών ακαδημαϊκών επιλογών.

<u>Ερώτηση 1:</u> Τι είναι hacking σύμφωνα με την εμπειρία σας;

(ανοικτού τύπου ερώτηση)

Οι απαντήσεις των επιστημόνων πληροφορικής[1188] είναι στη διατύπωσή τους πληρέστερες από αυτές των νομικών αλλά και πάλι, σε γενικές γραμμές, το hacking περιγράφεται ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, ιδίως με εκμετάλλευση κενών ασφαλείας[1189].

Ωστόσο, είναι γεγονός ότι αρκετοί διαχειριστές ηλεκτρονικών δεδομένων αποδίδουν στους hackers και πράξεις πέραν της χωρίς δικαίωμα πρόσβασης όπως η υποκλοπή δεδομένων[1190] ή η αλλοίωση, τροποποίηση ή καταστροφή τους[1191]. Στον αντίποδα, υπάρχουν αρκετές περισσότερες απαντήσεις οι οποίες δίνουν στο hacking την έννοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα χωρίς περαιτέρω αναφορές σαν τις ανωτέρω αλλά, αντίθετα, ανιχνεύονται σε απαντήσεις ως κίνητρα η ενασχόληση ελεύθερου χρόνου (hobby) και ο πειραματισμός[1192], η διόρθωση λαθών[1193] και η βελτιστοποίηση των ηλεκτρονικών συστημάτων[1194]. Εντύπωση δημιουργούν απαντήσεις οι οποίες αποδίδουν στους hackers οικονομικά κίνητρα ανακαλύπτοντας κενά ασφαλείας[1195] καθώς και απαντήσεις οι οποίες επί της ουσίας αφήνουν στον νομοθέτη (ή στο περί δικαίου αίσθημα) τον ορισμό του hacking επικαλούμενες πρόσβαση «με μη νόμιμο τρόπο»[1196]. Τέλος, και στις απαντήσεις των επιστημόνων πληροφορικής διαπιστώνεται (όπως και σε αυτές των νομικών) σχετική

[1188] Οι αριθμοί των ερωτηματολογίων που παρουσιάζονται εν προκειμένω είναι όπως έχουν τεθεί στο Παράρτημα ΙΙ της παρούσας (βλ. και ανωτέρω), το οποίο αφορά στα ερωτηματολόγια των επιστημόνων πληροφορικής.

[1189] Βλ. ερωτηματολόγια υπ' αρ. 7, 34, 35, 47, 48, 60, 67, 75, 97, 101.

[1190] Στα ερωτηματολόγια υπ' αρ. 16, 24, 43, 53, 54, 59, 70, 71, 72,80, 82, 83, 84, 86, 90, 92.

[1191] Στα ερωτηματολόγια υπ' αρ. 38, 42, 53, 54, 56, 73, 80, 82, 84, 99, 104.

[1192] Βλ. ενδεικτικά ερωτηματολόγιο υπ' αρ. 6.

[1193] Ερωτηματολόγιο υπ' αρ. 13.

[1194] Ερωτηματολόγιο υπ' αρ. 36.

[1195] Ενδεικτικά ερωτηματολόγιο υπ' αρ. 21.

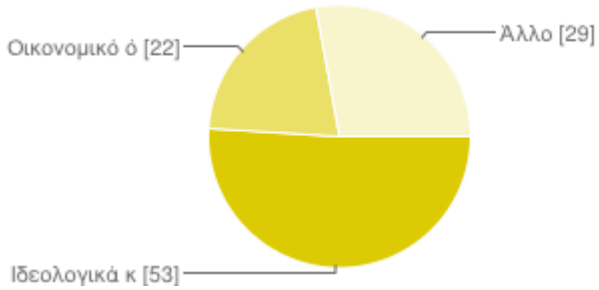
[1196] Ερωτηματολόγια υπ' αρ. 1, 25, 33.

αναφορά στον όρο «προσωπικά δεδομένα»[1197] (βλ. και σχετική προσέγγιση στις απαντήσεις της ερώτησης 1 του ερωτηματολογίου των νομικών).

Άξιες μνείας είναι και οι απαντήσεις στις οποίες ως hacking περιγράφεται η *παραβίαση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων (data) και των πληροφοριών (information*[1198]*)*, σύμφωνα και με την ανάλυση της έννοιας της ασφάλειας στο διαδίκτυο[1199]. Επίσης, διατυπώνεται η άποψη ότι στο hacking δεν περιλαμβάνονται τρόποι «κοινωνικής εξαπάτησης» (π.χ. "social engineering")[1200]. Τέλος, σε μόλις μία απάντηση ανιχνεύεται η προσέγγιση του hacking ως «εξαπάτηση μέσω Η/Υ», σε συνδυασμό με την υποκλοπή και παρακολούθηση προσωπικών δεδομένων[1201]. Κλείνοντας, σε δύο από τα ερωτηματολόγια δεν έχει δοθεί απάντηση στη συγκεκριμένη ερώτηση[1202].

<u>Ερώτηση 2:</u> Πιστεύετε ότι οι hackers ενεργούν με βάση ιδεολογικά κίνητρα ή με σκοπό το οικονομικό όφελος;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



[1197] Ερωτηματολόγια υπ' αρ. 2, 3, 24, 38, 77, 90.

[1198] Ερωτηματολόγιο υπ' αρ. 20.

[1199] … όπως αυτή λαμβάνει χώρα ανωτέρω στην σχετική ανάλυση για το προστατευόμενο έννομο αγαθό (παράγραφος 5.1.2) και σύμφωνα με την τεχνική έννοια της ασφάλειας στα συστήματα πληροφοριών (παράγραφος 1.3.2).

[1200] … όπως αναλύονται ανωτέρω.

[1201] Ερωτηματολόγιο υπ' αρ. 24.

[1202] Ερωτηματολόγια υπ' αρ. 4 και 29.

Ιδεολογικά κίνητρα	**53**	51%
Οικονομικό όφελος	**22**	21%
Άλλο	**29**	28%

Και σε αυτήν την περίπτωση οι απαντήσεις των επιστημόνων πληροφορικής έρχονται σε μερική έστω αντίθεση με τις απαντήσεις των νομικών, καθώς το 51% υποστηρίζει ότι οι hackers δρουν περισσότερο με ιδεολογικά κίνητρα (ενώ στους νομικούς αυτό υποστηρίζεται από το 35% του δείγματος, όπως καταδείχθηκε ανωτέρω). Αρκετά λιγότεροι, δε, ήτοι ποσοστό 21%, σε σχέση με τους νομικούς, υποστηρίζουν ότι οι hackers δρουν περισσότερο με κίνητρο το οικονομικό όφελος.

Από την επιλογή «Άλλο», η οποία έλαβε 29 απαντήσεις (28%), στις 21 εξ αυτών (ποσοστό 20,19% - αντίστοιχο με το 22,78% των νομικών) αναφέρεται «Και τα δύο» (δηλαδή ότι οι hackers ενεργούν και με βάση ιδεολογικά κίνητρα αλλά και με σκοπό το οικονομικό όφελος), παρά το ότι η ερώτηση περιλαμβάνει τη λέξη «περισσότερο» αναφορικά με τα ιδεολογικά ή οικονομικά κίνητρα των hackers. Προκύπτει, επομένως, ότι αρκετοί από όσους απάντησαν δεν κάνουν διάκριση ανάμεσα σε ιδεολογία και οικονομικό όφελος. Σε κάποιες από τις εν λόγω απαντήσεις προστίθεται ως κίνητρο και η πρόκληση[1203], η ευχαρίστηση από αυτή τους τη δράση[1204], η επίδειξη των δυνατοτήτων τους[1205] και η ανάδειξη κενών ασφαλείας[1206].

Τέλος, από τις λοιπές απαντήσεις[1207] εντύπωση προκαλεί η διατύπωση «επειδή μπορούν» (!) [1208] (κάνοντας σαφή την «απουσία κατάλληλου φύλακα» έτσι όπως

[1203] Ερωτηματολόγιο υπ' αρ. 11 καθώς και ερωτηματολόγιο υπ' αρ. 5 όπου η απάντηση αναφέρεται μόνο στην πρόκληση.

[1204] Ερωτηματολόγια υπ' αρ. 54 (όπου χαρακτηριστικά η απάντηση αναφέρει: «*και τα δύο, αλλά κυρίως προσωπική ευχαρίστηση. Το hacking απαιτεί πολύ χρόνο για κατανόηση και διάβασμα οπότε είναι σαν επιβράβευση του hacker.*») και 63.

[1205] Ερωτηματολόγιο υπ' αρ. 63 αλλά και 65 [όπως αυτό αναφέρεται κατωτέρω αφού δεν περιλαμβάνει ως απάντηση το ότι «*και τα 2*» (οικονομικό όφελος και ιδεολογία) αποτελούν εξίσου κίνητρο των hackers].

[1206] Ερωτηματολόγιο υπ' αρ. 31.

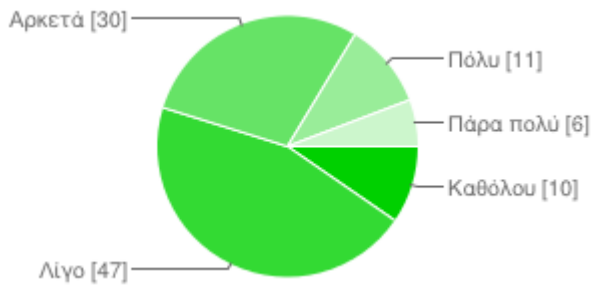
[1207] Απαντήσεις με μικρή επιρροή στη διαμόρφωση απόψεων διατυπώνονται στα ερωτηματολόγια υπ' αρ. 9 («*προσωπικοί λόγοι*»), 58 («*ανάλογα*»).

[1208] Ερωτηματολόγια υπ' αρ. 17 και 65. Χαρακτηριστικά στο ερωτηματολόγιο υπ' αρ. 17 εξειδικεύεται και το ότι «*είναι σίγουροι ότι δεν θα τους πιάσουν*».

περιγράφεται από την θεωρία καθημερινής δραστηριότητας – "routine activity theory"). Επίσης, σε μία απάντηση διευκρινίζεται ότι τα κίνητρα ήταν παλαιότερα ιδεολογικά αλλά σήμερα είναι οικονομικά[1209] (προφανώς ο απαντών έχει στον νου του τη μετάλλαξη του hacking μέσα στις τέσσερις γενιές των hackers[1210]) ενώ σε άλλες δύο απαντήσεις προκρίνονται με περιφραστική διατύπωση τα ιδεολογικά κίνητρα[1211].

<u>Ερώτηση 3:</u> Θεωρείτε ότι οι έλληνες επιστήμονες πληροφορικής είναι επαρκώς ενημερωμένοι σε σύγχρονα θέματα ασφάλειας των ηλεκτρονικών δεδομένων;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου	**10**	10%
Λίγο	**47**	45%
Αρκετά	**30**	29%
Πόλυ	**11**	11%
Πάρα πολύ	**6**	6%

[1209] Ερωτηματολόγιο υπ' αρ. 16

[1210] Βλ. ανωτέρω παράγραφο 2.4.

[1211] Ερωτηματολόγια υπ' αρ. 75 και 103.

Οι ίδιοι οι επιστήμονες πληροφορικής αναγνωρίζουν ότι είναι «Λίγο» ενημερωμένοι για τα σύγχρονα ζητήματα ασφάλειας των ηλεκτρονικών δεδομένων (45%) – αν σε αυτό το ποσοστό προστεθεί και το 10%, το οποίο απαντά ότι οι έλληνες επιστήμονες πληροφορικής δεν είναι καθόλου ενημερωμένοι σχετικώς, προκύπτει ότι το 55% έχει μια αρνητική εικόνα για τη γνώση των ελλήνων επιστημόνων πληροφορικής σε σύγχρονους τρόπους ενίσχυσης της ασφάλειας των ηλεκτρονικών δεδομένων. Οι απαντήσεις είναι αντίστοιχες με αυτές των νομικών – ωστόσο, στην προκειμένη περίπτωση η ανεπαρκής αυτή ενημέρωση δυστυχώς δεν δημιουργεί αισιοδοξία για την εύρεση και εφαρμογή αρκετών εναλλακτικών (και κυρίως εξωδικαιικών) τρόπων θωράκισης των ηλεκτρονικών πληροφοριών.

<u>Ερώτηση 4:</u> Πιστεύετε ότι οι δράσεις των hackers μπορούν να έχουν θετική συμβολή στην κοινωνία; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Μετά από αναλυτική προσέγγιση του περιεχομένου των απαντήσεων, διαπιστώνεται ότι από το δείγμα των 104 απαντήσεων σε 84 (ποσοστό 80,76%) από αυτές υποστηρίζεται ότι οι hackers μπορούν να έχουν συμβολή στην κοινωνία ενώ 16 ερωτώμενοι (ποσοστό 15,38%)[1212] πιστεύουν ότι οι hackers δεν μπορούν να έχουν θετική συμβολή στην κοινωνία. Στις υπόλοιπες 4 απαντήσεις, οι 3 εξ αυτών έχουν αφεθεί κενές[1213] ενώ σε μία απάντηση ο ερωτώμενος απάντησε «Δεν γνωρίζω»[1214].

Η πλειοψηφία των απόψεων που υποστηρίζουν ότι οι hackers μπορούν να έχουν θετική συμβολή στην κοινωνία (λαμβανομένης υπόψιν και σε αυτήν την περίπτωση της διασποράς των απαντήσεων) ομαδοποιείται στις εξής επιλογές:

[1212] Στα ερωτηματολόγια υπ' αρ. 3, 10, 27, 33, 37, 44, 48, 53, 79, 84, 85, 88, 92, 99, 101, 102. Στις απαντήσεις στα ερωτηματολόγια με αριθμό 37 και 102 προτάσσεται το γεγονός ότι η δράση του είναι παράνομη ενώ στο ερωτηματολόγιο υπ' αρ. 92 ότι «*η συμπεριφορά τους είναι εκτός ορίων*».

[1213] Τα ερωτηματολόγια υπ' αρ. 4, 29 και 34.

[1214] Στο ερωτηματολόγιο υπ' αρ. 74.

α) σε 10 απαντήσεις[1215] (ποσοστό 9,61 % από το γενικό σύνολο και 11,90% από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers (και συνεπώς οι αποκτώντες χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα) μπορούν να έχουν θετική συμβολή σε περιπτώσεις πρόληψης και καταστολής εγκληματικών πράξεων[1216] (με αρκετές απαντήσεις να δίνουν ιδιαίτερο βάρος σε υποθέσεις παιδικής πορνογραφίας και ηλεκτρονικών εγκλημάτων)

β) σε 30 απαντήσεις[1217] (ποσοστό 28,85% από το γενικό σύνολο και 35,71% από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers μπορούν να συμβάλλουν εντοπίζοντας τα κενά ασφαλείας συστημάτων και προωθώντας γενικότερα την ασφάλεια των προγραμμάτων ηλεκτρονικών υπολογιστών και των υπολογιστικών δικτύων

γ) σε 17 απαντήσεις[1218] (ποσοστό 16,35% από το γενικό σύνολο και 20,24% από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται η άποψη ότι οι hackers, μέσω της απόκτησης πρόσβασης ακόμη και χωρίς δικαίωμα σε δεδομένα, συμβάλλουν στη σφαιρική ενημέρωση των πολιτών και στην ανάπτυξη της διαφάνειας στη δημόσια ζωή αποκαλύπτοντας σκάνδαλα και πληροφορίες, οι οποίες σκοπίμως αποκρύβονται από τους εκάστοτε κρατούντες, και ότι με αυτόν τον τρόπο ενισχύουν την δημοκρατία[1219].

δ) σε 13 απαντήσεις[1220] (ποσοστό 12,5% από το γενικό σύνολο και 15,48% από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή) εντοπίζεται ως κεντρική ιδέα η ακτιβιστική δράση και η συμβολή των hackers σε ιδεολογικούς σκοπούς για την αφύπνιση των πολιτών (με ιδιαίτερο βάρος π.χ. στη δράση των "Anonymous", στους οποίους αναφέρονται συγκεκριμένα 4 απαντήσεις[1221]). Στην προκειμένη ομαδοποίηση άξιες αναφοράς είναι οι 4

[1215] Στα ερωτηματολόγια υπ' αρ. 2, 12, 49, 51, 54, 56, 64, 68, 75 και 104.

[1216] Η άποψη αυτή έχει άμεση σχέση με τη γενικότερη χρήση της τεχνολογίας για την εξιχνίαση εγκληματικών πράξεων [πρβλ. σχετικώς και ενδεικτικώς *Martin Innes, Nigel Fielding & Nina Cope*, The appliance of Science? The Theory and Practice of Crime Intelligence Analysis, British Journal of Criminology (2005) 45, 39–57].

[1217] Στα ερωτηματολόγια υπ' αρ. 1, 5, 7, 8, 9, 12, 16, 22, 25, 26, 31, 32, 36, 38, 43, 45, 50, 51, 57, 58, 61, 67, 71, 72, 73, 90, 91, 93, 95, 98.

[1218] Στα ερωτηματολόγια υπ' αρ. 6, 14, 17, 20, 30, 35, 36, 40, 56, 63, 69, 75, 76, 78, 83, 86, 91.

[1219] Έτσι στο ερωτηματολόγιο υπ' αρ. 40.

[1220] Στα ερωτηματολόγια υπ' αρ. 18, 39, 41, 47, 60, 65, 70, 80, 82, 89, 91, 94, 98.

[1221] Στα ερωτηματολόγια 18, 41, 47, 65.

απαντήσεις[1222] οι οποίες κάνουν ειδική μνεία στην περίπτωση κατά την οποία η ακτιβιστική δράση των hackers συνδράμει στην προάσπιση των ανθρωπίνων δικαιωμάτων.

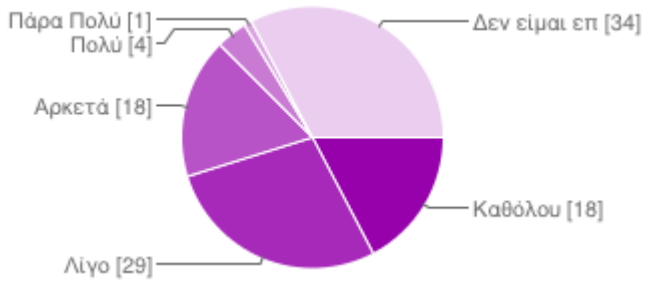
Η ως άνω ομαδοποίηση των απαντήσεων είναι ακριβώς η ίδια με αυτήν που πραγματοποιήθηκε στην ανάλυση της οικείας ερώτησης στο δείγμα των νομικών, γεγονός το οποίο καταδεικνύει ότι υπάρχει σχετική ομογνωμία αναφορικά με τον θετικό αντίκτυπο που μπορούν να έχουν οι δράσεις των hackers. Το εύρημα αυτό γίνται πιο σημαντικό αν ληφθεί υπόψιν ότι πρόκειται για ερώτηση ανοικτού τύπου στην οποία οι απαντήσεις μπορούν να θεωρηθούν τουλάχιστον απρόβλεπτες. Υπάρχουν και περαιτέρω απαντήσεις κοινές με αυτές των νομικών όπως οι 2 απαντήσεις των επιστημόνων πληροφορικής που αναφέρονται στη δυνατότητα των hackers να διαγράψουν χρέη ιδιωτών σε πιστωτικά ιδρύματα[1223] (1 αντίστοιχη απάντηση στο δείγμα νομικών[1224]). Επιπρόσθετα, το δείγμα των επιστημόνων πληροφορικής αναφέρεται, επίσης, σε 4 απαντήσεις[1225] στη συμβολή των hackers στην εξέλιξη της επιστήμης (ποσοστό 3,84% στο γενικό σύνολο και 4,76% από το σύνολο όσων πιστεύουν ότι οι hackers μπορούν να έχουν θετική συμβολή), σε 2 απαντήσεις στο ότι μας εφιστούν την προσοχή στο ποια δεδομένα εισάγουμε στο διαδίκτυο[1226], σε 2 απαντήσεις στο ότι καταπολεμούν την αθέμιτη χρήση προσωπικών πληροφοριών από εταιρείες (π.χ. για διαφημιστικούς λόγους)[1227], σε 1 απάντηση στο ότι με τη δράση τους συμβάλλουν στη μείωση τιμών π.χ. καλλιτεχνικών έργων[1228] και μόλις 1 απάντηση στο ότι συμβάλλουν στην ελευθερία της πληροφορίας[1229].

Από τη συνολική προσέγγιση των απαντήσεων σύμφωνα με τις οποίες δύναται να υπάρχει κάποιου είδους θετική συμβολή του hacking, διαπιστώνεται ότι αυτές δεν διατυπώνονται με επιφύλαξη αναφορικά με την κατάχρηση της χωρίς δικαίωμα πρόσβασης σε δεδομένα, σε αντίθεση με τις απαντήσεις των νομικών στην αντίστοιχη ερώτηση.

[1222] Στα ερωτηματολόγια υπ' αρ. 80, 91, 94, 98.
[1223] Στα ερωτηματολόγια υπ' αρ. 19 και 52.
[1224] Στο ερωτηματολόγιο υπ' αρ. 26 του Παραρτήματος Ι αναφορικά στο δείγμα των νομικών.
[1225] Στα ερωτηματολόγια υπ' αρ. 23, 28, 35 και 100.
[1226] Στα ερωτηματολόγια υπ' αρ. 13 και 59.
[1227] Στα ερωτηματολόγια υπ' αρ. 21 και 66.
[1228] Στο ερωτηματολόγιο υπ' αρ. 42.
[1229] Στο ερωτηματολόγιο υπ' αρ. 15.

<u>Ερώτηση 5:</u> Κατά τη γνώμη σας, η ελληνική νομοθεσία είναι αποτελεσματική για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου	**18**	17%
Λίγο	**29**	28%
Αρκετά	**18**	17%
Πολύ	**4**	4%
Πάρα Πολύ	**1**	1%
Δεν είμαι επαρκώς ενημερωμένος για τις νομικές προβλέψεις	**34**	33%

Η πλειονότητα των ερωτώμενων επιστημόνων πληροφορικής (33%) δηλώνει ότι δεν είναι επαρκώς ενημερωμένοι για τις νομικές προβλέψεις, αποτέλεσμα το οποίο είναι αναμενόμενο λόγω της μη ειδικής γνώσης τους. Μπορεί, επίσης, να υποστηριχθεί πως το αποτέλεσμα αυτό καταδεικνύει ότι οι ερωτώμενοι αντιμετώπισαν σοβαρά την έρευνα και δεν έδωσαν πρόχειρες απαντήσεις σε πεδίο το οποίο θεωρούν ότι δεν γνωρίζουν. Περαιτέρω, το 28% αυτών θεωρεί ότι η ελληνική νομοθεσία είναι ***λίγο*** αποτελεσματική σε επίπεδο διαφύλαξης της ασφάλειας των ηλεκτρονικών δεδομένων ενώ το 17% αυτών εκτιμά ότι η σχετική αποτελεσματικότητα της ελληνικής

νομοθεσίας είναι μηδενική. Αν προστεθούν αυτά τα δύο ποσοστά διαπιστώνεται ότι το 45% των επιστημόνων πληροφορικής θεωρεί ουσιαστικά ανεπαρκείς τις διατάξεις του ελληνικού δικαίου για την ασφάλεια των ηλεκτρονικών δεδομένων.

Από την άλλη, το 17% των ερωτώμενων επιστημόνων πληροφορικής πιστεύει σε μία αρκετά αποτελεσματική προληπτική λειτουργία των ελληνικών ποινικών κυρώσεων που προβλέπονται για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων (άρα και του hacking) ενώ πολύ ή πάρα πολύ ευχαριστημένοι από την αποτελεσματικότητα της ελληνικής νομοθεσίας για την ασφάλεια των ηλεκτρονικών δεδομένων είναι συνολικά μόλις το 5%.

<u>Ερώτηση 6:</u> Πρέπει να είναι ελεύθερη η πρόσβαση στην πληροφορία στο διαδίκτυο; Αν ναι, σε ποιες περιπτώσεις;

(ανοικτού τύπου ερώτηση)

Η ερώτηση αυτή αντιστοιχεί στην ερώτηση υπ' αρ. 6 του ερωτηματολογίου το οποίο απαντήθηκε από τους νομικούς, ως ανωτέρω. Προβαίνοντας σε ανάλυση περιεχομένου των απαντήσεων, διαπιστώνεται ότι από το δείγμα των 104 απαντήσεων σε 87 από αυτές (ποσοστό 83,65%) υποστηρίζεται ότι πρέπει η πρόσβαση στην ηλεκτρονική πληροφορία να είναι ελεύθερη, με προϋποθέσεις/ περιορισμούς ή χωρίς. Από αυτές τις 87 απαντήσεις, στις 30 από αυτές (ποσοστό 34,48% από τις θετικές απαντήσεις και 28,85% από το σύνολο) υποστηρίζεται η ελεύθερη πρόσβαση στην πληροφορία στο διαδίκτυο χωρίς απολύτως καμία προϋπόθεση και περιορισμό[1230]. Επιπρόσθετα, στις απαντήσεις στις οποίες υποστηρίζεται η ελεύθερη πρόσβαση στο διαδίκτυο υπό προϋποθέσεις, ο περιορισμός που τίθεται στις περισσότερες απαντήσεις είναι η προστασία των προσωπικών

[1230] Στα ερωτηματολόγια υπ' αρ. 2, 5, 7, 9, 10, 13, 18, 21 (με ιδιαίτερο βάρος στην ελευθερία της έκφρασης), 23, 24 (ιδιαίτερα για πληροφορίες πολιτικού χαρακτήρα), 27, 30, 36 (όπως αναφέρει: «*...Το διαδικτυο, ιδιαιτερα τα τελευταια χρονια, ειναι ο μονος τροπος αντιμετωπισης της κατευθυνομενης ενημερωσης αλλων μεσων.*»), 38, 39 (καθώς υποστηρίζεται ότι αυτή είναι η λογική του διαδικτύου), 40, 41, 47 (ιδίως για εκπαιδευτικού χαρακτήρα πληροφορίες), 53, 57, 62, 63, 65, 75, 79, 81, 82, 89, 98, 103.

δεδομένων (προκρίνεται ως προϋπόθεση σε 19 απαντήσεις[1231] – ποσοστό 21,84% από τις θετικές απαντήσεις και 18,27% στο σύνολο των απαντήσεων). Επιπρόσθετα, ιδιαίτερο βάρος δίνεται σε ορισμένες απαντήσεις αναφορικά με τον περιορισμό της ελεύθερης πρόσβασης στην ηλεκτρονική πληροφορία με σκοπό την προστασία των ανηλίκων (5 απαντήσεις[1232] – ποσοστό 5,74% από τις θετικές απαντήσεις και 4,81% από το σύνολο). Τέλος, σε ορισμένες απαντήσεις προκρίνεται η ελευθερία στην πρόσβαση στην ηλεκτρονική πληροφορία για ερευνητικές και εκπαιδευτικές δραστηριότητες (9 απαντήσεις[1233] – ποσοστό 10,34% από τις θετικές απαντήσεις και 8,65% από το σύνολο). Μία επιπλέον ομαδοποίηση απαντήσεων εν προκειμένω είναι αυτήν στην οποία η άποψη η οποία εκφράζεται έχει να κάνει με το ότι η πληροφορία πρέπει να είναι ελεύθερη στην περίπτωση κατά την οποία ο κάτοχός της, ο δημιουργός της ή ο χρήστης της το έχει επιλέξει (7 απαντήσεις[1234] - ποσοστό 8,05% από τις θετικές απαντήσεις και 6,73% από το σύνολο).

Οι ομαδοποιήσεις της ανωτέρω παραγράφου είναι αντίστοιχες με αυτές στην οικεία απάντηση των νομικών, ως ανωτέρω. Πέραν, όμως, αυτών, εντοπίζονται επιπρόσθετα απαντήσεις, οι οποίες υποστηρίζουν την ελεύθερη πρόσβαση στην πληροφορία, με τον περιορισμό, ωστόσο, της προστασίας των πνευματικών δικαιωμάτων (4 απαντήσεις[1235] – ποσοστό 4,60% από τις θετικές απαντήσεις και 3,85% από το σύνολο), απαντήσεις οι οποίες αποδέχονται την ελεύθερη πρόσβαση στην πληροφορία εκτός από περιπτώσεις εγκλημάτων (π.χ. παιδική πορνογραφία) (5 απαντήσεις[1236] – ποσοστό 5,75% από τις θετικές απαντήσεις και 4,81% από το σύνολο) καθώς και 5 απαντήσεις[1237] (ποσοστό 5,75% από τις θετικές απαντήσεις και 4,81% από το σύνολο) οι οποίες θέτουν ως περιορισμό την προστασία των (οικονομικών κυρίως) δικαιωμάτων και συμφερόντων (π.χ. η μη πρόκληση οικονομικής ζημίας). Τέλος, αναφορικά με τις απαντήσεις στις οποίες υποστηρίζεται η ελευθερία της πληροφορίας, εντοπίζονται 2 εξ αυτών[1238] οι οποίες δίνουν βάρος και

[1231] Στα ερωτηματολόγια υπ' αρ. 2, 3, 10, 11, 21, 22, 27, 28, 35, 38, 44, 45, 57, 61, 64, 65, 67, 71, 72, 74, 77, 78, 80, 84, 91, 94, 97, 103, 106, 114, 117, 120, 122, 124, 126, 135, 136, 138, 141, 145, 155 και 158.

[1232] Στα ερωτηματολόγια υπ' αρ. 25, 32, 33, 70, 78.

[1233] Στα ερωτηματολόγια υπ' αρ. 14, 34, 60, 74, 85, 86, 90, 100, 104.

[1234] Στα ερωτηματολόγια υπ' αρ. 29, 46, 51, 54, 58, 69 και 88.

[1235] Στα ερωτηματολόγια υπ' αρ. 1, 3, 54 και 72.

[1236] Στα ερωτηματολόγια υπ' αρ. 15, 16, 52, 91 και 99.

[1237] Στα ερωτηματολόγια υπ' αρ. 22, 68, 70, 94 και 97.

[1238] Στα ερωτηματολόγια 8 και 12.

υποστηρίζουν την ελευθερία με σκοπό τη διαφάνεια και την ενημέρωση των πολιτών και άλλες 2 εξ αυτών[1239] οι οποίες υποστηρίζουν την ελευθερία σε περιπτώσεις που το επιτρέπει ο νόμος – σε αυτό το πνεύμα και η διφορούμενη απάντηση, η οποία υποστηρίζει την ελευθερία της πληροφορίας αλλά παράλληλα προκρίνει καλύτερο έλεγχο από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος[1240].

Εντελώς αρνητικές αναφορικά με την ελεύθερη πρόσβαση στην πληροφορία καταγράφονται 8 απαντήσεις[1241] (7,69%) από τις οποίες ιδιαίτερο ενδιαφέρον παρουσιάζουν η απάντηση η οποία αναφέρεται στον οικονομικό αντίκτυπο που έχει η πληροφορία[1242] και ιδίως η απάντηση στην οποία γίνεται αναφορά στη διάσταση αναφορικά με το ότι η πληροφορία δεν πρέπει να είναι ελεύθερη διότι μπορεί να θίγονται τα πνευματικά δικαιώματα των προγραμματιστών και των δημιουργών ηλεκτρονικών προγραμμάτων[1243].

Επιπρόσθετα, υπάρχουν 5 απαντήσεις (ποσοστό 4,81%), οι οποίες ουσιαστικά δεν λαμβάνουν θέση υπέρ ή κατά της ελευθερίας της πρόσβασης και στις περισσότερες από αυτές αναφέρεται ότι εξαρτάται από την πληροφορία και τον σκοπό της πρόσβασης[1244]. Υπάρχει, επιπρόσθετα, ένα ακόμη ερωτηματολόγιο στο οποίο αναφέρεται ότι η πρόσβαση πρέπει να είναι ελεύθερη ως έχει σήμερα (δηλαδή ούτε περισσότερο, ούτε λιγότερο)[1245].

Τέλος, τρία ερωτηματολόγια έχουν αφεθεί κενά χωρίς καμία απάντηση[1246].

<u>Ερώτηση 7:</u> Έχετε να προτείνετε άλλα μέτρα – πέρα από ποινικές διατάξεις – που μπορούν να ληφθούν για την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων; Αν ναι, ποια;

(ανοικτού τύπου ερώτηση)

[1239] Στα ερωτηματολόγια υπ' αρ. 54 και 101.

[1240] Στο ερωτηματολόγιο υπ' αρ. 44.

[1241] Στα ερωτηματολόγια υπ' αρ. 11, 59, 61, 67, 84, 92, 96, 102.

[1242] Στο ερωτηματολόγιο υπ' αρ. 67.

[1243] Στο ερωτηματολόγιο υπ' αρ. 96.

[1244] Στα ερωτηματολόγια υπ' αρ. 31, 48, 55, 71 (όπου αναφέρεται το παράδειγμα των στοιχείων πιστωτικών καρτών) και 73.

[1245] Στο ερωτηματολόγιο υπ' αρ. 49.

[1246] Ερωτηματολόγιο υπ' αρ. 4, 29 και 66.

Οι απαντήσεις που ελήφθησαν από το δείγμα των επιστημόνων πληροφορικής και στην ανωτέρω ερώτηση παρουσιάζουν αρκετά μεγάλη ποικιλομορφία. Και στους επιστήμονες πληροφορικής, όπως και στους νομικούς, η κυρίαρχη πρόταση έχει να κάνει με την πληρέστερη ενημέρωση και εκπαίδευση των χρηστών του διαδικτύου αναφορικά με την προστασία των ηλεκτρονικών τους δεδομένων (37 από τους 104 απαντώντες[1247] - ποσοστό 35,58%). Επιπρόσθετα, προτείνεται η «δημιουργία ηλεκτρονικής κουλτούρας μέσα από τα blog που ο καθένας φτιάχνει ή είναι μέλος»[1248] καθώς και η πρόληψη γενικότερα[1249].

Η θέσπιση αυστηρών τεχνικών προτύπων έχουν, επίσης, σημαντική θέση στις πολυκερματισμένες και διαφορετικές απαντήσεις, με έμφαση στην πιστοποίηση των ιστοσελίδων[1250] (8 απαντήσεις[1251] – ποσοστό 7,69%). Σε τεχνικό επίπεδο, προτείνεται η χρήση προγραμμάτων καταπολέμησης ιών (antivirus) και «πύρινων τειχών» (firewall) (6 απαντήσεις – ποσοστό 5,77%)[1252], η κρυπτογράφηση των δεδομένων (3 απαντήσεις[1253]– ποσοστό 2,88%), το «κλείσιμο» των κενών ασφαλείας (2 απαντήσεις[1254]- ποσοστό 1,92%) και η ελεύθερη διακίνηση ανοιχτού κώδικα[1255] [1256]. Επιπρόσθετα, σε 4 απαντήσεις[1257] (ποσοστό 3,85%) οι απαντώντες προτείνουν την έρευνα και τη συνεχή ανανέωση των ηλεκτρονικών προγραμμάτων στα οποία εντοπίζονται τρωτά σημεία και, συνεπώς, την ενίσχυση της ασφάλειας μέσω των ίδιων των ηλεκτρονικών προγραμμάτων. Στη συνέχεια, οι επιστήμονες πληροφορικής, γνωρίζοντας εκ των έσω και ίσως καλύτερα από όλους το πεδίο, προτείνουν την αύξηση της διάθεσης κεφαλαίων για την ασφάλεια (3 απαντήσεις – ποσοστό 2,88%)[1258] και την πρόσληψη εξειδικευμένου προσωπικού (2 απαντήσεις[1259]

[1247] Στα ερωτηματολόγια υπ' αρ. 3, 5, 7, 8, 11, 15, 16, 17, 20, 24, 36, 37, 40, 41, 45, 46, 48, 50, 51, 53, 55, 57, 58, 62, 65, 68, 78, 79, 80, 82, 83, 87, 92, 93, 94, 102 και 104.

[1248] Στο ερωτηματολόγιο υπ' αρ. 30.

[1249] Στο ερωτηματολόγιο υπ' αρ. 18.

[1250] Όπως στο ερωτηματολόγιο υπ' αρ. 25 στις απαντήσεις των νομικών (Παράρτημα Ι)

[1251] Στα ερωτηματολόγια 2, 13 (πιστοποίηση ασφαλείας), 42 (ασφαλέστερο πρωτόκολλο διακίνησης δεδομένων), 47 (ψηφιακή υδατογράφηση), 60, 67, 69 και 90.

[1252] Στα ερωτηματολόγια υπ' αρ. 16, 39, 59, 68, 70 και 101.

[1253] Στα ερωτηματολόγια υπ' αρ. 21, 32, και 36.

[1254] Στα ερωτηματολόγια υπ' αρ. 14 και 31.

[1255] Στο ερωτηματολόγιο υπ' αρ. 15.

[1256] Βλ. σχετικές αναλύσεις στο κεφάλαιο 9 του παρόντος πονήματος.

[1257] Στα ερωτηματολόγια υπ' αρ. 49, 71, 78 και 85.

[1258] Στα ερωτηματολόγια 19, 52 και 97.

- ποσοστό 1,92%). Χαρακτηριστικές σχετικώς, είναι, επιπλέον, η απάντηση για την απόδοση «αδρών αμοιβών» σε hackers προκειμένου να ανευρίσκουν κενά ασφαλείας[1260] καθώς και η απάντηση η οποία αναφέρεται στην «κοινωνική ενσωμάτωση» των hackers[1261].

Από την άλλη πλευρά, και στις απαντήσεις των επιστημόνων πληροφορικής διατυπώνονται και απόψεις οι οποίες στρέφονται στον μεγαλύτερο έλεγχο του διαδικτύου, διάσπαρτες, όμως, και όχι με την αυστηρή διατύπωση των νομικών, ως ανωτέρω. Συγκεκριμένα, προτείνεται ο μεγαλύτερος έλεγχος του διαδικτύου (2 απαντήσεις[1262] - ποσοστό 1,92%), η εγρήγορση των υπηρεσιών[1263] ή η συγκρότηση ειδικής ομάδας για την προστασία των ηλεκτρονικών δεδομένων (2 απαντήσεις[1264] - ποσοστό 1,92%)[1265] και η διαφάνεια αναφορικά με τις διαδικασίες επεξεργασίας[1266].

Σε νομικό επίπεδο διατυπώνονται οι απόψεις ότι οι ποινικές διατάξεις καλύπτουν την απαίτηση για ασφάλεια των ηλεκτρονικών δεδομένων[1267], ότι μόνο η επιβολή ποινών μπορεί να ενισχύσει την ασφάλεια (4 απαντήσεις[1268] - ποσοστό 3,85%) και ότι είναι απαραίτητη μια νέα νομοθεσία (2 απαντήσεις[1269] - ποσοστό 1,92%). Προτείνεται, επίσης, η θέσπιση υπεύθυνου πολιτικής ασφάλειας για τα ηλεκτρονικά δεδομένα[1270], η υιοθέτηση κώδικα δεοντολογίας στο διαδίκτυο[1271], το κλείδωμα σελίδων[1272], η υποχρεωτική συγκατάθεση για την αποθήκευση και επεξεργασία προσωπικών δεδομένων (2 απαντήσεις[1273] - ποσοστό 1,92%) και ο αποκλεισμός στην πρόσβαση σε υλικό παιδικής πορνογραφίας[1274].

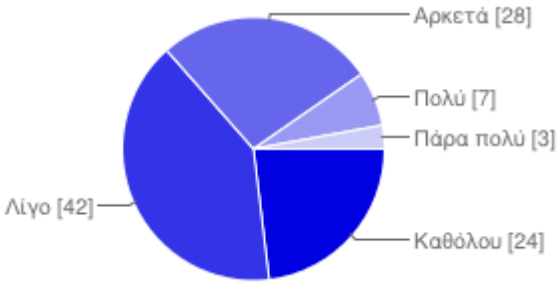
[1259] Στα ερωτηματολόγια υπ' αρ. 1 και 52.
[1260] Βλ. ερωτηματολόγιο υπ' αρ. 91.
[1261] Βλ. ερωτηματολόγιο υπ' αρ. 100.
[1262] Στα ερωτηματολόγια υπ' αρ. 32 και 58.
[1263] Στο ερωτηματολόγιο υπ' αρ. 22.
[1264] Στα ερωτηματολόγια υπ' αρ. 12 και 80.
[1265] ... μάλλον εννοούνται ομάδες τύπου CERT (βλ. παράγραφο 6.3.11.1).
[1266] Ερωτηματολόγιο υπ' αρ. 30.
[1267] Στο ερωτηματολόγιο υπ' αρ. 43.
[1268] Στα ερωτηματολόγια υπ' αρ. 61, 77, 83 και 96.
[1269] Στο ερωτηματολόγιο υπ' αρ. 72 και 75.
[1270] Στο ερωτηματολόγιο υπ' αρ. 38.
[1271] Στο ερωτηματολόγιο υπ' αρ. 9.
[1272] Στο ερωτηματολόγιο υπ' αρ. 44.
[1273] Στα ερωτηματολόγια υπ' αρ. 7 και 35.
[1274] Στο ερωτηματολόγιο υπ' αρ. 33.

Στα υπό επεξεργασία ερωτηματολόγια ανευρίσκονται και απαντήσεις οι οποίες αναφέρονται στην ευθύνη του ίδιου του χρήστη για προσοχή στη χρήση του διαδικτύου (3 απαντήσεις – ποσοστό 2,88%). Τέλος, διατυπώνεται και η άποψη ότι πρέπει στο διαδίκτυο να υπάρχει ελευθερία και δεν χρειάζεται ασφάλεια[1275] καθώς και ότι δεν υπάρχει ασφάλεια[1276].

Οι απαντώντες οι οποίοι δεν είχαν να προτείνουν άλλα μέτρα ανήλθαν στους 9[1277] (ποσοστό 8,65%) και όσοι δεν γνώριζαν ή δεν μπορούσαν να προτείνουν κάτι ανήλθαν σε 11[1278] (ποσοστό 10,58%). Κλείνοντας την επεξεργασία της ερώτησης, κατεγράφησαν 4 κενές απαντήσεις[1279].

<u>Ερώτηση 8:</u> Πόσο ασφαλής νιώθετε αναφορικά με τα ηλεκτρονικά σας δεδομένα στο διαδίκτυο;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου **24** 23%

Λίγο **42** 40%

Αρκετά **28** 27%

[1275] Στο ερωτηματολόγιο υπ' αρ. 89.

[1276] Στο ερωτηματολόγιο υπ' αρ. 103.

[1277] Ερωτηματολόγια υπ' αρ. 10, 23, 27, 54, 64, 84, 86, 88 και 98.

[1278] Στα ερωτηματολόγια υπ' αρ. 11, 32, 46, 56, 67, 70, 72, 81, 85, 95, 96, 101, 111, 112, 119, 120, 125, 127, 130, 137, 147, 148 και 155.

[1279] Στα ερωτηματολόγια υπ' αρ. 4, 29, 34 και 74.

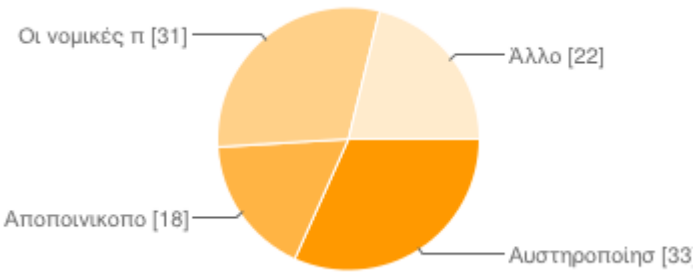
Πολύ **7** 7%

Πάρα πολύ **3** 3%

Αναφορικά με το αίσθημα ασφάλειας των επιστημόνων πληροφορικής σε ό,τι έχει να κάνει με τις ηλεκτρονικές τους πληροφορίες (με δεδομένο, μάλιστα, ότι γνωρίζουν καλύτερα από όλους τους κινδύνους που ελλοχεύουν στο διαδίκτυο), η πλειοψηφία αυτών βιώνει σε μεγάλο βαθμό αίσθημα ανασφάλειας (40% νιώθει λίγο ασφαλής για τις ηλεκτρονικές του πληροφορίες και 23 % δεν νιώθει καμία ασφάλεια – άρα, 63% των ερωτώμενων διάκειται αρνητικά αναφορικά με το αίσθημα ασφάλειας για τις ηλεκτρονικές του πληροφορίες στο διαδίκτυο, ποσοστό μικρότερο πάντως από το αντίστοιχο 80% των νομικών). Από την άλλη, απολύτως θετικό αίσθημα ασφάλειας βιώνει μοναχά το 10% των ερωτώμενων (7% νιώθει πολύ ασφαλής και 3% πάρα πολύ ασφαλής).

<u>Ερώτηση 9:</u> Ποια η γνώμη σας: χρειάζεται αυστηροποίηση των ποινικών κυρώσεων ή αποποινικοποίηση του hacking ή οι νομικές προβλέψεις να μείνουν ως έχουν;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Αυστηροποίηση των ποινικών κυρώσεων **33** 32%

Αποποινικοποίηση του hacking	**18** 17%
Οι νομικές προβλέψεις να μείνουν ως έχουν	**31** 30%
Άλλο	**22** 21%

Στο ερώτημα για αλλαγές στο ισχύον νομικό πλαίσιο η πλειοψηφία των επιστημόνων πληροφορικής δεν παίρνει απολύτως ξεκάθαρη θέση καθώς το 32% διάκειται υπέρ της αυστηροποίησης των ποινικών κυρώσεων και το 30% υπέρ του να μείνουν ως έχουν οι διατάξεις. Στον αντίποδα, σχετικά ισχυρό ποσοστό 17% υποστηρίζει την αποποινικοποίηση του hacking.

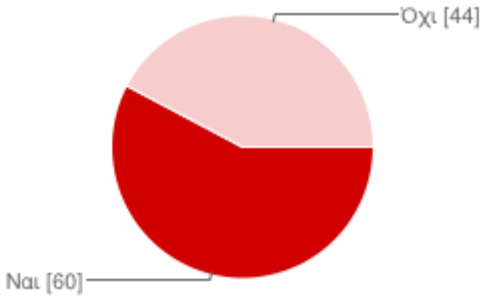
Στη συγκεκριμένη ερώτηση καταγράφεται σε ποσοστό 21% η επιλογή της απάντησης «***Άλλο***». Σε αυτήν την επιλογή υπάρχει για ακόμη μια φορά μεγάλη ποικιλομορφία απαντήσεων η οποία δύσκολα ομαδοποιείται. Κυρίαρχη τάση μπορεί να υποστηριχθεί ότι συνιστά η αντιμετώπιση του hacking ανάλογα με την περίπτωση (3 απαντήσεις[1280]), οι οποίες έχουν κοινή βάση με την απάντηση που αναφέρεται στη διάκριση των περιπτώσεων hacking και προστασία στις περιπτώσεις που στρέφεται κατά ατομικών ή συλλογικών δικαιωμάτων[1281], με την απάντηση που αναφέρεται σε διαβάθμιση και ποινικοποίηση επιθέσεων[1282] και με την απάντηση για τιμώρηση ανάλογα με το κίνητρο του δράστη[1283]. Επιπρόσθετα, διατυπώνεται η άποψη για επιβολή μικρότερων ποινών (2 απαντήσεις[1284]) ενώ στον αντίποδα υποστηρίζεται και η αυστηροποίηση των ποινικών κυρώσεων σε περιπτώσεις βλάβης του κοινωνικού συνόλου ή κλοπής χρημάτων ή δεδομένων[1285]. Ενημέρωση και παιδεία καταγράφονται και εδώ ως απαραίτητες και ως εναλλακτικές προτάσεις σε 3 απαντήσεις[1286] καθώς και η πρόληψη[1287]. Τέλος, διατυπώνονται οι απόψεις ότι πρέπει οι φορείς καταπολέμησης του ηλεκτρονικού εγκλήματος να ενισχυθούν με

[1280] Στα ερωτηματολόγιο υπ' αρ. 9, 14, και 104.
[1281] Στο ερωτηματολόγιο υπ' αρ. 80.
[1282] Στο ερωτηματολόγιο υπ' αρ. 95.
[1283] Στο ερωτηματολόγιο υπ' αρ. 12.
[1284] Στα ερωτηματολόγια υπ' αρ. 49 και 63.
[1285] Στο ερωτηματολόγιο υπ' αρ. 5.
[1286] Στα ερωτηματολόγια υπ' αρ. 1, 47, και 65.
[1287] Στο ερωτηματολόγιο υπ' αρ. 1.

κατάλληλο προσωπικό[1288] ενώ από την άλλη πλευρά υποστηρίζεται ότι οι hackers δεν αποτελούν πραγματικό πρόβλημα και ότι έχουν ετικετοποιηθεί[1289] και ότι πρέπει να «πριμοδοτηθούν»[1290]! Κλείνοντας, σε 4 ερωτηματολόγια του δείγματος εντοπίζεται απάντηση η οποία αναφέρεται στην άγνοια του νομικού πλαισίου εκ μέρους των επιστημόνων πληροφορικής[1291] και σε 3 ερωτηματολόγια απαντήσεις με ουσιαστικό περιεχόμενο «Δεν γνωρίζω»[1292].

<u>Ερώτηση 10:</u> Ως τεχνικός ασφαλείας ή διαχειριστής ηλεκτρονικών δεδομένων, έχετε αντιμετωπίσει περιστατικά hacking;

(κλειστού τύπου ερώτηση)



Ναι **60** 58%

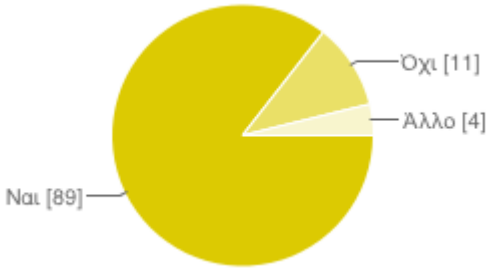
Όχι **44** 42%

Όπως προκύπτει από τις απαντήσεις ένα σημαντικό ποσοστό των επιστημόνων πληροφορικής του δείγματος (58%) έχει αντιμετωπίσει περιστατικά hacking, συνεπώς υπάρχει εκ μέρους του μεγαλύτερου μέρους του δείγματος άμεση επαφή και εμπειρία όχι μόνο με προβλήματα ασφάλειας αλλά και με περιπτώσεις χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και λοιπών δράσεων.

[1288] Στο ερωτηματολόγιο υπ' αρ. 47.
[1289] Στο ερωτηματολόγιο υπ' αρ. 103.
[1290] Στο ερωτηματολόγιο υπ' αρ. 91.
[1291] Στα ερωτηματολόγια υπ' αρ. 31, 42, 46 και 97.
[1292] Στα ερωτηματολόγια υπ' αρ. 28, 56, 66.

<u>Ερώτηση 11:</u> Θα συνεργαζόσασταν ποτέ με έναν hacker προκειμένου να βελτιώσετε μία πρακτική ασφαλείας;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Ναι **89** 86%

Όχι **11** 11%

Άλλο **4** 4%

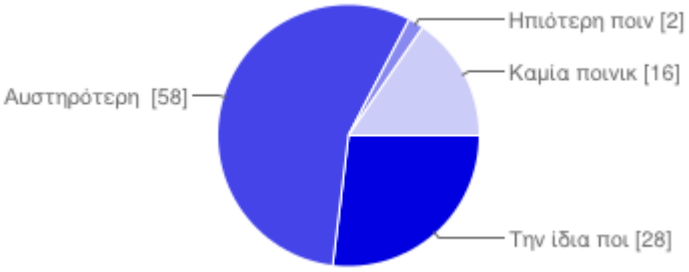
Η συντριπτική πλειοψηφία των επιστημόνων πληροφορικής (86%) θα συνεργαζόταν με κάποιον hacker προκειμένου να ενισχύσει την ασφάλεια των ηλεκτρονικών δεδομένων. Αρνητική στάση σε ένα τέτοιο ενδεχόμενο συνεργασίας λαμβάνει μόλις το 11% των ερωτηθέντων. Στις 4 περιπτώσεις που επέλεξαν την επιλογή «Άλλο» αναφέρονται ως απαντήσεις η θετική στάση αν πρόκειται για νόμιμο σκοπό[1293], η θετική επίσης στάση με επιφύλαξη για το αν θα υπήρχε καλή συνεννόηση μεταξύ τους[1294] αλλά και η απάντηση ότι «δεν χρειάζεται ασφάλεια»[1295] (άρα ο απαντών θεωρεί ότι παρέλκει μάλλον η όποια συνεργασία με hackers) και η απάντηση το ότι είναι ο ίδιος ο ερωτώμενος hacker[1296] (είναι γεγονός ότι κάποιοι hackers είναι

[1293] Στο ερωτηματολόγιο υπ' αρ. 31.
[1294] Στο ερωτηματολόγιο υπ' αρ. 88.
[1295] Στο ερωτηματολόγιο υπ' αρ. 89.
[1296] Στο ερωτηματολόγιο υπ' αρ. 62.

παράλληλα και επιστήμονες πληροφορικής[1297], οι οποίοι είναι υπεύθυνοι για την ασφάλεια δεδομένων).

<u>Ερώτηση 12:</u> Όποιος αποκτά χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα στο διαδίκτυο με σκοπό οικονομικό όφελος ή πρόκληση ζημίας πρέπει να έχει την ίδια, ηπιότερη ή αυστηρότερη ποινική μεταχείριση από τον νόμο σε σχέση με αυτόν που δεν έχει σκοπό το οικονομικό όφελος ή την πρόκληση ζημίας;

(κλειστού τύπου ερώτηση: Την ίδια ποινική μεταχείριση – Αυστηρότερη ποινική μεταχείριση – Ηπιότερη ποινική μεταχείριση – Καμία ποινική μεταχείριση για χωρίς δικαίωμα πρόσβαση ανεξαρτήτως σκοπού ή αποτελέσματος)



Την ίδια ποινική μεταχείριση	**28**	27%
Αυστηρότερη ποινική μεταχείριση	**58**	56%
Ηπιότερη ποινική μεταχείριση	**2**	2%
Καμία ποινική μεταχείριση για χωρίς δικαίωμα πρόσβαση ανεξαρτήτως σκοπού ή αποτελέσματος	**16**	15%

[1297] Βλ. ανωτέρω παράγραφο 7.6.5.2 και ειδικότερα τη συνέντευξη με μέλη του hackerspace.gr.

Το δείγμα των επιστημόνων πληροφορικής φαίνεται να πιστεύει σαφώς ότι ο σκοπός οικονομικού οφέλους ή πρόκλησης ζημίας σε περίπτωση χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα χρήζει αυστηρότερης ποινικής μεταχείρισης, καθώς αυτό υποστηρίζει το 56% των ερωτηθέντων. Το, δε, 27% των ερωτηθέντων πιστεύει ότι το κίνητρο δεν πρέπει να παίζει ρόλο στην ποινική μεταχείριση και, συνεπώς, πρέπει οι «παραβιαστές» να έχουν την ίδια ποινική μεταχείριση ανεξαρτήτως σκοπού. Μόλις 2 από το δείγμα (ποσοστό 2%) υποστήριξαν την ηπιότερη ποινική μεταχείριση σε περίπτωση σκοπού οικονομικού οφέλους ή πρόκλησης ζημίας. Τέλος, το 15% των ερωτηθέντων υποστηρίζει την αποποινικοποίηση της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα.

7.8.2.2 Συνολική θεώρηση απαντήσεων δείγματος επιστημόνων πληροφορικής

Το 45% (28% λίγο και 17% καθόλου) των ερωτηθέντων επιστημόνων πληροφορικής στην ερώτηση 5 που δεν θεωρεί αρκετά αποτελεσματική την ισχύουσα ποινική νομοθεσία για το hacking συμφωνεί με τα στην ερώτηση 9 ποσοστά του 32% των επιστημόνων πληροφορικής που τάσσεται υπέρ της αυστηροποίησης των σχετικών ποινών και του 17% αυτών που επιθυμούν την αποποινικοποίηση του hacking (σύνολο 49%). Επιπρόσθετα, σε κάθε περίπτωση το μεγάλο ποσοστό που υποστηρίζει την αυστηροποίηση των ποινικών διατάξεων ως ανωτέρω δικαιολογείται και εξηγείται από το ότι στην ερώτηση 8 το 23% των επιστημόνων πληροφορικής δηλώνει εντελώς ανασφαλής για τα δεδομένα του στο διαδίκτυο ενώ το ισχυρό 40% δηλώνει ότι αισθάνεται μόλις λίγο ασφαλής για τα ηλεκτρονικά δεδομένα. Ωστόσο, πρέπει να επισημανθεί ότι μόνο το 15,38% όσων απάντησαν πιστεύουν ότι οι hackers δεν μπορούν να έχουν καμία θετική συμβολή στην κοινωνία (ποσοστό σίγουρα μικρότερο από το 32% το οποίο υποστηρίζει την αυστηροποίηση των ποινικών κυρώσεων).

Στην ερώτηση 9 το 17% των ερωτηθέντων επιθυμεί την αποποινικοποίηση του hacking, ποσοστό παρεμφερές και αντίστοιχο με το 15% της ερώτησης 12 που υποστηρίζει ότι δεν πρέπει να υπάρχει καμία ποινή για την απόκτηση χωρίς δικαίωμα πρόσβασης σε δεδομένα (λαμβανομένου, μάλιστα, υπόψιν ότι στην ερώτηση 9

υπήρχε και η επιλογή «Άλλο» για τον ερωτώμενο σε αντίθεση με την ερώτηση 12). Ωστόσο, το 28,85% στην ερώτηση 6 δηλώνει ότι επιθυμεί ελεύθερη την πληροφορία στο διαδίκτυο χωρίς κανέναν περιορισμό (συμπεριλαμβανομένων και ποινικών διατάξεων).

Το 86% των επιστημόνων πληροφορικής, το οποίο αντιπροσωπεύει όσους θα συνεργάζονταν με κάποιον hacker για την ενίσχυση της ηλεκτρονικής ασφάλειας, καταδεικνύει το πόσο σημαντικό ρόλο μπορούν να διαδραματίσουν οι hackers αν ενταχθούν σε μια λογική καινοτομίας και συνεργασίας παράλληλα, με στόχο τελικώς την εμπέδωση του σεβασμού των δικαιωμάτων επί των δεδομένων και των συστημάτων πληροφοριών. Εξάλλου, είναι γνωστό ότι, πέρα από τους ηθικούς hackers, και παλαιότεροι hackers προσλαμβάνονται ως ειδικοί για την ενίσχυση της ασφάλειας ηλεκτρονικών πληροφοριών[1298].

Αναφορικά με την πρώτη υπόθεση έρευνας για τη σύγχρονη έννοια του hacking και της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, σε γενικές γραμμές οι ερωτηθέντες επιστήμονες πληροφορικής περιγράφουν στη διατύπωση το hacking ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα - σε κάποιες περιπτώσεις, ωστόσο, υπάρχει σύγχυση μεταξύ hacking και cracking καθώς και από αυτούς αποδίδονται στον hacker και πράξεις αλλοίωσης των δεδομένων κ.λπ. Και στις απαντήσεις των επιστημόνων πληροφορικής δεν ανευρέθη κάποια πιο μοντέρνα περιγραφή της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα με χαρακτηρισμούς και πράξεις οι οποίοι δεν έχουν καταγραφεί στη βιβλιογραφία[1299].

Σε ό,τι έχει να κάνει με τη δεύτερη υπόθεση έρευνας, οι επιστήμονες πληροφορικής κατά απόλυτη πλειοψηφία υποστηρίζουν ότι κίνητρο των hackers είναι η ιδεολογία τους. Το εύρημα αυτό αποκλείει τις θεωρίες ερμηνείας του hacking οι οποίες στηρίζονται στο οικονομικό όφελος ή ζημία, όπως π.χ. η θεωρία λευκού περιλαιμίου. Αντίστοιχα, οι επιστήμονες πληροφορικής υποστηρίζουν πάλι κατά απόλυτη

[1298] Ο ίδιος ο Κέβιν Μίτνικ (ο πιο γνωστός, ίσως, hacker – βλ. ανωτέρω) έχει φτιάξει δική του εταιρεία ασφαλείας συστημάτων πληροφοριών (βλ. την ιστοσελίδα της εταιρείας αυτής στο url: **http://mitnicksecurity.com/** - Πρβλ. συνέντευξη του Μίτνικ όπως περιλαμβάνεται στο πόνημα του *Ν. Κουράκη*, Εγκληματολογικοί Ορίζοντες, όπ. π., σελ. 201 επ.). Υπάρχουν, επίσης, δημοσιεύματα που αναφέρονται στην πρόσληψη hackers (βλ. ενδεικτικά *Bryan – Low Cassell*, Hackers-for-Hire Are Easy to Find, The Wall Street Journal, January 23, 2012, url: **http://online.wsj.com/news/articles/SB10001424052970203471004577145140543496380**) αλλά κυρίως ιστοσελίδες οι οποίες έχουν ως θέμα την πρόσληψη hackers (url: **http://hackerforhirereview.com/tips-for-hiring-a-hacker/**, **https://neighborhoodhacker.com/** και **http://www.hacker1337.com/**).

[1299] ...όπως αυτή προσεγγίζεται στο δεύτερο κεφάλαιο του παρόντος πονήματος.

πλειοψηφία (56%) την αυστηρότερη ποινική μεταχείριση όσων επιδιώκουν οικονομικό όφελος από την απόκτηση χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, όπως προκύπτει από τις απαντήσεις στην ερώτηση 12, καθώς οι ίδιοι προκρίνουν την ιδεολογία ως κίνητρο.

Οι απόψεις των επιστημόνων πληροφορικής για την αποτελεσματικότητα της νομοθεσίας αποσαφηνίζονται στα ευρήματα της ερώτησης 5 με αποτέλεσμα αρνητικό, όπως διατυπώνεται ο αντίστοιχος προβληματισμός στην οικεία υπόθεση έρευνας, και οι προθέσεις αλλαγής της νομοθεσίας στις ερωτήσεις 9 και 12.

Ως εναλλακτικοί τρόποι προώθησης της ασφάλειας των ηλεκτρονικών δεδομένων διατυπώθηκαν αρκετοί, ιδίως στην ερώτηση 7, με την εκπαίδευση να διαδραματίζει σημαντικό ρόλο στις προτάσεις αυτές (σε ποσοστό 35,58%), με δεδομένο ότι και οι ίδιοι οι επιστήμονες πληροφορικής αναγνωρίζουν ανεπάρκεια του κλάδου τους σε ό,τι αφορά στην ενημέρωσή τους για την ασφάλεια των πληροφοριών (βλ. αποτελέσματα ερώτησης 3), μολονότι το 58% αυτών έχει αντιμετωπίσει περιστατικά hacking. Μια ακόμη ενδιαφέρουσα πρόταση είναι η πιστοποίηση των ιστοσελίδων σε επίπεδο ασφάλειας. Τέλος, επισημαίνεται η ανάγκη για αύξηση στη διάθεση κεφαλαίων στον τομέα της έρευνας για την ασφάλεια των δεδομένων.

7.8.3 Συσχέτιση απαντήσεων νομικών και επιστημόνων πληροφορικής

Όπως ήδη αναφέρθηκε, οι περισσότερες ερωτήσεις στα δείγματα επιστημόνων πληροφορικής και νομικών είναι ίδιες ή παρεμφερείς. Τούτο προκειμένου να μπορέσουν να συσχετισθούν, να συγκριθούν, να καταδειχθούν ομοιότητες και διαφορές και να εξαχθούν χρήσιμα συμπεράσματα με μια προσέγγιση συμπληρωματική των απόψεων των ειδημόνων. Σε μια γενική εκτίμηση, οι επιστήμονες πληροφορικής είναι έως ένα βαθμό πιο επιεικείς με τους hackers (ενδεικτικά: τους αναγνωρίζουν σε μεγαλύτερο ποσοστό από ό,τι οι νομικοί ιδεολογικά κίνητρα, πιστεύουν περισσότερο από τους νομικούς στη δυνατότητα προσφοράς τους και στηρίζουν με μεγαλύτερο ποσοστό απόψεις όπως η αποποινικοποίηση του hacking). Παρακάτω, επομένως, ακολουθεί συσχέτιση μία

προς μία των κοινών πεδίων ή ακόμη και διατύπωσης ερωτήσεων των ως άνω δειγμάτων.

7.8.3.1 Τι είναι hacking σύμφωνα με την εμπειρία σας;

Και τα δύο ως άνω δείγματα περιγράφουν το hacking ως χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα. Περισσότερο οι νομικοί και λιγότερο οι επιστήμονες πληροφορικής αποδίδουν στους hackers και πράξεις οι οποίες καταλαμβάνονται εννοιολογικά από το cracking, όπως ανωτέρω αυτό περιγράφεται (φθορά των δεδομένων κ.λπ.). Ωστόσο, ελάχιστοι είναι οι συμμετέχοντες στην έρευνα και στα δύο δείγματα οι οποίοι αποδίδουν στους hackers πράξεις όπως η μόλυνση με ιούς ή το «μπλοκάρισμα» δεδομένων (π.χ. με DDoS επιθέσεις) παρά το ότι και αυτές οι πρακτικές συνδέονται με το hacking. Περαιτέρω, κοινό χαρακτηριστικό των απαντήσεων είναι προσήλωση στην προστασία των προσωπικών δεδομένων, η οποία, βεβαίως αναπτύσσεται με πολύ μικρότερη συχνότητα στους επιστήμονες πληροφορικής (μόλις σε 6 ερωτηματολόγια – 5,76%) σε σχέση με τις 42 απαντήσεις στα ερωτηματολόγια των νομικών (ποσοστό 26,58%), λόγω ίσως και επαγγελματικής «διαστροφής» ή συνήθειας, η οποία οδηγεί στην παραπάνω χρήση των σύγχρονων νομικών όρων.

7.8.3.2 Πιστεύετε ότι οι hackers ενεργούν περισσότερο με βάση ιδεολογικά κίντρα ή με σκοπό το οικονομικό όφελος;

Σε αυτήν την ερώτηση οι επιστήμονες πληροφορικής βασίζουν τη συμπεριφορά των hackers σε ιδεολογικά κίνητρα σε μεγαλύτερο βαθμό από ό,τι οι νομικοί (51% οι επιστήμονες πληροφορικής σε αντιδιαστολή με το 35% των νομικών). Από την άλλη πλευρά, οι νομικοί σε μεγαλύτερο ποσοστό από τους επιστήμονες πληροφορικής πιστεύουν ότι οι hackers δρουν περισσότερο με κίνητρο το οικονομικό όφελος (34% οι νομικοί σε αντιδιαστολή με το 21% των επιστημόνων πληροφορικής). Η διαφορετική αυτή προσέγγιση μπορεί να ερμηνεύεται λόγω του ότι οι νομικοί

έρχονται ίσως περισσότερο σε επαφή στο επάγγελμά τους με οικονομικά συμφέροντα τα οποία θίγονται σε περιπτώσεις χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα – από την άλλη, οι επιστήμονες πληροφορικής αντιμετωπίζουν περισσότερο την ηλεκτρονική πληροφορία και τα συστήματα πληροφοριών ως αντικείμενο δημιουργίας και αναγνωρίζουν ίσως περισσότερο την ικανοποίηση από το «σπάσιμο» ενός τέτοιου συστήματος, επομένως προσδίδουν και στους hackers τέτοιες προθέσεις.

Στην ερώτηση αυτή η απάντηση «Άλλο» καταλαμβάνει περίπου ίδιο ποσοστό στα δύο δείγματα (31% στο δείγμα νομικών, 28% στο δείγμα επιστημόνων πληροφορικής). Και στα δύο δείγματα κυρίαρχη και αντίστοιχη σε ποσοστά επεξήγηση αυτής της επιλογής είναι το ότι κίνητρα των hackers αποτελούν και τα δύο (και η ιδεολογία τους, δηλαδή, αλλά και η αποκόμιση οικονομικού οφέλους) και αυτό εκφράζεται με 36 απαντήσεις των νομικών (ποσοστό 22,78% από το σύνολο) και με 21 απαντήσεις των επιστημόνων πληροφορικής (ποσοστό 20,19% από το σύνολο). Τέλος, και στα δύο ερωτηματολόγια στην επιλογή «Άλλο» υπάρχουν κοινές απαντήσεις οι οποίες έχουν να κάνουν με την πρόκληση που αποτελεί για τους hackers το να αποκτήσουν χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα καθώς και με την επίδειξη των ικανοτήτων τους.

7.8.3.3 Θεωρείτε ότι οι έλληνες νομικοί που ασχολούνται με το δίκαιο της πληροφορικής είναι επαρκώς ενημερωμένοι και εκπαιδευμένοι σε θέματα πληροφορικής και ιδίως hacking; / Θεωρείτε ότι οι έλληνες επιστήμονες πληροφορικής είναι επαρκώς ενημερωμένοι σε σύγχρονα θέματα ασφάλειας των ηλεκτρονικών δεδομένων;

Στις δύο αυτές ερωτήσεις καλείται το δείγμα να αξιολογήσει το ίδιο τις δυνατότητές του και τις γνώσεις του για θέματα που έχουν να κάνουν με τη διαφύλαξη των ηλεκτρονικών δεδομένων. Η αξιολόγηση και οι δυνατότητες αυτές συναρτώνται άμεσα με τον ρόλο που μπορούν να διαδραματίσουν οι δύο αυτές ομάδες σε επίπεδο πρόληψης. Κοινό στοιχείο των απαντήσεων των δύο δειγμάτων είναι η αρνητική εκτίμηση των νομικών για τις γνώσεις των νομικών σε θέματα πληροφορικής

(ποσοστό 68%) και αντίστοιχα η αρνητική εκτίμηση των επιστημόνων πληροφορικής για την ενημέρωση των συναδέλφων τους (ποσοστό 55%).

7.8.3.4 Πιστεύετε ότι οι δράσεις των hackers μπορούν να έχουν θετική συμβολή στην κοινωνία; Αν ναι, σε ποιες περιπτώσεις;

Η πλειοψηφία και των δύο δειγμάτων υποστηρίζει ότι οι δράσεις των hackers μπορούν να έχουν συμβολή στην κοινωνία (ποσοστό 72,15% των νομικών και 80,76% των επιστημόνων πληροφορικής). Μάλιστα και στα δύο δείγματα, μολονότι η ερώτηση είναι ανοιχτού τύπου, η ομαδοποίηση και κατηγοριοποίηση των απαντήσεων είναι κοινή και αναφέρεται στη συμβολή των hackers στην πρόληψη και καταστολή εγκλημάτων[1300], στον εντοπισμό των κενών ασφαλείας των ηλεκτρονικών προγραμμάτων, στην ενίσχυση της διαφάνειας στη δημόσια ζωή καθώς και στη σφαιρική ενημέρωση και την ιδεολογική αφύπνιση των πολιτών. Το γεγονός αυτό καταδεικνύει ότι υπάρχει σχετική ομογνωμία αναφορικά με τον θετικό αντίκτυπο που μπορούν να έχουν οι δράσεις των hackers, όπως αναφέρθηκε ήδη.

Τα ποσοστά βέβαια σε αυτήν την κατηγοριοποίηση είναι διαφορετικά μεταξύ των δύο δειγμάτων: η πρόληψη και καταστολή εγκλημάτων υποστηρίζεται περισσότερο από τους νομικούς (ποσοστό 19,62%) σε σχέση με τους επιστήμονες πληροφορικής (ποσοστό 9,61%). Τούτο φαίνεται λογικό καθώς οι νομικοί λόγω του επαγγέλματός τους δίνουν μεγαλύτερη βάση στη χρήση της τεχνολογίας για σκοπούς οι οποίοι έχουν να κάνουν με τη γενικότερη εγκληματοπροληπτική πολιτική ή για τον εκσυγχρονισμό μεθόδων της ανακριτικής ή της ποινικής καταστολής.

Στη δεύτερη ομαδοποίηση απαντήσεων οι επιστήμονες πληροφορικής (με ποσοστό 28,85%) υποστηρίζουν περισσότερο από τους νομικούς (ποσοστό 12,65%) τη συμβολή των hackers στον εντοπισμό των κενών ασφαλείας ηλεκτρονικών προγραμμάτων. Το αποτέλεσμα αυτό της σύγκρισης των απαντήσεων των δύο δειγμάτων δεν προκαλεί εντύπωση καθώς οι επιστήμονες πληροφορικής, λόγω ειδικών γνώσεων αλλά ίσως και πάλι «επαγγελματικής διαστροφής», δίνουν

[1300] … η εξειδικευμένη τεχνολογία σήμερα χρησιμοποιείται και σε αυτόν τον τομέα (πρβλ. ενδεικτικά *William Schwabe,* Needs and prospects for crime-fighting technology, RAND, Science and Technology Policy Institute, 1999).

μεγαλύτερη βάση στα κενά ασφαλείας των προγραμμάτων ηλεκτρονικών δεδομένων (από τη στιγμή, μάλιστα, που το 86% αυτών θα συνεργαζόταν με κάποιον hacker για τη βελτίωση μιας πρακτικής ασφάλειας, όπως έχουν απαντήσει οι επιστήμονες πληροφορικής στην ανωτέρω ερώτηση 11 του οικείου ερωτηματολογίου).

Η τρίτη ομαδοποίηση απαντήσεων, η οποία αναφέρεται στη συμβολή των hackers στη διαφάνεια στη δημόσια ζωή, υποστηρίζεται και από τα δύο δείγματα με παρεμφερή ποσοστά (19,62% από τους νομικούς και 16,35% από τους επιστήμονες πληροφορικής).

Τέλος, η ιδεολογική αφύπνιση και δράση υποστηρίζεται από το 4,43% των νομικών αλλά από το 12,5% των επιστημόνων πληροφορικής. Οι νομικοί, δηλαδή, φαίνονται να επηρεάζονται λιγότερο από τις ιδεολογικές καταβολές και δράσεις των hackers σε σχέση με τους επιστήμονες πληροφορικής. Σε κάθε περίπτωση, επομένως, η διαφοροποίηση αυτή των ποσοστών που εντοπίζεται εν προκειμένω βρίσκεται σε άμεση συνάρτηση με τις ανωτέρω απαντήσεις στην ερώτηση 2 και των δύο ερωτηματολογίων στα οποία, όπως καταδείχθηκε ανωτέρω, οι επιστήμονες πληροφορικής προσδίδουν στους hackers ιδεολογικά κίνητρα σε μεγαλύτερο ποσοστό απ' ό,τι οι νομικοί.

Τέλος, η βασική διαφορά στις διατυπώσεις των απαντήσεων στα δύο ερωτηματολόγια είναι ότι σε αρκετές από τις απαντήσεις των νομικών διατυπώνεται επιφύλαξη αναφορικά με τη θετική συμβολή των hackers σε αντίθεση με τους επιστήμονες πληροφορικής, οι οποίοι φαίνονται πιο σίγουροι για τη δυνατότητα θετικής συμβολής των hackers.

7.8.3.5Κατά τη γνώμη σας, η ελληνική νομοθεσία είναι αποτελεσματική για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων;

Το αποτέλεσμα των απαντήσεων σε αυτήν την ερώτηση είναι δύσκολο να συγκριθεί καθώς είναι γεγονός ότι οι νομικοί τεκμαίρεται ότι έχουν μεγαλύτερη γνώση και εμπειρία αναφορικά με τις νομικές προβλέψεις και την εφαρμογή τους. Ωστόσο, οι επιστήμονες πληροφορικής αποτελούν χρήστες των υπηρεσιών πληροφορικής - επιπρόσθετα, είναι οι ειδικοί οι οποίοι ενδεχομένως να καλούνται σε δικαστικές

διαδικασίες ακόμη και ως πραγματογνώμονες ή τεχνικοί σύμβουλοι[1301]. Εξάλλου, έχει ούτως ή άλλως τεθεί η επιλογή «Δεν είμαι ενημερωμένος για τις νομικές προβλέψεις», προκειμένου να υπάρχει η δυνατότητα επιλογής σε αυτούς που δεν είναι σίγουροι για την απάντησή τους – την επιλογή αυτή, εξάλλου, ακολούθησε περίπου ο ένας στους τρεις επιστήμονες πληροφορικής που απάντησε στη συγκεκριμένη ερώτηση (33%).

Κατά τη δυαδική, πάντως, θεώρηση, κοινός τόπος είναι το ότι η πλειοψηφία και των δύο δειγμάτων δεν είναι ευχαριστημένη από την αποτελεσματικότητα της ελληνικής ποινικής νομοθεσίας για τη διαφύλαξη της ασφάλειας των δεδομένων (και στις δύο περιπτώσεις πρώτη σε ποσοστό έρχεται η επιλογή «Λίγο»). Δεύτερη σε προτιμήσεις και στα δύο ερωτηματολόγια έρχεται η επιλογή «Αρκετά» (23% στο δείγμα των νομικών και 17% στο δείγμα των επιστημόνων πληροφορικής – ποσοστό βέβαια ακριβώς ίδιο με την επιλογή «Καθόλου» στο ίδιο τελευταίο δείγμα).

7.8.3.6 Πρέπει να είναι ελεύθερη η πρόσβαση στην πληροφορία στο διαδίκτυο; Αν ναι, σε ποιες περιπτώσεις;

Η ερώτηση αυτή έχει τεθεί προκειμένου οι συμμετέχοντες να ορίσουν κατά τη δική τους εκτίμηση τα όρια της ελευθερίας στην πρόσβαση της πληροφορίας στο διαδίκτυο. Συντριπτικό ποσοστό και στα δύο δείγματα υποστηρίζει την ελευθερία της πληροφορίας στο διαδίκτυο (80,37 % από το δείγμα των νομικών και 83,65% από το δείγμα των επιστημόνων πληροφορικής). Ωστόσο, η απάντηση που κάνει εντύπωση και στα δύο δείγματα είναι ότι υποστηρίζεται η ελευθερία στην πρόσβαση στην ηλεκτρονική πληροφορία χωρίς κανέναν περιορισμό (20,88% των νομικών και 28,85% των επιστημόνων πληροφορικής).

Και στα δύο δείγματα καταγράφονται, επιπρόσθετα, σε επίπεδο περιπτώσεων κοινές απαντήσεις όπως η προστασία των ανηλίκων (ποσοστό 4,81% από τους επιστήμονες πληροφορικής και 6,96% από τους νομικούς), η ελευθερία σε ερευνητικές και εκπαιδευτικές δραστηριότητες (ποσοστό 7,59% από τους νομικούς και 8,65% από

[1301] Βλ. ά. 183 επ. Κώδικα Ποινικής Δικονομίας - διατάξεις αναφορικά με πραγματογνώμονες και τεχνικούς συμβούλους στην ποινική διαδικασία.

τους επιστήμονες πληροφορικής), η προστασία των προσωπικών δεδομένων (ποσοστό 26,58% των νομικών και 18,27% των επιστημόνων πληροφορικής) και η επιλογή του δημιουργού ή κατόχου της ηλεκτρονικής πληροφορίας για το επίπεδο της ελευθερίας (ποσοστό 7,59% των νομικών και 6,73% των επιστημόνων πληροφορικής). Περιορισμός ο οποίος εντοπίζεται σε 9 απαντήσεις των νομικών (ποσοστό 5,69%) ενώ δεν αναφέρεται σε καμία από τις απαντήσεις των επιστημόνων πληροφορικής είναι η προστασία της κρατικής ασφάλειας. Από την άλλη πλευρά, οι επιστήμονες πληροφορικής αναφέρονται στην προστασία των πνευματικών δικαιωμάτων, σε περιπτώσεις εγκλημάτων και σε περιπτώσεις πρόκλησης ζημίας, στοιχεία στα οποία δεν αναφέρονται οι νομικοί.

7.8.3.7 Έχετε να προτείνετε άλλα μέτρα – πέρα από ποινικές διατάξεις – που μπορούν να ληφθούν για την προαγωγή της ασφάλειας των ηλεκτρονικών δεδομένων; Αν ναι, ποια;

Το μέτρο πρόληψης που προκρίνεται και στα δύο δείγματα έχει να κάνει με την πληρέστερη εκπαίδευση αναφορικά με θέματα τεχνολογίας (ποσοστό 28,48% των νομικών και 35,58% των επιστημόνων πληροφορικής)[1302]. Οι λοιπές απαντήσεις είναι πλήρως κατακερματισμένες με τις περισσότερες, όμως, να επικεντρώνονται στη χρήση προγραμμάτων προστασίας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών (π.χ. firewall), στην πιστοποίηση των υπηρεσιών ασφαλείας και των προγραμμάτων στο διαδίκτυο κ.ά.

7.8.3.8 Πόσο ασφαλής νιώθετε αναφορικά με τα ηλεκτρονικά σας δεδομένα στο διαδίκτυο;

[1302] Ο *Ulrich Sieber* αναφέρει ότι σε αρκετές περιπτώσεις τα θύματα ηλεκτρονικών εγκλημάτων ευθύνονται τα ίδια λόγω της άγνοιάς τους (έτσι *Ulrich Sieber,* Legal aspects of computer-related crime in the Information society, January 1998, prepared for the European Commission, p. 5).

Και σε αυτήν την ερώτηση εντοπίζεται κοινός τόπος στις απαντήσεις των δύο δειγμάτων. Και στα δύο δείγματα είναι αρκετά έντονη η ανασφάλεια (54% των νομικών δηλώνει «Λίγο» ασφαλής και 26% «Καθόλου» ασφαλής και από τους επιστήμονες πληροφορικής 40% δηλώνει «Λίγο» ασφαλής και 23% «Καθόλου» ασφαλής). Βεβαίως, προκαλεί εντύπωση το μεγάλο ποσοστό ανασφάλειας που καταγράφεται στους επιστήμονες πληροφορικής, λαμβανομένου υπόψιν ότι οι επιστήμονες πληροφορικής γνωρίζουν και δύνανται να προστατευθούν καλύτερα από τον απλό χρήστη – πρέπει, όμως, να επισημανθεί ότι δεύτερη σε προτιμήσεις απάντηση στους επιστήμονες πληροφορικής είναι η επιλογή «Αρκετά» (27%) αναφορικά με το αίσθημα ασφάλειας των επιστημόνων πληροφορικής για τα ηλεκτρονικά τους δεδομένα.

7.8.3.9 Ποια η γνώμη σας: χρειάζεται αυστηροποίηση των ποινικών κυρώσεων, αποποινικοποίηση του hacking ή οι νομικές προβλέψεις να μείνουν ως έχουν;

Σε αυτήν την ερώτηση, οι προθέσεις νομικών και επιστημόνων πληροφορικής συγκλίνουν ως προς την αυστηροποίηση των ποινικών κυρώσεων (48% των νομικών και 32% των επιστημόνων πληροφορικής). Το ποσοστό των νομικών που υποστηρίζουν την αυστηροποίηση είναι αρκετά μεγαλύτερο από αυτό των επιστημόνων πληροφορικής αλλά, σε κάθε περίπτωση, η συγκεκριμένη είναι η κυρίαρχη τάση και στα δύο δείγματα. Περαιτέρω, ωστόσο, οι επιστήμονες πληροφορικής υποστηρίζουν σε ποσοστό 30% τη διατήρηση των προβλέψεων ως έχουν σε αντίθεση με το 13% των νομικών που ασπάζονται την εν λόγω άποψη. Επιπρόσθετα, είναι σημαντικό το ότι καταγράφεται ποσοστό 11% των νομικών και σχεδόν αντίστοιχο ποσοστό 17% των επιστημόνων πληροφορικής που υποστηρίζουν την αποποινικοποίηση του hacking.

Στην επιλογή «Άλλο» άξιες αναφοράς είναι οι απόψεις των νομικών για σχετικές διοικητικές κυρώσεις, άποψη την οποία βεβαίως δεν δύνανται να διατυπώσουν οι επιστήμονες πληροφορικής καθώς είναι γεγονός ότι βρίσκεται εκτός του πεδίου γνώσεών τους.

7.8.3.10 Όποιος αποκτά χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα στο διαδίκτυο με σκοπό οικονομικό όφελος ή πρόκληση ζημίας πρέπει να έχει την ίδια, ηπιότερη ή αυστηρότερη ποινική μεταχείριση από τον νόμο σε σχέση με αυτόν που δεν έχει σκοπό το οικονομικό όφελος ή την πρόκληση ζημίας; (ερώτηση 10 του ερωτηματολογίου των νομικών και ερώτηση 12 του ερωτηματολογίου των επιστημόνων πληροφορικής)

Η ποινική μεταχείριση των hackers ανάλογα με το κίνητρό τους είναι το τελευταίο πλην κρίσιμο ζήτημα που εξετάζεται στα υπό επεξεργασία ερωτηματολόγια. Και στα δύο δείγματα υποστηρίζεται η άποψη ότι σε περίπτωση που ο hacker επιδιώκει οικονομικό κέρδος ή ζημία πρέπει να τιμωρείται αυστηρότερα (65% των νομικών και 56% των επιστημόνων πληροφορικής). Δεύτερη στις προτιμήσεις τάση είναι η ίδια ποινική μεταχείριση ανεξαρτήτως σκοπού (22% των νομικών και 27% των επιστημόνων πληροφορικής) και τρίτη η άποψη για καμία ποινική μεταχείριση, δηλαδή η αποποινικοποίηση του hacking (13% των νομικών και 15% των επιστημόνων πληροφορικής) – τα ποσοστά που υποστηρίζουν την αποποινικοποίηση του hacking είναι αντίστοιχα με τα ανωτέρω ποσοστά της ερώτησης 9 και των δύο ερωτηματολογίων αναφορικά με όσους υποστηρίζουν την αποποινικοποίηση του hacking. Τέλος, 2 απαντήσεις επιστημόνων πληροφορικής υποστηρίζουν την ηπιότερη μεταχείριση σε περίπτωση σκοπού οικονομικού οφέλους μέσω hacking.

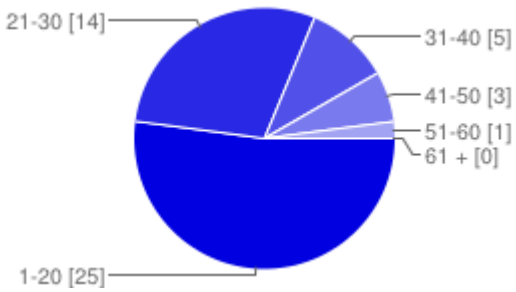
Συμπερασματικά, σε αυτήν την τελευταία ερώτηση οι απαντήσεις και των δύο δειγμάτων είναι αντίστοιχες και τα ποσοστά τους παρεμφερή – επομένως, η εικόνα που έχουμε από την έρευνα αναφορικά με την εν λόγω προσέγγιση μπορεί να χαρακτηριστεί ξεκάθαρη.

7.8.4 Δείγμα hackers

7.8.4.1 Απαντήσεις[1303]

Σε επίπεδο δημογραφικών στοιχείων, ζητήθηκε και από τους hackers να δηλώσουν την ηλικία τους, το φύλο τους και το επίπεδο σπουδών τους.

Ηλικία



1-20	**25**	52%
21-30	**14**	29%
31-40	**5**	10%
41-50	**3**	6%
51-60	**1**	2%
61 +	**0**	0%

Από τα παραπάνω ποσοστά είναι άξιο ανάλυσης ότι κατ' απόλυτη πλειοψηφία οι hackers που απάντησαν στο ερωτηματολόγιο (52%) είναι έως 20 ετών και οι hackers του δείγματος από 21 έως 30 ετών αντιπροσωπεύουν το 29%. Επομένως, το 81% των

[1303] Οι αριθμοί των ερωτηματολογίων που παρουσιάζονται εν προκειμένω είναι όπως έχουν τεθεί στο Παράρτημα ΙΙΙ της παρούσας (βλ. και ανωτέρω), το οποίο αφορά στα ερωτηματολόγια των hackers.

hackers που συμμετείχε στην έρευνα έχουν ηλικία έως 30 ετών[1304]. Ερμηνεύοντας το μεγάλο αυτό ποσοστό, μπορούμε βάσιμα να εκτιμήσουμε ότι είναι λογικό η «περιπέτεια» της αναζήτησης των τεχνολογικών δυνατοτήτων να είναι περισσότερο θελκτική για τις νεότερες ηλικίες[1305]. Αναφορικά, δε, με το ποσοστό του 52% που αναφέρεται στην ηλικία έως 20 ετών, μας δίνει εν προκειμένω ένα σημαντικό εύρημα το οποίο συνίσταται στο ότι αρκετοί hackers είναι ανήλικοι[1306] [1307] (κυρίως έφηβοι[1308]) ή σε κάθε περίπτωση βρίσκονται σε μετεφηβική ηλικία, επιβεβαιώνοντας το γεγονός ότι η συσχέτιση hacking και παραβατικότητας ανηλίκων[1309] απασχολεί τα τελευταία χρόνια την επιστημονική κοινότητα[1310] [1311] ως «νεανικό πρόβλημα» κατά

[1304] Το εύρημα αυτό αντιστοιχίζεται και με τη διατύπωση του Παπαθεοδώρου, κατά τον οποίο οι hackers είναι «*στην πλειονότητά τους νεαροί στην ηλικία (18-30 ετών)*» (*Θ. Παπαθεοδώρου,* Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 206), καθώς και με την ανάπτυξη του Furnell κατά την οποία οι hackers είναι κατά βάση ηλικίας από 15 έως 25 ετών (βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 59).

[1305] Βλ. τα αποτελέσματα της έρευνας των *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 28 (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf) κατά τα ευρήματα της οποίας ο μέσος όρος της ηλικίας των hackers είναι τα 23 έτη και οι ηλικίες με τη μεγαλύτερη συχνότητα είναι μεταξύ 16 και 21 ετών.

[1306] Αναφορικά με την προβληματική της συμμετοχής των ανηλίκων στην έρευνα και την εκ μέρους των γονέων τους συναίνεση, ο Παπάνης επισημαίνει ότι «*δεν υπάρχει κάτι που να αποδεικνύει ότι οι γονείς είναι ενήμεροι για τις δραστηριότητες των παιδιών τους στο Διαδίκτυο, αλλά, ακόμη κι αν είναι, δεν υπάρχει κάτι που να τους διαβεβαιώνει ότι τα προσωπικά στοιχεία του παιδιού τους χρησιμοποιούνται για έρευνα (Turow, 2001). Εκτός αυτού, δεν υπάρχουν στοιχεία που να διαβεβαιώνουν τον ερευνητή ότι η συγκατάθεση δίνεται από τον "πραγματικό γονέα" ...*» (*Ευστράτιος Παπάνης*, Μεθοδολογία έρευνας και διαδίκτυο, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012, σελ. 52).

[1307] Βλ. ενδεικτικά τα δημοσιεύματα της ενημερωτικής ιστοσελίδας in.gr "Μέλη του «Greek Hacking Scene» - Σε τρεις μαθητές λυκείου αποδίδεται η κυβερνοεπίθεση στο υπουργείο Δικαιοσύνης", 20 Φεβρουαρίου 2012, url: http://news.in.gr/science-technology/article/?aid=1231182589 και «Με τους Greek Hacking Scene... Δεκατριάχρονος κατηγορείται από την αστυνομία για συμμετοχή σε ομάδα χάκερ», 27 Ιουνίου 2012, url: http://news.in.gr/greece/article/?aid=1231202376 καθώς και το δημοσίευμα της 06/08/2014 «Ρώσοι χάκερς υπέκλεψαν 1,2 δισ. ονόματα χρηστών και κωδικούς πρόσβασης» της ιστοσελίδας του τηλεοπτικού καναλιού alphatv (url: http://www.alphatv.gr/news/international/rosoi-hakers-ypeklepsan-12-dis-onomata-hriston-kai-kodikoys-prosvasis) το οποίο επισημαίνει ότι η πράξη αυτή είναι ίσως η μεγαλύτερη «υποκλοπή» δεδομένων που έχει μέχρι σήμερα λάβει χώρα και αποδίδεται σε ομάδα δέκα περίπου ***εικοσάχρονων*** hackers που βρίσκονται στη Ρωσία και εντοπίζονται γεωγραφικά μεταξύ Καζακστάν και Μογγολίας.

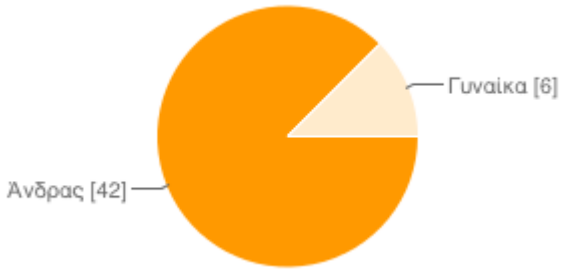
[1308] Αντίστοιχα το ότι οι περισσότεροι hackers είναι έφηβοι υποστηρίζεται και από τους *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 91.

[1309] Πρβλ. *Ν. Κουράκη*, Δίκαιο παραβατικών ανηλίκων, εκδ. Σάκκουλα, Αθήνα – Κομοτηνή, β' εκδ., 2012 και *Αγγ. Πιτσελά*, Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, όπ. π., 2013.

[1310] Υπάρχει, όπως έχει αναφερθεί ήδη, σχετική επιστημονική συζήτηση τα τελευταία χρόνια για τη συσχέτιση του hacking με την νεανική παραβατικότητα (βλ. ενδεικτικά *Majid Yar*, Computer Hacking: Just Another Case of Juvenile Delinquency?, Howard Journal of Criminal Justice, Vol. 44, No. 4, pp. 387-399, September 2005) – συσχέτιση η οποία επιβεβαιώνεται και από τα ως άνω παρουσιαζόμενα αποτελέσματα της έρευνας.

τον Yar[1312]. Το δεδομένο αυτό πρέπει να ληφθεί υπόψιν και σε κάθε σχεδιασμό αντεγκληματικής πολιτικής[1313] για το hacking και τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα καθώς και για τη μελέτη της παραβατικότητας ανηλίκων, η οποία, με την εξέλιξη των τεχνολογικών μέσων και την αμεσότητα στην πρόσβαση σε αυτά, φαίνεται να έχει μεταφερθεί πλέον στον ψηφιακό κόσμο.

Φύλο



Άνδρας **42** 88%

Γυναίκα **6** 13%

Το 88% των συμμετεχόντων (42) είναι άνδρες και μόλις το 13% (6) γυναίκες. Ανέκαθεν η τεχνολογία μάλλον ήταν περισσότερο ελκυστική για τους άνδρες παρά για τις γυναίκες[1314]. Εν προκειμενω, επιβεβαιώνεται και σε αυτό το σημείο ο Furnell

[1311] Σχετικά και τα πορίσματα της Dreyfus αναφορικά με το ότι η ηλικία των περισσότερων hackers είναι μεταξύ 16 και 24 ετών (βλ. *Suelette Dreyfus*, Computer hackers: Juvenile Deliquents or International Saboteurs?, εισήγηση η οποία παρουσιάστηκε στο συνέδριο "Internet Crime" το οποίο έλαβε χώρα στη Μελβούρνη της Αυστραλίας στις 16-17 Φεβρουαρίου 1998 και διοργανώθηκε από το Australian Institute of Criminology).

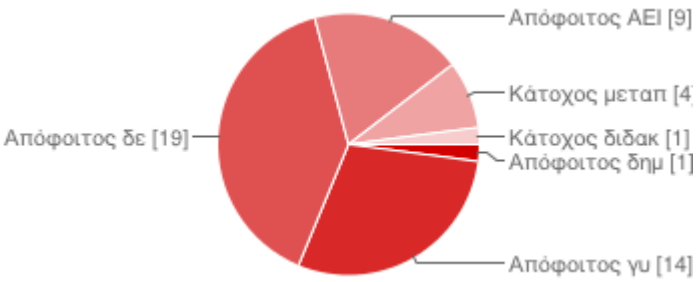
[1312] Όπως αναφέρθηκε ανωτέρω και συγκεκριμένα στην παράγραφο 3.8 του παρόντος πονήματος.

[1313] Βλ. σχετικές αναπτύξεις στην παράγραφο 8.4 της παρούσας διατριβής.

[1314] Ο Taylor εξηγεί αυτήν την υπεροχή των αρρένων στα ποσοστά συμμετοχής σε ενέργειες hacking σύμφωνα με τις ψυχοσεξουαλικές θεωρίες, θεωρώντας το hacking ως εναλλακτική επιλογή αντί της σεξουαλικής δραστηριότητας (έτσι ο *Ales Zavrsnik*, Cybercrime: Definitional challenges and criminological particularities, Masaryk University Journal of Law and Technology, url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf, p. 19).

ο οποίος αναφέρει ότι οι hackers είναι σχεδόν πάντα άνδρες[1315]. Βέβαια, οι γυναίκες hackers αντιμετωπίζονται ως ίσες από τους ίδιους τους hackers[1316].

Επίπεδο Σπουδών



Απόφοιτος δημοτικού	**1**	2%
Απόφοιτος γυμνασίου	**14**	29%
Απόφοιτος δευτεροβάθμιας εκπαίδευσης (λύκειο κ.ά.)	**19**	40%
Απόφοιτος ΑΕΙ - ΑΤΕΙ	**9**	19%
Κάτοχος μεταπτυχιακού διπλώματος	**4**	8%
Κάτοχος διδακτορικού διπλώματος	**1**	2%

Οι περισσότεροι hackers συμμετέχοντες στο δείγμα είναι απόφοιτοι δευτεροβάθμιας εκπαίδευσης (40%) και η δεύτερη σε σειρά επιλογής απάντηση είναι οι απόφοιτοι γυμνασίου (29%). Σε μία απάντηση, μάλιστα, καταγράφεται ότι ο συμμετέχων στην έρευνα είναι απόφοιτος δημοτικού![1317] Τα ποσοστά αυτά βρίσκονται σε αντιστοιχία

[1315] Βλ. *Steven Furnell*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, όπ. π., σελ. 59.

[1316] *Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 12. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

[1317] Έχει καταγραφεί ότι η ηλικία έναρξης δραστηριοτήτων hacking μπορεί να είναι ακόμη και αυτή των 11-12 ετών (έτσι *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of

με τα ποσοστά των ηλικιών των συμμετεχόντων ως άνω, επιβεβαιώνοντας ακόμη μια φορά ότι η έρευνα καταδεικνύει πως το hacking αφορά σε μεγάλο βαθμό ανήλικους.

Είναι αλήθεια ότι θα περίμενε κανείς αυτοί που ασχολούνται με το hacking να έχουν κατακτήσει κάποια εξειδίκευση – η οποία θα αντιστοιχεί και στο μορφωτικό τους επίπεδο – προκειμένου να έχουν αποκτήσει εξειδικευμένες γνώσεις που θα τους βοηθούσαν στη δραστηριότητά τους αυτή. Ωστόσο, είναι πιθανό οι hackers να περιφρονούν όχι βέβαια τη γνώση αλλά τους τίτλους σπουδών, οι οποίοι δίνονται μέσα από θεσμοθετημένες δομές[1318].

Πέραν όμως αυτών, 29% των hackers φαίνεται να έχουν λάβει πανεπιστημιακή εκπαίδευση (19% απόφοιτοι ΑΕΙ/ΑΤΕΙ, 8% κάτοχοι μεταπτυχιακού διπλώματος και 1 κάτοχος διδακτορικού διπλώματος)[1319].

<u>Ερώτηση 1</u>: Τί είναι hacking σύμφωνα με την εμπειρία σας;

(ανοικτού τύπου ερώτηση)

Στην ερώτηση αυτή οι ίδιοι οι hackers καλούνται να ορίσουν οι ίδιοι τι σημαίνει hacking για αυτούς. Οι απαντήσεις που ελήφθησαν όχι μόνο δεν ομαδοποιούνται αλλά ουσιαστικά κάθε μία από αυτές μπορεί να υποστηριχθεί ότι αναδεικνύει μια διαφορετική διάσταση του hacking. Πάντως, η χωρίς δικαίωμα πρόσβαση σε δεδομένα βρίσκεται στον πυρήνα των συμπεριφορών hacking εντοπιζόμενη σε 15

Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 122).

[1318] Βλ. ανωτέρω τη συνέντευξη με μέλος του hackerspace.gr στην οποία υποστήριξε ότι δεν συνέχισε τις σπουδές του σε τμήμα ΑΤΕΙ σχετικό με την πληροφορική στο οποίο είχε εγγραφεί λόγω του ότι θεωρούσε πως δεν του προσφέρεται εκεί γνώση.

[1319] Αντίστοιχα είναι και τα αποτελέσματα έρευνας στο πόνημα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 76 κατά την οποία σε δείγμα 128 hackers 34% των ερωτηθέντων (44) δήλωσαν ότι είχαν διπλώματα δευτεροβάθμιας εκπαίδευσης, 29% (37) διπλώματα από σχολές επαγγελματικής κατάρτισης, 19% (24) είχε απολυτήριο γυμνασίου, 7% (9) είχε ολοκληρώσει μεταπτυχιακές σπουδές, 4% (5) είχαν σταματήσει στο επίπεδο του δημοτικού σχολείου και 7% (9) είχαν πανεπιστημιακό πτυχίο.

απαντήσεις (ως ηλεκτρονική παραβίαση, ως πρόσβαση χωρίς έγκριση, ως σπάσιμο κωδικών κ.λπ.)[1320].

Επιπλέον κοινό στοιχείο απαντήσεων μπορεί να θεωρηθεί η υποστήριξη της καινοτομίας για επίλυση προβλημάτων τεχνολογικής φύσης[1321], της γνώσης[1322] και της περιέργειας[1323]. Χαρακτηριστικές είναι και οι απαντήσεις που αναφέρονται στη χρήση της τεχνολογίας και των επιτευγμάτων του πολιτισμού με διαφορετικό τρόπο και για διαφορετικό σκοπό από αυτόν για τον οποίο προορίζονται[1324] [1325] και η φαντασία στη χρήση της τεχνολογίας[1326]. Σχετικές με τους ανωτέρω πειραματισμούς είναι μάλλον και οι απαντήσεις οι οποίες αναφέρονται στο ότι το hacking είναι διαφορετικός τρόπος σκέψης και ότι αποτελεί μάλλον «μια άλλη ζωή!»[1327] καθώς και η απάντηση ότι το hacking αποτελεί «παιχνίδι γρίφων»[1328].

Επιπρόσθετα, υπάρχουν απαντήσεις οι οποίες αναφέρονται στον προγραμματισμό (που θα μπορούσε να υποστηριχθεί τελικά ότι αποτελεί την «γλώσσα» των «γνήσιων πρακτικών hacking» – όπως αυτές αναλύθηκαν ανωτέρω), είτε ως μεγαλύτερη εμπειρία από τον απλό χρήστη[1329], είτε ως εξέλιξη της επιστήμης[1330], είτε με σκοπό την εκμετάλλευση των κενών ασφαλείας[1331], είτε ως αντίδραση στην κοινωνική αδικία[1332].

Περαιτέρω, υπάρχουν απαντήσεις που αναφέρονται στην ιδεολογία[1333] και στο κίνητρο του hacking το οποίο λαμβάνει χώρα με σκοπό την διαφάνεια και την ελεύθερη κυκλοφορία των ιδεών[1334].

[1320] Στα ερωτηματολόγια υπ' αρ. 7, 8, 9, 13, 14, 19, 20, 21, 26 (απάντηση στην οποία αναφέρεται «*gnosi gia th leitoyrgia systimaton kai na mpaineis xoris na se stamataei tipota*»), 29, 35, 36, 39, 42, 46.

[1321] Στα ερωτηματολόγια υπ' αρ. 2, 3, 4, 23, 31.

[1322] Στα ερωτηματολόγια υπ' αρ. 4, 11, 12, 15, 28.

[1323] Στο ερωτηματολόγιο υπ' αρ. 12.

[1324] Στα ερωτηματολόγια υπ' αρ. 27 και 24.

[1325] Βλ. παράγραφο 2.2 του παρόντος πονήματος όπου καταγράφεται ότι hacking θεωρείται η χρήση της τεχνολογίας με ανορθόδοξο τρόπο.

[1326] Στα ερωτηματολόγια υπ' αρ. 30 και 33.

[1327] Στα ερωτηματολόγια υπ' αρ. 6 και 14.

[1328] Στο ερωτηματολόγιο υπ' αρ. 16.

[1329] Στο ερωτηματολόγιο υπ' αρ. 5.

[1330] Στο ερωτηματολόγιο υπ' αρ. 11 («*βήματα παραπέρα*»).

[1331] Στα ερωτηματολόγια υπ' αρ. 1, 9, 37, 38, 41, 45,

[1332] Στα ερωτηματολόγια υπ' αρ. 17, 25, 32, 48

[1333] Στο ερωτηματολόγιο υπ' αρ. 44.

Μεταξύ των ερωτηματολογίων υπάρχουν απαντήσεις οι οποίες έρχονται σε απόλυτη αντίθεση μεταξύ τους, όπως ο ορισμός του hacking ως μοντέρνου τρόπου χρήσης των ηλεκτρονικών υπολογιστών[1335] από τη μια και η «κακή χρήση γνώσεων πληροφορικής»[1336] από την άλλη. Τέλος, απαντήσεις άξιες προσοχής είναι αυτές οι οποίες αναφέρουν ότι hacking δεν είναι η μη εγκεκριμένη πρόσβαση σε ηλεκτρονικό υπολογιστή[1337] και ότι το hacking δεν είναι κακόβουλο καθώς είναι αντίθετο από το cracking[1338] καθώς και η απάντηση η οποία αναφέρεται σε διάφορες περιπτώσεις hacking (hardware κ.λπ.)[1339]. Σε ένα ερωτηματολόγιο δεν απαντήθηκε η συγκεκριμένη ερώτηση[1340].

Σε μια συνολική θεώρηση των απαντήσεων, μπορεί να υποστηριχθεί ότι τελικά ελάχιστη είναι η συνεισφορά των hackers σε τυχόν εμπλουτισμό του ορισμού του hacking, σε σχέση με όσα αναλύθηκαν ανωτέρω. Επίσης, σε ελάχιστες απαντήσεις φαίνεται οι hackers να παραδέχονται ότι δρουν κακόβουλα – τουναντίον, στις περισσότερες περιπτώσεις προβάλλεται η καινοτομία και η θέληση για γνώση και η ελευθερία της πληροφορίας ως -έστω έμμεση- δικαιολόγηση των ενεργειών αυτών.

<u>Ερώτηση 2</u>: Ποιος ο σκοπός της δράσης σας; Υπάρχει ιδεολογικό υπόβαθρο; Είχατε ποτέ έως τώρα οποιουδήποτε είδους οικονομική ωφέλεια από την ενασχόλησή σας με το hacking;

(ανοικτού τύπου ερώτηση)

[1334] Στα ερωτηματολόγια υπ' αρ. 18, 19, 34, 39 («*tropoi na spas ta oria gia na yparhei eleftheria tis pliroforias»),* 40 («*hrisi toy pc gia na peraseis tis apopseis sou*»).

[1335] Στο ερωτηματολόγιο υπ' αρ. 22.

[1336] Στο ερωτηματολόγιο υπ' αρ. 47.

[1337] Στο ερωτηματολόγιο υπ' αρ. 2.

[1338] Στο ερωτηματολόγιο υπ' αρ. 15.

[1339] Στο ερωτηματολόγιο υπ' αρ. 11.

[1340] Ερωτηματολόγιο υπ' αρ. 10.

Η ως άνω ερώτηση έχει ουσιαστικά τρία σκέλη: α. ο σκοπός της δράσης των hackers[1341], β. αν υπάρχει ή όχι ιδεολογικό υπόβαθρο και γ. αν οι συμμετέχοντες έχουν αποκομίσει οικονομικό όφελος από την δραστηριότητά τους αυτή.

Ως προς το πρώτο σκέλος οι απαντήσεις ποικίλουν. Οι επικρατέστερες είναι οι εξής: σε 6 απαντήσεις[1342] (ποσοστό 12,5%) ανιχνεύεται ως σκοπός δράσης η «ηλεκτρονική επανάσταση» και αντίδραση, σε 4 απαντήσεις[1343] (ποσοστό 8,33%) η ελευθερία της πληροφορίας και σε 4 επίσης απαντήσεις[1344] (ποσοστό 8,33%) η ανίχνευση πληροφοριών για τα ηλεκτρονικά συστήματα και τα κενά ασφαλείας σε επίπεδο ελέγχου των δυνατοτήτων διείσδυσης. Επιπρόσθετα, σε 6 απαντήσεις[1345] (ποσοστό 12,5%) εντοπίζεται ως σκοπός η συμμετοχή στις δράσεις και τα «πιστεύω» της Ελληνικής Hacking Σκηνής (Greek Hacking Scene – GHS)[1346].

Περαιτέρω, ως σκοποί δράσης δηλώνονται σε 2 απαντήσεις[1347] (ποσοστό 4,16%) η βελτίωση των λειτουργιών του ελεύθερου λογισμικού. Σε άλλες 2 απαντήσεις[1348] (ποσοστό 4,16%), επίσης, αναφέρεται η εξάσκηση (training). Σε έτερες απαντήσεις προκίνονται η κατασκευή τεχνολογίας ακόμη και σε επίπεδο hardware[1349], η προσπάθεια για καλύτερο μέλλον[1350] και για διαφάνεια[1351], η προσωπική

[1341] Στην έρευνα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 77 -78 στην ερώτηση σε hackers "Ποιοι είναι το κίνητρό σας;» το υψηλότερο ποσοστό των hackers (30%, 213 ερωτηθέντες) ισχυρίζεται ότι έχει ως κίνητρο την φιλοπεριέργεια και έπειτα 14% (99 ερωτηθέντες) απάντησαν ότι κάνουν hacking για το καλό των χρηστών καθώς ψάχνουν για αδυναμίες στα συστήματα πληροφοριών, λογισμικού και τηλεπικοινωνιών. Επιπλέον, 13% (96 ερωτηθέντες) απάντησαν «άλλο», χωρίς να διευκρινίσουν την απάντησή τους, γεγονός που ερμηνεύεται από τους συγγραφείς ως έλλειψη δικαιολογίας ή ως θέληση για μη αποκάλυψη των λόγων. 12% (86 ερωτηθέντες) κάνουν hacking, διότι θεωρούν «βαρετή» τη ζωή τους και 9% (66 ερωτηθέντες) δήλωσαν ότι είναι εξαρτημένοι από το hacking. Άλλο ένα 9% (64 ερωτηθέντες) θέλουν να αποκτήσουν εξουσία σε κυβερνητικούς οργανισμούς. Συνολικά 47 ερωτηθέντες (7%) κάνουν hacking για να κερδίσουν την αναγνώριση και τον σεβασμό στην ομάδα hacking που ανήκουν ενώ το 6% (45 ερωτηθέντες) κάνουν hacking για να ανέλθουν επίπεδο στην εσωτερική ιεραρχία στην ομάδα hackers στην οποία ανήκουν.

[1342] Στα ερωτηματολόγια υπ' αρ. 1, 12, 25, 35, 43 («*opios adiki ine stoxos*»), 44 («*τιμωρία αυτών που εκμεταλλεύονται την τεχνολογία για να επιβάλουν συνειδήσεις*»).

[1343] Στα ερωτηματολόγια υπ' αρ. 19, 28, 30, 34.

[1344] Στα ερωτηματολόγια υπ' αρ. 26, 28 («*penetration testing*»), 31, 38.

[1345] Στα ερωτηματολόγια υπ' αρ. 7, 11, 13, 14, 32 και 40.

[1346] Βλ. αναλυτικά στο παράρτημα IV του παρόντος πονήματος.

[1347] Στα ερωτηματολόγια υπ' αρ. 2 και 4.

[1348] Στα ερωτηματολόγια υπ' αρ. 16 και 47.

[1349] Στο ερωτηματολόγιο υπ' αρ. 23.

[1350] Στο ερωτηματολόγιο υπ' αρ. 17.

[1351] Στο ερωτηματολόγιο υπ' αρ. 18.

ικανοποίηση[1352] και η θέληση για τον hacker να «ακονίσει το μυαλό του»[1353] και η «ελευθερία»[1354]. Επιπρόσθετα, σε 2 απαντήσεις[1355] (ποσοστό 4,16%) ως σκοπός δηλώνεται η βούληση να παρακολουθεί ο hacker κινήσεις ανθρώπων που τον ενδιαφέρουν.

Ιδεολογικό υπόβαθρο προκύπτει σε 22 από τους συμμετέχοντες hackers[1356] (ποσοστό 45,83%) ενώ αρνούνται το ιδεολογικό υπόβαθρο μόλις 7 απαντώντες[1357] (ποσοστό 14,58%) εκ των οποίων υποστηρίζεται ότι προβαίνουν σε ενέργειες hacking μόνο για επέκταση των γνώσεων[1358], ως ασχολία στον ελεύθερο χρόνο (hobby)[1359] καθώς και για εξάσκηση[1360]. Τέλος, από την ανάλυση των υπολοίπων 18 απαντήσεων[1361] δεν προκύπτει σαφής απάντηση σε αυτό το σκέλος της ερώτησης.

Οικονομική ωφέλεια από το hacking παραδέχονται ότι είχαν μόλις 6 από τους συμμετέχοντες στην έρευνα[1362]. Ωστόσο, οι δύο από αυτούς διευκρινίζουν ότι είχαν οικονομικό όφελος είτε «*χωρίς να κάνω κάτι κακό*»[1363] είτε παλαιότερα πραγματοποιώντας δωρεάν τηλεφωνικές κλήσεις[1364]. Σε μία από τις απαντήσεις ο hacker παραδέχεται ότι είχε οικονομική ωφέλεια γιατί έχει φτιάξει «πατέντες»[1365] στις οποίες, βέβαια, ίσως και να περιλαμβάνονται και προγράμματα χωρίς δικαίωμα πρόσβασης σε δεδομένα ή ιοί καθώς στο ίδιο ερωτηματολόγιο στην ερώτηση 10 ο ίδιος hacker αναφέρεται σε χρήση προγραμμάτων sniffer[1366]. Εντύπωση, πάντως, προκαλούν οι 5 απαντήσεις[1367] (ποσοστό 10,42%) στις οποίες υποστηρίζεται ότι το οικονομικό όφελος το οποίο έχουν αποκομίσει οι εν λόγω συμμετέχοντες στην

[1352] Στο ερωτηματολόγιο υπ' αρ. 1.

[1353] Στο ερωτηματολόγιο υπ' αρ. 29.

[1354] Στο ερωτηματολόγιο υπ' αρ. 42.

[1355] Στα ερωτηματολόγια υπ' αρ. 20 και 46.

[1356] Στα ερωτηματολόγια υπ' αρ. 1, 4, 7, 11, 12, 13, 14, 17, 18, 19, 22, 25, 28, 30, 32, 34, 35, 40, 42, 43, 44, 48.

[1357] Στα ερωτηματολόγια υπ' αρ. 8, 9, 15, 16, 20, 29, 39.

[1358] Στο ερωτηματολόγιο υπ' αρ. 8.

[1359] Στα ερωτηματολόγια υπ' αρ. 9 και 15 καθώς και στο ερωτηματολόγιο υπ' αρ. 18 από τους απαντώντες που υποστήριξαν στην απάντησή τους ότι διακατέχονται από ιδεολογία κατά την ενάσκηση δραστηριοτήτων hacking.

[1360] Στο ερωτηματολόγιο υπ' αρ. 16.

[1361] Στα ερωτηματολόγια υπ' αρ. 2, 3, 5, 6, 21, 23, 24, 26, 27, 31, 33, 36, 37, 38, 41, 45, 46, 47.

[1362] Στα ερωτηματολόγια υπ' αρ. 5, 11, 21, 24, 27, 29.

[1363] Στο ερωτηματολόγιο υπ' αρ. 24.

[1364] Στο ερωτηματολόγιο υπ' αρ. 29.

[1365] Στο ερωτηματολόγιο υπ' αρ. 27.

[1366] Βλ. χαρακτηριστικά ανωτέρω παράγραφο 2.11.2.2.4.

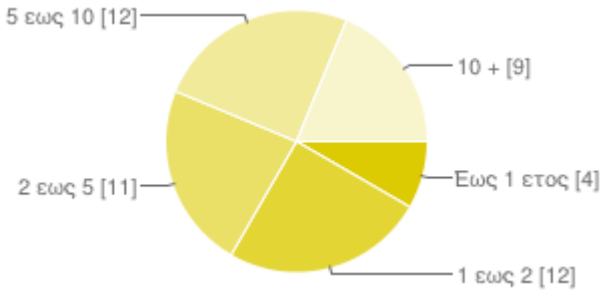
[1367] Στα ερωτηματολόγια υπ' αρ. 1, 4, 33, 37 και 41.

έρευνα δεν προέκυψε από τις ίδιες τις ενέργειες hacking αλλά οι γνώσεις που απέκτησαν από το hacking τους βοήθησαν να βγάλουν χρήματα επειδή βελτίωσαν τις ικανότητές τους ιδίως ως προγραμματιστές.

Εντούτοις, η συντριπτική πλειοψηφία του δείγματος, και συγκεκριμένα 22 απαντήσεις[1368] (ποσοστό 45,83%), ισχυρίζεται ότι δεν έχει αποκομίσει από το hacking οικονομικό όφελος (σε κάποιες απαντήσεις επισημαίνεται ότι ο hacker επέλεξε να μην έχει οικονομικό όφελος αν και θα μπορούσε[1369] ή αν και του προτάθηκε[1370]). Επιπρόσθετα, σε 14 απαντήσεις[1371] δεν προκύπτει αν οι απαντώντες έχουν αποκομίσει οικονομικό όφελος. Τέλος, επισημαίνεται ότι στο ερωτηματολόγιο υπ' αρ. 38 ο συμμετέχων στην έρευνα δεν έχει αποκομίσει περιουσιακό όφελος αλλά αναφέρει ότι έχει «αντιγράψει προγράμματα» και στο ερωτηματολόγιο υπ' αρ. 48 ο συμμετέχων στην έρευνα δεν απαντά αλλά δηλώνει ότι έχει βοηθήσει ανθρώπους που θα πάθαιναν οικονομική ζημία χωρίς, ωστόσο, να διευκρινίζει τον τρόπο. Κλείνοντας, σε ένα ερωτηματολόγιο δεν απαντήθηκε καθόλου αυτή η ερώτηση[1372].

<u>Ερώτηση 3</u>: Πόσα χρόνια ασχολείστε με το hacking;

(κλειστού τύπου ερώτηση: έως 1 έτος – 1 έως 2 έτη – 2 έως 5 έτη – 5 έως 10 έτη – 10 και άνω έτη)



[1368] Στα ερωτηματολόγια υπ' αρ. 1, 2, 3, 6, 7, 8, 9, 12, 13, 14, 16, 17, 19, 20, 22, 32, 33, 36, 38, 39, 46, 48.

[1369] Στα ερωτηματολόγια υπ' αρ. 7 και 36.

[1370] Στα ερωτηματολόγια υπ' αρ. 10 και 15.

[1371] Στα ερωτηματολόγια υπ' αρ. 15, 18, 23, 25, 30, 31, 34, 35, 40, 42, 43, 44, 45, 47.

[1372] Στο ερωτηματολόγιο υπ' αρ. 10.

Έως 1 ετος	**4**	8%
1 εως 2	**12**	25%
2 εως 5	**11**	23%
5 εως 10	**12**	25%
10 +	**9**	19%

Οι hackers που συμμετείχαν στην έρευνα φαίνεται να έχουν αρκετή εμπειρία καθώς μόλις 4 εξ αυτών (ποσοστό 8%) ασχολούνται με το hacking για λιγότερο από ένα έτος. Οι περισσότεροι -12 εξ αυτών (ποσοστό 25%)- είναι νεοεισελθέντες στην «περιπέτεια» του hacking (1-2 έτη) αλλά εξίσου υπάρχουν άλλοι 12 hackers οι οποίοι ασχολούνται με το hacking από πέντε έως 10 έτη. Επιπρόσθετα, δεν είναι διόλου αμελητέο το ποσοστό 19% το οποίο ασχολείται με το hacking εδώ και πάνω από 10 χρόνια καθώς και το ποσοστό 23% που ασχολείται με το hacking από 2 έως 5 έτη.

<u>Ερώτηση 4</u>: Σημαίνει κάτι για εσάς ο όρος "ethical hacking";

(ανοικτού τύπου ερώτηση)

Η συγκεκριμένα ερώτηση ετέθη ως ανοικτού τύπου προκειμένου να μπορέσουμε να διακρίνουμε αρχικώς αν γνωρίζουν τον όρο και να απαντήσουν ελεύθερα στον αν οι ίδιοι αναλαμβάνουν δράση με τέτοια κριτήρια.

Σε 18 από τις 48 απαντήσεις[1373] (ποσοστό 37,5%) οι συμμετέχοντες στην έρευνα υποστηρίζουν -ή προκύπτει από τις απαντήσεις τους- ότι τις ενέργειες στις οποίες προβαίνουν τις κατατάσσουν στην ιδεολογία του ηθικού hacking. Μάλιστα, σε 3 από τις απαντήσεις επισημαίνεται ότι το hacking μόνο ηθικό μπορεί να είναι[1374]. Παρά ταύτα, όμως, σημειώνεται ότι δεν μπορείς να κάνεις «καλό hacking» χωρίς πριν να

[1373] Στα ερωτηματολόγια υπ' αρ. 2, 6, 11, 16, 18, 21, 22, 24, 27, 28, 30, 32, 34, 35, 36, 37, 47 και 48.
[1374] Στα ερωτηματολόγια υπ' αρ. 27, 30 και 38.

έχεις κάνει «κακό hacking»[1375] καθώς και ότι «*καθένας έχει τη δική του ηθική. δεν μπορούν οι απόψεις όλων των hackers να μπουν κάτω από μια ομπρέλα*»[1376].

Επίσης, σε 18 από τις 48 απαντήσεις[1377] (ποσοστό 37,5%) οι συμμετέχοντες υποστηρίζουν -ή προκύπτει από τις απαντήσεις τους- ότι προβαίνουν σε ενέργειες τις οποίες δεν κατατάσσουν στο λεγόμενο ηθικό hacking, καθώς αυτό δεν σημαίνει τίποτα για αυτούς. Ενδιαφέρουσες είναι οι απαντήσεις σύμφωνα με τις οποίες το ηθικό hacking θεωρείται κάτι σαν «διαγωνισμός» και για αυτόν τον λόγο ο συγκεκριμένος συμμετέχων «*το απεχθάνεται*»[1378] καθώς και η απάντηση σύμφωνα με την οποία το ηθικό hacking θεωρείται μέσο προκειμένου κάποιοι να επωφεληθούν οικονομικά, χρησιμοποιώντας και εκμεταλλευόμενοι κάποιους hackers με τους τελευταίους να εργάζονται και να εισφέρουν τις γνώσεις τους δωρεάν στο όνομα ενός καλού σκοπού όπως φαινομενικά το ηθικό hacking[1379]. Επιπρόσθετα, υποστηρίζεται ότι όποιος ασχολείται με ηθικό hacking «*κλείνει τις possibilities*» και ότι αν ο απαντών ήθελε να βγάλει χρήματα θα ασχολείτο με το ηθικό hacking[1380]. Σε μία άλλη απάντηση ο συμμετέχων δηλώνει ότι κάνει hacking για καλό σκοπό αλλά δεν ταυτίζει τις πράξεις του με την ιδεολογία του ηθικού hacking.

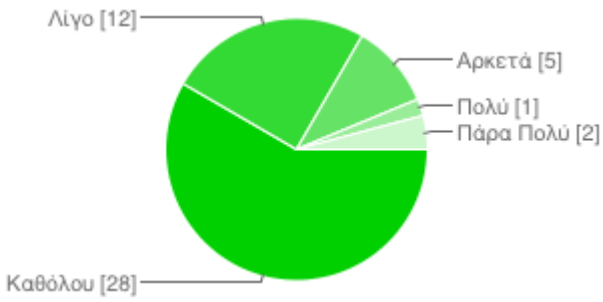
Σε 8 απαντήσεις[1381] δεν προκύπτει ξεκάθαρα η θέση του συμμετέχοντος στην έρευνα για το πώς εκτιμά ο ίδιος το ηθικό hacking και το αν προβαίνει σε τέτοιες πράξεις, εκ των οποίων χαρακτηριστική είναι η απάντηση ότι και το ηθικό hacking αποτελεί και αυτό «ταμπέλα», όπως και το hacking[1382]. Άλλες απαντήσεις οι οποίες είναι άξιες μνείας, ανεξαρτήτως της ανωτέρω κατηγοριοποίησης, είναι οι 4 απαντήσεις στις οποίες αναφέρεται ότι οι hackers στο ηθικό hacking ανακαλύπτουν τα κενά ασφαλείας και στέλνουν τα σχετικά στοιχεία στους διαχειριστές των ηλεκτρονικών

[1375] Στο ερωτηματολόγιο υπ' αρ. 11.
[1376] Στο ερωτηματολόγιο υπ' αρ. 48.
[1377] Στα ερωτηματολόγια υπ' αρ. 1, 3, 7, 12, 13, 17, 20, 23, 25, 26, 29, 31, 33, 39, 40, 43, 45, 46.
[1378] Στο ερωτηματολόγιο υπ' αρ. 1.
[1379] Στο ερωτηματολόγιο υπ' αρ. 7.
[1380] Στο ερωτηματολόγιο υπ' αρ. 13.
[1381] Στα ερωτηματολόγια υπ' αρ. 4, 5, 8, 14, 15, 19, 38 και 41.
[1382] Στο ερωτηματολόγιο υπ' αρ. 41.

δεδομένων[1383].Τέλος, 3 συμμετέχοντες άφησαν κενή τη συγκεκριμένη απάντηση[1384] και ένας απάντησε προφανώς εσφαλμένως[1385].

<u>Ερώτηση 5</u>: Η ισχύουσα ελληνική νομοθεσία σας έχει αποτρέψει από την επέκταση της δράσης σας;

(κλειστού τύπου ερώτηση: Καθόλου – Λίγο – Αρκετά – Πολύ – Πάρα πολύ)



Καθόλου	**28**	58%
Λίγο	**12**	25%
Αρκετά	**5**	10%
Πολύ	**1**	2%
Πάρα Πολύ	**2**	4%

Αναφορικά με την αποτελεσματικότητα της ελληνικής νομοθεσίας σε επίπεδο γενικής πρόληψης ετέθη η ανωτέρω ερώτηση. Διαπιστώνεται ότι οι hackers σε ποσοστό 58% δεν έχουν αποτραπεί καθόλου από την ισχύουσα ελληνικό νομοθεσία και 25% έχουν αποτραπεί μόλις σε λίγες περιπτώσεις. Τούτο σημαίνει ότι οι κρατούσες διατάξεις

[1383] Στα ερωτηματολόγια υπ' αρ. 14, 15, 19, και 21.

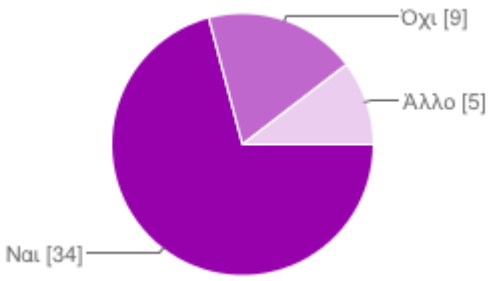
[1384] Στα ερωτηματολόγια υπ' αρ. 10, 42 και 44.

[1385] Στο ερωτηματολόγιο υπ' αρ. 9 όπου εννοούσε ότι ethical hacking είναι ο εθισμός στο hacking από τον οποίο, ωστόσο, μπορείς να απαλλαγείς!

ασκούν μικρή ή καθόλου επήρεια στο 83% των hackers ενώ αρκετά, πολύ και πάρα πολύ έχει αποτραπεί να δράσει λόγω της νομοθεσίας μόλις το 16% των hackers (με το 10% να αντιπροσωπεύει το αρκετά).

<u>Ερώτηση 6</u>:

α. Εσείς έχετε πληροφορίες στο διαδίκτυο στις οποίες δεν θα θέλατε κάποιος να έχει πρόσβαση (π.χ. e-mail, facebook account κ.λπ.); *(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)*



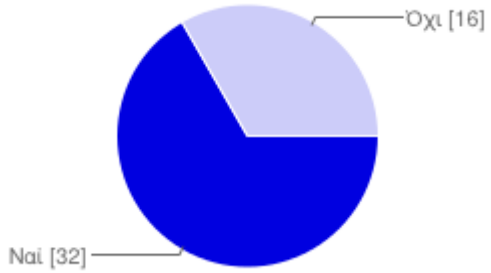
Ναι	**34**	71%
Όχι	**9**	19%
Άλλο	**5**	10%

Στο διαδίκτυο οι hackers αποκτούν χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα αλλά σε αυτήν την ερώτηση θα διαπιστώσουμε κατά πόσον οι ίδιοι αφήνουν τις πληροφορίες τους εντελώς ελεύθερες στο διαδίκτυο. Το συντριπτικό ποσοστό του 71% αυτών δηλώνει ότι έχει πληροφορίες στο διαδίκτυο στις οποίες θα ήθελε να μην έχει κανείς άλλος πρόσβαση. Από την άλλη, το 19% δεν έχει τέτοιου είδους πληροφορίες στο διαδίκτυο.

Στις 5 απαντήσεις[1386] (ποσοστό 10%) στις οποίες επελέγη η απάντηση «Άλλο» στη μία εξ αυτών η απάντηση είναι «Όχι»[1387] (άρα αν προστεθεί και αυτή η απάντηση στο ανωτέρω ποσοστό του «Όχι» αυτό μετατρέπεται σε 20,83%), σε άλλη η απάντηση είναι «*Σε ιστοσελίδες*» από την οποία προκύπτει ότι ο απαντών έχει δεδομένα σε ιστοσελίδες[1388] (άρα αν προστεθεί και αυτή η απάντηση στο ανωτέρω ποσοστό του «Ναι» αυτό μετατρέπεται σε 72,92%), σε έτερη εξ αυτών αναφέρεται ότι όλοι έχουν ιδιωτικές πληροφορίες στο διαδίκτυο αλλά ότι έτσι κι αλλιώς μας παρακολουθούν[1389] και, τέλος, σε μία απάντηση ο συμμετέχων στην έρευνα αναφέρει ότι δεν κινδυνεύει[1390].

β. Αποδέχεστε την ελεύθερη κυκλοφορία στο διαδίκτυο μίας ταινίας ή ενός βιβλίου 2 ημέρες μετά την πρώτη κυκλοφορία του;

(κλειστού τύπου ερώτηση)



Ναί **32** 67%

Όχι **16** 33%

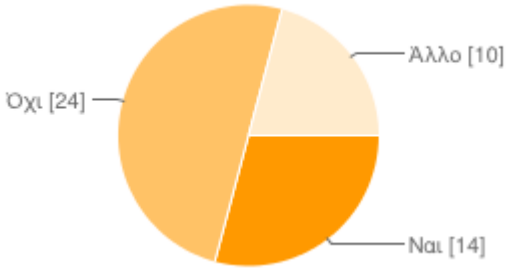
Όπως βλέπουμε ανωτέρω, οι 2 στους τρεις hackers, πιστοί στην ελευθερία της πληροφορίας στο διαδίκτυο, αποδέχονται την κυκλοφορία ενός πνευματικού έργου

[1386] Στα ερωτηματολόγια υπ' αρ. 7, 11, 13, 18, 43.
[1387] Στο ερωτηματολόγιο υπ' αρ. 7.
[1388] Στο ερωτηματολόγιο υπ' αρ. 18.
[1389] Στο ερωτηματολόγιο υπ' αρ. 11.
[1390] Στο ερωτηματολόγιο υπ' αρ. 43.

στο διαδίκτυο σε χρόνο κατά τον οποίο θίγονται αμεσότατα και σε χρονικό επίπεδο τα δικαιώματα των δημιουργών. Ωστόσο, σημαντικό είναι και το ποσοστό του 33% που καταγράφει ανωτέρω τη διαφωνία του.

<u>Ερώτηση 7</u>: Πιστεύετε ότι μια αυστηρή νομοθεσία αποτρέπει από ενέργειες hacking;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Ναι **14** 29%

Όχι **24** 50%

Άλλο **10** 21%

Αφού ήδη είδαμε ότι η ισχύουσα νομοθεσία δεν αποτελεί ιδιαίτερο ανασχετικό παράγοντα στους hackers για τη δράση τους, οι απαντήσεις στην ερώτηση αυτή θα καταδείξουν ποια η στάση των hackers απέναντι σε μια αυστηρή νομοθεσία και αν αυτή θα δρούσε ανασχετικά στην παράνομη ή όχι δράση τους. Ακριβώς οι μισοί από τους συμμετέχοντες στην έρευνα δηλώνουν ότι δεν θα σταματούσαν ένεκα μιας αυστηρής νομοθεσίας, ενώ το σημαντικό ποσοστό του 29% δηλώνει ότι θα αποτρεπόταν αν ίσχυε μια αυστηρή νομοθεσία.

Σε 10 περιπτώσεις επελέγη η απάντηση «Άλλο»[1391]. Οι 2 από αυτές τις απαντήσεις αναφέρουν ότι μια αυστηρότερη νομοθεσία θα απέτρεπε από ενέργειες hacking τους ανηλίκους αλλά όχι το οργανωμένο έγκλημα[1392] ή αυτούς που βγάζουν χρήματα[1393] (παραπέμποντας στην τελευταία περίπτωση ευθέως στις θεωρίες ορθολογικής επιλογής). Στις υπόλοιπες περιπτώσεις αναφέρονται ως απαντήσεις το ότι η νομοθεσία δεν σχετίζεται με το hacking[1394], ότι το hacking δεν περιορίζεται με νόμους[1395], ότι είναι θέμα του θύτη[1396] και ότι εξαρτάται από το τί κάνει ο hacker κάθε φορά[1397]. Σε μια από τις απαντήσεις προκύπτει ότι μια αυστηρή νομοθεσία δεν θα απέτρεπε από ενέργειες hacking[1398] (άρα, αν προστεθεί και αυτή η απάντηση στις ανωτέρω το σχετικό ποσοστό μετατρέπεται σε 52,08%). Τέλος, ένας συμμετέχων αναφέρει ότι δεν γνωρίζει καλά τους νόμους[1399] και σε έτερη απάντηση ζητείται η διευκρίνιση του όρου «ενέργειες hacking»[1400]. Κλείνοντας, η απάντηση αυτή σε ένα ερωτηματολόγιο έχει αφεθεί κενή[1401].

<u>Ερώτηση 8</u>: Τι είκονα νομίζετε ότι έχει ο μέσος έλληνας (γνώστης περί του φαινομένου του hacking) για τους hackers;

(ανοικτού τύπου ερώτηση)

Η ερώτηση αυτή προσπαθεί να αναγνωρίσει αν οι hackers διακρίνουν και με ποιον τρόπο την ετικετοποίησή τους. Οι 6 εξ αυτών[1402] (ποσοστό 12,5 %) επισημαίνουν ότι ο μέσος έλληνας αποδίδει στους hackers ιδιότητες των crackers ή των black hat hackers και σε 4 απαντήσεις (ποσοστό 8,33 %) προκύπτει ότι η εικόνα που υπάρχει

[1391] Στα ερωτηματολόγια υπ' αρ. 2, 4, 7, 11, 14, 18, 24, 31, 44, 47.
[1392] Στο ερωτηματολόγιο υπ' αρ. 11.
[1393] Στο ερωτηματολόγιο υπ' αρ. 14.
[1394] Στο ερωτηματολόγιο υπ' αρ. 4.
[1395] Στο ερωτηματολόγιο υπ' αρ. 24.
[1396] Στο ερωτηματολόγιο υπ' αρ. 18.
[1397] Στο ερωτηματολόγιο υπ' αρ. 31.
[1398] Στο ερωτηματολόγιο υπ' αρ. 7.
[1399] Στο ερωτηματολόγιο υπ' αρ. 47.
[1400] Στο ερωτηματολόγιο υπ' αρ. 2
[1401] Στο ερωτηματολόγιο υπ' αρ. 44.
[1402] Στα ερωτηματολόγια υπ' αρ. 2, 4, 15, 16 (στο οποίο αναφέρεται ότι η εικόνα για τους hackers είναι ότι είναι «*σατανικοί*» και «*καταστροφή του κόσμου*»), 24, 31.

για τους hackers είναι ότι κερδίζουν χρήματα ή ότι έχουν αυτή τη δυνατότητα[1403]. Επίσης, σε 6 απαντήσεις (ποσοστό 12,5 %) εμφαίνεται ότι η άποψη της κοινής γνώμης είναι εσφαλμένη[1404] και σε άλλες 5 απαντήσεις[1405] (ποσοστό 10,42%) ότι ο μέσος έλληνας δεν έχει ιδέα. Σε άλλη δέσμη απαντήσεων, ανιχνεύεται η αντίληψη ότι μάλλον δεν υπάρχει άποψη του μέσου έλληνα και ότι αυτή διαμορφώνεται ανάλογα με τις γνώσεις του (4 απαντήσεις[1406] - ποσοστό 8,33 %) καθώς και το ότι όσοι δεν ασχολούνται είναι μπερδεμένοι επειδή τα μέσα μαζικής ενημέρωσης ψεύδονται αναφορικά με τους hackers[1407] [1408]. Μόλις 3 hackers[1409] (ποσοστό 6,25 %) παραδέχονται ότι ο μέσος έλληνας έχει κακή εικόνα για τους hackers και σε άλλες 3 απαντήσεις (ποσοστό 6,25 %), μάλιστα, οι συμμετέχοντες αποδέχονται ότι τους θεωρούν περίεργους και μανιώδεις χρήστες των ηλεκτρονικών υπολογιστών[1410]. Σε μία ακόμη απάντηση θεωρείται ότι η εικόνα είναι αυτή της κολεκτίβας "Anonymous"[1411]. Στα ερωτηματολόγια υπάρχουν και απαντήσεις hackers που πιστεύουν ότι ο μέσος έλληνας έχει καλή εικόνα για αυτούς: σε 4 απαντήσεις[1412] (ποσοστό 8,33 %) οι συμμετέχοντες hackers πιστεύουν ότι τους θεωρούν επαναστάτες που στοχεύουν να αλλάξουν τον κόσμο με μεθόδους αντίδρασης του μέλλοντος και προστάτες των δικαιωμάτων, ότι τους θεωρούν έξυπνους[1413] και τους έχουν για «Θεούς»[1414] και ότι τους αντιμετωπίζουν απλώς ως χρήστες του internet με μεγαλύτερη εμπειρία[1415]. Τέλος, επισημαίνεται ότι άλλοι τους θεωρούν εγκληματίες

[1403] Στα ερωτηματολόγια υπ' αρ. 3, 7, 11, 13.

[1404] Στα ερωτηματολόγια υπ' αρ. 7 (αναφέρεται ότι οι hackers έχουν «*μυθοποιηθεί*», 13, 18 (ότι «*χακάρουν social media*», 22, 24, 27 (εσφαλμένη γιατί πιστεύει ότι hacking γίνεται μόνο ηλεκτρονικά).

[1405] Στα ερωτηματολόγια υπ' αρ. 29, 32, 33, 44, 45.

[1406] Στα ερωτηματολόγια υπ' αρ. 12, 17, 23 (ότι παρουσιάζεται από «*ταινίες*»), 42.

[1407] Στο ερωτηματολόγιο υπ' αρ. 48.

[1408] Χαρακτηριστικά, επαναλαμβάνεται ότι ο όρος cracker δημιουργήθηκε από τους hackers προκειμένου να διαχωριστούν με αφορμή την υπερβολική και εσφαλμένη χρήση του όρου hacker από τους δημοσιογράφους! [*Christian S. Fötinger & Wolfgang Ziegler*, Understanding a hacker's mind – A psychological insight into the hijacking of identities, White Paper by the Danube-University Krems, Austria, p. 9 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf)].

[1409] Στα ερωτηματολόγια υπ' αρ. 14, 41 και 47 (αναφέρεται ότι θεωρούνται «*σύγχρονη απειλή*» και ότι συνδέονται με την «*τρομοκρατία*»).

[1410] Στα ερωτηματολόγια υπ' αρ. 19 («*oti einai nerds kai kollimenoi me ta pcs*»), 20 («*περίεργοι*») και 34 («*ΟΤΙ ΕΙΝΑΙ ΚΑΤΙ ΤΥΠΟΙ ΜΕ ΓΥΑΛΙΑ ΚΑΙ ΣΠΥΡΑΚΙΑ ΠΟΥ ΚΑΘΟΝΤΑΙ ΟΛΗ ΜΕΡΑ ΜΠΡΟΣΤΑ ΣΤΟ ΚΟΜΠΙΟΥΤΕΡ*»).

[1411] Στο ερωτηματολόγιο υπ' αρ. 37.

[1412] Στα ερωτηματολόγια υπ' αρ. 25, 30, 35 και 39.

[1413] Στο ερωτηματολόγιο υπ' αρ. 26.

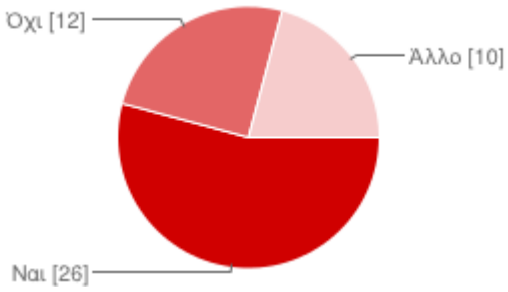
[1414] Στο ερωτηματολόγιο υπ' αρ. 28.

[1415] Στο ερωτηματολόγιο υπ' αρ. 5.

και άλλοι «καλούς»[1416] ή ότι αγαπούν τη χώρα τους[1417] καθώς και ότι δεν είναι όλοι ίδιοι[1418]. Κλείνοντας, δεν προκύπτει σαφής απάντηση σε 6 ερωτηματολόγια[1419], σε 2 ερωτηματολόγια η απάντηση ήταν «*Δεν ξέρω*»[1420] και σε 1 ερωτηματολόγιο δεν έχει δοθεί απάντηση[1421].

<u>Ερώτηση 9</u>: Η Πολιτεία πρέπει να θέτει όρια στο hacking;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Ναι **26** 54%

Όχι **12** 25%

Άλλο **10** 21%

Η εν λόγω ερώτηση είναι καίρια γιατί καταδεικνύει την αναγνώριση της Πολιτείας ως ρυθμιστικού πόλου στην ελευθερία της πληροφορίας και στη χρήση των συστημάτων πληροφοριών εκ μέρους των hackers. Τεράστια εντύπωση προκαλεί το γεγονός ότι το 54% των hackers που συμμετείχαν στην έρευνα (απο)δέχονται την Πολιτεία ως

[1416] Στο ερωτηματολόγιο υπ' αρ. 8.
[1417] Στο ερωτηματολόγιο υπ' αρ. 6 – ο απαντών φαίνεται ότι ανήκει στην GHS.
[1418] Στα ερωτηματολόγια υπ' αρ. 40 και 47.
[1419] Στα ερωτηματολόγια υπ' αρ. 1, 9, 21, 40, 43 και 46.
[1420] Στα ερωτηματολόγια υπ' αρ. 36 και 38.
[1421] Ερωτηματολόγιο υπ' αρ. 10.

κατάλληλη να θεσμοθετήσει τα όρια της πρόσβασης στην πληροφορία και, άρα, τα όρια του hacking. Επιπρόσθετα, η αποδοχή αυτή σημαίνει ότι το ποσοστό αυτό παραδέχεται, αρχικά τουλάχιστον, ότι πρέπει να υπάρχουν κάποια όρια στο hacking. Με τα παραπάνω διαφωνεί το 25% των συμμετεχόντων στην έρευνα hackers.

Σε 10 περιπτώσεις επελέγη η απάντηση «Άλλο»[1422]. Οι αναπτύξεις αυτής της απάντησης αναφέρονται στο ότι hacking και cracking δεν είναι το ίδιο[1423] και τελικά ότι εξαρτάται από το αν «*παράγεται*» κάτι παράνομο[1424] αλλά και ανάλογα τον σκοπό και με μέτρο[1425], στο ότι η Πολιτεία δεν έχει σχέση με το hacking[1426] και στο ότι τα όρια πάντα θα παραβιάζονται[1427] καθώς και ότι είναι μάλλον απαραίτητα για να παραβιάζονται(!)[1428]. Συμπληρωματικά, αξίζει να αναφερθούν οι απαντήσεις σύμφωνα με τις οποίες πρέπει να υπάρχουν δομές και άνθρωποι ενήμεροι για τα σημερινά δεδομένα[1429], οι οποίοι θα ασχολούνται σχετικά, προκειμένου η Πολιτεία να εντάξει τις δράσεις του hacking και να απομονώσει τα «*κακά στοιχεία*»[1430]. Τέλος, υποστηρίζεται ότι χρειάζονται όρια σε κάποιες περιπτώσεις[1431] καθώς και ότι η Πολιτεία δεν μπορεί να θέσει όρια στο hacking[1432].

<u>Ερώτηση 10</u>: Σε γενικές γραμμές, ποια είναι η μέχρι τώρα δράση σας και ποιες τεχνικές χρησιμοποιείτε; *(ανοικτού τύπου ερώτηση)*

Η ερώτηση αποτελείται από δύο σκέλη: κατά πρώτον, αναφορικά με τη δράση των hackers και κατά δεύτερον, αναφορικά με τις χρησιμοποιούμενες από αυτούς τεχνικές. Είναι εν μέρει αναμενόμενο ότι κάποιοι εκ των ερωτηθέντων μπορεί να εκλάβουν μερικώς το νόημα της ερώτησης και να απαντήσουν μόνο στο ένα εκ των

[1422] Στα ερωτηματολόγια υπ' αρ. 2, 4, 5, 7, 13, 14, 15, 18, 20 και 27.
[1423] Στο ερωτηματολόγιο υπ' αρ. 2.
[1424] Στο ερωτηματολόγιο υπ' αρ. 27.
[1425] Στο ερωτηματολόγιο υπ' αρ. 14.
[1426] Στο ερωτηματολόγιο υπ' αρ. 4.
[1427] Στο ερωτηματολόγιο υπ' αρ. 5.
[1428] Στο ερωτηματολόγιο υπ' αρ. 18.
[1429] Στο ερωτηματολόγιο υπ' αρ. 7.
[1430] Στο ερωτηματολόγιο υπ' αρ. 13.
[1431] Στο ερωτηματολόγιο υπ' αρ. 15.
[1432] Στο ερωτηματολόγιο υπ' αρ. 20.

δύο σκελών – σε κάθε περίπτωση, όμως, η ερώτηση τέθηκε ως ανοικτού τύπου προκειμένου να δοθεί περιθώριο στους hackers να αναπτύξουν τη σκέψη τους και την άποψή τους, λαμβανομένου υπόψη ότι αρκετές φορές δράση και τεχνικές αποτελούν παραπληρωματικές ή αλληλοεξαρτώμενες έννοιες, και έπειτα μέσω της ποιοτικής ανάλυσης να ανιχνευθούν ενδιαφέροντα ερευνητικά δεδομένα.

Αναφορικά, επομένως, αρχικά με τη δράση των hackers, άξιες μνείας απαντήσεις είναι αυτές οι οποίες αναφέρονται σε πρόσβαση σε δεδομένα[1433] και κλειδωμένες πληροφορίες[1434], σε «χτυπήματα» σε ιστοσελίδες[1435] κυβερνητικού περιεχομένου[1436] καθώς και κρατών εχθρικών με την Ελλάδα[1437] και καταστροφή ιστοσελίδων[1438]. Περαιτέρω, εντύπωση προκαλεί η απάντηση κατά την οποία ο hacker υποστηρίζει ότι δεν επιτίθεται σε «μεγάλες» ιστοσελίδες γιατί καταλαβαίνει ότι έχουν δοθεί πολλά χρήματα για την κατασκευή αυτών των ιστοσελίδων[1439] και οι απαντήσεις που αναφέρονται σε μικρή και ασήμαντη δραστηριότητα[1440]. Επιπρόσθετα, υπάρχουν απαντήσεις οι οποίες είναι γεγονός ότι δεν αναφέρονται ειδικότερα σε χωρίς δικαίωμα πρόσβαση σε δεδομένα και οι οποίες ίσως έχουν θετικό αντίκτυπο όπως π.χ. η ανάπτυξη προγραμματιστικών εφαρμογών[1441], το bio-hacking[1442], η βελτίωση «προϊόντων»[1443], η ρομποτική και οι μετατροπές συσκευών[1444] - σε μία απάντηση,

[1433] Στο ερωτηματολόγιο υπ' αρ. 1.

[1434] Στο ερωτηματολόγιο υπ' αρ. 42.

[1435] Βλ. π.χ. στα ερωτηματολόγια υπ' αρ. 7 και 13.

[1436] Στα ερωτηματολόγια υπ' αρ. 22 και 25.

[1437] Βλ. π.χ. στο ερωτηματολόγιο υπ' αρ. 32.

[1438] Στο ερωτηματολόγιο υπ' αρ. 35.

[1439] Στο ερωτηματολόγιο υπ' αρ. 6.

[1440] Στα ερωτηματολόγια υπ' αρ. 8 («*Η μέχρι τώρα δράση μου είναι σχετικά ασήμαντη σε σύγκριση με το τι σχεδίαζα να κάνω στο παρελθόν. Λόγω έλλειψης χρόνου, η δράση μου περιορίστηκε σε πολύ μικρό επίπεδο όσο και αν προσπαθούσα να την επεκτείνω*») και 16.

[1441] Στο ερωτηματολόγιο υπ' αρ. 4.

[1442] Στο ερωτηματολόγιο υπ' αρ. 27.

[1443] Στο ερωτηματολόγιο υπ' αρ. 2.

[1444] Στο ερωτηματολόγιο υπ' αρ. 13 – ολόκληρη η ενδιαφέρουσα απάντηση στο εν λόγω ερωτηματολόγιο έχει ως εξής: «*Η δράση μου περιλαμβάνει bots σε δίκτυα, sniffing δικτύων οργανισμών και οτιδήποτε μου κινεί το ενδιαφέρον και μπορώ να πάρω πρόσβαση, χτυπήματα σε πολιτικά sites, επιθέσεις σε τούρκικα και σκοπιανικά sites μαζίκες επιθέσεις, εισχώρηση σε μεγάλα sites παγκοσμοίος, μπαίνω σε διάφορες σελίδες, φορτώνω κώδικα ο οποίος παιρνάει στους χρήστες και τους έχω ως bots και δεν με απασχολούν τα αρχεία των χρηστών αλλά τα bots σαν επεξεργαστική δύναμη για κάποια πράγματα που κάνω, parallel cracking (σπάσιμο κωδικοποιημένων κωδικών) κ.ά. τεχνικές είναι αναλόγως την κάθε περίπτωση, exploits είτε από το ίντερνετ είτε δικα μου, είτε από το ίντερνετ που τα τροποποιώ και τα κάνω καλύτερα, bots, password cracking, exploiting sql, overflows, phishing, reverse, remote file inclusion διάφορα. επίσης πέρα από web hacking ασχολούμαι και με άλλου είδους χάκινγκ, ρομποτική, μετατροπές σε συσκευές κ.λπ.*».

μάλιστα, ο συμμετέχων στην έρευνα hacker αναφέρεται σε white hat hacking[1445]. Επίσης, σε μία απάντηση ο hacker αναφέρει το ότι βλέπει το πώς λειτουργούν τα συστήματα[1446], άλλος ένας hacker (γυναίκα) απαντάει ότι του αρέσει να μπαίνει οπουδήποτε απαγορεύεται και να κοιτάει[1447] και τρίτος hacker (γυναίκα και εδώ) αναφέρει ότι αποκτά παράνομη πρόσβαση σε σελίδες της ιστοσελίδας κοινωνικής δικτύωσης facebook.com[1448]. Οι δύο τελευταίες απαντήσεις μάλλον δείχνουν ότι η γυναικεία φύση ρέπει ίσως περισσότερο προς την περιέργεια να ανιχνεύσει και να εξερευνήσει δεδομένα στα οποία δεν επιτρέπεται η πρόσβαση από το να ακολουθήσει πιο δημιουργικές δραστηριότητες του hacking (π.χ. δημιουργία προγραμμάτων). Τέλος, αναφορικά με την επεξεργασία αυτού του σκέλους υπάρχουν απαντήσεις στις οποίες ο συμμετέχων δηλώνει ότι δεν αναφέρει τη δράση του[1449] και σε μία απάντηση ότι δεν πρέπει να αναφέρει τη δράση του[1450].

Σχετικά με τις χρησιμοποιούμενες από τους hackers τεχνικές, οι περισσότερες από αυτές που αναφέρονται είναι οι αναλυθείσες σε προηγούμενο κεφάλαιο της παρούσας[1451] (π.χ. sql injection[1452], exploits[1453], sniffers[1454], Trojan horses και joomla bugs[1455], phising[1456] και pharming[1457], dumpster diving[1458], social engineering[1459], vulnerability και penetration testing[1460], virus[1461], DoS και DDoS attacks[1462]). Απαντήσεις άξιες μνείας είναι μία στην οποία αναφέρεται ως τεχνική η ευγένεια[1463] καθώς ότι έτερος hacker χρησιμοποιεί γνωστές αλλά και μη γνωστές τεχνικές[1464]

[1445] Στο ερωτηματολόγιο υπ' αρ. 28.
[1446] Στο ερωτηματολόγιο υπ' αρ. 24.
[1447] Στο ερωτηματολόγιο υπ' αρ. 34.
[1448] Στο ερωτηματολόγιο υπ' αρ. 20.
[1449] Στα ερωτηματολόγια υπ' αρ. 17, 23, 30, 31, 43 και 47.
[1450] Στο ερωτηματολόγιο υπ' αρ. 48.
[1451] Βλ. κεφάλαιο 2 παράγραφος 2.11.
[1452] Βλ. ενδεικτικά τα ερωτηματολόγια υπ' αρ. 11, 12, 14, 17.
[1453] Βλ. ενδεικτικά τα ερωτηματολόγια υπ' αρ. 11, 13, 14.
[1454] Βλ. π.χ. στο ερωτηματολόγιο υπ' αρ. 26.
[1455] Βλ. το ερωτηματολόγιο υπ' αρ. 39.
[1456] Βλ. ενδεικτικά ερωτηματολόγια υπ' αρ. 9 και 21.
[1457] Βλ. το ερωτηματολόγιο υπ' αρ. 29.
[1458] Ερωτηματολόγια υπ' αρ. 21 και 29.
[1459] Βλ. ερωτηματολόγια υπ' αρ. 19, 29, και 34.
[1460] Βλ. ερωτηματολόγια υπ' αρ. 8, 26, 35, 37, 38, 41 και 45.
[1461] Βλ. ερωτηματολόγιο υπ' αρ. 40.
[1462] Βλ. ερωτηματολόγια 9, 22, 32, 40.
[1463] Στο ερωτηματολόγιο υπ' αρ. 2.
[1464] Στο ερωτηματολόγιο υπ' αρ. 7.

αλλά και ότι χρησιμοποιούνται διάφορες τεχνικές[1465] (συνδυασμός, δηλαδή, τεχνικών). Υπάρχουν αρκετές απαντήσεις (7 απαντήσεις – ποσοστό 14,58%) στις οποίες οι hackers δεν θέλουν να αναφέρουν ποιες τεχνικές χρησιμοποιούν[1466] και σε μία απάντηση ο hacker αναφέρει ότι «δεν πρέπει» να απαντήσει[1467].

<u>Ερώτηση 11</u>: Τι συμβουλές θα δίνατε σε ένα χρήστη διαδικτύου ως προς την ασφάλεια των δεδομένων του;

(ανοικτού τύπου ερώτηση)

Οι περισσότερες απαντήσεις σε επίπεδο συμβουλών για την ασφάλεια του διαδικτύου έχουν να κάνουν με την ιδιαίτερη προσοχή που πρέπει να επιδεικνύει ο ίδιος ο χρήστης ηλεκτρονικών συσκευών σε δίκτυο, οι οποίες, βέβαια, αναλύονται σε προσοχή στο σε ποιους ιστότοπους δίνει προσωπικά του στοιχεία[1468], προσοχή στο ποια προγράμματα εγκαθιστά ή ποια αρχεία «κατεβάζει»[1469] και ακόμη και προσοχή γενικότερα σε τέτοιο βαθμό που να επιδεικνύουν ιδιαίτερη επιμέλεια αναφορικά ακόμη και με το πού κάνουν «κλικ» (πού επιλέγουν δηλαδή να περιηγηθούν στο διαδίκτυο) καθώς και να κάνουν logout (να αποσυνδέουν, δηλαδή, τον προσωπικό τους λογαριασμό) όταν έχουν συνδεθεί σε υπολογιστή στον οποίο μπορεί να έχουν και άλλα άτομα πρόσβαση[1470]. Επισημαίνεται, εξάλλου, ότι ακόμη και ο «καλύτερος φίλος» μπορεί να αποδειχθεί «εχθρός»[1471]. Η προσοχή των χρηστών πρέπει, επίσης, να συνίσταται (σύμφωνα με τις συμβουλές των ίδιων των hackers) στο να μην αποκαλύπτουν τους κωδικούς τους (και να μην τους σημειώνουν βέβαια σε σημεία από τα οποία μπορούν να τα διαβάσουν και άλλοι – π.χ. χαρτάκια που μπορεί να χαθούν, κινητό τηλέφωνο κ.λπ.)[1472], στο να κρατούν φυλαγμένα τα δεδομένα τους και να προσέχουν τί αποκαλύπτουν και σε ποιον[1473], στο να μη χρησιμοποιούν παντού

[1465] Βλ. τα ερωτηματολόγια υπ' αρ. 3 και 18.
[1466] Βλ. τα ερωτηματολόγια υπ' αρ. 15, 23, 25, 29, 31, 43 και 47.
[1467] Στο ερωτηματολόγιο υπ' αρ. 48.
[1468] Στα ερωτηματολόγια υπ' αρ. 4, 17, 27, 28.
[1469] Στα ερωτηματολόγια υπ' αρ. 4, 5, 28, 29.
[1470] Στα ερωτηματολόγια υπ' αρ. 6, 7, 8, 11, 12, 13, 14.
[1471] Στο ερωτηματολόγιο υπ' αρ. 28.
[1472] Στα ερωτηματολόγια υπ' αρ. 20, 34, 37, 38, 44, 46.
[1473] Στα ερωτηματολόγια υπ' αρ. 19 και 40.

τον ίδιο κωδικό αριθμό (password)[1474], στο να αλλάζουν συχνά τους κωδικούς τους[1475] αυτούς και στο να διατηρούν στο διαδίκτυο μόνο απολύτως απαραίτητα στοιχεία[1476].

Περαιτέρω, σε επίπεδο ενίσχυσης της ασφάλειας με ηλεκτρονικά μέσα και προγράμματα, προτείνεται ως συμβουλή η συνεχής ενημέρωση (update) των προγραμμάτων (προφανώς γιατί σε μεταγενέστερες εκδόσεις των προγραμμάτων «κλείνουν» τα κενά ασφαλείας)[1477]. Επίσης, ως συμβουλές καταγράφονται η χρήση προγραμμάτων ανοιχτού κώδικα[1478], η χρήση εικονικού ιδιωτικού δικτύου (virtual private network - vpn)[1479] ή διακομιστών μεσολάβησης (proxy)[1480] [1481], η προσοχή στα προγράμματα που χρησιμοποιούνται[1482], η γνώση των κενών ασφαλείας της σελίδας του[1483] και η απόκτηση γνώσεων προγραμματισμού[1484]. Προς αυτήν την κατεύθυνση, βέβαια, υπάρχουν 4 απαντήσεις στις οποίες καταγράφεται η άποψη ότι ο απλός χρήστης δεν μπορεί να κάνει τίποτα και ότι μόνο ο προγραμματιστής (με ειδικές γνώσεις για τα ηλεκτρονικά προγράμματα και τα συστήματα πληροφοριών) μπορεί με κάποιο τρόπο να αμυνθεί[1485] και για αυτόν τον λόγο καταγράφεται και ως συμβουλή το να απευθύνεται ο χρήστης σε ειδικούς (προγραμματιστές) για να ενισχύσει την ασφάλεια των δεδομένων του πριν αυτά κινδυνεύσουν[1486].

[1474] Στο ερωτηματολόγιο υπ' αρ. 14.

[1475] Στο ερωτηματολόγιο υπ' αρ. 12.

[1476] Στα ερωτηματολόγια υπ' αρ. 21, 39 και 47.

[1477] Στο ερωτηματολόγιο υπ' αρ. 8.

[1478] Στο ερωτηματολόγιο υπ' αρ. 2.

[1479] Για το εικονικό ιδιωτικό δίκτυο βλ. σχετικό λήμμα ηλεκτρονικής εγκυκλοπαίδειας «Βικιπαιδεία» στο url: http://el.wikipedia.org/wiki/%CE%95%CE%B9%CE%BA%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF. Βλ. παραδείγματα vpn του ΕΚΠΑ στο url: http://www.noc.uoa.gr/syndesh-sto-diktyo/eikoniko-idiwtiko-diktyo-vpn.html και του ΕΜΠ στο url: http://www.noc.ntua.gr/index.php?module=ContentExpress&file=index&func=display&ceid=165&meid=174.

[1480] Για τους διακομιστές μεσολάβησης βλ. σχετικό λήμμα ηλεκτρονικής εγκυκλοπαίδειας «Βικιπαιδεία» στο url: http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%BA%CE%BF%CE%BC%CE%B9%CF%83%CF%84%CE%AE%CF%82_%CE%BC%CE%B5%CF%83%CE%BF%CE%BB%CE%AC%CE%B2%CE%B7%CF%83%CE%B7%CF%82.

[1481] Στο ερωτηματολόγιο υπ' αρ. 9.

[1482] Στο ερωτηματολόγιο υπ' αρ. 41.

[1483] Στο ερωτηματολόγιο υπ' αρ. 21.

[1484] Στο ερωτηματολόγιο υπ' αρ. 48.

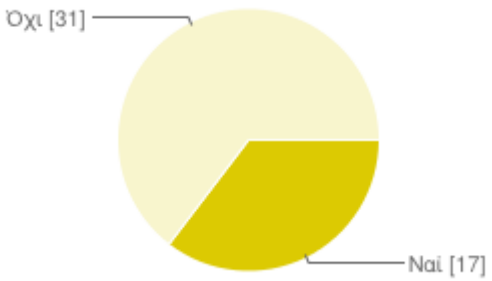
[1485] Στα ερωτηματολόγια υπ' αρ. 22, 26, 31 και 45.

[1486] Στο ερωτηματολόγιο υπ' αρ. 33.

Έχουν δοθεί απαντήσεις σύμφωνα με τις οποίες δεν υπάρχει ασφάλεια στο διαδίκτυο[1487] αφού «ό,τι κρυπτογραφείται αποκρυπτογραφείται»[1488] και, συνεπώς, θα υπάρχουν παντού και πάντα ευπάθειες[1489]. Τέλος, καταγράφεται η άποψη ότι αν δεν θέλει κάποιος να κινδυνεύει θα πρέπει να μην εκμεταλλεύεται τους αδύναμους[1490] και να εκτιμά τους hackers (προκειμένου, μάλλον, να μη γίνεται στόχος από αυτούς)[1491] και, επίσης, ότι «το μυαλό σώζει» και όχι τα προγράμματα που εγγυώνται ασφάλεια (π.χ. antivirus)[1492]. Κλείνοντας, σε δύο απαντήσεις δεν δίνεται καμία συμβουλή γιατί θεωρείται πως ό,τι υπάρχει στο διαδίκτυο είναι κοινό[1493], σε τρεις περιπτώσεις δεν προκύπτει απάντηση στην ερώτηση[1494] και σε τρία ερωτηματολόγια δεν έχει καν συμπληρωθεί η απάντηση[1495].

<u>Ερώτηση 12</u>: Θεωρείτε τον εαυτό σας χακτιβιστή;

(κλειστού τύπου ερώτηση)



Ναί **17** 35%

Όχι **31** 65%

[1487] Στο ερωτηματολόγιο υπ' αρ. 24.
[1488] Στο ερωτηματολόγιο υπ' αρ. 15.
[1489] Στο ερωτηματολόγιο υπ' αρ. 18.
[1490] Στα ερωτηματολόγια υπ' αρ. 35 και 43.
[1491] Στο ερωτηματολόγιο υπ' αρ. 2.
[1492] Στο ερωτηματολόγιο υπ' αρ. 8.
[1493] Στα ερωτηματολόγια υπ' αρ. 23 και 31.
[1494] Στα ερωτηματολόγια υπ' αρ. 3, 16, και 32.
[1495] Ερωτηματολόγια υπ' αρ. 10, 36 και 42.

Φαίνεται ότι περίπου 1 στους 3 hackers συμμετέχοντες στην έρευνα (ποσοστό 35%) θεωρεί ότι η δράση του εντάσσεται και συγγενεύει με τις δράσεις που περιγράφονται ως χακτιβισμός[1496]. Το υπόλοιπο 65% δεν συνδέει τη δράση του με το εν λόγω κίνημα, τις αρχές και τους στόχους του.

<u>Ερώτηση 13</u>: Ποια η γνώμη σας για τους "Anonymous";

(ανοικτού τύπου ερώτηση)

Οι περισσότεροι hackers έχουν γνώμη αναφορικά με τους "Anonymous" καθώς είναι ίσως η πιο γνωστή κολεκτίβα – ομάδα hackers των τελευταίων χρόνων με σημαντικές δράσεις και "χτυπήματα"[1497]. Θετική γνώμη για τη δράση τους έχουν αρκετοί hackers[1498] και τους υποστηρίζουν[1499] (σε δύο, μάλιστα, απαντήσεις χρησιμοποιείται ως απάντηση το σύνθημα των "Anonymous" "justice is coming"[1500]) ή έχουν συνεργαστεί[1501] μαζί τους καθώς θεωρείται ότι συμβάλλουν στην αφύπνιση του λαού και στη διαμαρτυρία[1502] και ότι προσπαθούν να βοηθήσουν[1503]. Πάντως, καταγράφεται και η άποψη ότι υπάρχει προσδοκία για περισσότερες δράσεις εκ μέρους τους[1504].

Ωστόσο, είναι, επίσης, αρκετές και σημαντικές οι απαντήσεις που προσεγγίζουν τους "Anonymous" τουλάχιστον κριτικά. Καταρχάς, καταγράφεται η άποψη ότι δεν έχουν κακές προθέσεις αλλά δίνουν πολλές υποσχέσεις[1505] και ότι κάνουν μεν κριτική στο σύστημα, δεν επιλαμβάνονται, όμως, με τη διαγραφή χρεών από τραπεζικά

[1496] Βλ. παράγραφο 2.9.2 του παρόντος πονήματος.

[1497] Για την κολεκτίβα των "Anonymous" πρβλ. *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756.

[1498] Βλ. ερωτηματολόγια υπ' αρ. 6, 21, 22, 42, 44, 47.

[1499] Βλ. ερωτηματολόγια υπ' αρ. 8, 25, 32, 35, 36, 40, 43.

[1500] Στα ερωτηματολόγια υπ' αρ. 40 και 43.

[1501] Στο ερωτηματολόγιο υπ' αρ. 28.

[1502] Ερωτηματολόγια υπ' αρ. 6 και 16.

[1503] Στο ερωτηματολόγιο υπ' αρ. 5.

[1504] Στο ερωτηματολόγιο υπ' αρ. 43.

[1505] Στο ερωτηματολόγιο υπ' αρ. 1.

ιδρύματα[1506]. Σε δύο απαντήσεις οι hackers τονίζουν την ενασχόληση της κολεκτίβας αυτής με την πολιτική σε αντίθεση με τους ίδιους[1507] και σε τρεις απαντήσεις υποστηρίζεται το ότι οι "Anonymous" χρησιμοποιούν το hacking για πολιτικούς λόγους[1508]. Μάλιστα, σε μία εξ αυτών των απαντήσεων υποστηρίζεται ότι τελικώς δημιουργούν μεγαλύτερο πρόβλημα σε σύγκριση με την όποια θετική τους συνεισφορά γιατί δεν φέρνουν αποτέλεσμα[1509] - αντίστοιχα, έτερος hacker απαντά ότι δημιουργούν πρόβλημα στο hacking γιατί ο κόσμος τους φοβάται[1510].

Υπάρχουν, άρα, και αρνητικές προσεγγίσεις των hackers για τους "Anonymous". Καταρχάς, σε 3 απαντήσεις καταγράφεται ρητή διαφωνία[1511]. Ειδικότερα, υποστηρίζεται ότι δεν σχετίζονται με το hacking[1512] και ότι, ακόμη περισσότερο, είναι κατά κάποιον τρόπο «εγκάθετοι» του συστήματος προκειμένου να δικαιολογείται η λήψη αυστηρότερων μέτρων ελέγχου του διαδικτύου[1513]. Επικρίνονται, δε, σε 4 απαντήσεις για το γεγονός ότι χρησιμοποιούν ως τεχνική τις επιθέσεις DDoS, κάτι το οποίο – όπως υποστηρίζουν κάποιοι από τους συγκεκριμένους απαντώντες – δεν είναι hacking[1514] (μάλλον θεωρώντας το hacking μοναχά πρόσβαση σε συστήματα πληροφοριών). Επιπρόσθετα, υπάρχει η άποψη ότι αρκετοί «κρύβονται» πίσω από την ετικέτα των "Anonymous" για να κάνουν επιθέσεις χωρίς να αποκαλυφθεί η ταυτότητά τους[1515] καθώς και ότι οι "Anonymous" «δεν είναι τίποτα»[1516]. Σε άλλες δύο περιπτώσεις οι συμμετέχοντες απάντησαν ότι οι "Anonymous" τους είναι αδιάφοροι[1517].

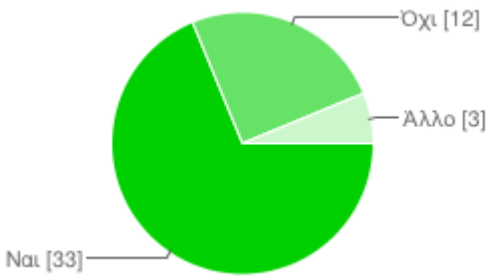
Τέλος, καταγράφονται δύο σχόλια τα οποία αναφέρουν ότι «*η μάσκα έχει πλάκα*»[1518] [1519] αλλά και το σχόλιο ότι οι "Anonymous" είναι «τα καλύτερα παιδιά»[1520] (χωρίς να

[1506] Στο ερωτηματολόγιο υπ' αρ. 19.
[1507] Στα ερωτηματολόγια υπ' αρ. 30 και 34.
[1508] Στα ερωτηματολόγια υπ' αρ. 24, 27 και 31.
[1509] Στο ερωτηματολόγιο υπ' αρ. 31.
[1510] Στο ερωτηματολόγιο υπ' αρ. 37.
[1511] Στα ερωτηματολόγια υπ' αρ. 2, 12 (όπου αναφέρεται ο χαρακτηρισμός «*χάλια*») και 41 (υποστηρίζεται ότι οι "Anonymous" κάνουν cracking).
[1512] Στα ερωτηματολόγια υπ' αρ. 13, 17 και 18.
[1513] Στα ερωτηματολόγια υπ' αρ. 14, 29 και 38.
[1514] Βλ. τα ερωτηματολόγια υπ' αρ. 7, 11, 14, 17.
[1515] Στο ερωτηματολόγιο υπ' αρ. 9.
[1516] Στο ερωτηματολόγιο υπ' αρ. 11 (χρησιμοποιείται, μάλιστα, ο χαρακτηρισμός «*μπαρούφα*»).
[1517] Στα ερωτηματολόγια υπ' αρ. 4 και 7.
[1518] Στα ερωτηματολόγια υπ' αρ. 20 και 26.

μπορεί να ανιχνευθεί αν ο ερωτώμενος κυριολεκτεί ή ειρωνεύεται). Κλείνοντας, σε 2 περιπτώσεις δεν προκύπτει απάντηση[1521], σε 4 περιπτώσεις οι ερωτηθέντες δήλωσαν ότι δεν γνωρίζουν[1522] και ένα ερωτηματολόγιο αφέθηκε κενό[1523].

<u>Ερώτηση 14</u>: Ως hacker χρησιμοποιείτε ψευδώνυμο;

(κλειστού τύπου ερώτηση με επιλογή «Άλλο» για διατύπωση τυχόν διαφορετικής άποψης)



Ναι **33** 69%

Όχι **12** 25%

[1519] Οι "Anonymous" στις δημόσιες εμφανίσεις τους (είτε στο διαδίκτυο είτε σε διαδηλώσεις – όπως περιγράφεται στο σχετικό άρθρο του γράφοντος το οποίο παραπέμπεται ανωτέρω) χρησιμοποιούν μάσκες με τη μορφή του Guy Fawkes (εικόνα εμπνευσμένη από το βιβλίο κόμικ των Alan Moore και David Lloyd της δεκαετίας του 80 «V for Vendetta»). Εξάλλου, οι "Anonymous" εμπνέονται από την ιστορία του Guy Fawkes, ο οποίος προσπάθησε να ανατινάξει το Βρετανικό Κοινοβούλιο στις 5 Νοεμβρίου 1605 και να οργανώσει τη "Συνωμοσία της Πυρίτιδας" ως αντίδραση στην τυραννική βασιλεία του προτεστάντη βασιλιά Ιακώβου Α΄ και στα σκληρά μέτρα του απέναντι στους καθολικούς - για αυτόν τον λόγο η 5η Νοεμβρίου είναι για τους "Anonymous" σημαντική ημερομηνία (πρβλ. για περαιτέρω πληροφορίες το άρθρο της ενημερωτικής ιστοσελίδας www.tvxs.gr με τίτλο "Συνωμοσία της Πυρίτιδας: Remember, remember, the 5th of November", url: http://tvxs.gr/news/%CF%83%CE%B1%CE%BD-%CF%83%CE%AE%CE%BC%CE%B5%CF%81%CE%B1/%CE%B8%CF%85%CE%BC%CE%AE%CF%83%CE%BF%CF%85-%CF%84%CE%B7%CE%BD-5%CE%B7-%CE%BD%CE%BF%CE%B5%CE%BC%CE%B2%CF%81%CE%AF%CE%BF%CF%85-%CF%84%CE%B7-%CF%83%CF%85%CE%BD%CF%89%CE%BC%CE%BF%CF%83%CE%AF%CE%B1-%CF%84%CE%B7%CF%82-%CF%80%CF%85%CF%81%CE%AF%CF%84%CE%B9%CE%B4%CE%B1%CF%82).

[1520] Στο ερωτηματολόγιο υπ' αρ. 15.

[1521] Στα ερωτηματολόγια υπ' αρ. 3 και 23.

[1522] Στα ερωτηματολόγια 33, 39, 45 και 46.

[1523] Ερωτηματολόγιο υπ' αρ. 10.

Άλλο **3** 6%

Η χρήση ψευδώνυμου για τους hackers αποτελεί σε αρκετές περιπτώσεις χαρακτηριστικό στοιχείο της δράσης τους και το όνομα με το οποίο συνήθως αναγνωρίζονται. Ωστόσο, το ψευδώνυμο ουσιαστικά χρησιμοποιείται όταν ο hacker αναπτύσσει μια τρόπον τινά δημόσια δράση – μπορεί, δηλαδή, να δρα και χωρίς ψευδώνυμο σε περιπτώσεις όπου επιδιώκει απλώς να αποκτά χωρίς δικαίωμα πρόσβαση σε δεδομένα χωρίς να το μάθει κανείς. Από τους συμμετέχοντες στην έρευνα hackers το 69% εξ αυτών χρησιμοποιεί ψευδώνυμο και το 25% δεν χρησιμοποιεί ψευδώνυμο. Οι 3 απαντώντες, οι οποίοι επέλεξαν την απάντηση «Άλλο», διευκρινίζουν ότι η χρήση ψευδωνύμου εξυπηρετεί στη συμμετοχή σε Internet Relay Chat (IRC)[1524] [1525] (άρα η απάντηση δύναται να συγκαταλεχθεί στις θετικές απαντήσεις οπότε το αντίστοιχο ποσοστό θα μπορούσε να διαμορφωθεί σε 70,83%) και ότι χρησιμοποιούν ψευδώνυμο ενίοτε (άλλοτε ναι και άλλοτε όχι) και διαφορετικό κάθε φορά[1526] ή «*όπου χρειάζεται*»[1527].

<u>Ερώτηση 15</u>: Τί σημαίνει για εσάς η αναγνώριση και η αποδοχή σας ως hacker από τους υπόλοιπους hackers;

(ανοικτού τύπου ερώτηση)

Σε αυτήν την ερώτηση τα αποτελέσματα φαίνονται μάλλον με μικρότερη διασπορά από ό,τι στις άλλες ερωτήσεις. 17 hackers[1528] (ποσοστό 35,42%) υποστηρίζουν ότι η αναγνώριση και η αποδοχή τους από την κοινότητα των hackers δεν σημαίνει τίποτα για αυτούς. Κάποιοι εξειδικεύουν, δε, τις απαντήσεις τους υποστηρίζοντας ότι

[1524] Αναφορικά με το Internet Relay Chat (IRC) βλ. το σχετικό λήμμα της ηλεκτρονικής εγκυκλοπαίδειας «Βικιπαιδεία» στο url: http://el.wikipedia.org/wiki/Internet_Relay_Chat.

[1525] Στο ερωτηματολόγιο υπ' αρ. 2.

[1526] Στο ερωτηματολόγιο υπ' αρ. 7.

[1527] Στο ερωτηματολόγιο υπ' αρ. 22.

[1528] Στα ερωτηματολόγια υπ' αρ. 1, 7, 8, 11, 12, 13, 14, 17, 18, 19, 23, 24, 25, 29, 37, 39, 47.

σημασία έχει τί (μπορείς να) κάνεις[1529] ή τί μήνυμα περνάς[1530] αλλά και ότι ως hacker πρέπει να σε αναγνωρίζει ο λαός[1531].

Στον αντίποδα, 22 hackers[1532] (ποσοστό 45,83%) επιθυμούν την αποδοχή τους από τους υπόλοιπους hackers για διαφορετικούς όμως λόγους, οι οποίοι ομαδοποιούνται ως εξής: σε 7 απαντήσεις[1533] (ποσοστό 14,58%) ότι προκρίνεται η δυνατότητα συνεργασίας και αλληλοβοήθειας και σε 10 απαντήσεις[1534] (ποσοστό 20,83%) ότι αποτελεί ευχαρίστηση και ικανοποίηση, στις περισσότερες περιπτώσεις ιδίως για το λόγο ότι τους αναγνωρίζουν και τους παραδέχονται[1535]. Επίσης, η αναγνώριση αυτή εκτιμάται ως τίτλος τιμής[1536] και θεωρείται, επίσης, σημαντικό το να είσαι μέλος μια κοινότητας[1537] γιατί «οι αλλαγές γίνονται μαζικά»[1538].

Επιπλέον απαντήσεις έχουν να κάνουν με το ότι δεν τίθεται θέμα αναγνώρισης καθώς προσπαθούν για καλό σκοπό χωρίς αξιώματα[1539] και είναι απλώς συνάδελφοι[1540]. Τέλος, σε μία απάντηση επισημαίνεται ότι κανείς δεν αποκαλεί τον άλλον "hacker"[1541] – συμπεραίνεται, δηλαδή, ότι δεν υπάρχει τέτοιου είδους αναγνώριση- και σε δύο περιπτώσεις ότι είναι προτιμητέα η αναγνώριση ως προγραμματιστή[1542] (δηλαδή στον τομέα που αναπτύσσουν επιβοηθούμενοι από το hacking). Κλείνοντας,

[1529] Ερωτηματολόγια υπ' αρ. 8, 11, και 12.

[1530] Ερωτηματολόγιο υπ' αρ. 7.

[1531] Ερωτηματολόγια υπ' αρ. 1 και 13.

[1532] Στα ερωτηματολόγια υπ' αρ. 4, 5, 6, 9, 16, 20, 21, 22, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 41, 42, 44, 45.

[1533] Στα ερωτηματολόγια υπ' αρ. 4, 5, 9, 22, 33, 34, 44.

[1534] Στα ερωτηματολόγια υπ' αρ. 20, 21, 26, 27, 28, 30, 35, 36, 38, 45.

[1535] Όπως είδαμε ανωτέρω στην έρευνα των *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 77 -78, 47 ερωτηθέντες (7%) κάνουν hacking για να κερδίσουν την αναγνώριση και τον σεβασμό στην ομάδα hacking που ανήκουν ενώ το 6% (45 ερωτηθέντες) κάνουν hacking για να ανέλθουν επίπεδο στην εσωτερική ιεραρχία στην ομάδα hackers στην οποία ανήκουν. Συνολικά, δηλαδή, ποσοστό 13% των hackers έχει καταγραφεί ότι κίνητρό τους για τις ενέργειες hacking είναι σε γενικές γραμμές η αναγνώριση από την ομάδα.

[1536] Στο ερωτηματολόγιο υπ' αρ. 32.

[1537] Στο ερωτηματολόγιο υπ' αρ. 41.

[1538] Ερωτηματολόγιο υπ' αρ. 42.

[1539] Στο ερωτηματολόγιο υπ' αρ. 48.

[1540] Στο ερωτηματολόγιο υπ' αρ. 15.

[1541] Στο ερωτηματολόγιο υπ' αρ. 3.

[1542] Στα ερωτηματολόγια υπ' αρ. 31 και 41.

σε 2 περιπτώσεις δεν προκύπτει σαφής θέση του ερωτώμενου[1543] και σε δύο ερωτηματολόγια η συγκεκριμένη ερώτηση δεν έχει καθόλου απαντηθεί[1544].

7.8.4.2 Συνολική θεώρηση απαντήσεων δείγματος hackers

Στο ερωτηματολόγιο που απάντησαν οι hackers καταγράφονται και απαντήσεις οι οποίες ενδεχομένως να μη μπορούν να χαρακτηριστούν απολύτως αναμενόμενες.

Ειδικότερα, αναφορικά με το ζήτημα της (μη) επίδρασης της ποινικής νομοθεσίας στην ένταση της δραστηριότητας του hacking, όπως αυτο τίθεται στις δύο σχετικές ερωτήσεις υπ' αρ. 5 και 7, διακρίνεται εμφανώς μία συνοχή και συνέχεια στις απαντήσεις των hackers. Ωστόσο, εν προκειμένω πρέπει να λάβουμε υπόψη μας και την υποκουλτούρα βάσει της οποίας αναπτύσσονται κάποιες φορές οι συμπεριφορές hacking και η οποία ενδεχομένως να επηρεάζει τις απαντήσεις ως άνω. Η υποκουλτούρα αυτή δύναται να εκφράζεται με την επίδειξη ενός «ατρόμητου» χαρακτήρα απέναντι σε κονφορμιστικές αντιλήψεις[1545] γενικότερα και στον ποινικό νομοθέτη ειδικότερα, γεγονός το οποίο ίσως αβασάνιστα οδηγεί σε απαντήσεις και θέσεις με νόημα «δεν με σταματάει ο ποινικός νομοθέτης!». Πιστεύω ότι ο ως άνω προβληματισμός πρέπει να ληφθεί σοβαρά υπόψιν στην ανάγνωση των ανωτέρω αποτελεσμάτων. Περαιτέρω, σε αντίστοιχο πνεύμα – όπως επισημαίνεται και από τη Λαμπροπούλου – «*εάν υπάρχουν υποπολιτισμικοί κανόνες ισχυρότεροι από τον ποινικό νόμο, μειώνονται σημαντικά οι πιθανότητες να λειτουργήσει η απειλή της ποινής αποτρεπτικά*»[1546]. Στην προκειμένη περίπτωση, το σύνολο της ιδεολογίας και υποκουλτούρας των hackers[1547] – όπως δηλώνεται στην έρευνα και σε επίπεδο κινήτρων (π.χ. ελευθερία της πληροφορίας κ.λπ.)[1548] – να σταθμίζεται από αυτούς ως σημαντικότερο αγαθό από ό,τι προστατεύει ο ποινικός νομοθέτης.

[1543] Στα ερωτηματολόγια υπ' αρ. 2 και 46.

[1544] Ερωτηματολόγια υπ' αρ. 10 και 40.

[1545] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38 όπου καταγράφεται η αντικομφορμιστική στάση των hackers.

[1546] Έτσι *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 187.

[1547] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 2 του παρόνος πονήματος.

[1548] Βλ. απαντήσεις στην ερώτηση 2 στο ερωτηματολόγιο των hackers.

Γεγονός είναι, πάντως, ότι προκαλεί εντύπωση το σημαντικό ποσοστό των ερωτηθέντων hackers που συμφωνεί με τα όρια στο hacking και ότι θα περίμενε κανείς ένα μεγαλύτερο ποσοστό των ερωτηθέντων hackers να λαμβάνει θετική στάση απέναντι στην ιδέα της δίχως όρια πρόσβασης σε δεδομένα τρίτων. Αυτή η προσέγγιση έρχεται βέβαια σε αντίθεση με τις θεωρίες της ορθολογικής επιλογής[1549] καθώς η μη ύπαρξη ορίων σημαίνει αυτομάτως μικρότερο κόστος σε σχέση με το όφελος το οποίο οι hackers επιδιώκουν. Άρα, ίσως να μπορούμε να εξάγουμε το συμπέρασμα – σε συσχέτιση με τις ανωτέρω απαντήσεις των hackers, οι οποίες αναφέρονται στην μικρή γενικοπροληπτική επιρροή των διατάξεων (που θεσπίζει βέβαια η Πολιτεία) – ότι οι hackers επιθυμούν έως έναν βαθμό η Πολιτεία να τους θέτει όρια προκειμένου αυτοί να τα παραβαίνουν (αφού και κατά τους Chiesa, Ducci και Ciappi είναι «παθιασμένοι» με το να ξεπερνούν όρια[1550], σε εκτέλεση, ενδεχομένως, και αυτοεκπληρούμενης προφητείας!

Περαιτέρω, σύμφωνα με τις απαντήσεις στην ερώτηση 6α, ένα μεγάλο μέρος των ερωτηθέντων hackers παραδέχεται ότι κατέχει πληροφορίες στο διαδίκτυο, στις οποίες δεν επιθυμεί την πρόσβαση τρίτων. Βλέπουμε, εδώ, δηλαδή, ότι οι hackers αναγνωρίζουν, έτσι, ενός είδους «προσωπικό χώρο» στο διαδίκτυο – αντίθετα, δηλαδή, με τις αντιλήψεις τους για ελευθερία της πληροφορίας κ.λπ. Από την άλλη, στην ερώτηση 6β οι hackers τάσσονται σε μεγάλο βαθμό υπέρ της ελεύθερης κυκλοφορίας ταινίας ή βιβλίου αμέσως μετά την κυκλοφορία του επί πληρωμή.

Οι δύο αυτές ερωτήσεις συνδυαστικά αποσκοπούν στο να ελέγξουν τη συνέπεια των θέσεων των hackers ως προς το ζήτημα της ελεύθερης και ακώλυτης διακίνησης της πληροφορίας στο διαδίκτυο. Ειδικότερα, στην ερώτηση 6α φαίνεται ότι οι περισσότεροι hackers αναγνωρίζουν την ιδιωτικότητα στο διαδίκτυο ως στοιχείο το οποίο θέλουν να υπάρχει – οι θέσεις τους δηλαδή για ελευθερία της πληροφορίας στο διαδίκτυο κλονίζονται άμεσα όταν και οι ίδιοι επιθυμούν την ασφάλεια ιδιωτικών τους ηλεκτροικών δεδομένων. Επιπρόσθετα, η απάντηση αυτή πρέπει, ίσως, να δώσει αφορμή για ψύχραιμη θεώρηση της ελευθερίας της πληροφορίας στο διαδίκτυο σε συνδυασμό με τη διαφύλαξη της ιδιωτικότητας. Στην ερώτηση 6β, οι hackers είναι

[1549] Βλ. αναπτύξεις για θεωρία ορθολογικής επιλογής και παράγωγες θεωρίες στο κεφάλαιο 3 του παρόντος πονήματος.

[1550] Βλ. *Raoul Chiesa, Stefania Ducci & Silvio Ciappi*, Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications - Taylor & Francis Group, 2009, p. 38 κατά την αναφορά τους στο «Μανιφέστο του hacker».

συνεπείς αναφορικά με την ελευθερία της πληροφορίας στο διαδίκτυο – ωστόσο, φαίνεται ότι η πλειοψηφία των hackers αδιαφορεί για το ηθικό δικαίωμα των δημιουργών και, άρα, μπορεί να θεωρηθεί ότι ασπάζεται αυτήν την ελευθερία της πληροφορίας στο διαδίκτυο ενδεχομένως ως υπερατομικό αγαθό. Βέβαια, η συσχέτιση των δύο ανωτέρω ερωτήσεων, έτσι όπως έχουν τεθεί, απαιτεί προσοχή διότι το αντικείμενο της δεύτερης ερώτησης (βιβλίο, ταινία κ.λπ.) είναι δεδομένα προορισμένα προς δημοσίευση σε αντίθεση με τα ιδιωτικά δεδομένα της πρώτης ερώτησης.

Σε κάθε περίπτωση, πάντως, η κουλτούρα για ελευθερία της πληροφορίας φαίνεται να πλήττεται και να μην είναι, τελικά, τόσο σταθερή. Το εύρημα αυτό της «μη συνεπούς» στάσεως μπορεί να συνδυαστεί και με τις θεωρίες της ηθικής ανάπτυξης, του αυτοελέγχου αλλά και με την έλλειψη ηθικού κριτηρίου (όπως επισημαίνεται από τον Yar)[1551], λαμβανομένου υπόψιν ότι οι περισσότεροι hackers, οι οποίοι συμμετείχαν στην έρευνα, είναι νεαρής ηλικίας. Ως αποτέλεσμα, φαίνεται η θέσπιση ορίων στο διαδίκτυο να νομιμοποιείται ως παράγοντας δημιουργίας συνείδησης κατά το μέτρο του δυνατού σε παρεκκλίνοντες, οι οποίοι δεν έχουν κατασταλάξει ακόμη σε επίπεδο ηθικών κριτηρίων.

Σε ό,τι αφορά στη σημασία που αποδίδουν οι hackers στην αναγνώρισή τους ως μέλη μιας κοινότητας, η πλέον σημαντική κατηγορία απαντήσεων ίσως να αποτελεί αυτή στην οποία οι hackers αναφέρονται σε περιπτώσεις αλληλοβοήθειας – τούτο, διότι, η αλληλοβοήθεια αυτή μπορεί να συνίσταται σε προώθηση και ανταλλαγή hacking tools και γενικότερα malware (προγραμμάτων, δηλαδή, τα οποία δύνανται να εξασφαλίσουν ή να συνδράμουν στην χωρίς δικαίωμα πρόσβαση σε δεδομένα)[1552], τα οποία μπορούν ουσιαστικά να θεωρηθούν επικίνδυνα αναφορικά με την ασφάλεια των ηλεκτρονικών πληροφοριών. Άρα, η αναγνώρισή τους αυτή από τους υπόλοιπους hackers λειτουργεί βοηθητικά στην εξέλιξη της δράσης τους και επιβεβαιώνει σε σημαντικό βαθμό τη θεωρία του «διαφορικού συγχρωτισμού» ή της «διαφοροποιούσας συναναστροφής» (differential association theory)[1553].

Σε ό,τι έχει να κάνει με την πρώτη υπόθεση έρευνας αναφορικά με τον ορισμό του hacking, ανωτέρω καταγράφηκε αναλυτικά η θέση των hackers. Στο συμπέρασμα ότι

[1551] Βλ. τις σχετικές αναπτύξεις στις παραγράφους 3.5, 3.7 και 3.8 του παρόντος πονήματος.
[1552] Βλ. ανωτέρω παράγραφο 2.11 του παρόντος πονήματος.
[1553] Βλ. ανωτέρω παράγραφο 3.9 του παρόντος πονήματος.

οι hackers δεν φαίνεται να επικαλούνται στον ορισμό παραμέτρους εντελώς διαφορετικές από όσες έχουν ήδη καταγραφεί στη σχετική βιβλιογραφία και αρθρογραφία, συμπληρώνονται και τονίζονται η συσχέτιση του hacking με τη χωρίς δικαίωμα πρόσβαση σε δεδομένα καθώς και η καινοτόμος δράση των hackers. Εάν οι δύο αυτές θέσεις συνδυαστούν, θα μπορούσε ίσως να υποστηριχθεί το ότι, σύμφωνα με τους hackers, για την καινοτομία σε επίπεδο ηλεκτρονικών συστημάτων πληροφοριών είναι αρχικώς απαραίτητη η πρόσβαση στην πληροφορία, ως βασικό στοιχείο του hacking. Βέβαια, στην ερώτηση υπ' αρ. 13 υπάρχουν hackers οι οποίοι δεν θεωρούν hackers τους "Anomynous" γιατί χρησιμοποιούν τακτικές επιθέσεων DoS, τις οποίες οι εν λόγω απαντώντες δεν θεωρούν hacking[1554]. Επιπρόσθετα, μπορεί κανείς να ανιχνεύσει στις απαντήσεις του τρόπου δράσης των hackers ότι σε γενικές γραμμές υπάρχουν hackers οι οποίοι χρησιμοποιούν προφανώς συνδυασμό εξωπρογραμματιστικών[1555] και γνησίων[1556] πρακτικών hacking[1557] αλλά υπάρχουν και hackers οι οποίοι (σύμφωνα με τια απαντήσεις τους) χρησιμοποιούν μόνο εξωπρογραμματιστικές[1558] ή μόνο γνήσιες[1559] πρακτικές hacking- πιστεύω οτι ενδεχομένως αυτοί που χρησιμοποιούν γνήσιες πρακτικές hacking δεν θεωρούν hackers (και αντίστοιχα hacking) ή δεν παραδέχονται όσους χρησιμοποιούν εξωπρογραμματιστικές πρακτικές hacking. Τίθεται, επομένως, τελικά, ένα ζήτημα stricto ή lato sensu ορισμού του hacking: εν ευρεία εννοία hacking θεωρείται οτιδήποτε πλήττει την ασφάλεια των συστημάτων πληροφοριών[1560] με οποιονδήποτε τρόπο (π.χ. επίθεση άρνησης υπηρεσίας – DoS attack[1561] – η οποία πλήττει τη διαθεσιμότητα των ηλεκτρονικών πληροφοριών) – εν στενή εννοία, hacking θεωρείται μόνο η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα (άρα η προσβολή της εμπιστευτικότητας σε επίπεδο ασφάλειας ηλεκτρονικών πληροφοριών) και μάλιστα, σε μια πιο περιορισμένη εκδοχή, μόνο με χρήση σχετικών προγραμμάτων και ψηφιακών προγραμματιστικών πρακτικών.

[1554] Βλ. κατωτέρω στο Παράρτημα ΙΙΙ της παρούσας τις απαντήσεις των hackers στην ερώτηση 13 και συγκεκριμένα στα ερωτηματολόγια υπ' αρ. 7, 11, 14, 17 .

[1555] Βλ. ανωτέρω παράγραφο 2.11.2.1.

[1556] Βλ. ανωτέρω παράγραφο 2.11.2.2.

[1557] Βλ. χαρακτηριστικά απάντηση στην ερώτηση υπ' αρ. 10 στο ερωτηματολόγιο υπ' αρ. 22 του Παραρτήματος ΙΙΙ του παρόντος πονήματος.

[1558] Βλ. χαρακτηριστικά απαντήσεις στην ερώτηση υπ' αρ. 10 στα ερωτηματολόγια υπ' αρ. 20,21 και 35 του Παραρτήματος ΙΙΙ του παρόντος πονήματος.

[1559] Βλ. χαρακτηριστικά απαντήσεις στην ερώτηση υπ' αρ. 10 στα ερωτηματολόγια υπ' αρ. 12, 13, 14, 15 και 18 του Παραρτήματος ΙΙΙ του παρόντος πονήματος.

[1560] Βλ. ανωτέρω παράγραφο 1.3.2.

[1561] Βλ. παράγραφο 2.11.2.2.2.

Οι περισσότεροι hackers επικαλούνται την ιδεολογία τους ως περίβλημα των ενεργειών τους, η οποία φαίνεται βασίμως να λειτουργεί εδώ ως τεχνική ουδετεροποίησης, όπως προκύπτει από τις απαντήσεις της ερώτησης 2 σε συνδυασμό με τις 18 απαντήσεις της ερώτησης 4, στις οποίες αναφέρεται ότι η δράση των εντάσσεται ή υποστηρίζει πρακτικές ηθικού hacking, καθώς και με τους αυτοπροσδιορισθέντες «χακτιβιστές» στην ερώτηση 13 και τους υποστηρικτές των "Anonymous" στην ερώτηση 14. Ωστόσο, η «ομπρέλα» της ιδεολογίας (όπως αυτή αναλύεται ανωτέρω και, εξάλλου, υπάρχει και σε κείμενα που έχουν «χαράξει» την ιστορία του hacking, όπως π.χ. το «Μανιφέστο του hacker»), ενδεχομένως να μην καλύπτει σε όλες τις περιπτώσεις τις δράσεις των hackers, έτσι όπως αυτή προσδιορίζεται από τους ίδιους τους hackers στις απαντήσεις της ερώτησης 10 του οικείου ερωτηματολογίου. Εν προκειμένω, περιγράφονται και ενέργειες οι οποίες παραπέμπουν και στην κριτική εγκληματολογία αλλά και στις θεωρίες ορθολογικής επιλογής.

Η ελληνική νομοθεσία, όπως καταδείχθηκε ανωτέρω, δεν φαίνεται να αποτρέπει τους hackers. Επίσης, αν λάβουμε υπόψιν ότι οι hackers αρέσκονται στο να παραβαίνουν τα όρια, είναι λογική και παρεπόμενη η απάντηση κατά την οποία δεν πιστεύουν ότι ενδεχόμενη αυστηροποίηση της νομοθεσίας λειτουργεί αποτρεπτικά για αυτούς.

Ωστόσο, έκπληξη σίγουρα αποτελεί η απάντηση των hackers σύμφωνα με την οποία αυτοί επιθυμούν η Πολιτεία να θέτει όρια στο hacking. Η απάντηση αυτή φαίνεται να υπαγορεύεται από το γεγονός ότι οι hackers έχουν και αυτοί προσωπικές τους πληροφορίες στο διαδίκτυο για των οποίων την ασφάλεια ενδιαφέρονται ειδικώς (όπως ανωτέρω αναφέρεται) και συνεπώς αναγνωρίζουν την ανάγκη επιβολής ορίων και λήψης μέτρων. Από την άλλη πλευρά, όμως, ο συνδυασμός αυτός ίσως βγάζει στην επιφάνεια μια ιδεολογική ένδεια και αστάθεια των σύγχρονων hackers, οι οποίοι θέλουν από τη μια ελευθερία κινήσεων σε ό,τι αφορά σε πληροφορίες άλλων αλλά και προστασία και όρια όταν αντιλαμβάνονται ότι και τα δικά τους δεδομένα τίθενται σε κίνδυνο (δεν είναι εξάλλου τυχαίο το γεγονός ότι η εν λόγω ερώτηση 9 για το αν η Πολιτεία πρέπει να θέτει όρια στο hacking έχει τεθεί μετά την ερώτηση 6α, η οποία «θυμίζει» στους hackers τα δεδομένα στα οποία αυτοί έχουν τον έλεγχο). Επί της ουσίας, όμως, είναι αυτή η απάντηση η οποία μπορεί να δείξει τον δρόμο για την ένταξη στο κοινωνικό γίγνεσθαι των hackers και επί της ουσίας της απορρόφησής τους για σκοπούς εξέλιξης και θωράκισης της ηλεκτρονικής πληροφορίας (όπως

ανωτέρω «επιθυμεί» το μεγαλύτερο ποσοστό των επιστημόνων πληροφορικής σε επίπεδο συνεργασίας για την ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων).

Στην ερώτηση 11 οι συμβουλές οι οποίες δίνονται από τους hackers έχουν στο μεγαλύτερο μέρος τους να κάνουν με την «κουλτούρα» της ασφάλειας, η οποία πρέπει να διέπει τους χρήστες δικτυακών και διασυνδεδεμένων συσκευών. Είναι, τελικώς, αυτή η κουλτούρα πάνω στην οποία μπορούν να βασιστούν εναλλακτικοί τρόποι πρόληψης και ενίσχυσης της ηλεκτρονικής ασφάλειας, η οποία μπορεί να αποτελείται από το να μην έχουν οι χρήστες γραμμένους τους κωδικούς τους σε σημεία στα οποία μπορεί κάποιος να έχει ακόμη και οπτική πρόσβαση (π.χ. κολλημένο χαρτί στο πίσω μέρος του κινητού τηλεφώνου) ή να είναι σχετικώς εύκολο να κλαπούν (σημείωμα σε πορτοφόλι) μέχρι το να καταφέρουν να διακρίνουν «ύποπτα» αρχεία και ιστοσελίδες και να μην συνδέονται με αυτά. *Η εκπαίδευση στην χρήση συσκευών διαχείρισης ηλεκτρονικών πληροφοριών, η ενημερωση και η παιδεία, έννοιες οι οποίες προτείνονται ανωτέρω ως εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών πληροφοριών και δεδομένων, πρέπει να έχει ως στόχο την εμπέδωση και ενίσχυση αυτής την κουλτούρα ασφάλειας των ηλεκτρονικών δεδομένων*.

8. ΣΥΣΧΕΤΙΣΗ ΠΟΡΙΣΜΑΤΩΝ ΕΡΕΥΝΑΣ ΣΕ ΣΥΝΑΡΤΗΣΗ ΚΑΙ ΜΕ ΤΙΣ ΥΠΟΘΕΣΕΙΣ ΤΗΣ ΕΡΕΥΝΑΣ

8.1 Η σύγχρονη ένοια της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking

Σύμφωνα με τα ως άνω πορίσματα της έρευνας, βλέπουμε, αρχικώς, ότι οι απαντήσεις των συμμετεχόντων και στα τρία δείγματα δεν έδωσαν κάποιον ρηξικέλευθο ορισμό ή ερμηνεία στο hacking, που να μην έχει μέχρι σήμερα καταγραφεί στην θεωρία.

Το πλέον ενδιαφέρον ερευνητικό εύρημα είναι, ουσιαστικά, η καταγραφή της σύγχυσης ακόμη και σε δείγματα ειδικών αναφορικά με πράξεις οι οποίες εντάσσονται από τη μια στην έννοια του hacking και από την άλλη στην έννοια του cracking. Τούτο καταδεικνύει τα λεπτά και ρευστά όρια μεταξύ hacking και cracking, αφού τελικά μπορεί να υποστηριχθεί ότι πρόκειται για τις δυο όψεις του ίδιου νομίσματος. Εξάλλου, η αλλοίωση, τροποποίηση, καταστροφή και κάθε άλλη επιβλαβής για τα δεδομένα πράξη προϋποθέτει κατ' αρχήν τις περισσότερες φορές μια χωρίς δικαίωμα πρόσβαση στο σύστημα πληροφοριών. Η διαφορά, τελικώς, εντοπίζεται στο κίνητρο και στο αποτέλεσμα. Σε κάθε περίπτωση, όμως, σε περίπτωση που το θύμα υπολαβάνει ως προσβολή και πλήγμα των δικαιωμάτων και των συμφερόντων του πράξεις hacking, οι οποίες λαμβάνουν χώρα επί ηλεκτρονικών του δεδομένων, οι ενέργειες hacking δεν μπορούν μάλλον εύκολα να δικαιολογηθούν και, τελικά, δύνανται, ίσως, να χαρακτηριστούν ακόμη και cracking. Επίσης, η επίκληση της ιδεολογίας του hacking για δικαιολόγηση πράξεων οι οποίες θα μπορούσαν να θεωρηθούν cracking ενδεχομένως εντάσσεται στις τεχνικές ηθικής ουδετεροποίησης σύμφωνα με την ως άνω θεωρία των Matza και Sykes.

Η σύγχυση που καταγράφεται ανωτέρω δημιουργεί σίγουρα πρόβλημα σε ενδεχόμενη απόπειρα νομικού και τιμωρητικού διαχωρισμού των συμπεριφορών και, συνεπώς, η συνδρομή των δειγμάτων στην κατάρτιση πρακτικών αντεγκληματικής πολιτικής φαίνεται περιορισμένη. Η επιφανειακή κατάρτιση των συμμετεχόντων και στα δύο δείγματα σκοπιμότητας των νομικών και των επιστημόνων πληροφορικής ενισχύει την ανάγκη για ενημέρωση και εκπαίδευση[1562], όπως προτείνεται από τους ίδιους του νομικούς και επιστήμονες πληροφορικής.

Το hacking εκδηλώνεται κυρίως με (χωρίς δικαίωμα) πρόσβαση σε ηλεκτρονικά δεδομένα. Σε επίπεδο συστημάτων πληροφοριών και δεδομένων είναι η (χωρίς δικαίωμα) πρόσβαση σε δεδομένα –είτε πλήττωντας το απόρρητο αυτών, είτε καθιστώντας την πρόσβαση αδύνατη – αυτή η οποία αποτελεί τον πυρήνα συμπεριφορών hacking. Ακόμη και η εισβολή σε σύστημα με την αποστολή ενός ιού ουσιαστικά και τεχνικά μπορεί να θεωρηθεί ότι αποτελεί χωρίς δικαίωμα πρόσβαση σε δεδομένα, αφού φαίνεται ότι ακόμη και το κατέβασμα ενός ιού και η προσωρινή αποθήκευσή του στην προσωρινή μνήμη του ηλεκτρονικού υπολογιστή συνιστά πρόσβαση στη μνήμη άρα και σε δεδομένα υπολογιστή. Συνεπώς, σε ό,τι αφορά στα ηλεκτρονικά δεδομένα, το ζήτημα της χωρίς δικαίωμα πρόσβασης φαίνεται αρχικά να καλύπτει μεγάλο μέρος πρακτικών hacking και είναι αυτή η οποία πρέπει να αντιμετωπιστεί νομοθετικά αλλά και με ενναλλακτικές μεθόδους πρόληψης. Περαιτέρω, όμως, πρέπει να λάβουμε υπόψιν μας ότι υπάρχουν περιπτώσεις hacking στις οποίες, ανάλογα με τον τρόπο που λαμβάνουν χώρα, μπορεί να μη θεμελιώνεται η έννοια της πρόσβασης σε δεδομένα αλλά να αποκλείεται η πρόσβαση σε αυτά (π.χ. DoS attack) (lato sensu θεώρηση της έννοιας του hacking[1563]). Με αυτό το δεδομένο, η ως άνω πρόταση για υιοθέτηση εννόμου αγαθού που θα αναφέρεται στην ακεραιότητα, στην εμπιστευτικότητα και στη διαθεσιμότητα των ηλεκτρονικών δεδομένων (όπως αναφέρεται στο οικείο κεφάλαιο της παρούσας) ενισχύεται ακόμη περισσότερο από το περιεχόμενο των ως άνω απαντήσεων στις ερωτήσεις ανοικτού τύπου της έρευνας.

[1562] Βλ. κατωτέρω παραγράφους 8.4 και 9.2.

[1563] Βλ. σχετικώς παράγραφο 7.8.4.2.

8.2 Το κίνητρο των hackers

Από τις απαντήσεις των δειγμάτων της έρευνας μπορούν να εξαχθούν δύο συμπεράσματα: κατά πρώτον, η εικόνα για το κίνητρο των hackers, την οποία έχουν οι νομικοί και οι επιστήμονες πληροφορικής - κατά δεύτερον, η εικόνα που δίνουν οι ίδιοι οι hackers για τους εαυτούς τους.

Οι hackers στη συντριπτική τους πλειοψηφία επικαλούνται ως κίνητρα την ιδεολογία τους ή την εξάσκησή τους (επιβεβαιώνοντας με αυτόν τον τρόπο τις θεωρίες της ηθικής ουδετεροποίησης, της κριτικής εγκληματολογίας, της θεωρίας ηθικών πεποιθήσεων αλλά και τη θεωρία της έντασης[1564]). Σε επιβεβαίωση αυτού, και οι περισσότεροι επιστήμονες πληροφορικής αλλά και αρκετοί νομικοί προκρίνουν την ιδεολογία ως κίνητρο. Η «επανάσταση» ή η αντίδραση μέσα από το διαδίκτυο φαίνεται να κερδίζει έδαφος στην σύγχρονη ψηφιακή κοινωνία. Εξάλλου, οι νομικοί και οι επιστήμονες πληροφορικής, όσο κι αν στέκονται απέναντι στο hacking, όπως είδαμε βασίζουν την ελπίδα τους πολλές φορές στους hackers και ιδίως σε όσους αποκτούν χωρίς δικαίωμα πρόσβαση σε δεδομένα, προκειμένου να επιτευχθεί διαφάνεια στη δημόσια ζωή και να αποκαλυφθούν πληροφορίες, οι οποίες αφορούν το ευρύ κοινό. Άρα, πέρα από τις εγκληματολογικές θεωρίες που φαίνεται να ταιριάζουν σε ό,τι αφορά στην ερμηνεία και την αιτιολόγηση του hacking, ουσιαστικά φαίνεται να τίθεται ως ζήτημα δυνάμει των ανωτέρω μια ενδεχόμενη ηθική νομιμοποίηση του hacking, αφού ο περιορισμός του θα σήμαινε περιορισμό της ανάπτυξης ξεχωριστών ικανοτήτων αλλά και τάσεων αλλαγής της καθεστηκυίας τάξης. Παρόλα αυτά, εκτιμώ πως είναι γεγονός ότι και από τις απαντήσεις των hackers αναφορικά με τη δράση τους αλλά και από επισκόπηση δημοσιευμάτων μέχρι σήμερα είναι λίγες οι περιπτώσεις στις οποίες η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα χρησιμοποιήθηκε προς όφελος του κοινωνικού συνόλου, ιδίως σε ό,τι αφορά στα όποια επαναστατικά του χαρακτηριστικά. Από την άλλη πλευρά, βέβαια, είναι σημαντική η προσφορά των hackers σε επίπεδο ανίχνευσης κενών ασφαλείας συστημάτων – "ethical hacking" ή «χακτιβισμός»– δράση, όμως, την οποία φέρονται να ακολουθούν όχι και τόσοι πολλοί hackers.

[1564] ...όπως αναλύονται στο κεφάλαιο 3 του παρόντος πονήματος.

Περαιτέρω, οι hackers απαρνούνται ουσιαστικά στο μεγαλύτερο ποσοστό τους το οικονομικό όφελος από (κακόβουλες) ενέργειες hacking, μολονότι φαίνεται από τα αποτελέσματα των άλλων δύο δειγμάτων ότι η εικόνα που υπάρχει για αυτούς σε σημαντικό βαθμό φαίνεται να είναι συνδεδεμένη με την αποκόμιση κερδών (βλ. σχετική ανάλυση υπαγωγής του hacking στη θεωρία εγκλημάτων λευκού περιλαιμίου).

Οι θεωρίες της ορθολογικής επιλογής σε σχέση και με τη δράση των hackers, όπως περιγράφεται στην έρευνα, κινούνται σε επίπεδο το οποίο μάλλον μπορεί να εξηγήσει συμπεριφορές των hackers με ιδεολογικά και οικονομικά κίνητρα. Η ανάλυση κόστους-οφέλους των θεωριών της ορθολογικής επιλογής μπορεί να λαμβάνει χώρα είτε για οικονομικό όφελος, είτε για την επίτευξη ενός στόχου με ιδεολογικό περίβλημα. Περαιτέρω, ακόμη και η εξάσκηση ή η διασκέδαση ως κίνητρο μπορεί να υπόκειται από τον hacker σε ανάλυση κόστους (π.χ. ο κίνδυνος ανακάλυψής του) και οφέλους.

Δυνάμει και των ανωτέρω αναπτύξεων αλλά λαμβανομένων υπόψιν και όσων αναπτύχθηκαν στην προηγούμενη παράγραφο καθώς και της θέσης νομικών και επιστημόνων πληροφορικής για αυστηρότερη ποινική αντιμετώπιση του hacking σε περίπτώσεις οικονομικού οφέλους ή ζημίας, είναι ίσως σκόπιμη με την προοπτική της υιοθέτησης μέτρων η σαφής πλέον διάκριση στον νόμο του hacking και του cracking, και η συνακόλουθη (αυστηρότερη) τιμώρηση όσων παραβιαστών αποκτούν οικονομικό όφελος ή προβαίνουν σε οικονομική ζημία.

8.3 Έλεγχος γενικοπροληπτικής αποτελεσματικότητας της ελληνικής ποινικής νομοθεσίας και προτάσεις de lege ferenda για τη σύγχρονη νομοθετική αντιμετώπιση του hacking

Ο συνδυασμός των απαντήσεων των δειγμάτων καταδεικνύει σαφώς ότι οι ποινικές διατάξεις, όπως ισχύουν στην ελληνική έννομη τάξη, είναι λίγο έως καθόλου αποτελεσματικές για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων, επιβεβαιώνοντας την υπόθεση της έρευνας περί ανεπάρκειας αυτών. Εκφάνσεις της

αναποτελεσματικότητας αυτής προκύπτουν ειδικότερα από τις απαντήσεις των τριών δειγμάτων. Χαρακτηριστικά, οι ίδιοι οι hackers υποστηρίζουν σαφώς ότι δεν αποτρέπονται από τις εν λόγω διατάξεις (λαμβανομένων, βέβαια, υπόψιν των επιφυλάξεων που έχουν διατυπωθεί ανωτέρω). Από την έρευνα προκύπτει, επίσης, αβίαστα ότι η περιορισμένη νομολογιακή εφαρμογή τους (μόλις μία δημοσιευμένη στον νομικό τύπο απόφαση εφαρμογής του ά. 370Γ παρ. 2 ΠΚ – περίπτωση στην οποία, μάλιστα, δεν χρησιμοποιήθηκε το διαδίκτυο) καταδεικνύει περισσότερο ότι μάλλον δεν εντάχθηκαν ποτέ στη νομική κουλτούρα εφαρμοστών του δικαίου αλλά και κοινωνών αυτού (χαρακτηριστικά, ακόμη και νομικοί δηλώνουν ότι δεν είναι ενημερωμένοι για τις νομικές προβλέψεις!).

Η αυστηροποίηση της νομοθεσίας (μόλις ένα μικρό ποσοστό υποστηρίζει την αποποινικοποίηση του hacking, το οποίο όμως πιστεύω ότι δεν είναι αρκετό προκειμένου να επηρεάσει αυτή τη στιγμή την κατεύθυνση της νομοθεσίας) υποστηρίζεται από το δείγμα νομικών και επιστημόνων πληροφορικής στις σχετικές ερωτήσεις. Εξάλλου, «*όταν οι νόμοι συμπορεύονται με τα πολιτικά, ηθικά, κοινωνικά και αξιακά πρότυπα μιας κοινωνίας ή μεγάλου μέρους της, έχουν μεγάλες πιθανότητες αποδοχής και συμμόρφωσης των ατόμων σ' αυτούς*»[1565]. Υπάρχει, όμως, σοβαρή επιφύλαξη λόγω του ότι οι hackers απάντησαν πως μια αυστηρή νομοθεσία δεν πρόκειται να τους αποτρέψει από τη δράση τους. Εξάλλου, σύμφωνα και με την Βασιλάκη, ο σύγχρονος ρόλος του ποινικού δικαίου για τις ανωτέρω συμπεριφορές (πρέπει να) είναι περιορισμένος, ως μη έχων την επιθυμητή προληπτική επίδραση[1566]. Άρα, ως αρχικό συμπέρασμα μπορούμε ενδεχομένως να εξάγουμε το ότι η αυστηροποίηση των ποινικών κυρώσεων ίσως να εξακολουθεί να μην είναι αποτελεσματική αναφορικά με την προώθηση της ασφάλειας των συστημάτων πληροφοριών.

Ωστόσο, οι hackers σε σημαντικό ποσοστό αποδέχονται τον ρόλο της Πολιτείας στο να θέτει όρια στο hacking (ακόμη ίσως και με κάποιες προϋποθέσεις). Αυτή η δεκτικότητα των hackers είναι ίσως το πρώτο βήμα για τη χάραξη αντεγκληματικής

[1565] Έτσι *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 212.

[1566] Έτσι *Ειρ. Βασιλάκη*, Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής τους καταστολής – Προετοιμάζοντας το ποινικό δίκαιο του 21ου αιώνα;, εις: *Ν. Κουράκη* (εκδ. επιμ.), Αντεγκληματική πολιτική ΙΙ, σειρά «Ποινικά», αρ. 59, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή 2000, σελ. 31.

πολιτικής[1567], καθώς θα περίμενε ίσως κανείς να είναι αρνητικοί απέναντι σε κάθε είδους παρέμβαση, πράγμα το οποίο δεν φαίνεται να συμβαίνει. Η αντεγκληματική αυτή πολιτική θα πρέπει λογικά να έχει ως επίκεντρο την ενημέρωση για τη χρήση της τεχνολογίας (βλ. επόμενη υπόθεση εργασίας και ανάλυση) καθώς και την εύρεση τρόπων προκειμένου οι hackers να εκτονώνουν την ευρηματικότητα και την περιέργειά τους.

Το δείγμα σε μεγάλο ποσοστό φαίνεται να επιθυμεί την αυστηρότερη τιμώρηση όσων αποκομίζουν οικονομικό όφελος ή επιφέρουν οικονομική ζημία, είτε αυτοτελώς είτε ως επιβαρυντική περίσταση (προκειμένου και να διαχωριστούν ενέργειες hacking και cracking, όπως ανωτέρω), σύμφωνα και με τη σχετική πρόταση που διατυπώθηκε ανωτέρω κατά την επισκόπηση της ελληνικής ποινικής νομοθεσίας[1568]. Η, δε, ενδεχόμενη μη τιμώρηση της χωρίς δικαίωμα πρόσβασης σε δεδομένα δημιουργεί προβληματισμό λόγω της εγνωσμένης οικονομικής αξίας της πληροφορίας. Χαρακτηριστικές είναι οι περιπτώσεις βιομηχανικής κατασκοπείας, με τις οποίες οικονομική ζημία μπορεί να προκύψει ακόμη και από την αποκάλυψη μιας πληροφορίας και όχι απαραίτητα π.χ. με μεταφορά χρημάτων μέσω ηλεκτρονικών συστημάτων ή καταστροφή μιας ιστοσελίδας). Σε περίπτώσεις οικονομικού οφέλους ή ζημίας το δείγμα φαίνεται να υποστηρίζει τη σαφή πλέον διάκριση στον νόμο του hacking και του cracking, με την (αυστηρότερη) τιμώρηση όσων παραβιαστών αποκτούν οικονομικό όφελος ή προβαίνουν σε οικονομική ζημία[1569].

Ουσιαστικά, τα στοιχεία που πρέπει να σταθμιστούν είναι από τη μια η οικονομική ζημία, η οποία μπορεί να προκύψει από ενέργειες hacking, ακόμη και από την απλή περιέλευση σε γνώση της πληροφορίας, και από την άλλη η ελευθερία της πληροφορίας στο διαδίκτυο ακόμη και για μορφωτικούς λόγους, στο πλαίσιο του

[1567] Πρβλ. για σύγχρονη θέαση της αντεγκληματικής πολιτικής το πόνημα της *Σοφίας Βιδάλη*, Αντεγκληματική πολιτική: από τη μικροεγκληματικότητα έως το οργανωμένο έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013. Επιπρόθετα, πρβλ. εμπεριστατωμένη ανάπτυξη για τα κριτήρια άσκησης αντεγκληματικής πολιτικής *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 39 επ.

[1568] Στην παράγραφο 5.5 του παρόντος πονήματος.

[1569] Πρβλ. *Steven Penney*, Updating Canada's Communications surveillance laws: Privacy and security in the digital age, 2008, 12 Canadian Criminal Law Review 115, 2008, p. 15 f. όπου και σχετική ανάπτυξη αναφορικά με τον αποτρεπτικό ρόλο που δύναται να έχει η ποινική νομοθεσία όταν η πράξη χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα επικοινωνίας έχει τελεστεί από μεμονωμένους δράστες ή εκπροσώπους εταιρειών. Ο Penney σε κάθε περίπτωση προτείνει την ποινικοποίηση της κακόβουλης ή με σκοπό οφέλους χωρίς δικαίωμα πρόσβασης.

γνωστού διπόλου ελευθερίας και ασφάλειας[1570]. Το δίλημμα αυτό, όμως, ίσως παρακάμπτεται από την ανάγνωση των απαντήσεων και των τριών δειγμάτων: από τη μια η αποποινικοποίηση του hacking (στο πλαίσιο ελεύθερης χρήσης της πληροφορίας προφανώς) υποστηρίζεται μεν από νομικούς και επιστήμονες πληροφορικής αλλά όχι από ποσοστό το οποίο θα μπορούσε να επηρεάσει τη νομοθεσία προς αυτήν την κατεύθυνση – από την άλλη, αρκετοί από τους ίδιους τους hackers φαίνεται να έχουν πληροφορίες στο διαδίκτυο οι οποίες δεν θα ήθελαν να είναι κοινοποιήσιμες. Ο συνδυασμός αυτών των δύο ερευνητικών δεδομένων δίνει ως συμπέρασμα το ότι η ηλεκτρονική πληροφορία είναι αρκετά σημαντική και, συνεπώς, ότι δεν μπορει να είναι εντελώς ελεύθερη.

8.4 Εναλλακτικοί τρόποι ενίσχυσης της ασφάλειας των ηλεκτρονικών δεδομένων

Οι προβληματισμοί αναφορικά με την αποτελεσματικότητα του ποινικού δικαίου ανεπτύχθησαν ήδη ανωτέρω, ιδίως αναφορικά με την ανταποδοτική και την ωφελιμιστική θεώρηση[1571]. Για αυτόν τον λόγο ετέθησαν και στα τρία δείγματα σχετικές ερωτήσεις για τρόπους, προτάσεις και συμβουλές για την ασφάλεια των δεδομένων[1572]. Κοινός τόπος όλων των απαντήσεων είναι η εκπαίδευση και η ενημέρωση αναφορικά με τη χρήση και τις πολιτικές ασφάλειας ηλεκτρονικών συστημάτων πληροφοριών. Είναι, επομένως, σαφές ότι η ασφάλεια των ηλεκτρονικών πληροφοριών απαιτεί ειδικές γνώσεις αναφορικά με μέτρα τα οποία πρέπει να λαμβάνονται και αφετέρου με τον συντονισμό αυτών των μέτρων και

[1570] Αναφορικά με τη «σχέση» ελευθερίας και ασφάλειας στη σύγχρονη αντεγκληματική πολιτική βλ. τις πολύ ενδιαφέρουσες αναπτύξεις του *Ν. Κουράκη,* Ασφάλεια και ελευθερία – Τα μεταξύ τους στατικά και δυναμικά όρια και του *Θ. Παπαθεοδώρου*, Κυβερνητική της Ασφάλειας και Αντεγκληματική πολιτική: η ποινική διαχείριση των δικαιωμάτων· και τα δύο πονήματα εις: *Χ. Ζαραφωνίτου (επιμ.)*, (Αν)Ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, υπ' αρ. 7 σειράς εκδόσεων Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2007, σελ. 7 επ. και 59 επ. αντίστοιχα. Πρβλ. επίσης *Ν. Κουράκη,* Το δικαίωμα του πολίτη στην ασφάλειά του, εις: Εγκληματολογικοί Ορίζοντες, τομ. Α', εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, σελ. 159 επ.

[1571] Στην παράγραφο 4.1 της διατριβής.

[1572] Η σύνοψη των σχετικών απαντήσεων ως ανωτέρω αποτελεί χαρακτηριστική αποκρυστάλλωση της εμπεδωμένης κουλτούρας σε ειδικούς (νομικούς και επιστήμονες πληροφορικής) και hackers αναφορικά με την ασφάλεια των ηλεκτρονικών συστημάτων πληροφοριών.

πρακτικών. Το συμπέρασμα το οποίο μπορούμε να εξάγουμε (ιδίως αξιοποιώντας τις απαντήσεις των hackers) είναι ότι η ασφάλεια των ηλεκτρονικών δεδομένων αποτελεί από μόνη της κουλτούρα[1573] (από την απλή παρατήρηση μπορούμε καθημερινά να επιβεβαιώσουμε γιατί οι ίδιοι οι hackers επιμένουν να μας δίνουν συμβουλές ακόμη και για ζητήματα τα οποία ίσως θεωρούνται αυτονόητα π.χ. να μην σημειώνουμε τους κωδικούς μας σε χαρτί το οποίο μπορεί να βρεθεί με οποιονδήποτε τρόπο στην κατοχή οποιουδήποτε). Η εκπαίδευση, η ενημέρωση και η επιμόρφωση[1574] για τη δημιουργία κουλτούρας ασφάλειας αποτελεί sine qua non στοιχείο αυτής, με δεδομένο τον καίριο ρόλο του ανθρώπινου παράγοντα στην προστασία των ηλεκτρονικών δεδομένων και συστημάτων πληροφοριών[1575]. Το συμπέρασμα αυτό ενισχύεται και από το γεγονός ότι ακόμη και στον ορισμό της ασφάλειας πληροφοριακών συστημάτων στο ά. 3 ν. 3979/2011[1576] αναφέρονται στοιχεία όπως «αντιλήψεις», τα οποία είναι προφανές ότι δεν μπορούν να θεσμοθετηθούν αλλά αποτελούν συστατικά στοιχεία τρόπου σκέψης και, άρα, κουλτούρας κατά τη διαχείριση των συστημάτων πληροφοριών.

Βεβαίως, προτάθηκαν, όπως καταγράφονται ανωτέρω, και πολλά άλλα μέτρα τα οποία μπορούν να λειτουργήσουν ως «αναχώματα» (κατά τις αναπτύξεις της διαχειριστικής εγκληματολογίας) ή ως «κατάλληλοι φύλακες» (σύμφωνα με την θεωρία της καθημερινής δραστηριότητας). Τα περισσότερα από αυτά (όπως η «ευταξία» της επιχείρησης, ο έλεγχος της πρόσβασης κ.ά.) πράγματι έχουν να κάνουν με την «κουλτούρα της ασφάλειας», όπως αυτή διατυπώθηκε ανωτέρω.

Διάσταση στην οποία πρέπει να δοθεί ιδιαίτερο βάρος είναι αυτή κατά την οποία το hacking φαίνεται (και ερευνητικά σύμφωνα με τα ανωτέρω αποτελέσματα – υπενθυμίζεται ότι το 52% των hackers δήλωσε ότι είναι κάτω των 20 ετών) να είναι δραστηριότητα η οποία αφορά κυρίως ανηλίκους[1577]. Σε τέτοιες περιπτώσεις, επομένως, είναι σκόπιμο να στρέψουμε τη θεώρηση της αντεγκληματικής πολιτικής

[1573] Βλ. και παράγραφο 9.2 του παρόντος πονήματος.

[1574] Βλ. και πρόταση του *Ιωάν. Αγγελή*, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, ΠοινΔικ 8-9/2005, σελ. 1066, για εκπαίδευση του αρμόδιου για την έρευνα, δίωξη και εκδίκαση ηλεκτρονικών εγκλημάτων εκ μέρους της Πολιτείας (με σεμινάρια και μετεκπαιδεύσεις) με στόχο την απονομή ορθής δικαιοσύνης σε θέματα ηλεκτρονικού εγκλήματος.

[1575] Για τον σημαντικό ρόλο του ανθρώπινου παράγοντα στην ασφάλεια των ηλεκτρονικών πληροφοριών βλ. *Budi Arief & Denis Besnard,* Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 9 καθώς και παράγραφο 9.2 του παρόντος πονήματος κατωτέρω.

[1576] ...όπως παρουσιάστηκε στην παράγραφο 1.3 του παρόντος πονήματος.

[1577] Πρβλ. ενδεικτικά *Αγγ. Πιτσελά*, Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, εκδ. Π. Ν. Σάκκουλα, ζ' εκδ., Αθήνα-Θεσσαλονίκη, 2013.

στην ένταξη των ανηλίκων σε δικαιοκρατούμενο περιβάλλον, με δεδομένο ότι έρευνες αυτοομολογούμενης παραβατικής δραστηριότητας έχουν καταδείξει ότι «*η παραβατική συμπεριφορά κατά την περίοδο της ανήλικης νεότητας είναι παροδική, εφήμερη και από στατιστική άποψη κανονική, συνοδεύει δηλαδή τη διαδικασία ωρίμανσης του ανθρώπου και δεν αποτελεί σύμπτωμα μιας κυοφορούμενης εγκληματικής κατάπτωσης, ενώ εμφανίζεται αυθόρμητα με την ομαλή μετάβαση στην ενηλικότητα*»[1578]. Αναφορικά, λοιπόν, με τη δικαιική πρόληψη σε περιπτώσεις παραβατικών ανηλίκων πρέπει να αποφεύγονται τα μέτρα με κατασταλτικό χαρακτήρα[1579]. Εξάλλου, υποστηρίζεται ότι για το ευρύ κοινωνικό σύνολο λειτουργούν αποτρεπτικά κυρίως άτυποι εσωτερικευμένοι μηχανισμοί ελέγχου[1580]. Η ενημέρωση και η εκπαίδευση (ως ανωτέρω[1581]) και η στροφή των ενδιαφερόντων τους π.χ. προς ασφαλέστερο διαδίκτυο μπορούν να αναπτύξουν αυτούς τους μηχανισμούς και να ενδυναμώσουν τους βασικούς κοινωνικοποιητικούς θεσμούς, οι οποίοι θα συνδράμουν τους ανήλικους παραβάτες στο να ενταχθούν ομαλά στο σύγχρονο «ψηφιακό περιβάλλον». Βέβαια, είναι απαραίτητες δομές στις οποίες οι «περίεργοι» νέοι που γοητεύονται από το hacking να μπορούν να εκδηλώσουν την

[1578] Έτσι *Αγγ. Πιτσελά,* Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002, σελ. 540.

[1579] Βλ. αναλυτικά για την κοινωνική, τη δικαιική και την περιστασιακή πρόληψη και γενικότερα για την αντεγκληματική πολιτική σε περιπτώσεις παραβατικών ανηλίκων το λεπτομερές πόνημα του *Ν. Κουράκη*, Δίκαιο παραβατικών ανηλίκων, εκδ. Αντ. Ν. Σάκκουλας, β' εκδ., Αθήνα – Κομοτηνή, 2012, σελ. 643 επ. καθώς και επίσης του *Ν. Κουράκη*, Η πρόληψη της παραβατικότητας των ανηλίκων στην Ελλάδα, εις: *Αγ. Τσήτσουρα (υπεύθυνη έκδοσης)*: Αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997, σελ. 63 επ. Κριτική στα κατασταλτικά μέτρα κάνει και ο *Αντώνης Μαγγανάς,* Οι δύο όψεις του κοινωνικού ελέγχου: καταστολή και εναλλακτικά μέτρα, εις: *Αγ. Τσήτσουρα (υπεύθυνη έκδοσης)*: Αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997, σελ. 129 επ. και ο *Στρ. Γεωργούλας*, Η παραβατικότητα ανηλίκων ως προβληματική κατάσταση, ΠοινΔικ 8-9/2003, σελ. 987, ο οποίος υποστηρίζει ότι η κατασταλτική παρέμβαση σε περιπτώσεις παραβατικότητας ανηλίκων έχει φθάσει σε «αδιέξοδο».

Συγκεκριμένα για την «αποδικαστικοποίηση» της παραβατικότητας των ανηλίκων βλ. *Χ. Ζαραφωνίτου*, Εμπειρική εγκληματολογία, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 212 επ. Εξάλλου, και κατά την Πιτσελά «*Δεδομένης της ελαφράς φύσης, της κανονικότητας, του παροδικού και του επεισοδιακού χαρακτήρα ενός μεγάλου μέρους της παραβατικότητας των ανηλίκων, η διεξαγωγή της ποινικής διαδικασίας θα πρέπει να θεωρηθεί ως δυσανάλογη*» (έτσι *Αγγ. Πιτσελά*, Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσσαλονίκη, 2002, σελ. 540). Βλ. επίσης στο εν λόγω πόνημα της Πιτσελά σελ. 549 επ. αναφορικά με την ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων. Σύμφωνα με όλα τα ανωτέρω και ο Παπαθεοδώρου υποστηρίζει ότι «*Η αντιμετώπιση της παραβατικότητας – εγκληματικότητας των ανηλίκων στηρίζεται παραδοσιακά στις ιδέες της δικαιοσύνης, της παιδαγωγικής μεταχείρισης και της επανένταξης*» (βλ. *Θ. Παπαθεοδώρου*, Δικαιοσύνη ενηλίκων και ανήλικοι δράστες: Τα έσχατα όρια της «μηδενικής ανοχής» στις ΗΠΑ, ΠοινΔικ 1/2000, σελ. 77).

[1580] Βλ. *Έφη Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 188.

[1581] ... αλλά και στην παράγραφο 9.2 του παρόντος πονήματος.

περιέργειά τους (π.χ. ιστοσελίδες με εικονικά «προβλήματα hacking προς λύση»[1582] κ.ά.).

Σε κάθε περίπτωση, διαπιστώθηκε ότι είναι προκριτέα η πρόληψη και η ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων με τη διατύπωση αρκετών προτάσεων και ότι δεν εξαντλείται η προσπάθεια ενίσχυσης της ασφάλειας των ηλεκτρονικών συστημάτων πληροφοριών στην ποινική νομοθεσία. Ακόμη και η πρόταση για διοικητικές ποινές[1583] καθιστά πιο ισχυρή την άποψη ότι η ποινική καταστολή (πρέπει να) χρησιμοποιείται ως ultimum refugium[1584]. Σε αυτό ίσως το πνεύμα οι hackers αποδέχονται τον ρόλο της Πολιτείας. Ακόμη πιο πέρα, η «επιθυμία» των περισσότερων τεχνικών πληροφορικής να συνεργαστούν με hackers για τη βελτίωση μιας πρακτικής ασφάλειας ενδεχομένως να ανοίγει τον δρόμο για τον ποινικό νομοθέτη προκειμένου να θεσπίσει ενός είδους «έμπρακτη μετάνοια»[1585] στο πλαίσιο και της συμφιλιωτικής δικαιοσύνης[1586] σε περιπτώσεις αδικημάτων χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα, ούτως ώστε να δοθεί η ευκαιρία σε hackers να αξιοποιήσουν το ταλέντο τους για την ενίσχυση της ασφάλειας των ηλεκτρονικών υπολογιστών και τη βελτίωση των προγραμμάτων αλλά και να μην αποκοπούν λόγω της στιγματιστικής λειτουργίας της ποινής[1587] από το κοινωνικό γίγνεσθαι.

[1582] Σύμφωνα και με τον Raymond (βλ. παράγραφο 2.7 του παρόντος πονήματος).

[1583] Αναφορικά με τις διοικητικές ποινές βλ. *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 31 επ.

[1584] Κατά την εύστοχη διατύπωση του Κουράκη «... *στη σύγχρονη ελληνική κοινωνία οι διοικητικές ποινές, λόγω πολλές φορές των σημαντικών επιπτώσεών τους, θεωρούνται από τους ενδιαφερόμενους ως εξίσου, τουλάχιστον, επώδυνες και στιγματιστικές προς τις συνήθεις γνήσιες ποινές...*» (έτσι *Ν. Κουράκης*, Η ουσιαστική έννοια του εγκλήματος ως έρεισμα για τη διάκριση γνήσιων και μη γνήσιων ποινών, εις: *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π., σελ. 80).

[1585] Πρβλ. ενδεικτικά για την έμπρακτη μετάνοια: *Γ. Γεωργάτου*, Ο θεσμός της έμπρακτης μετάνοιας και η δικαστηριακή πρακτική σε σχέση με αυτόν, ΠΕΙΡΝ 2002/5, *Ν. Λίβου*, Η απαλλαγή από την ποινή επί ικανοποιήσεως του ζημιωθέντος μέχρι εκδόσεως της οριστικής αποφάσεως (Σκέψεις για την ποινική συνδιαλλαγή και την αποκατάσταση του θύματος στο ισχύον Ποινικό δίκαιο), ΠοινΧρ 2000, σελ. 289 επ., *Κ. Γκρόζου*, Το άρθρο 379 ΠΚ μετά την τροποποίησή του με το άρθ. 14 παρ. 13 του ν. 2721/99, Υπεράσπιση, 2000, σελ. 521 επ.

[1586] Πρβλ. *του γράφοντος*, Οι «κατά παρέκκλιση» διαδικασίες και η αποκαταστατική-συμφιλιωτική δικαιοσύνη / Ιστορική και δογματική προσέγγιση, ηλεκτρονικό εγκληματολογικό περιοδικό τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 7, Φεβρουάριος 2008, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1207246182.

[1587] Για τον στιγματιστικό χαρακτήρα της ποινής πρβλ. *Ν. Κουράκη*, Εισαγωγή στη θεωρία της ποινής, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 11 επ.

9. ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Πέρα από νομοθετικές ρυθμίσεις, τα φυσικά και ψηφιακά μέσα προστασίας έχουν βαρύνουσα σημασία χάρη στη δυνατότητά τους να αναχαιτίζουν μία πληροφορική προσβολή. Η ενίσχυση της ασφάλειας ως όρος έχει ως κεντρική ιδέα την πρακτική της ισχυροποίησης του στόχου (hardening the target)[1588] είτε με τεχνικές μεθόδους είτε με πρακτικές, οι οποίες στοχεύουν στο να προφυλάξουν το σύστημα πληροφοριών. Ο συνδυασμός τεχνικών, πρακτικών και νομοθετικών ρυθμίσεων ουσιαστικά προβλέπεται και από το ά. 3 του ν. 3979/2011 στο οποίο ορίζεται η ασφάλεια πληροφοριακών συστημάτων ως *«ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος (εφεξής ΠΣ), αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή»*. Η συνδυαστική εφαρμογή αυτή, με διεθνικό βλέμμα [ίσως και ακόμη και με μορφή «άγουρου/ήπιου δικαίου» ("soft law")[1589]][1590] μπορεί να λειτουργήσει ανασχετικά στις προσβολές που πιθανόν στην κοινωνία ηλεκτρονικής διακινδύνευσης να δεχθούν οι ηλεκτρονικές πληροφορίες και τα συστήματα πληροφοριών.

[1588] Για τον όρο "hardening the target" πρβλ. *Andrew Newton, Michelle Rogerson and Alex Hirschfield*, Relating Target Hardening to Burglary Risk Experiences from Liverpool, University of Huddersfield, 2008, url: http://britsoccrim.org/volume8/10Newton08.pdf.

[1589] Για το "soft law" πρβλ. *Kenneth W. Abbot and Duncan Snidal*, Hard and Soft Law in International Governance, International Organization, Vol. 54, p. 421, 2000 (url: file:///C:/Users/FSpyropoulos/Downloads/SSRN-id1402966.pdf).

[1590] Βλ. και *Jovan Kurbalija*, Internet governance and international law, Reforming Internet Governance: Perspectives from WGIG, url: http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf, pp. 112-114.

9.1 Τεχνικές και πρακτικές για την ασφάλεια των ηλεκτρονικών συστημάτων πληροφοριών

9.1.1 Έλεγχος της πρόσβασης – προφύλαξη ηλεκτρονικών δεδομένων

Η πρώτη γραμμή άμυνας ενός πληροφορικού συστήματος είναι αναμφισβήτητα ο έλεγχος της πρόσβασης (access control). Το σύστημα πρέπει να εξασφαλίζει ότι οι χρήστες δηλώνουν την πραγματική τους ταυτότητα και ότι είναι εξουσιοδοτημένοι να χρησιμοποιούν το σύστημα (με έναν συγκεκριμένο τρόπο). Ένα πρώτο βήμα για την εξασφάλιση του ελέγχου της πρόσβασης σε συστήματα υπολογιστών είναι η εμπέδωση βασικών αρχών ασφάλειας, που αφορούν στους ηλεκτρονικούς υπολογιστές και τα συστήματα πληροφοριών, από όλους τους χρήστες. Στις βασικές αυτές αρχές συγκαταλέγονται η διασφάλιση της εισόδου μέσω κωδικών λέξεων (passwords) και η προσοχή για αποφυγή κλοπής ταυτότητας (όπως αναπτύχθηκε ανωτέρω). Επιπρόσθετα, σημαντικές είναι και οι διαδικασίες προφύλαξης (με κατάλληλα προγράμματα) εξωτερικών συσκευών που συνδέονται με τον υπολογιστή (π.χ. εξωτερικές συσκευές αποθήκευσης) ή προγραμμάτων (λογισμικό)[1591]. Τέλος και σημαντικότερο ίσως είναι η ιδιαίτερη προσοχή στο ποιος έρχεται σε επαφή με τις ψηφιακές συσκευές καθενός. Έχοντας ως δεδομένο ότι στις ηλεκτρονικές συσκευές που χρησιμοποιούνται σήμερα («έξυπνα» τηλέφωνα, tablets κ.ά.) σχεδόν σε όλες τις περιπτώσεις ο χρήστης έχει αποθηκεύσει αυτόματα τους κωδικούς πρόσβασής του για περιήγηση σε ιστοσελίδες από τη συγκεκριμένη συσκευή, απαιτείται ιδιαίτερη επιμέλεια στο να μην εγκαταλείπεται εκτός της προσοχής η ψηφιακή αυτή συσκευή και έτσι να αποκλείεται η φυσική πρόσβαση στο σύστημα πληροφοριών των επίδοξων παραβιαστών.

Σε αυτό το πνεύμα της ιδιαίτερης προσοχής εκ μέρους των χρηστών κινούνται και οι απαντήσεις των hackers στην ερώτηση 11 του οικείου ερωτηματολογίου, όπως παρουσιάζονται παραπάνω. Όπως ήδη είδαμε, οι ίδιοι οι hackers εστιάζουν τις

[1591] Βλ. *D. Russell and G. Gangemi*, Computer Security Basics, O'Reilly and Associates, 1991, σελ. 52.

συμβουλές τους στην προσοχή για το ποιος έρχεται σε επαφή με στοιχεία τα οποία μπορούν να του παράσχουν πρόσβαση σε σύστημα πληροφοριών (π.χ. passwords) και στα ηλεκτρονικά προγράμματα τα οποία εισάγονται σε συσκευή πληροφορικής.

9.1.2 Χρήση τεχνολογικών κατασκευών για την ασφάλεια των πληροφοριών (αυτοματοποιημένα συστήματα ανίχνευσης – βιομετρικός έλεγχος – «πύρινα τείχη»...)

Το ζήτημα του ελέγχου πρόσβασης, όπως παρουσιάστηκε στην προηγούμενη παράγραφο, συναρτάται άμεσα με την εξουσιοδοτημένη πρόσβαση. Σε αυτό το πλαίσιο, η βιομηχανία ασφάλειας των πληροφοριών έχει αναπτύξει μία σειρά από πραγράμματα αλλά και επιτηδευμένες τεχνικές για την αποτροπή της μη εξουσιοδοτημένης / χωρίς δικαίωμα πρόσβασης σε συστήματα πληροφοριών.

Προγράμματα τα οποία λειτουργούν προστατευτικά για κάθε σύστημα πληροφοριών και μπορούν να «εγκατασταθούν» (κατά την τεχική έννοια – να τεθούν δηλαδή σε λειτουργία) σε αυτό είναι, ενδεικτικά, τα ***προγράμματα antivirus*** (προστατεύουν το σύστημα από τους ιούς[1592]). Η συχνή αναβάθμισή των προγραμμάτων και επικαιροποίηση αυτών είναι απαραίτητη ώστε να μπορούν να αντιμετωπίζουν κάθε καινούριο ιό που εμφανίζεται (τα περισσότερα, βέβαια, antivirus, προβαίνουν σε αυτόματη εγκατάσταση των ενημερώσεων). Λειτουργούν, μάλιστα, με τέτοιο τρόπο ώστε να εντοπίζουν τον ιό πριν αυτός εκτελεστεί και προσβάλει το υπολογιστικό σύστημα. Άλλου τύπου προγράμματα προστασίας είναι τα ***προγράμματα anti-spam*** [εγκαθίστανται στον κεντρικό εξυπηρετητή ηλεκτρονικού ταχυδρομείου του συστήματος πληροφοριών και συνδράμουν στο να αποφευχθεί η ανεπιθύμητη και ενοχλητική αλληλογραφία (SPAM)]. Επιπρόσθετα, και τα ***πύρινα τείχη (firewalls)*** συνιστούν μέσα που προστατεύουν τα πληροφορικά συστήματα από το hacking[1593]. Τα πιο επιτηδευμένα firewalls προστατεύουν το σύστημα από παράνομη πρόσβαση

[1592] Βλ. ανωτέρω παράγραφο 2.11.2.2.6 του παρόντος πονήματος. Πρβλ. και ένα από τα κλασικά πονήματα για την προστασία από ιούς *Colin Haynes*, Τεχνικές προστασίας από τους ιούς υπολογιστών, Μετάφραση: *Ελένη Καλογήρου*, εκδ. Μ. Γκιούρδας, Αθήνα, 1991.

[1593] Σχετικά προγράμματα προτείνονται στα αποτελέσματα της έρευνας (βλ. ανωτέρω) και από το δείγμα των νομικών και από το δείγμα των επιστημόνων πληροφορικής (βλ. απαντήσεις στην ερώτηση 7 αντίστοιχα στο ερωτηματολόγιο κάθε δείγματος).

προερχόμενη από εξωτερική του πληροφορικού συστήματος πηγή. Ένα firewall δεν είναι αναγκαίο να είναι εγκατεστημένο στη συνολική περίμετρο ενός πληροφορικού συστήματος, ενώ είναι ικανό να προστατεύσει από τη μη εξουσιοδοτημένη πρόσβαση και ένα μόνο μέρος του συστήματος, όπως για παράδειγμα έναν τομέα απορρήτων[1594]. Ωστόσο, στα μειονεκτήματα των firewalls καταλογίζονται το υψηλό οικονομικό τους κόστος (ιδίως για πολύ αποτελεσματικά firewalls) και η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και, τέλος, το γεγονός ότι η προστασία που παρέχουν είναι μερική και σχετική[1595].

Σημαντική, επίσης, είναι και η ***ενημέρωση του λειτουργικού συστήματος (update)***[1596] ούτως ώστε να διασφαλίζεται η ομαλή λειτουργία του και να βελτιώνεται η προστασία του υπολογιστή, καθώς τα συστήματα ενημερώνονται με βάση την προστασία από νέες απειλές. Περαιτέρω, για την προστασία ενός συστήματος πληροφοριών χρειάζεται συχνή εγκατάσταση των τελευταίων ενημερώσεων (update) του web browser (προγράμματος περιήγησης στο διαδίκτυο). Επιπλέον, καλό είναι να αφαιρεθεί η δυνατότητα αποθήκευσης των cookies (Third Party Cookies)[1597], να ενεργοποιηθεί η εμπλοκή αναδυόμενων παραθύρων (pop–up windows), να γίνεται συχνή εκκαθάριση του ιστορικού και των προσωρινών αρχείων του προγράμματος περιήγησης στο διαδίκτυο (browser) και να απενεργοποιηθούν τα πρόσθετα (Add-On και Plugins) τα οποία δεν χρησιμοποιούνται[1598].

Αναφορικά με επιτηδευμένες τεχνικές, από τις πιο σημαντικές είναι τα ***αυτοματοποιημένα συστήματα ανίχνευσης παρείσδυσης***, συσκευές που έχουν σχεδιαστεί ώστε να αναγνωρίζουν διάφορες ανωμαλίες στα πρότυπα χρήσης. Έτσι, όταν κάποιος χρήστης επιχειρήσει μία λειτουργία χωρίς έγκριση ή εξουσιοδότηση γίνεται άμεσα αντιληπτός. Επίσης, οι ***βιομετρικές συσκευές***[1599] [1600] αναγνωρίζουν

[1594] Βλ. *Γρηγόρης Λάζος*, Πληροφορική & Έγκλημα, όπ. π., σελ. 225-226.

[1595] Έχει καταγραφεί π.χ. ότι τα modems (σ.σ. σήμερα τα routers) είναι ένα σημείο εισόδου στο δίκτυο που υπερφαλλαγγίζει κάθε firewall (βλ. *Αναστασία Ζάννη*, Το διαδικτυακό έγκλημα, όπ. π. σελ. 134).

[1596] Σχετική συμβουλή για ενημέρωση των προγραμμάτων δίνεται και στις απαντήσεις των hackers, ως ανωτέρω.

[1597] Αναφορικά με τα "cookies" και την νομοθετική τους αντιμετώπιση βλ. ανωτέρω και παράγραφο 5.4.1 του παρόντος πονήματος.

[1598] Βλ. αναλυτικές συμβουλές στην ιστοσελίδα του Κέντρου Πληροφορικής & Νέων Τεχνολογιών Ηλείας (url: http://dide.ilei.sch.gr/keplinet/tech/virus.php).

[1599] *Russell G. Smith*, Identification systems: a risk assessment framework, TRENDS & ISSUES in crime and criminal justice, Australian Institute of Criminology, No. 324, September 2006 και *Russell G. Smith*, Travelling in Cyberspace on a False Passport: Controlling Transnational Identity related crime, The British Criminology Conference: Selected Proceedings. Volume 5, Papers from the British

την ταυτότητα του χρήστη με βάση κάποια φυσικά χαρακτηριστικά, όπως είναι η φωνή, το δακτυλικό αποτύπωμα[1601] ή η εικόνα του αμφιβληστροειδούς χιτώνα του ματιού. Αυτά τα χαρακτηριστικά θεωρούνται αναλλοίωτα και μοναδικά για κάθε άνθρωπο, καθώς είναι πολύ δύσκολη η αντιγραφή τους. Πέρα όμως από την ταυτότητα του χρήστη, οι βιομετρικές συσκευές μπορούν να παρέχουν και άλλες πληροφορίες, όπως ο χρόνος (ενεργοποίησης, παραμονής και λήξης της πρόσβασης) και ο γεωγραφικός τόπος του χρήστη[1602]. Υπάρχουν, βέβαια, και οι ***επιτηδευμένες τεχνικές επικύρωσης της ταυτότητας***, μέσω των οποίων ο υπολογιστής εξυπηρέτησης δικτύου (server) διατυπώνει απροειδοποίητα ένα πρόβλημα (π.χ. μία ερώτηση) σε ένα χρήστη, ο οποίος υπολογίζει την απάντηση χρησιμοποιώντας κάποιο σύμβολο επικύρωσης.

9.1.3 Σωστή λειτουργία της επιχείρησης αναφορικά με την ασφάλεια των ηλεκτρονικών πληροφοριών

Μία σημαντική πρακτική «άμυνας» ενάντια στο hacking συνιστά η «ευταξία» στην επιχείρηση ("housekeeping"). Σε αυτή συμπεριλαμβάνονται ενδεικτικά το προσηλωμένο στην ασφάλεια των πληροφοριών σύστημα διοίκησης, η διατήρηση και συνεχής ενημέρωση λίστας που να περιέχει τους ισχύοντες ηλεκτρονικούς λογαριασμούς, το κλείσιμο αδρανών ηλεκτρονικών λογαριασμών και ο περιορισμός των χρηστών με άδεια προνομιακής πρόσβασης. Η «ευταξία» μπορεί να επιτευχθεί σε μία επιχείρηση μέσω ειδικών προγραμμάτων λογισμικού ή μέσω μίας ενσυνείδητης διοίκησης, η οποία με διάφορα μοντέλα να επιθεωρεί τη λειτουργία του συστήματος και να παρεμβαίνει κάθε φορά που διαπιστώνει κάποια ανωμαλία στη χρήση ή το

Society of Criminology Conference, Keele, July 2002, published August 2003. Editor: Roger Tarling. ISSN 1464-4088.

[1600] Βλ. αναφορικά με την εφαρμογή της βιομετρίας στην πράξη, την τεχνική ανάλυση και την νομική αντιμετώπιση των βιομτρικών εφαρμογών το αναλυτικό άρθρο του *Γ. Λαζαράκου*, Βιομετρία: Προστασία των προσωπικών δεδομένων μέσω της επεξεργασίας ευαισθήτων (σωματικών) πληροφοριών, ΠοινΔικ 11/2001, σελ. 1165 επ.

[1601] Πάντως κατά τον Φαρσεδάκη δράστες έχουν καταφέρει ακόμη και να πλαστογραφήσουν δακτυλικά αποτυπώματα (*Ιακ. Φαρσεδάκης,* Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π., σελ. 4).

[1602] Βλ. *D. Denning and P. McDoran,* Location-Based System Delivers User Authentication Breakthrough, Computer Security Alert, 1999, σελ. 1.

συγχρονισμό καθώς και, βεβαίως, με τον συνδυασμό και των δύο. Η ως άνω πρακτική λειτουργεί προληπτικά σε τεχνικές των hackers, όπως π.χ. το dumpster diving, και υπαγορεύεται από μια γενικότερη κουλτούρα δημιουργίας ασφάλειας για της ηλεκτρονικές πληροφορίες[1603].

9.1.4 Αξιοποίηση της πείρας και κατάρτισης των hackers

Ένα από τα πιο δημιουργικά μέσα βελτίωσης της άμυνας των πληροφορικών συστημάτων από τεχνολογικής πλευράς αποτελεί η αξιοποίηση των hackers στην κατεύθυνση της ένταξης των ικανοτήτων τους στην ανάπτυξη της ασφάλειας των υπολογιστών[1604] [1605]. Ήδη έχουμε αναφερθεί στο "ethical hacking" και στο πώς οι ηθικοί hackers μπορούν να λειτουργήσουν για την ανακάλυψη κενών ασφαλείας και την ενίσχυση της ασφάλειας υπολογιστικών συστημάτων[1606]. Άξιο, όμως, στοιχείο αναφοράς εν προκειμένω είναι και το γεγονός ότι, σύμφωνα με τα αποτελέσματα της ανωτέρω έρευνας, το 86% των επιστημόνων πληροφορικής θα συνεργαζόταν με κάποιον hacker για τη βελτίωση μιας πρακτικής ασφάλειας[1607] καθώς και το ότι σε ποσοστό 28,85% από το γενικό σύνολο οι επιστήμονες πληροφορικής διατυπώνουν την άποψη ότι οι hackers μπορούν να συμβάλλουν εντοπίζοντας τα κενά ασφαλείας συστημάτων και προωθώντας γενικότερα την ασφάλεια των προγραμμάτων ηλεκτρονικών υπολογιστών και των υπολογιστικών δικτύων.

Στον βαθμό κατά τον οποίο οι hackers κινητοποιούνται από την περιέργειά τους για τα ηλεκτρονικά συστήματα πληροφοριών, θα πρέπει να τους δοθεί η δυνατότητα πρόσβασης στην τεχνολογία για την εξέλιξη αυτής. Οι ομάδες των hackers πρέπει να

[1603] Βλ. αναπτύξεις στην παράγραφο 8.4 και ιδίως στην παράγραφο 9.2 του παρόντος πονήματος σχετικά με την κουλτούρα ασφάλειας των ηλεκτρονικών πληροφοριών.

[1604] Βλ. *P. N. Grabosky and R. G. Smith*, Crime in the digital age, Annandale: Transaction, 1998, σελ. 57.

[1605] Βλ. ρεπορτάζ ενημερωτικής ιστοσελίδας www.in.gr «100.000 δολάρια η ανταμοιβή επαγγελματία χάκερ για κενό στα Windows 8.1», url: http://tech.in.gr/news/article/?aid=1231268796.

[1606] Βλ. παράγραφο 2.9.1. του παρόντος πονήματος.

[1607] Στο δείγμα των επιστημόνων πληροφορικής προτείνεται η καταβολή «αδρών αμοιβών» σε hackers για τη συνεργασία τους σχετικά με την ασφάλεια των ηλεκτρονικών δεδομένων (έτσι στο ερωτηματολόγιο 91 του δείγματος επιστημόνων πληροφορικής).

προσεγγιστούν από την κυρίαρχη κουλτούρα[1608] με κοινό στόχο την τεχνολογική εξέλιξη, χωρίς τεχνοφοβικές αντιλήψεις. Εξάλλου, τα όποια όρια, τα οποία είναι ίσως αναγκαίο να καθοριστούν, υπάρχει περίπτωση να γίνουν αποδεκτά και από τους ίδιους τους hackers (όπως κατεδείχθη ανωτέρω από τα ερευνητικά αποτελέσματα). Εν ολίγοις, η κυρίαρχη κουλτούρα αναφορικά με την ασφάλεια των συστημάτων πληροφοριών έχει να μάθει αρκετά από τους hackers, κάποιες φορές όχι μόνο αναφορικά με την ασφάλεια των πληροφοριών αλλά και με τη διαχείριση αυτών[1609].

9.1.5 Κρυπτογραφία

Μία από τις βασικότερες μεθόδους προστασίας των πληροφοριών που μεταβιβάζονται από πληροφορικό σύστημα σε πληροφορικό σύστημα μέσω δικτύων είναι το τεχνικό μέσο της κρυπτογράφησης[1610]. Καταρχάς, η κρυπτογράφηση ή κρυπτογραφία ορίζεται ως η επιστήμη της κρυφής γραφής, μέσω της οποίας τα δεδομένα μπορούν να κωδικοποιηθούν με τέτοιο τρόπο ώστε το μήνυμα να εμφανιστεί μόνο στον άμεσα ενδιαφερόμενο.

Σε γενικές γραμμές, με την τεχνική της κρυπτογραφίας οι αναγνώσιμες πληροφορίες κωδικοποιούνται σε σειρές από ακατανόητες διατάξεις αλφαριθμητικών χαρακτήρων, οι οποίες επιτρέπουν την ασφαλή διατήρηση και διαβίβαση κρίσιμων ή εμπιστευτικών πληροφοριών μέσω ηλεκτρονικών δικτύων. Εν συνεχεία, οι κρυπτογραφημένες πληροφορίες αποκωδικοποιούνται και καθίστανται προσβάσιμες και αναγνώσιμες μόνο από τα άτομα με την κατάλληλη εξουσιοδότηση, δηλαδή από όσους κατέχουν τις σχετικές τεχνικές αποκρυπτογράφησής τους.

Η χρησιμότητα, δε, της κρυπτογράφησης των πληροφοριών εδράζεται σε τέσσερεις βασικές ιδιότητες. Πρώτον, στην ***εμπιστευτικότητα (confidentiality)***, στην εξασφάλιση, δηλαδή, ότι οι πιθανοί υποκλοπείς δεν θα μπορέσουν να αποκτήσουν

[1608] Βλ. αναπτύξεις σχετικές με την (υπο)κουλτούρα των hackers στο κεφάλαιο 2 παραγραφος 2.8 της παρούσας.

[1609] Βλ. ανωτέρω απαντήσεις των hackers σχετικά με την παροχή συμβουλών για ενίσχυση της ασφάλειας στα ηλεκτρονικά συστήματα πληροφοριών.

[1610] Προτείνεται και από το δείγμα νομικών και από το δείγμα επιστημόνων πληροφορικής ως πρακτική, σύμφωνα με την καταγραφή των αποτελεσμάτων της ανωτέρω έρευνας. Ωστόσο, επισημαίνεται η απάντηση hacker κατά την οποία «ό,τι κρυπτογραφείται αποκρυπτογραφείται» (ερωτηματολόγιο υπ' αρ. 15 στο δείγμα hackers).

πρόσβαση στο περιεχόμενο των κρυπτογραφημένων πληροφοριών. Δεύτερον, στην ***εξακρίβωση (authentication)***, στην εξασφάλιση της ταυτοπροσωπίας του αποστολέα της πληροφορίας από τον νόμιμο αποδέκτη του μέσω της διαπίστωσης της ψηφιακής υπογραφής του τελευταίου. Τρίτον, στην ***αρτιότητα (integrity)***, στην εξασφάλιση, δηλαδή, ότι το περιεχόμενο των πληροφοριών δεν έχει αλλοιωθεί κατά τη διαβίβασή τους από τον αποστολέα στον παραλήπτη και τέταρτον, στη ***μη αποκηρυξιμότητα (non-repudation)***, στην εξασφάλιση, δηλαδή, ότι ο συντάκτης της πληροφορίας δεν μπορεί ψευδώς να αρνηθεί ούτε τη σύνταξή της αλλά ούτε και την αποστολή της[1611].

Ειδικότερα, το ζεύγος *ένκρυψη και απόκρυψη* αναφέρεται σε ορισμένα προγράμματα, τα οποία επιτρέπουν την κρυπτογράφηση ενός αρχείου με τέτοιο τρόπο ώστε να μην εκτίθεται δημόσια. Η διαδικασία που ακολουθείται για την ένκρυψη των δεδομένων είναι απλή: πριν την κρυπτογράφηση το πρόγραμμα ζητά να πληκτρολογηθεί ένα συνθηματικό. Αμέσως μετά, το πρόγραμμα κρυπτογραφεί τα δεδομένα που περιέχονται στο αρχείο. Όταν επιλεγεί η αποκρυπτογράφηση του αρχείου στο πρόγραμμα ζητείται το συνθηματικό, προκειμένου να υπάρξει επαναφορά σε χρησιμοποιήσιμη μορφή. Η μεταμφίεση, λοιπόν, του μηνύματος ώστε να κρύβεται το περιεχόμενό του είναι γνωστή ως *ένκρυψη*. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext) ενώ το ακατάληπτο μήνυμα είναι γνωστό ως ciphertext, του οποίου η διαδικασία μετατροπής του σε απλό κείμενο ονομάζεται *απόκρυψη*[1612].

Ωστόσο, στο παρόν σημείο είναι αναγκαία η οριοθέτηση της κρυπτογραφίας από την ένκρυψη και την απόκρυψη, αφού οι έννοιες αυτές βρίσκονται τόσο κοντά ώστε τείνουν να ταυτιστούν. Η κρυπτογραφία είναι η βάση, το «αρχιτεκτονικό σχέδιο» μέσα στο οποίο θα λάβει χώρα η διαδικασία της ένκρυψης και της απόκρυψης, όπως αυτές ορίστηκαν παραπάνω. Κρυπτογράφηση είναι ουσιαστικά ο αλγόριθμος (cipher), ο οποίος χρησιμοποιείται τόσο για την ένκρυψη όσο και την απόκρυψη[1613]. Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή του αντίστροφου αλγόριθμου[1614].

[1611] Βλ. *Γρηγόρης Λάζος*, Πληροφορική & έγκλημα, όπ. π., σελ. 225-228.

[1612] Βλ. σχετικά με τους ορισμούς αυτούς βλ. συγκεκριμένη ανάπτυξη του *Ιωάννη Αγγελή*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 12/2001, 1295.

[1613] Βλ. *Αναστασία Ζάννη*, Το διαδικτυακό έγκλημα, όπ. π., σελ. 141.

[1614] Βλ. *Χρήστος Ε.Τσουραμάνης*, Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου, όπ. π., σελ. 134.

Ιδίως πριν την εξάπλωση του διαδικτύου ο όρος «κρυπτογραφία» περιοριζόταν μόνο στον στρατιωτικό και τον διπλωματικό χώρο. Σήμερα, φυσικά ή νομικά πρόσωπα τα οποία ελέγχουν συστήματα πληροφοριών με σημαντικό περιεχόμενο μπορούν να απευθυνθούν σε ειδικούς προγραμματιστές προκειμένου να κρυπτογραφήσουν τα δεδομένα τους και με αυτόν τον τρόπο να τα προφυλάξουν περισσότερο από κάποια τυχόν χωρίς δικαίωμα/αθέμιτη πρόσβαση ή/και ηλεκτρονική επίθεση[1615].

9.2 Ηθική διαπαιδαγώγηση, ενημέρωση και εκπαίδευση

Στο κεφάλαιο 3 του παρόντος πονήματος παρουσιάστηκαν θεωρίες σύμφωνα με τις οποίες το hacking αποδίδεται στην μειωμένη ανάπτυξη του ηθικού κριτηρίου των επιχειρούντων τέτοιες ενέργειες (θεωρία «ηθικής ανάπτυξης»[1616], "Moral Beliefs and Moral Judgment Theory"[1617]). Σε αυτό το πνεύμα προσδίδεται στη βιβλιογραφία πρωτεύων ρόλος στην ηθική διαπαιδαγώγηση σε ό,τι αφορά στη χρήση των ηλεκτρονικών υπολογιστών[1618]. Το γεγονός της έλλειψης ηθικών νορμών στο διαδίκτυο, το οποίο έχει ήδη επισημανθεί και στην παρούσα (κατά παραπομπή και σε σημαντικούς επιστήμονες[1619]), καθιστά περισσότερο από αναγκαία τη διαμόρφωση

[1615] Η κρυπτογράφηση φαίνεται τόσο αποτελεσματική που χρησιμοποιείται στο διαδίκτυο ακόμη και για τη διενέργεια παράνομων πράξεων, οι οποίες πρέπει να κρατηθούν κρυφές και από την κοινή θέα αλλά και από τις αρχές (*«εν κρυπτώ και παραβύστω»*!). Βλ. ενδεικτικά το αναλυτικό άρθρο-ρεπορτάζ του *Κ. Δεληγιάννη*, Ο κόσμος του σκοτεινού Ίντερνετ, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 4 Μαΐου 2014, σελ. 29, στο οποίο εξηγείται και αναλύεται η έννοια του «Σκοτεινού Διαδικτύου» ("darknet"). Ειδικότερα, το darknet είναι ένα δίκτυο το οποίο αποτελείται από servers οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα «καμουφλάροντας» και αποκρύπτοντας τα ηλεκτρονικά ίχνη και πρόσβαση σε αυτό έχουν μόνο χρήστες που έχουν εγκαταστήσει ανάλογο μηχανισμό στη συσκευή τους (πρόσφατα μάλιστα το "darknet" απέκτησε τη δική του μηχανή αναζήτησης σελίδων με το όνομα "Grams"). Το darknet χρησιμοποιείται κυρίως για παράνομες δραστηριότητες και συναλλαγές.

[1616] Βλ. παράγραφο 3.5 της παρούσας διατριβής.

[1617] Βλ. παράγραφο 3.8 της παρούσας διατριβής.

[1618] Βλ. *R. C. Hollinger and L. Lanza-Kaduce*, The process of criminalization: The case of computer crime laws, Criminology, 1988, σελ. 104-105.

[1619] Κατά την ωραία διατύπωση του Κιούπη «*Λόγω της ταχύτατης εξέλιξης του διαδικτύου δεν έχουν διαμορφωθεί ακόμη καθολικά ισχύοντες και παγιωμένοι κώδικες σωστής συμπεριφοράς. Το αποτέλεσμα είναι ότι πολλές αξιόποινες πράξεις που τελούνται στο διαδίκτυο (ίσως οι λιγότερο σοβαρές) δεν φορτίζονται αρνητικά με την ηθική απαξία που θα είχαν αντίστοιχες συμπεριφορές στον φυσικό κόσμο. Οι ηθικές / αξιολογικές αναστολές είναι ακόμη λιγότερες, καθώς οι περισσότεροι δράστες είναι νεαρής ηλικίας και και δεν έχουν (ακόμη) εγκολπωθεί βασικές αξιακές επιλογές "της κοινωνίας των μεγάλων" ή ανήκουν σε κάποιες μικρές μειοψηφίες φανατικών χρηστών των υπολογιστών, οι οποίοι δρουν αποκλειστικά στον αξιολογικά ουδέτερο χώρο που ορίζουν οι τεχνικές παράμετροι του Internet.»* (έτσι *Δημ. Κιούπης*, Ποινικό Δίκαιο και Internet, όπ. π., σελ., 122).

αυτών σύμφωνα και με την άποψη ότι η συντεταγμένη κοινωνία δεν θα πρέπει να περιμένει τη σταδιακή ανάπτυξη μιας ηθικής[1620] μέσω της καθημερινής πράξης και επαφής με την πληροφορική τεχνολογία. Αντίθετα, η κοινωνία οφείλει να χαράξει μία πολιτική ενεργητικής μετάδοσης των βασικών ηθικών αρχών, δηλαδή να προχωρήσει σε μία ηθική διαπαιδαγώγηση και εκπαίδευση[1621] όχι μόνο των χρηστών αλλά και του συνολικού πληθυσμού, προκειμένου να διαμορφωθεί και να ισχυροποιηθεί η κυρίαρχη κουλτούρα αναφορικά με την ασφάλεια των ηλεκτρονικών πληροφοριών[1622]. Κι αυτό διότι στην περίπτωση του hacking και γενικότερα του πληροφορικού εγκλήματος, η πλειονότητα των κοινωνών βλέπει πολλές φορές ένα έγκλημα χωρίς θύμα ή που τα θύματά του είναι απρόσωπες γραφειοκρατικές δομές και πανίσχυρες επιχειρήσεις ή έστω ένα έγκλημα που δεν αφορά τους ίδιους, καθώς θεωρούν ότι δεν θα υπάρξουν ποτέ θύματά του[1623].

Γενικότερα, η ενημέρωση[1624] για τους τυχόν κινδύνους και η γνώση αυτών είναι το πρώτο και σημαντικότερο βήμα για την πρόληψη και την ενίσχυση της ασφάλειας των ηλεκτρονικών συστημάτων και δεδομένων[1625]. Η εκπαίδευση των χρηστών του διαδικτύου για την προώθηση της ασφάλειας των ηλεκτρονικών συστημάτων πληροφοριών[1626] θεωρείται σημαντική[1627] και ως πρόταση διατυπώνεται στην ανωτέρω έρευνα από τα δείγματα και των νομικών και των επιστημόνων πληροφορικής (σε ποσοστό 28,48% και 35,58% αντίστοιχα, λαμβανομένου υπόψιν ότι πρόκειται για ανοικτού τύπου ερώτηση) με δεδομένη και την ελλιπή ενημέρωση

[1620] Πρβλ. *Ιακ. Φαρσεδάκη*, Ηθική και εγκληματικότητα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2000.

[1621] Όπως ήδη αναφέρθηκε, ο *Ulrich Sieber* στο βασικό αναφορικά με το ποινικό δίκαιο του διαδικτύου πόνημά του Legal aspects of computer-related crime in the Information society, January 1998, prepared for the European Commission αναφέρεται στο ότι στο μέλλον πρέπει να προωθηθούν εξωδικαιικές λύσεις όπως η εκπαίδευση και η αυτορρύθμιση.

[1622] Για την κυρίαρχη κουλτούρα και την υποκουλτούρα του hacking βλ. σχετικές αναπτύξεις στην παράγραφο 2.8 του παρόντος πονήματος.

[1623] Βλ. *J. J. Bloombecker*, Computer Crime Update: The View as we exit 1984, New England Law Review, 1985, σελ. 627.

[1624] Βλ. περιεχόμενο στρατηγικών ασφάλειας στο διαδίκτυο αρκετών ευρωπαϊκών και όχι μόνο χωρών, όπως παρουσιάζονται στην ιστοσελίδα του ENISA (url: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world) στις οποίες βασικό χαρακτηριστικό σχεδόν αποτελεί σε μεγάλο βαθμό η ενημέρωση όσων ασχολούνται με το διαδίκτυο.

[1625] Βλ. και σχετικά Ψηφίσματα του Συμβουλίου της ΕΕ ως ανωτέρω παρουσιάζονται στις παραγράφους 6.3.4 και 6.3.5 του παρόντος πονήματος.

[1626] ... η οποία προκρίνεται και από την Ζαραφωνίτου (έτσι *Χρ. Ζαραφωνίτου και συν.*, Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο, όπ. π., σελ. 5).

[1627] Έτσι οι *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle upon Tyne, March 2003, όπ. π., σελ. 14.

των ιδίων σε θέματα hacking[1628]. Η ανάγκη για ενημέρωση και εκπαίδευση όπως διατυπώνεται από τα δύο δείγματα φαίνεται να συνάδει και με το γεγονός ότι οι συμμετέχοντες και στα δύο δείγματα χαρακτηρίζουν αντίστοιχα τους συναδέλφους τους ως μη επαρκώς ενημερωμένους σε θέματα ασφάλειας των ηλεκτρονικών δεδομένων[1629].

Βασίμως μπορεί να υποστηριχθεί ότι η προστασία ενός συστήματος μόνο από τεχνική άποψη (π.χ. firewall, antivirus, IDS) δεν είναι επαρκής για να ελαχιστοποιηθεί η απειλή των επιθέσεων. Η κατάλληλη πολιτική ασφάλειας πρέπει να λαμβάνει υπόψη της κοινωνικο-τεχνικά ζητήματα[1630]. Αυτό σημαίνει ότι, πέρα από τη θωράκιση του περιβάλλοντος του συστήματος πληροφοριών (με την εγκατάσταση κατάλληλων προγραμμάτων κ.λπ.) πρέπει (μεταξύ άλλων) οι διαχειριστές καθώς και οι χρήστες κάθε συστήματος πληροφοριών (μικρού ή μεγάλου / προσωπικού ή επιχειρησιακού) να είναι εκπαιδευμένοι[1631]. Ο ανθρώπινος παράγοντας είναι σημαντικός[1632] γιατί αρκετές φορές μπορεί να παρεκκλίνει από τους κανόνες ασφαλείας με τρόπο που είναι δύσκολο να προβλεφθεί[1633], ιδίως σε ό,τι αφορά τους κινδύνους με κοινωνική διάσταση (π.χ. "social engineering"[1634]) και έχει καταγραφεί ως ο ένας από τους πλέον «αδύναμους κρίκους» της αλυσίδας της ασφάλειας[1635]. Για τον λόγο αυτό, οι πολιτικές ασφάλειας πρέπει να σχεδιάζονται λαμβάνοντας υπόψη την πρακτικότητά τους (στο πλαίσιο π.χ. της οργανωμένης λειτουργίας του περιβάλλοντος του

[1628] ... όπως ομολογούν οι ίδιοι και προέκυψε από τα αποτελέσματα της έρευνας ως ανωτέρω.

[1629] Βλ. αντίστοιχα τις απαντήσεις στην ερώτηση υπ' αρ. 3 στο ερωτηματολόγιο κάθε δείγματος.

[1630] Βλ. *Eneken Tikk*, Ten Rules for Cyber Security, NATO Cooperative Cyber Defence Centre of Excellence, 2011, url: http://citizenlab.org/cybernorms2011/rules.pdf, όπου και αναλύονται δέκα κανόνες οι οποίοι αποτελούν τους πυλώνες της προφύλαξης από κυβερνοεπιθέσεις και, άρα, της κουλτούρας ασφάλειας των συστημάτων πληροφοριών.

[1631] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 15.

[1632] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 9.

[1633] Χαρακτηριστικό το περιστατικό το οποίο εισέφερε προς συζήτηση μέλος της ερευνητικής ομάδας της εν λόγω έρευνας. Διαπιστώθηκε ότι στην εταιρεία παροχής ασφάλειας σε ηλεκτρονικές πληροφορίες, στην οποία εργάζεται, η γραμματέας του προϊσταμένου είχε σημειώσει σε χαρτί τους κωδικούς administrator όλου του δικτύου της εταιρείας και είχε τοποθετήσει το χαρτί αυτό κάτω από το πληκτρολόγιό της!

[1634] Για την «κοινωνική μηχανική» βλ. ανωτέρω παράγραφο 2.11.2.1.1.1 του παρόντος πονήματος.

[1635] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 15. Έτσι δηλώνουν και οι ίδιοι οι hackers (βλ. το ρεπορτάζ του *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy).

συστήματος πληροφοριών[1636]). Η ασφάλεια δεν θα πρέπει να θεωρηθεί μόνο ως σύνολο μέτρων προστασίας, αλλά και ως ένα σύνολο κανόνων[1637] για την κατάρτιση και ανανέωση των οποίων απαιτείται συνεχής ενημέρωση και για την εφαρμογή των οποίων είναι απαραίτητη η εκπαίδευση. Οι κανόνες αυτοί θα εμπεδώσουν μια «κουλτούρα» ασφάλειας[1638] για τα συστήματα πληροφοριών, η οποία θα λειτουργήσει και αυτή αποτρεπτικά αναφορικά με προσβολές των ηλεκτρονικών δεδομένων[1639].

Για τους ανωτέρω λόγους η ενημέρωση και η εκπαίδευση[1640] είναι σημαντική. Το γεγονός αυτό, όμως επιτείνεται και από το ότι, όπως καταδείχθηκε και στην έρευνα, το hacking φαίνεται ότι αφορά κυρίως ανηλίκους[1641]. Η Τσήτσουρα υποστηρίζει ότι είναι απαραίτητη η πρώιμη ψυχοκοινωνική επέμβαση ως μέτρο αντιμετώπισης της εγκληματικότητας των ανηλίκων και αναφέρει ότι «*...οι παράγοντες κινδύνου παραβατικής εξέλιξης του ανηλίκου, που αναφέρονται είτε στα ατομικά χαρακτηριστικά του είτε στο εγκληματικό περιβάλλον του, πρέπει να καταπολεμηθούν στην προσχολική ήδη ηλικία με την κατάλληλη βοήθεια των ειδικών*»[1642]. Άξια λόγου, λοιπόν, είναι η άποψη που έχει διατυπωθεί αναφορικά με το ότι προτεραιότητα πρέπει να δοθεί στην ενημέρωση[1643] σε επίπεδο σχολείου σχετικά με την ασφάλεια των ηλεκτρονικών δεδομένων. Εξάλλου, είναι γεγονός ότι «τρέχουν» σχετικώς αρκετά προγράμματα σε χώρες του εξωτερικού προσανατολισμένα στην πρόληψη της θυματοποίησης

[1636] Βλ. και ανάπτυξη σχετική με τη λειτουργία («ευταξία») της επιχείρησης αναφορικά με την ασφάλεια των ηλεκτρονικών πληροφοριών στην παράγραφο 9.1.3 ως άνω.

[1637] *Budi Arief & Denis Besnard*, Technical and Human Issues in Computer-Based Systems Security, όπ. π., σελ. 14-15.

[1638] Βλ. και ανωτέρω παράγραφο 8.4 του παρόντος πονήματος ιδίως αναφορικά με το απόσταγμα από τα ερευνητικά δεδομένα της παρούσας έρευνας.

[1639] Πιστεύω ότι η «κουλτούρα ασφάλειας» των συστημάτων πληροφοριών μπορεί να συνίσταται στο σύνολο όσων οι hackers προτείνουν ως συμβουλές για την ενίσχυση της ασφάλειας των συστημάτων πληροφοριών ως απαντήσεις στην αντίστοιχη ερώτηση 11 του οικείου ερωτηματολογίου (βλ. ανωτέρω παράγραφο 7.8.4.1). Χαρακτηριστική είναι η απάντηση: «*το μυαλό σώζει*»!

[1640] Και η ίδια η GHS αναφέρεί ότι «*Η παιδεία είναι μια βασική δομή για την εξέλιξη, όπως και για την ελευθερια» (βλ. Παράρτημα IV).*

[1641] ... σύμφωνα και με το πρότυπο της «προστασίας» (ή «πρόνοιας» ή «πατερναλιστικό πρότυπο») στην αντεγκληματική πολιτική για ανήλικους παραβάτες κατά τις αναπτύξεις του Παπαθεοδώρου (βλ. *Θ. Παπαθεοδώρου*, Δικαιοσύνη ενηλίκων και ανήλικοι δράστες: Τα έσχατα όρια της «μηδενικής ανοχής» στις ΗΠΑ, ΠοινΔικ 1/2000, σελ. 77 επ.) όπως παραπέμπει και στους *Κ. Δ. Σπινέλλη, Στ. Αλεξιάδη, Γ. Πανούση, Ν. Κουράκη, Ιακ. Φαρσεδάκη, Αν. Μαγγανά, Β. Αρτινοπούλου, C. Blatier* και *J. Zermatten* (υποσ. 7 και 8).

[1642] *Αγλαΐα Τσήτσουρα*, Πρώιμη ψυχοκοινωνική επέμβαση για την πρόληψη της εγκληματικότητας των ανηλίκων, εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 1033 επ.

[1643] Για ειδικότερες πτυχές επιμόρφωσης και ενημέρωσης βλ. *Steven Furnell*, όπ. π., σελ. 357-358.

ανηλίκων στο διαδίκτυο (κυρίως για περιπτώσεις cyber bullying)[1644]. Η εκπαίδευση ανηλίκων είναι σημαντική επιπλέον για τον λόγο ότι η γνώση και η επιζητούμενη κουλτούρα ασφάλειας θα χρησιμοποιηθεί αργότερα τόσο στην ιδιωτική τους ζωή όσο και στον μελλοντικό εργασιακό τους χώρο[1645].

Τέλος, η εκπαίδευση και η ενημέρωση για το διαδίκτυο μπορούν να βοηθήσουν στην ενίσχυση της ασφάλειας των συστημάτων πληροφοριών καθώς σημαντικές πληροφορίες γενικότερα για την ασφάλεια των πληροφορικών συστημάτων μπορεί κάθε ενδιαφερόμενος να αντλήσει μέσα από τον ίδιο τον κυβερνοχώρο σε συγκεκριμένους δικτυακούς τόπους[1646]. Το ίδιο το διαδίκτυο αποτελεί πολύ σημαντικό εργαλείο ενημέρωσης. Ενδεικτικά, οι χρήστες των υπολογιστικών συστημάτων (ιδιώτες, εταιρίες, οργανισμοί) έχουν τη δυνατότητα να ενημερώνονται τόσο για τους δράστες (hackers ή crackers) και το modus operandi που χρησιμοποιούν καθώς και για τα θύματα που προτιμούν[1647].

9.3 Αυτορρύθμιση (self-regulation)

Οι υποστηρικτές της *ήπιας πρόληψης* υπογραμμίζουν ότι φαινόμενα όπως το hacking είναι δυνατόν να διευθετηθούν μέσω της *αυτορρύθμισης*[1648], δηλαδή των κανόνων

[1644] Βλ. αναφορικά με προγράμματα σε σχολεία για ορθολογική χρήση της τεχνολογίας παραδείγματα στο πόνημα *του γράφοντος*, «Digital και cyber bullying και αθέμιτη χρήση ηλεκτρονικών πληροφοριών ως το "bullying" του μέλλοντος – Γνώση και πρόληψη», πρακτικά 2ου συνεδρίου Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος ΕΛ.ΑΣ., 2013, σελ. 69 επ.

[1645] Βλ. *C. D. Chen*, Computer Crime and the Computer Fraud and Abuse Act of 1986, Computer and Law Journal, 1990, σελ. 84.

[1646] Βλ. *Χρήστος Τσουραμάνης*, Internet και ποινικής δικαιοσύνη, Ασφάλεια πληροφοριών στο Διαδικτυο, ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 160, όπου παραθέτει τους ακόλουθους δικτυακούς τόπους: www.itpolicy.gsa.gov,

www.ncsl.nist.gov,

www.securityportal.com,

www.microsoft.com/security/default.asp,

www.novel.com/corp/security/solutions.html,
www.brs.ibm.com/services/brs/ers/brswers.nsf/Info/Resources,

www.sgi.com/Support/security/security.html,

www.calderasystems.com/news/security/index.html.

[1647] Βλ. *Χρήστος Τσουραμάνης*, Εγκλήματα του κυβερνοχώρου και δικτυακοί τόποι (web sites) που αναφέρονται στην ασφαλεία των Η/Υ, ΠοινΔικ 12/2001 (Έτος 40), σελ. 1275.

[1648] Βλ. σχετικά με την αυτορρύθμιση στο διαδίκτυο και την ανάπτυξη της *Λίλιαν Μήτρου,* Το δίκαιο στην κοινωνία της πληροφορίας, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002, σελ. 69 επ.

συμπεριφοράς που οι «χρήστες - ρυθμιστές του διαδικτύου» μπορούν να επιβάλλουν σε τεχνολογικό και δεοντολογικό επίπεδο (δημιουργία και τήρηση κανόνων δεοντολογίας και όρων χρήσης διαδικτυακών τόπων, δημιουργία συστήματος επίβλεψης επικίνδυνης συμπεριφοράς χρηστών, συστήματα διαιτησίας, τήρηση αρχείων κίνησης και ιχνηλάτηση των ενεργειών των hackers). Η δόμηση μιας «κοινωνίας των ψηφιακών/ ηλεκτρονικών πολιτών» (αντίστοιχης με τη σημερινή «κοινωνία των πολιτών») μπορεί και πρέπει να διαδραματίσει ρόλο στην προώθηση της ασφάλειας στα ηλεκτρονικά συστήματα πληροφοριών, προωθώντας αρχές και σχετική ενημέρωση και λειτουργώντας ως κοινωνικού τύπου απάντηση σε παρεκκλίνουσες συμπεριφορές[1649]. Η αυτορρύθμιση, στην οποία οι ίδιοι οι χρήστες έχουν σημαντικό ρόλο, μπορεί και πρέπει να λειτουργήσει ως υποστηρικτική πολιτική των κανόνων δικαίου, οι οποίοι είτε ήδη υφίστανται είτε πρόκειται να θεσπισθούν[1650]. Δεδομένου, μάλιστα, ότι σε πολλές περιπτώσεις μπορεί να υπάρχει (ή να δημιουργηθεί) «νομικό κενό» λόγω και της συνεχούς εξέλιξης της τεχνολογίας, η ύπαρξη δεσμευτικών κωδίκων δεοντολογίας (όχι απλώς κανόνων καλής συμπεριφοράς) υποστηρίζεται ότι είναι απολύτως αναγκαία[1651]. Κατά τη Μήτρου, στην αυτορρύθμιση μπορούν να συμμετάσχουν και κρατικοί φορείς σε ό,τι αφορά στη διαμόρφωση κοινωνικών διαδικασιών για να συντελεστεί αυτή (ρυθμιζόμενη αυτορρύθμιση)[1652].

Επίσης, προτείνεται και η ανάπτυξη ενός μοντέλου «καλής γειτονίας», το οποίο σκοπό έχει να μετατρέψει το διαδίκτυο σε ένα ασφαλές πεδίο δραστηριοτήτων. Παρομοιάζεται η σχέση μεταξύ των χρηστών με αυτή των κατοίκων μίας γειτονιάς, όπου ο ενοποιητικός παράγοντας συνοχής της είναι η εμπιστοσύνη. Οι ίδιοι οι χρήστες πρέπει να αναλάβουν την ευθύνη από κοινού να προσέχουν οποιαδήποτε ύποπτη συμπεριφορά και να την αναφέρουν είτε στα κατάλληλα άτομα είτε στους παροχείς πρόσβασης στο διαδίκτυο. Το ζήτημα δεν είναι η επιβολή νέων κανόνων από τις αρχές αλλά η δημιουργία άτυπων συμφωνιών (γενικές άτυπες συμβάσεις

[1649] Βλ. σχετικές αναπτύξεις στο κλασικό έργο της *Mireille Delmas – Marty*, Πρότυπα και τάσεις αντεγκληματικής πολιτικής, Μετάφραση: Χριστίνα Ζαραφωνίτου, Βιβλιοθήκη εγκληματολογίας αρ. 8, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996, σελ. 86.

[1650] Για την αυτορρύθμιση στο διαδίκτυο βλ. και *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, όπ. π., σελ. 293 επ., ο οποίος αναφέρεται και σε πρακτικές online dispute resolution – ODR (βλ. σχετική υποσημείωση στο κεφάλαιο 10 του παρόντος πονήματος).

[1651] Βλ. *Αναστασία Ζάννη*, Το διαδικτυακό έγκλημα, όπ. π., σελ. 153.

[1652] Βλ. χαρακτηριστικά *Λίλιαν Μήτρου,* Το δίκαιο στην κοινωνία της πληροφορίας, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002, σελ. 70 επ.

επικοινωνίας) και πολύ περισσότερο υπεύθυνων χρηστών. Ενέργειες όπως η μη εξουσιοδοτημένη πρόσβαση, η δημιουργία και διάδοση ιών και η κατασκευή παράνομων αντιγράφων από προγράμματα ή αρχεία θα πρέπει να θεωρηθούν, σχεδόν αυτόματα και αυτονόητα, ως μη αποδεκτές[1653].

9.4 Ανάγκη διεθνοποίησης μέτρων για το κυβερνοέγκλημα

Παρά όλα τα ανωτέρω, είναι σαφές ότι οποιαδήποτε δράση για την ενίσχυση της ασφάλειας των ηλεκτρονικών δεδομένων πρέπει να λαμβάνει χώρα με μια διεθνή οπτική[1654] [1655]. Στην προκειμένη περίπτωση των εγκλημάτων του κυβερνοχώρου η «ανησυχία» και το «άγχος» των κρατών αναφορικά με την όποια εκχώρηση εθνικής κυριαρχίας σε περίπτωση ποινικής αντιμετώπισης κυβερνοεγκλημάτων σκόπιμο είναι να κάμπτεται δεδομένων των υπερκρατικών συνθηκών στις οποίες λαμβάνουν χώρα οι ενέργειες αυτές[1656]. Ο κυβερνοχώρος είναι ένας νέος χώρος προς ρύθμιση και, συνεπώς, τα κράτη δύσκολα μπορούν να επικαλεστούν δικαικά «κεκτημένα» ή παγιωθείσες πρακτικές στην αντιμετώπιση των προβλημάτων σε συστήματα πληροφοριών τα οποία να είναι τόσο σημαντικά «χάριν εντοπιότητος»[1657]. Τουναντίον, η αντιμετώπισή του στη βάση διεθνούς και διασυνοριακής συνεργασίας (ακόμη και με θεσμοθετηθέμες ασκήσεις ασφαλείας)[1658] είναι πολύ σημαντική γιατί

[1653] Βλ. *Γρηγόρης Λάζος*, Πληροφορική & Έγκλημα, Εκδόσεις Νομική Βιβλιοθήκη, 2001, σελ. 234, παραπομπή υπ' αρίθ. 436 σε *D. G. Johnson*, Crime, abuse and hacker ethics, Computer Ethics, New Jersey, Prentice Hall, 1994.

[1654] *David S. Wall*, Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, Police Practice and Research, 8:2, 183 205. Την ανάγκη συνεργασίας σε διεθνές επίπεδο τονίζει και ο Παπαθεοδώρου (*Θ. Παπαθεοδώρου,* Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 207).

[1655] Αναφορικά με τη διεθνοποίηση των ερευνητικών διαδικασιών και τη σχέση τους με την τεχνολογία πρβλ. *Mathieu Deflem*, Technology and the Internationalization of Policing: A Comparative-Historical Perspective, Justice Quarterly 19(3), 2002, pp. 453-475.

[1656] Βλ. και *Steven Furnell*, όπ. π., σελ. 285 επ.

[1657] *Fausto Pocar*, New challenges for international rules against cyber-crime, European Journal on Criminal Policy and Research 10: 27–37, Kluwer Academic Publishers, 2004, σελ. 36.

[1658] Βλ. ενδεικτικά και ανωτέρω παράγραφο 6.3.8, στην οποία παρουσιάζεται Ανακοίνωση της Ευρωπαϊκής Επιτροπής με επίκεντρο τη διασυνοριακή συνεργασία ως ουσιώδη παράγοντα για την ενίσχυση της ασφάλειας των συστημάτων πληροφοριών καθώς και δράσεις του ENISA αναφορικά με την ασφάλεια στον κυβερνοχώρο, όπως η άσκηση Cyber Europe 2014 (βλ. url: https://www.enisa.europa.eu/media/press-releases/i-cyber-europe-2014-lamvani-hora-simera). Σε άσκηση ασφαλείας των συστημάτων πληροφοριών του προβαίνει κάθε χρόνο από το 2005 και το ΓΕΕΘΑ – η άσκηση αυτή ονομάζεται «Πανόπτης» (βλ. ενδεικτικά url:

μπορεί να αποτελέσει αποτελεσματικό τρόπο αντιμετώπισης εγκληματικών συμπεριφορών[1659]. Σε αυτό το πνεύμα, εξάλλου, έχουν ληφθεί αντίστοιχα και πρωτοβουλίες σε υπερεθνικό επίπεδο αναφορικά με την «ηλεκτρονική δικαιοσύνη» [1660], στην οποία χρήσιμο εργαλείο θεωρούνται τα ηλεκτρονικά συστήματα πληροφοριών.

---

http://www.defencenet.gr/defence/item/%CE%B3%CE%B5%CE%B8%CE%B1-%CE%AC%CF%83%CE%BA%CE%B7%CF%83%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1%CF%82-%E2%80%9C%CF%80%CE%B1%CE%BD%CE%BF%CF%80%CF%84%CE%B7%CF%83-2013%E2%80%9D και *Γ. Παπαδόπουλου*, Οι Ελληνες «πειρατές» του Διαδικτύου, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10/08/2014, url: http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy).

[1659] Βλ. ενδεικτικά την εντελώς πρόσφατη σχετική προσέγιση ΕΕ και ΗΠΑ όπως παρουσιάζεται στο ρεπορτάζ του *Eric Chabrow*, "U.S., European Union Issue Cyber Accord - Cooperation on Data Protection, Promoting Online Human Rights", March 27, 2014 (url: http://www.bankinfosecurity.com/us-european-union-issue-cyber-accord-a-6684/op-1).

[1660] Σε ό,τι αφορά την «ηλεκτρονική δικαιοσύνη (e-justice)» καταρχάς πρβλ. σχετικώς την Ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή με θέμα «Προς μια Ευρωπαϊκή στρατηγική σε θέματα ηλεκτρονικής δικαιοσύνης (e-Justice)» (url: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52008DC0329&from=EN). Στην παράγραφο 2 της ανακοίνωσης αυτής διασαφηνίζεται ότι «*ως "ηλεκτρονική δικαιοσύνη" μπορεί να ορισθεί η χρησιμοποίηση των τεχνολογιών της πληροφορίας και επικοινωνίας για τη βελτίωση της πρόσβασης των πολιτών στη δικαιοσύνη, καθώς και η αποτελεσματικότητα της δικαστικής δράσης νοούμενης ως κάθε είδους δραστηριότητα που συνίσταται στη ρύθμιση μιας διαφοράς ή στην επιβολή ποινικών κυρώσεων για κάποια πράξη*».

Επιπρόθετα, η χρησιμοποίηση του διαδικτύου για επίλυση των διαφορών που ανακύπτουν σε αυτό το περιβάλλον αλλά και εκτός διαδικτύου έχει οδηγήσει στη θέσπιση ενός συστήματος επίλυσης των διαφορών στο διαδίκτυο (ODR – online dispute resolution) με αντίστοιχες πρακτικές με την εναλλακτική επίλυση συγκρούσεων (ADR – alternative dispute resolution). Αναλυτικότερα, η ηλεκτρονική επίλυση διαφορών (ODR) είναι κλάδος επίλυσης διαφορών που χρησιμοποιεί την τεχνολογία για να διευκολύνει την επίλυση των διαφορών μεταξύ των μερών σε επίπεδο διαπραγμάτευσης, μεσολάβησης ή διαιτησίας ή συνδυασμού και των τριών. Η ως άνω πρακτική αναφέρεται ως επίλυση διαφορών μεταξύ των δύο εμπλεκομένων, ενός διαιτητή που τα μέρη αναγνωρίζουν και τη συνδρομή της τεχνολογίας ακόμη και με εργαλεία τεχνολογικά σχεδιασμένα ειδικά για την περίσταση (π.χ. διαχείριση των πληροφοριών της επίλυσης της διαφοράς όχι μόνο από φυσικά πρόσωπα αλλά και από λογισμικό!). Στην εφαρμογή αυτών των πρακτικών κορμό αποτελούν οι αρχές της αποκαταστατικής, της επανορθωτικής και της συμφιλιωτικής δικαιοσύνης [πρβλ. αναλυτικότερα και ενδεικτικά *Julio César Betancourt & Elina Zlatanska*, Online Dispute Resolution (ODR): What Is It, and Is It the Way Forward?, 79 International Journal of Arbitration, Mediation and Dispute Management, Issue 3, 2013 (url: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325422) και γενικά για την επανορθωτική δικαιοσύνη *Βάσω Αρτινοπούλου*, Επανορθωτική δικαιοσύνη: η πρόκληση των σύγχρονων δικαιικών συστημάτων, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2010) και *Α. Μαγγανά*, Το εγκληματικό φαινόμενο στην πράξη, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004, σελ. 17 επ].

Ενδεικτικά, ένα από τα πιο σημαντικά παραδείγματα ODR είναι η Ενιαία Πολιτική Επίλυσης Διαφορών Ονόματος (Uniform Domain Name Dispute Resolution Policy - UDRP) που δημιουργήθηκε από το Internet Corporation for Assigned Names and Numbers (ICANN) (μη κερδοσκοπική εταιρεία που ιδρύθηκε το 1998 στην Καλιφόρνια των ΗΠΑ και διαχειρίζεται ζητήματα διαδικτύου όπως τα πρωτόκολλα επικοινωνίας στο διαδίκτυο IPv4 and IPv6) (βλ. url: https://www.icann.org/resources/pages/udrp-2012-02-25-en). Στο ως άνω πλαίσιο, η UDRP είναι μια διαφανής διαδικασία παγκόσμιας ODR που επιτρέπει σε κατόχους εμπορικών σημάτων να καταπολεμήσουν αποτελεσματικά την κατάληψη του κυβερνοχώρου. Η UDRP χρησιμοποιείται για

Σε διεθνές επίπεδο πρέπει να ρυθμιστεί το διαδίκτυο[1661] - ως «κτήμα της ανθρωπότητας». Αυτή η ανάγκη διεθνοποίησης των μέτρων έχει γίνει ήδη αντιληπτή από διεθνείς οργανισμούς και fora[1662] καθώς και την Ευρωπαϊκή Ένωση[1663] και το Συμβούλιο της Ευρώπης και εξ αυτού του λόγου και προς αυτήν την κατεύθυνση έχει αναληφθεί σειρά νομοθετικών πρωτοβουλιών[1664]. Έτι περαιτέρω, όμως, έχουν

την επίλυση διαφορών μεταξύ ιδιοκτητών-κατόχων εμπορικού σήματος και εκείνων που έχουν αγοράσει το domain name που αναφέρεται στο ως άνω σήμα κακόπιστα ή με σκοπό την μεταπώληση με σκοπό το κέρδος ή προκειμένου να εκμεταλλευτούν τη φήμη ενός εμπορικού σήματος [συμπεριφορά η οποία καλείται cyber – squatting ή domain grabbing – βλ. σχετικά *Δ. Κιούπη*, Ηλεκτρονικά οικονομικά εγκλήματα, εις: *Ν. Κουράκης* (εκδ. επιμ.), Τα οικονομικά εγκλήματα, τομος ΙΙ, όπ. π., σελ. 427 επ.].

Τέλος, η αντιμετώπιση το φαινόμενο του online dispute resolution έχει αποκτήσει ρίζες και στην ευρωπαϊκή έννομη τάξη καθώς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ στις 21/05/2013 εξέδωσαν τον Κανονισμό 424/2013 σχετικά με την εφαρμογή ODR για την προστασία καταναλωτών (url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:EN:PDF).

Η ενδοκοινοτική αυτή επίλυση των προβλημάτων εντός της ίδιας της κοινότητας στο διαδίκτυο συνάδει και με το πρότυπο της «συμμετοχής» στην αντεγκληματική πολιτική για ανήλικους παραβάτες (βλ. σχετικά *Θ. Παπαθεοδώρου*, Δικαιοσύνη ενηλίκων και ανήλικοι δράστες: Τα έσχατα όρια της «μηδενικής ανοχής» στις ΗΠΑ, ΠοινΔικ 1/2000, σελ. 78).

Πρβλ. σχετικά με εξωδικαιικές μορφές επίλυσης των συγκρούσεων και εναλλακτικές δικαιικές διαδικασίες την ομώνυμη παράγραφο 3 του κεφαλαίου 8 στο πόνημα της *Έφης Λαμπροπούλου*, Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης, εκδ. Ι. Σιδέρης, Αθήνα, 2012, σελ. 278 επ. καθώς και *του γράφοντος*, Συνδιαλλαγή δράστη - θύματος στα πλαίσια της αποκαταστατικής και συμφιλιωτικής δικαιοσύνης / Οι "κατά παρέκκλιση" διαδικασίες και η αποκαταστατική-συμφιλιωτική δικαιοσύνη - Ιστορική και δογματική προσέγγιση, ηλεκτρονικό επιστημονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τευχ. 7, Φεβρουάριος 2008, url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1207246182. Τέλος, ειδικά για τους ανηλίκους πρβλ. *Σ. Γιοβάνογλου*, Η ενσωμάτωση της αποκαταστατικής δικαιοσύνης στα διεθνή κείμενα αντεγκληματικής πολιτικής για τους ανηλίκους, ΠοινΔικ 11/2006, σελ. 1310 επ.

[1661] *Jovan Kurbalija*, Internet governance and international law, Reforming Internet Governance: Perspectives from WGIG, url: http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf, pp. 106-107 και *Martha L. Arias*, Internet Law - Computer Hacking: A global Problem that Requires a Global Solution, url: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2513.

[1662] Βλ. σχετικές πρωτοβουλίες εις: *Fausto Pocar*, New challenges for international rules against cyber-crime, European Journal on Criminal Policy and Research 10: 27–37, Kluwer Academic Publishers, 2004 και εις *Gregor Urbas & Kim-Kwang Raymond Choo*, Resource materials on technology-enabled crime, Australian Institute of Criminology, Technical and Background Paper, No. 28, pp. 9 f.

[1663] Βλ. δράσεις του Ευρωπαϊκού Κέντρου για τα εγκλήματα στον Κυβερνοχώρο όπως παρουσιάστηκαν σε δελτίο τύπου για την ετήσια λειτουργία του (url: http://europa.eu/rapid/press-release_IP-14-129_el.htm).

Επιπρόσθετα, για την ανάγκη ολοκλήρωσης της λειτουργίας της ενιαίας αγοράς πρβλ. την Ανακοίνωση του Συμβουλίου της ΕΕ (url: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/144112.pdf) για την υιοθέτηση κανονισμού (url: http://register.consilium.europa.eu/doc/srv?l=EN&f=PE%2060%202014%20INIT) σχετικά με την αμοιβαία αναγνώριση ηλεκτρονικής ταυτοποίησης (electronic identification) (π.χ. ηλεκτρονική υπογραφή) φυσικών και νομικών προσώπων.

[1664] Όπως αναλυτικά παρατίθενται στο κεφάλαιο 6 του παρόντος πονήματος. Βλ. επίσης την περιεκτική ανάλυση του *Ιακ. Φαρσεδάκη*, Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π., σελ. 5 και 6 και ιδίως την αναφορά των διακυβερνητικών οργανισμών οι οποίοι ασχολούνται και αναλαμβάνουν δράσεις στο πεδίο του κυβερνοεγκλήματος καθώς και την ανάπτυξη της *Αγ. Τσήτσουρα*, Εγκληματικότητα και αντεγκληματική πολιτική στην εποχή της παγκοσμιοποίησης, εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική

αναπτυχθεί και άλλες πρωτοβουλίες: ενδεικτικά, τον Σεπτέμβριο του 2011 η Κίνα, η Ρωσία, το Τατζικιστάν και το Ουζμπεκιστάν έστειλαν επιστολή στον Γενικό Γραμματέα του ΟΗΕ[1665] Ban Ki-Moon προτείνοντας έναν κώδικα για τη χρήση της πληροφορικής που θα πρέπει να υπογραφεί μεταξύ των χωρών για την προώθηση της εθνικής σταθερότητας, την καταπολέμηση του κυβερνοεγκλήματος και την πρόληψη της χρήσης του διαδικτύου για πράξεις κυβερνοτρομοκρατίας σε αντιστοίχιση με την πρόταση της Ρωσίας για την υπογραφή νέας σύμβασης για το Κυβερνοέγκλημα, με δεδομένο ότι έχουν περάσει πια αρκετά χρόνια από τη σύμβαση της Βουδαπέστης. Χαρακτηριστικό, επίσης, είναι ότι πλέον υπάρχουν προτάσεις για ίδρυση διεθνούς δικαστηρίου για το διαδίκτυο [An International Criminal Court or Tribunal for Cyberspace (ICTC)] [πρόταση του Νορβηγού δικαστή Stein Schjolber στο EastWest Institute (EWI) Cybercrime Legal Working Group τον Μάιο του 2011] σε συνδυασμό με την πρόταση του ιδίου για σύμβαση για το Κυβερνοέγκλημα ενώπιον του ΟΗΕ[1666].

Βιβλιοθήκη, Αθήνα, 2003, τομ. ΙΙ, σελ. 1418 επ. αναφορικά με δράσεις που είχαν αναληφθεί κατά την περίοδο σύνταξης του εν λόγω άρθρου σε πνεύμα διεθνούς συνεργασίας.

[1665] Στο πλαίσιο του ΟΗΕ, ως ειδικευμένος φορέας για τα θέματα ασφαλείας στον κυβερνοχώρο σημαντικό ρόλο διαδραματίζει η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union - ITU) (βλ. αναλυτικά url: http://en.wikipedia.org/wiki/International_Telecommunication_Union).

[1666] Judge *Stein Schjolberg*, The Third Pillar for Cyberspace, An International Court or Tribunal for Cyberspace [Draft UN Treaty on an International Criminal Court or Tribunal for Cyberspace (9th edition, June 2014)], (url: http://www.cybercrimelaw.net/documents/140615_Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf).

10. ΣΥΝΟΨΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ

Σε αυτό το κεφάλαιο παρουσιάζονται τα σημαντικότερα πορίσματα της ανωτέρω αναλυτικής προσέγγισης του θέματος της χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα και του hacking. Βέβαια, είναι προφανές ότι σε κάθε κεφάλαιο ο αναγνώστης θα μπορέσει να βρει πολύ περισσότερες πληροφορίες και θέσεις οι οποίες δύνανται ειδικώς να του κεντρίσουν το επιστημονικό – και όχι μόνο – ενδιαφέρον. Τα συμπεράσματα που ακολουθούν, επομένως, αποτελούν ενδεικτική προσέγγιση και απόπειρα να αποδοθούν σε σύντομες παραγράφους σκέψεις οι οποίες καλύφθηκαν διεξοδικά σε παραπάνω αναπτύξεις, προκειμένου να σχηματιστεί μια συνολική εικόνα.

Ως πρώτη επισήμανση, είδαμε οτι ο hacker («παραβιαστής» σύμφωνα με την απόδοση της Ακαδημίας Αθηνών[1667]) κατά την πάροδο των χρόνων μεταλλάχθηκε από εξειδικευμένος επιστήμονας, ο οποίος κατασκεύαζε προγράμματα για την καλύτερη λειτουργία των συστημάτων πληροφοριών, σε κακόβουλο χρήστη συστημάτων πληροφοριών ο οποίος μετέρχεται πρακτικές που υπό προϋποθέσεις μπορούν να καταστούν επικίνδυνες για την ασφάλεια των πληροφοριών[1668].

Και από την *αναλυτική παρουσίαση μεθόδων των hackers*[1669] προκύπτει ότι είναι τελικά *σκόπιμη η ερμηνευτική προσέγγιση του hacking lato sensu*, κατά την οποία περιλαμβάνει και δράσεις οι οποίες δεν συνιστούν μόνο χωρίς δικαίωμα πρόσβαση αλλά και π.χ. αποκλεισμό της πρόσβασης (ενδεικτικώς με επιθέσεις άρνησης υπηρεσίας – Denial of Service – κατά τις οποίες το σύστημα «μπλοκάρει» και

[1667] Έτσι ο *Νέστωρ Ε. Κουράκης*, Εγκληματολογικοί Ορίζοντες. Β΄: Πραγματολογική προσέγγιση και επιμέρους ζητήματα, Δεύτερη Ανανεωμένη Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ. 183.
[1668] Βλ. ανωτέρω παράγραφο 2.2 και 2.4.
[1669] Βλ. ανωτέρω παράγραφο 2.11.

δυσλειτουργεί ή παύει να λειτουργεί) σε αντίθεση με μια stricto sensu προσέγγιση κατά την οποία η έννοια του hacking καταλαμβάνει μόνο περιπτώσεις χωρίς δικαίωμα πρόσβασης[1670]. Εξάλλου, η τελευταία αυτή προσέγγιση είναι σύμφωνη και με την έννοια της ασφάλειας των πληροφοριών η οποία σωρευτικά αποτελείται από τρεις ειδικότερες εκφάνσεις και, συγκεκριμένα, την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) των δεδομένων[1671]. Για αυτόν τον λόγο προτείνεται η εν λόγω προσέγγιση της ασφάλειας ως προστατευτέο έννομο αγαθό[1672].

Σημαντικός είναι ο *διαχωρισμός των πρακτικών των hackers σε «εξωπρογραμματιστικές»[1673] και «γνήσιες»[1674]*. Οι πρώτες εμπεριέχουν δράσεις ενημέρωσης των hackers για το σύστημα και προσπάθειες εξαπάτησης του εξουσιοδοτημένου χρήστη με σκοπό την ανεύρεση των στοιχείων που θα επιτρέψουν τη χωρίς δικαίωμα είσοδο στο σύστημα. Οι «γνήσιες» πρακτικές αφορούν σε χρήση τεχνικών μέσων και προγραμμάτων. Με τη διάκριση αυτή αποσαφηνίζονται ερμηνευτικά οι εν λόγω συμπεριφορές και γίνονται πληρέστερα κατανοητές.

Οι ενέργειες των hackers μπορούν να εξηγηθούν από πλείστες εγκληματολογικές θεωρίες[1675]. Θεωρώ ότι η «ποικιλία» των κινήτρων των hackers[1676] προσφέρει την δυνατότητα της συγκεκριμένης πολυσυλλεκτικής προσέγγισης σε ό,τι αφορά τις εγκληματολογικές θεωρίες κατά τις οποίες δύναται να ερμηνευθεί, να αναλυθεί ή/και να προληφθεί η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα και συστήματα πληροφοριών.

Η κείμενη ελληνική νομοθεσία αναφορικά με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα είναι αναποτελεσματική, σύμφωνα και με την περιορισμένη έως

[1670] Βλ. και παράγραφο 7.8.4.2.
[1671] Βλ. ανωτέρω παράγραφο 1.3.2.
[1672] Βλ. ανωτέρω παράγραφο 5.1.2.
[1673] Βλ. ανωτέρω παράγραφο 2.11.2.1.
[1674] Βλ. ανωτέρω παράγραφο 2.11.2.2.
[1675] Βλ. συσχέτιση αρκετών εγκληματολογικών θεωριών με το hacking στο κεφάλαιο 3 του παρόντος πονήματος.
[1676] Βλ. παράγραφο 2.5.

τώρα νομολογιακή εφαρμογή της[1677] και σύμφωνα με την αποτίμηση της γενικοπροληπτικής και αποτρεπτικής της λειτουργίας, όπως προκύπτει από την έρευνα[1678].

Τα τελευταία χρόνια έχουν θεσπιστεί αρκετές διατάξεις, οι οποίες αναφέρονται σε χωρίς δικαίωμα πρόσβαση ή παρέμβαση σε λογισμικό ή περιέλευση σε γνώση ηλεκτρονικών δεδομένων, κυρίως για την προστασία των τηλεπικοινωνιών[1679]. Η εφαρμογή των διατάξεων αυτών, όμως, πέρα από το γεγονός ότι καλύπτει ένα μικρό μέρος των ηλεκτρονικών δεδομένων (όσα αφορούν σε τηλεπικοινωνίες), λόγω των αλληλεπικαλυπτόμενων διατυπώσεων, αποτελεί τελικά δύσκολο εγχείρημα για τον έλληνα νομικό. Εξ αυτού του λόγου και αυτές οι διατάξεις, μολονότι σύγχρονες, τυγχάνουν και αυτές ανεφάρμοστες.

Είναι *απαραίτητη μια νέα νομοθετική ρύθμιση*, η οποία θα προστατεύει συνολικά την ασφάλεια του συστήματος πληροφοριών σε όλες τις εκφάνσεις της (προκειμένου να τιμωρείται και ο αποκλεισμός της πρόσβασης, η δημιουργία και χρήση botnet, κ.ά.). Η ρύθμιση αυτή πρέπει να περιλαμβάνει μία διάταξη, η οποία θα καλύπτει όλες τις περιπτώσεις hacking, προκειμένου να αποφεύγεται η πολυνομία και οι αλληλεπικαλύψεις, και η οποία θα δημιουργηθεί με παράδειγμα την ευελιξία των σχετικών διατάξεων άλλων εννόμων τάξεων[1680] και έχοντας λάβει υπόψιν όλους τους σύγχρονους προβληματισμούς αναφορικά με την αξιόποινη θέαση του hacking[1681] αλλά και τις σύγχρονες νομοθετικές εξελίξεις σε ευρωπαϊκό επίπεδο [αναφορά στον όρο «συστήματα πληροφοριών» προκειμένου να περιλαμβάνονται στο προστατευτικό πλαίσιο και νέου τύπου συσκευές λόγω και της ανάπτυξης του «διαδικτύου των πραγμάτων» (“internet of things”) προστασία από επιθέσεις “botnet” κ.ά.][1682].

[1677] Βλ. παράγραφο 5.5.
[1678] Βλ. παράγραφο 8.3.
[1679] Βλ. αναλύσεις στο κεφάλαιο 5 της παρούσας.
[1680] Βλ. ανωτέρω τις παραγράφους 4.4.2, 4.4.3 και 4.4.4.
[1681] Βλ. ανωτέρω τις παραγράφους 4.1, 4.2 και 4.3.
[1682] Βλ. σχετικές αναπτύξεις στο κεφάλαιο 6.

Ειδικότερα, η νέα διάταξη, η οποία είναι απαραίτητο να εισαχθεί στην ελληνική έννομη τάξη, θα πρέπει να τιμωρεί την πρόσβαση σε περίπτωση παραβίασης μέτρου ασφαλείας (π.χ. κωδικού)[1683]. Με αυτόν τον τρόπο ενισχύεται η δημιουργία κουλτούρας ασφάλειας στους χρήστες του διαδικτύου και αφήνεται ένα περιθώριο ικανοποίησης της περιέργειας του hacker που θα του επιτρέπει τον πειραματισμό στην τεχνολογία και ενδέχεται να οδηγήσει και σε νέα τεχνολογικά επιτευγματα. Εξάλλου, σύμφωνα με τα αποτελέσματα της έρευνας, το ποσοστό που υποστηρίζει την πλήρη αποποινικοποίηση του hacking δεν αντιπροσωπεύει την κυρίαρχη τάση[1684]. De lege ferenda, σε κάθε περίπτωση και ανεξαρτήτως από την παραβίαση μέτρου ασφαλείας, η εν λόγω διάταξη θα πρέπει να λαμβάνει υπόψιν τη συγκατάθεση του διαχειριστή του συστήματος πληροφοριών σε περίπτωση φυσικής πρόσβασης (με δεδομένο ότι είναι φυσιολογικό πολλοί χρήστες σε μια ψηφιακή συσκευή να έχουν μονίμως «αποθηκευμένο» τον κωδικό τους στη μνήμη της ηλεκτρονικής συσκευής τους) καθώς και την εξέλιξη και χρήση των επιβλαβών προγραμμάτων (malware) τα οποία δύνανται να υπονομεύουν την ασφάλεια των συστημάτων πληροφοριών και των ηλεκτρονικών δεδομένων. Επίσης, χαρακτηριστικό αυτής της ποινικής διάταξης θα πρέπει να είναι η τιμώρηση όσων αποκτούν χωρίς δικαίωμα πρόσβαση με σκοπό το οικονομικό όφελος ή ζημία, όπως προκύπτει και από την άποψη που καταγράφεται από τα αποτελέσματα της έρευνας[1685].

Η lato ή stricto sensu προσέγγιση της έννοιας του hacking[1686] σε κάθε περίπτωση δεν επηρεάζει την ανάγκη της προστασίας της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας των συστημάτων πληροφοριών. Εξάλλου, σκοπός της ρύθμισης αυτής δεν (πρέπει να) είναι η τιμώρηση του hacking αλλά η θωράκιση και προστασία των ηλεκτρονικών πληροφοριών ως ανωτέρω και σύμφωνα με τις εκφάνσεις της ασφάλειας των πληροφοριών.

[1683] Οι συμβουλές των ίδιων των hackers για την διαφύλαξη της ασφάλειας είχαν κυρίως να κάνουν με την ιδιαίτερη προσοχή που πρέπει να επιδεικνύουν οι χρήστες συστημάτων ηλεκτρονικών πληροφοριών ως προς τους κωδικούς πρόσβασης.

[1684] Βλ. παράγραφο 8.3.

[1685] Βλ. παράγραφο 8.3.

[1686] Βλ. παράγραφο 7.8.4.2.

Η κρατική αντίδραση στο έγκλημα κατά συστημάτων πληροφοριών δεν είναι απαραίτητο να συνίσταται μοναχά σε ποινικές κυρώσεις αλλά πρέπει να εξεταστεί και η περίπτωση επιβολής διοικητικών ποινών[1687] [1688], σε ένα πλαίσιο χρήσης του ποινικού δικαίου και των ποινών με φειδώ.

Η διερευνητική/ περιγραφική/ επεξηγητική και αξιολογητική *έρευνα* βασίστηκε κυρίως σε ερωτηματολόγια σε δείγμα 158 νομικών, 104 επιστημόνων πληροφορικής και 48 hackers (συνολικά συνελέγησαν 310 ερωτηματολόγια), στα οποία έλαβε χώρα ποσοτική και ποιοτική ανάλυση. Στόχοι της έρευνας απετέλεσαν η διασαφήνιση του όρου hacking, η ανίχνευση του αν υπερέχει η ιδεολογία ή το οικονομικό όφελος ως κίνητρο του hacking, η αξιολόγηση της αποτελεσματικότητας της ισχύουσας ποινικής νομοθεσίας και η διατύπωση (με αφορμή τις απαντήσεις των συμμετεχόντων) προτάσεων εγκληματοπροληπτικών πρακτικών. Πρέπει να σημειωθεί ότι ιδιαίτερο στοιχείο της έρευνας αυτής είναι ο εντοπισμός του δείγματος και η διεξαγωγή της μέσω διαδικτύου[1689]. Το γεγονός ότι η ως άνω έρευνα διεξήχθη και σε δείγμα hackers (με δεδομένη και τη δυσκολία ανεύρεσης του δείγματος αυτού[1690]) προσδίδει στα αποτελέσματα και πορίσματα ιδιαίτερη σημασία.

Σε *επίπεδο αποτελεσμάτων της έρευνας*, καταρχάς οι απαντήσεις των συμμετεχόντων και στα τρία δείγματα δεν έδωσαν κάποιον ρηξικέλευθο ορισμό ή ερμηνεία στο hacking, ανέδειξαν, ωστόσο, τα λεπτά και ρευστά όρια μεταξύ hacking και cracking. Η επιφανειακή κατάρτιση των συμμετεχόντων στα δείγματα νομικών και επιστημόνων πληροφορικής ενισχύει την ανάγκη για ενημέρωση και εκπαίδευση. Αναφορικά με το κυρίαρχο κίνητρο της συμπεριφοράς των hackers, οι hackers στη συντριπτική τους πλειοψηφία επικαλούνται ως κίνητρα την ιδεολογία τους ή την εξάσκησή τους – την ιδεολογία των hackers αποδίδουν ως κίνητρο στους hackers και οι περισσότεροι επιστήμονες πληροφορικής αλλά και αρκετοί νομικοί. Ο συνδυασμός των απαντήσεων των δειγμάτων καταδεικνύει σαφώς ότι οι ποινικές διατάξεις, όπως

[1687] Πρβλ. σχετικά *Χρ. Μυλωνόπουλου*, Εφαρμογές Ποινικού Δικαίου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997, παρ. 2 - Ποινικό και διοικητικό άδικο, σελ. 23-39 και *Ν. Ανδρουλάκη*, Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000, σελ. 7 επ.
[1688] Βλ. παράγραφο 8.4.
[1689] Βλ. παράγραφο 7.5.2.
[1690] Βλ. παράγραφο 7.5.5.2.

ισχύουν στην ελληνική έννομη τάξη, είναι λίγο έως καθόλου αποτελεσματικές για τη διαφύλαξη της ασφάλειας των ηλεκτρονικών δεδομένων, επιβεβαιώνοντας την υπόθεση της έρευνας περί ανεπάρκειας αυτών. Επίσης, ως αρχικό συμπέρασμα μπορεί ενδεχομένως να εξαχθεί το ότι η αυστηροποίηση των ποινικών κυρώσεων – η οποία υποστηρίζεται από νομικούς και επιστήμονες πληροφορικής – ίσως να εξακολουθεί να μην είναι αποτελεσματική αναφορικά με την προώθηση της ασφάλειας των συστημάτων πληροφοριών. Ωστόσο, οι hackers σε σημαντικό ποσοστό αποδέχονται τον ρόλο της Πολιτείας στο να θέτει όρια στο hacking (ακόμη ίσως και με κάποιες προϋποθέσεις). Σε περίπτώσεις οικονομικού οφέλους ή ζημίας το δείγμα φαίνεται να υποστηρίζει τη σαφή πλέον διάκριση στον νόμο του hacking και του cracking, με την (αυστηρότερη) τιμώρηση όσων παραβιαστών αποκτούν οικονομικό όφελος ή προβαίνουν σε οικονομική ζημία. Τέλος, σε επίπεδο χάραξης αντεγκληματικής πολιτικής, ως εναλλακτικός τρόπος ενίσχυσης της ασφάλειας των ηλεκτρονικών δεδομένων, κοινός τόπος όλων των απαντήσεων είναι η εκπαίδευση και η ενημέρωση αναφορικά με τη χρήση και τις πολιτικές ασφάλειας ηλεκτρονικών συστημάτων πληροφοριών καθώς η ασφάλεια των ηλεκτρονικών πληροφοριών αποτελεί από μόνη της «κουλτούρα», έστω και υπό την έννοια της καλής πρακτικής ή συνήθειας. Η διαπίστωση αυτή συνδυάζεται και με το εύρημα ότι το hacking είναι δραστηριότητα που αφορά κυρίως ανηλίκους (το 52% των hackers δήλωσε ότι είναι κάτω των 20 ετών).

Σε *επίπεδο πρόληψης και αντεγκληματικής πολιτικής* καταρχάς πρέπει να ληφθεί υπόψιν ότι οι περισσότεροι hackers είναι έφηβοι ή μετεφηβικής ηλικίας. Ενόψει αυτού, σε αυτές τις περιπτώσεις, είναι απαραίτητη η υιοθέτηση αντεγκληματικής πολιτικής η οποία θα πρέπει να στοχεύει στην πρόληψη και την αποτροπή των ανήλικων δραστών[1691], χωρίς να έχει στο επίκεντρο μέτρα κατασταλτικού χαρακτήρα. Επίσης, σημαντική είναι η ανάγκη της προώθησης της διεθνούς συνεργασίας μεταξύ των κρατών προκειμένου να αντιμετωπίσουν το

[1691] Για τον ανήλικο ως δράστη πρβλ. ενδεικτικά το πόνημα του *Κ. Βουγιούκα*, Οι ανήλικοι ως δράστες εγκλημάτων και ως θύματα εγκληματικών πράξεων στους χώρους της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης και του Οργανισμού Ηνωμένων Εθνών. Οι συμβάσεις για τα δικαιώματα του παιδιού του Συμβουλίου της Ευρώπης και του Ο.Η.Ε., εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. ΙΙ, σελ. 1487 επ.

κυβερνοέγκλημα[1692]. Πρέπει, δε, σε κάθε περίπτωση να ληφθεί υπόψη η άποψη ότι οι hackers μπορούν να προσφέρουν με τη δράση τους στο κοινωνικό σύνολο (η άποψη αυτή συνδυάζεται και με τη θέληση για διαφάνεια στη δημόσια ζωή καθώς και για ενημέρωση του κοινού)[1693], ενώ και η κατάρτιση και η πείρα τους δύναται να αξιοποιηθεί[1694].

Τέλος, φαίνεται ότι υπάρχει γενικότερη ελλιπής ενημέρωση και εκπαίδευση ακόμη και σε επίπεδο επαγγελματικών ομάδων[1695] οι οποίες ασχολούνται με το δίκαιο της πληροφορικής και τα συστήματα πληροφοριών. Επομένως, για τη δημιουργία κουλτούρας ασφάλειας[1696] για τα συστήματα πληροφοριών σημαντικό ρόλο ενέχει η επιμόρφωση, η εκπαίδευση και η ενημέρωση. Αποτέλεσμα αυτής θα είναι και η ζύμωση για τη δημιουργία μιας πραγματικής «κοινωνίας των ψηφιακών πολιτών», η οποία θα μπορεί να διαδραματίσει ενεργό ρόλο στη διαμόρφωση απαντήσεων κοινωνικού τύπου σε παρεκκλίνουσες συμπεριφορές σε συστήματα πληροφοριών. Μέσω της ίδιας «κοινωνίας των ψηφιακών πολιτών» δύναται σε ύστερο στάδιο να προωθηθεί και η αυτορρύθμιση του κυβερνοχώρου[1697].

[1692] Βλ. παράγραφο 9.4.
[1693] Βλ. χαρακτηριστικά παράγραφο 7.8.3.4.
[1694] Βλ. παράγραφο 9.1.4.
[1695] Συμπέρασμα που προκύπτει απο το αποτέλεσμα της ερώτησης 3 αντίστοιχα για τα δείγματα νομικών και επιστημόνων πληροφορικής αλλά και από την ποιοτική ανάλυση των απαντήσεων των δειγμάτων αναφορικά με τον ορισμό του hacking.
[1696] Βλ. σχετικές αναπτύξεις στην παράγραφο 8.4 και ιδίως 9.2 του παρόντος πονήματος.
[1697] Βλ. παράγραφο 9.3

11. ΕΠΙΜΥΘΙΟ

Το πόνημα αυτό στόχευσε, μεταξύ άλλων, στην αξιολόγηση της ελληνικής ποινικής νομοθεσίας όχι απλώς μέσω μιας θεωρητικής προσέγγισης αλλά μέσω της διενέργειας έρευνας πεδίου. Είναι, δε, η πρώτη προσπάθεια στην ελληνική επιστημονική κοινότητα η οποία κατέγραψε απόψεις, θέσεις και στάσεις των hackers. Είναι γεγονός ότι οι hackers αποτελούν ένα πολύ ενδιαφέρον δείγμα για περαιτέρω μελέτη, ιδίως στο πλαίσιο της παραβατικότητας ανηλίκων καθώς, όπως καταγράφηκε, πολλοί από αυτούς είναι έφηβοι. Οι προβληματισμοί αυτοί μπορούν σίγουρα να αποτελέσουν ενδιαφέρον αντικείμενο επόμενων ερευνών[1698].

Είναι γεγονός ότι το ηλεκτρονικό έγκλημα πρέπει να αντιμετωπιστεί, καθώς, όπως εύστοχα υπογραμμίζει και ο Παπαθεοδώρου, «*λόγω των διαστάσεων που έχει λάβει και των διασυνδέσεών του με το οργανωμένο έγκλημα και την τρομοκρατία* (σ.σ. το ηλεκτρονικό έγκλημα) *αποτελεί ήδη μια σημαντική απειλή τόσο για τη δημόσια και τη διεθνή ασφάλεια, όσο και για τη σταθερότητα της διεθνούς οικονομίας*»[1699]. Αναφορικά, ωστόσο, με την ασφάλεια των συστημάτων πληροφοριών θα ήθελα να εισφέρω μια ύστερη σκέψη: όσες νομοθετικές προσπάθειες και όσες πρακτικές αντεγκληματικής πολιτικής και εάν υιοθετηθούν, η ασφάλεια στη χρήση των συστημάτων πληροφοριών ίσως να παραμένει πάντοτε τρωτή. Τούτο διότι πάντοτε το όποιο κενό ασφαλείας ενός συστήματος θα είναι γνωστό στον ίδιο τον δημιουργό του (ο οποίος το άφησε εκεί επίτηδες και, ενδεχομένως, να μπορεί ο ίδιος ή προστηθείς αυτού να δράσει χωρίς να αφήσει κανένα ίχνος). Οι απόψεις για χρήση ανοιχτού λογισμικού καταρρίπτονται με αυτόν τον τρόπο: αυτός ο οποίος προσφέρει το ανοιχτό λογισμικό γνωρίζει καλύτερα από όλους πώς αυτό το λογισμικό μπορεί να παραβιαστεί. Αλλά ακόμη και σε περιπτώσεις που δεν αναφερόμαστε σε ανοιχτό

[1698] Για προτάσεις ερευνών αναφορικά με δείγμα hackers ωραίες ιδέες περιέχονται στον επίλογο του πονήματος του Michael Bachmann, όπ. π.

[1699] *Θ. Παπαθεοδώρου,* Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002, σελ. 207.

λογισμικό, ενδέχεται ακόμη και η ίδια η εταιρεία κατασκευής ή μια κρατική δομή να έχει δημιουργήσει ένα τρωτό σύστημα προκειμένου να έχουν αν(εξ)έλεγκτη πρόσβαση σε ηλεκτρονικά δεδομένα του συστήματος[1700]. Άρα, όσοι έχουν στα χέρια τους την τελευταία «λέξη» της τεχνολογίας και τη δυνατότητα χρήσης αυτής φαίνεται ότι πάντοτε θα υπερέχουν και ενδεχομένως να μπορούν να αποκτούν πρόσβαση σε δεδομένα χρηστών.

Συνεπώς, πιστεύω πως δεν πρέπει να «κοπούν τα φτερά» σε καινοτόμες πρακτικές, καθώς τούτο φαίνεται μάλλον αλυσιτελές. Οφείλουμε να αναγνωρίσουμε ότι η καινοτομία και η εξέλιξη δεν περιορίζεται από «μέτρα ασφαλείας». Χωρίς υπερβολή, η καινοτομία που εισέφερε στο ανθρώπινο γένος ο μυθικός Προμηθέας, ο οποίος ξεγέλασε τον Δία και του πήρε τη φωτιά και το κρέας των ζώων για χάρη του ανθρώπου, μπορεί κάποτε να συγκρίνεται με τις καινοτομίες των hackers. Ο φόβος του ανθρώπου για το άγνωστο δεν πρέπει να επηρεάσει τις νομοθετικές και κοινωνικές αντιδράσεις και να θέτει παρωπίδες. Οι κοινωνίες, αντί να κατασβήνουν κάθε διαφορετική οπτική, πρέπει να αφήνουν «σπίθες» προκειμένου κάποια από αυτές να μπορεί να γίνει η «φωτιά του Προμηθέα»...

[1700] Βλ. χαρακτηριστικά το ρεπορτάζ «Πώς οι χάκερς «κλέβουν» τα προσωπικά μας δεδομένα από τα iPhone» της εφημερίδας «Πρώτο Θέμα» στις 27/07/2014 (url: http://www.protothema.gr/technology/article/398146/iphone-allow-extraction-of-personal-data/) το οποίο, μάλιστα αναφέρει κατά λέξη τα εξής:

«*... Σε ένα πρόσφατο συνέδριο ο ερευνητής ασφαλείας Τζόναθαν Ζιντράσκι ανέφερε πως κανένας χρήστης iPhone δεν είναι σε θέση να γνωρίζει ποια στοιχεία μπορούν να υποκλέπτουν ανά πάσα στιγμή από τη συσκευή τους είτε να εμποδίσουν όσους μπορούν να υποκλέψουν τα προσωπικά τους στοιχεία.*

"Δεν υπάρχει κανένας τρόπος να προστατευτείτε, εκτός αν διαλύσετε εντελώς τη συσκευή σας και πάλι χωρίς πολλές ελπίδες" ανέφερε χαρακτηριστικά ο κ. Ζιντράσκι στο συνέδριο Hackers on Planet Earth με σκοπό να δείξει τη ***συνεργασία ανάμεσα στην Apple και τις μυστικές υπηρεσίες των Ηνωμένων Πολιτειών της Αμερικής****. ...*» (η υπογράμμιση δική μου).

Επίσης, βλ. συνέντευξη του Edward Snowden στους *Alan Rusbridger & Ewen MacAskill*, "I, spy: Edward Snowden in exile", εφημερίδα "The Guardian", Σάββατο 19 Ιουλίου 2014 (url: http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill) στην οποία ο συνεντευξιαζόμενος αποτρέπει από τη χρήση νεφελοειδών αποθηκευτικών συστημάτων (όπως η ιστοσελίδα www.dropbox.com) υποστηρίζοντας ότι δεν εξασφαλίζεται η ιδιωτικότητα και αναφέροντας ως παράδειγμα το ότι στο συμβούλιο διοίκησης της συγκεκριμένης εταιρείας είναι μέλος η πρώην Υπουργός Εξωτερικών των ΗΠΑ Condoleezza Rice [την οποία, μάλιστα, χαρακτηρίζει ως προφανώς την κάτοχο δημόσιας θέσης με τις πλέον αντιτιθέμενες στην ιδιωτικότητα απόψεις ("*probably the most anti-privacy official you can imagine*")]. Αφήνει, επομένως, σοβαρές αιχμές για τρωτά και ανασφαλή συστήματα πληροφοριών. Ο ίδιος συμβουλεύει τους χρήστες να χρησιμοποιούν πλατφόρμες κρυπτογράφησης των αρχείων τους ακόμη και για νεφελοειδή αποθήκευση

(για τον Edward Snowden πρβλ. http://el.wikipedia.org/wiki/%CE%88%CE%BD%CF%84%CE%BF%CF%85%CE%B1%CF%81%CE%BD%CF%84_%CE%A3%CE%BD%CF%8C%CE%BF%CF%85%CE%BD%CF%84%CE%B5%CE%BD).

Θεωρώ πως αυτές οι προτάσεις μπορούν να αποτελέσουν θρυαλλίδα για την εξέλιξη της σκέψης μας προκειμένου το διαδίκτυο να αποτελεί έναν χώρο ελευθερίας της έκφρασης, πρόσβασης στην πληροφορία, ανάπτυξης της προσωπικότητας, αυτοδιάθεσης, με όλους όμως τους περιορισμούς που ενυπάρχουν στην άσκηση των ως άνω δικαιωμάτων[1701], αλλά και χωρίς να χάνεται το σπέρμα της καινοτομίας. Προς αυτήν ακριβώς την κατεύθυνση οφείλει και η επιστημονική κοινότητα να εργαστεί - με σημείο αναφοράς την αξία του ανθρώπου[1702] - και ο ίδιος ο άνθρωπος να στρέψει το βλέμμα του. Η καλύτερη πρόκληση για το ανθρώπινο γένος στην «*ψηφιακή εποχή»* είναι να αποδείξουμε ότι πράγματι ισχύει μια φράση, η οποία αποδίδεται στον πρώτο Προέδρο της Ομοσπονδιακής Δημοκρατίας της Γερμανίας Theodor Heuss (1884-1963) και την οποία ίσως αγαπούν πολύ και οι hackers (!):

> «***Ίσως μια μέρα οι μηχανές θα μπορούν να σκέφτονται, όμως ποτέ δεν θα αποκτήσουν φαντασία***»
>
> "***Eines Tages werden Maschinen vielleicht denken können aber sie werden niemals Phantasie haben***"[1703].

[1701] Ο Φαρσεδάκης αναφέρεται σε «*...προστασία των δικαιωμάτων των πολιτών τόσο από την κεντρική εξουσία, όσο και από τις πιθανές προσβολές τους από τους κυβερνοεγκληματίες*» (*Ιακ. Φαρσεδάκης,* Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του, όπ. π., σελ. 12).

[1702] Βλ. την εξαιρετική προσέγγιση αναφορικά με τον σύγχρονο ρόλο του εγκληματολόγου στο άρθρο του *Ν. Κουράκη*, Ο μετέωρος ρόλος του εγκληματολόγου στη χάραξη αντεγκληματικής πολιτικής, εις: *Ν. Κουράκη*, Εγκληματολογικοί ορίζοντες, τομ. Α': Ιστορική και θεωρητική προσέγγιση, όπ. π., σελ. 141 επ. καθώς και την ανάπτυξη του *Ν. Δημητράτου*, Ποινικό δίκαιο και κράτος δικαίου στη σύγχρονη εποχή, ΠοινΔικ 5/2004, σελ. 598-599 κατά την οποία «*Σε ένα αληθινά λειτουργικό και όχι μόνο κατ' επίφαση κράτος δικαίου η φιλελεύθερη λειτουργία του ποινικού συστήματος ενυπάρχει και στην προστατευτική των εννόμων αγαθών αποστολή του, είναι δηλαδή αυτή συμφυής με τη γενικότερη* ***ανθρωποκεντρική αντεγκληματική πολιτική****»*.

[1703] ... εννοώντας βέβαια ότι η φαντασία είναι αποκλειστικά ανθρώπινο χαρακτηριστικό απαραίτητο για την εξέλιξη και την πρόοδο! Βλ. ενδεικτικά url: http://www.woelfersheim.de/leseobjekte.pdf?id=1322 και http://geboren.am/person/Theodor_Heuss.

Σοφοκλέους ***Ἀντιγόνη (ed. Sir Richard Jebb, Cambridge. 1891)***

Χορός (Α' Στάσιμο)

πολλὰ τὰ δεινὰ κοὐδὲν ἀνθρώπου δεινότερον πέλει.
τοῦτο καὶ πολιοῦ πέραν πόντου χειμερίῳ νότῳ
χωρεῖ, περιβρυχίοισιν
περῶν ὑπ᾽ οἴδμασιν.
θεῶν τε τὰν ὑπερτάταν, Γᾶν
ἄφθιτον, ἀκαμάταν, ἀποτρύεται
ἰλλομένων ἀρότρων ἔτος εἰς ἔτος
ἱππείῳ γένει πολεύων.
κουφονόων τε φῦλον ὀρνίθων ἀμφιβαλὼν ἄγει
καὶ θηρῶν ἀγρίων ἔθνη πόντου τ᾽ εἰναλίαν φύσιν
σπείραισι δικτυοκλώστοις,περιφραδὴς ἀνήρ·
θηρὸς ὀρεσσιβάτα, λασιαύχενά θ᾽
ἵππον ὀχμάζεται ἀμφὶ λόφον ζυγῶν
οὔρειόν τ᾽ ἀκμῆτα ταῦρον.
καὶ φθέγμα καὶ ἀνεμόεν φρόνημα καὶ ἀστυνόμους
ὀργὰς ἐδιδάξατο καὶ δυσαύλων
πάγων ὑπαίθρεια καὶ δύσομβρα φεύγειν βέλη
παντοπόρος· ἄπορος ἐπ᾽ οὐδὲν ἔρχεται
τὸ μέλλον· Ἅιδα μόνον φεῦξιν οὐκ ἐπάξεται·
νόσων δ᾽ ἀμηχάνων φυγὰς ξυμπέφρασται.
σοφόν τι τὸ μηχανόεν τέχνας ὑπὲρ ἐλπίδ᾽ ἔχων
τοτὲ μὲν κακόν, ἄλλοτ᾽ ἐπ᾽ ἐσθλὸν ἕρπει,
νόμους γεραίρων χθονὸς θεῶν τ᾽ ἔνορκον δίκαν,
ὑψίπολις· ἄπολις ὅτῳ τὸ μὴ καλὸν
ξύνεστι τόλμας χάριν. μήτ᾽ ἐμοὶ παρέστιος
γένοιτο μήτ᾽ ἴσον φρονῶν ὃς τάδ᾽ ἔρδει.

Μετάφραση (Κ. Χ. Μύρης, εκδ. Κάκτος, Αθήνα, 1994)

Πολλά γεννούν το δέος˙ το μέγα δέος ο άνθρωπος γεννά˙ περνά τον αφρισμένο πόντο με τις φουρτούνες του νοτιά, στη μέση σκάβει το βαθύ και φουσκωμένο κύμα˙ και την υπέρτατη θεά, τη Γη, την άφθαρτη παιδεύει την ακάματη οργώνοντας με τα καματερά χρόνο το χρόνο φιδοσέρνοντας τ' αλέτρι.

Και των αστόχαστων πτηνών τις φυλές κυνηγά με τα βρόχια, των αγρίων θηρίων τα έθνη, των βυθών την υδρόβια φύτρα με δίχτυα πλεγμένα στριφτά, ο τετραπέρατος˙ τ' αγρίμι της βουνοκορφής δαμάζει με τεχνάσματα˙ φορεί στων αλόγων την πλούσια χαίτη ζυγό και στον ταύρο, που βαρβάτος βοσκάει στα όρη.

Ένας τον άλλο δίδαξε λαλιά, τη σκέψη, σαν το πνεύμα των ανέμων, την όρεξη να ζει σε πολιτείες˙ πώς να γλιτώνει το χαλάζι μες στ' αγιάζι, την άγρια δαρτή βροχή μέσα στον

κάμπο, ο πολυμήχανος˙ αμήχανος δε ϑ' αντικρύσει τα μελλούμενα˙ το χάρο μόνο να ξεφύγει δεν μπορεί˙ μόλο που βρήκε ψάχνοντας και γιατρειές σ’ αγιάτρευτες αρρώστιες.

Τέχνες μαστορικές σοφίστηκε που δεν τις βάζει ο νους, κι όμως μια στο καλό, μια στο κακό κυλάει˙ όποιος κρατεί τον ανϑρώπινο νόμο και του ϑεού το δίκιο, που όρκος το δένει φριχτός, πολίτης˙ αλήτης και φυγάς, όποιος κλωσάει τ' άδικο, μακάρι και μ' αποκοτιά, ποτέ σε τράπεζα κοινή ποτέ μου βούληση κοινή με κείνον που τέτοια τολμάει.

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Ι: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ ΝΟΜΙΚΩΝ

[επισυνάπτεται]

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ ΕΠΙΣΤΗΜΟΝΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

[επισυνάπτεται]

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ ΔΕΙΓΜΑΤΟΣ HACKERS

[επισυνάπτεται]

ΠΑΡΑΡΤΗΜΑ IV: ΕΠΙΣΤΟΛΗ ΤΗΣ GREEK HACKING SCENE

Το κείμενο που ακολουθεί αναφορικά με την ίδρυση, τη δράση και την ιδεολογία της Ελληνικής Χάκινγκ Σκηνής (Greek Hacking Scene - GHS) εστάλη από τον ίδιο τον διαχειριστή του ως άνω λογαριασμού της Ελληνικής Χάκινγκ Σκηνής (GHS) στην ιστοσελίδα κοινικής δικτύωσης www.facebook.com. Κατά δήλωση των αποστολέων, το εν λόγω κείμενο έχει συνταχθεί από την GHS προκειμένου να χρησιμοποιηθεί σε δημοσίευμα της εφημερίδας «Ελεύθερος Τύπος» αναφορικά με την GHS[1704].

Παρατίθεται χωρίς να έχει υποστεί επεξεργασία (εκτός βεβαίως από την προσθήκη από τον γράφοντα διευκρινιστικών παραπομπών και υποσημειώσεων όπου κρίθηκε απαραίτητο):

«Η Ελληνική Χάκινγκ Σκηνή είναι Ιδέα για Ελευθερια, Δημοκρατία, Δικαιοσύνη και Παιδεία. Η Σκηνή πιστεύει ότι η Ελευθερια είναι το μεγαλύτερο ιδανικό του ανθρώπου. Η Δημοκρατία είναι ένα βασικό στοιχειο της ζωής και της συμβιώσεις των ανθρώπων, και όταν μιλάμε για δημοκρατία δεν εννοούμε την πλειοψηφία και μονο. Με βάση των ορισμό που δίνετε από την ΕΧΣ, Δημοκρατία είναι η στέγη υπό την οποια μπορούν όλοι να επιβιώσουν χωρίς να προσπαθεί κανεις να μεταπείσει κανέναν διά τις επιβολής, και να εκπροσωπούνται όλοι με βάση το αντίστοιχο ποσοστό τους που κατέχουν στην κοινωνία. Παράλληλα κάθε τι που προσπαθεί να επιβληθεί διά της βίας και του εξαναγκασμού η με άλλες σχετικές τεχνικές, είναι αντίθετο με την Ελεύθερη Δημοκρατία και πρέπει να απομακρύνεται. Η Δικαιοσύνη πρέπει να είναι πραγματικά δίκαιη και αμερόληπτη. Μια δικαιοσύνη ίση για όλους που να προστατεύει την Ελευθερια και τη Δημοκρατία. Η Παιδεία

[1704] Αποσπάσματα του κειμένου αυτού πράγματι χρησιμοποιήθηκαν στο δημοσίευμα με τίτλο «Η Ελληνική Χάκινγκ Σκηνή ανοίγει τα χαρτιά της», περιοδικό GADGET, αρ. τ. 129, εφημερίδα «Ελεύθερος Τύπος», Σάββατο 25 Αυγούστου 2012, url: https://docs.google.com/viewer?url=http://www.e-typos.com/content/entheta_pdf/25hacker.pdf. Το δημοσίευμα αυτό δεν υπεδείχθη από την GHS αλλά ανευρέθη κατά την έρευνα στον Τύπο για την εν λόγω διατριβή.

πρέπει να είναι ελεύθερη και για όλους. Η GHS πιστεύει ότι όλοι μπορούμε να ζήσουμε ειρηνικά και αρμονικά. Παιδεία δεν είναι μονο οι γνώσεις και πληροφορίες που αποκτά ο άνθρωπος διά τις μάθησης, αλλα είναι και η συπεριφορά μας προς τον συνάνθρωπο μας. Η Παιδεία είναι βασικό στοιχειο για την διατήρηση τις ελευθερίας και την διαφύλαξη της αρμονίας, καθώς και της εξέλιξης.

Η Ελληνική Χάκινγκ Σκηνή ξεκίνησε το 1993 σαν μια ομάδα δημιουργίας λογισμικού για μεταφορά αρχείων μεταξύ απομακρυσμένων υπολογιστών και εξελίχθηκε σαν ιδεολογία. Ασχολείται με πάντως είδους hacking, προγραμματισμό, τεχνολογία και σε αυτήν ανήκουν όλοι οι Έλληνες η όσοι μπορούν να διαβάσουν και να μιλήσουν Ελληνικά, ασχολούνται με το hacking, και εφόσον κατανοούν την ιδεολογία.

Βασικές αρχές λειτουργίας και σήμα κατατεθέν είναι η Ενότητα, Αγιότητα, Καθολικότητα και Αποστολικότητα. Όλα τα μέλη είναι ισα αναμεταξύ τους, "προεχρομαινοι" από διαφορετικές πολιτικές και πληθυσμιακές μερίδες. Σε καμια περίπτωση δεν υποστηρίζεται κανένα είδος οικονομικού hacking, και οτιδήποτε είναι αντίθετο με την ιδεολογία.

Η λειτουργία της Greek Hacking Scene γίνετε από τα μέλη της οργανωμένα σε μικρές ομάδες, από μεμονωμένα άτομα που κινούνται με βάση την ιδεολογία και από την mailing-list.

Η mailing-list είναι ένα σύστημα ανταλλαγής μηνυμάτων μεταξύ των μελών της. Μέλη σε αυτήν γίνονται όσοι ασχολούνται ενεργά σε βάθος χρόνου και έχουν σταθερή ιδεολογία, είτε άλλοι που μοιράζονται τα ίδια ιδανικά με τη Σκηνή. Τα ενδιαφερόμενα μέλη, δεν γνωρίζουν σε καμια περίπτωση για την mailing-list. Έρχονται σε επαφή με μέλη της λίστας και εκφράζουν την επιθυμία τους να συμβάλουν στην Greek Hacking Scene. Τα μέλη της λίστας σε πρώτη φάση, τους ενθαρρύνουν να διευρύνουν τις γνώσεις τους, κυρίως δίνοντας έμφαση στην τεχνολογία και προτρέποντας τους σε ουσιαστικές γνώσεις όπως τον προγραμματισμό, κάτι που μπορεί να τους φανεί και χρήσιμο στο μέλλον, και παράλληλα τους αποθαρρύνουν στο να ασχοληθούν με το hacking και τη Σκηνή. Η GHS δεν προσηλυτίζει κόσμο και ούτε προσπαθεί να προτρέψει κάποιον για την ιδεολογία της. Όταν αυτά τα άτομα παρόλα αυτά συνεχίζουν να ασχολούνται

ενεργά με την GHS έχοντας σταθερή ιδεολογία σε βάθος χρόνου, και σε συνάρτηση με την εμπιστοσύνη που χτίζεται στη πάροδο του χρόνου, τότε είναι σε θέση να ενταχτούν στην mailing-list. Είναι μια μακρά διαδικασία και αυτός είναι ένας σημαντικός λόγος για τον οποιο δεν είναι εύκολο κάποιος να εισχωρήσει σε αυτήν. Είναι πολλά τα μέλη της GHS που ασχολούνται χρονια και δεν έχουν επίγνωση της λίστας λόγο της αστάθειας στην ιδεολογία τους, η κυρίως λόγο μόδας της κάθε περιόδου. Στη λίστα εισάγονται μέλη που έχουν τα ίδια ιδανικά και πιστεύω, και σε καμια περίπτωση δεν προσηλυτίζονται, αλλα αντίθετα οι ίδιοι τους θέλουν. Η εισαγωγή στη λίστα γίνετε από το μέλος. Το μέλος έχει το δικαίωμα να προτείνει κάποιον για εισαγωγή, τότε και με θετική ομόφωνη ψηφοφορία εντάσσεται ο ενδιαφερόμενος στη λίστα. Πρώτα προτείνεται από το μέλος χωρίς την επίγνωση του ενδιαφερομενου, και εφόσον υπάρχει θετική ομόφωνη ψηφοφορία, τότε το μέλος μπορεί να κάνει διάλογο στον ενδιαφερόμενο για την ύπραξη της λίστας και να του προτείνει την εισαγωγή του εφόσον θέλει. Σε περίπτωση αρνητικού αποτελέσματος στην ψηφοφορία, ταυτόχρονα διαγράφεται και το μέλος από αυτήν. Με την εισαγωγή στην λίστα, ο ενδιαφερόμενος καταχωρεί και επαληθεύει τα στοιχεια του. Μέσα στη λίστα όλα τα μηνύματα διακινούνται ανώνυμα, καθώς δεν υπάρχουν nicknames αλλα automatic generated codes. Τα μηνύματα είναι κρυπτογραφημένα και η προβολή τους δεν απαιτεί μονο την αποκρυπτογράφηση, αλλα και την δυνατότητα ανάγνωση τους από τα μέλη καθώς χρησιμοποιούνται ειδικοί χαρακτήρες. Τα μέλη δεν γνωρίζονται αναμεταξύ τους, συνήθως γνωρίζουν μονο το άτομο από το οποιο προτάθηκαν στη λίστα, η από αυτά που πρότειναν. Η πλειοψηφία της λίστας δεν χρησιμοποιεί nicknames, και ασχολούνται κυρίως με νέες τεχνικές και την ανάπτυξη της τεχνολογίας. Τα μέλη θέτουν προτάσεις οι οποιες ψηφίζονται, μέσα σε συγκεκριμένο χρονικό περιθώριο, και ανάλογος υλοποιούνται. Όλοι έχουν δικαίωμα ψήφου εκτος από τους διαχειριστές του συστήματος. Οι διαχειριστές ψηφίζονται ομόφωνα και δεν έχουν δικαίωμα στις ψηφοφορίες. Υπάρχει μεγάλη κίνηση στην συλλογή και αρχειοθέτηση πληροφοριών και τεχνογνωσίας. Αυτή είναι η Ελεύθερη Πολιτεία, η αλλιώς mailing-list.

Έχουν γίνει στο παρελθόν και ενέργειες για προσπάθεια μιας πιο γενικευμένης τύπου λίστας προσβάσιμη ποιο εύκολα στο ευρύ κοινό, κάτι που είναι εξαιρετικά δύσκολο πληθυσμιακά, λόγο των πολιτικών πεποιθήσεων που επικρατούν υπεράνω του συμφέροντος του Έλληνα πολίτη.

Τα κόμματα προσηλυτίζουν κόσμο για τα πολιτικά τους συμφέροντα, μένοντας μακρυά από το κοινό καλο. Η Greek Hacking Scene πιστεύει ότι ο Ελληνικός λαός θέλει να έχει μια αξιοπρεπή ζωή, να μπορεί να δουλεύει, να υπάρχει ασφάλεια και να γίνετε η ζωή του καλύτερη.

Η GHS απευθύνεται στο λαό και όχι στον κόσμο του IT. Δεν επιτίθεται ποτε σε προσωπικό επίπεδο, σε κανέναν και για κανένα λόγο, αλλα επιτίθεται σε συνολική βάση σε όσους προσπαθούν να φιμώσουν την Ελευθερια, Δημοκρατία, Δικαιοσύνη και Παιδεία. Η Σκηνή πράττει αυτό που πιστεύει ότι είναι το γενικό κοινό καλο όλων.

Οποιαδήποτε αρχή κινηθεί εναντίον, αυτόματα αυτοπροσδιορίζετε αντι-δημοκρατική και τρομοκρατική καθώς λειτουργει αυθαίρετα και έξω από τους νόμους του ίδιου του Ελληνικού κράτους. Ενέργειες που περιορίζουν την Δημοκρατία, θα πρέπει να τιμωρούνται δια του νόμου. Ο λαός έχει το δικαίωμα να προστατέψει την Δημοκρατία, εφόσον αυτοί που κυβερνάνε και οι σχετικές αρμόδιες αρχές την καταπατάνε. Τότε ο λαός πρέπει να προστατέψει την Δημοκρατία όπως και αναγράφετε και στο σύνταγμα. Όλοι αυτοί που περιορίζουν την Δημοκρατία πρέπει να οδηγηθούνε στην Δικαιοσύνη.

Άρθρο 120 του Συντάγματος:

Η τήρηση του Συντάγματος επαφίεται στον πατριωτισμό των Ελλήνων, που δικαιούνται και υποχρεούνται να αντιστέκονται με κάθε μέσο εναντίον οποιουδήποτε επιχειρεί να το καταλύσει με τη βία.

We deploy an ιdea for ελευθερία, δημοκρατία, δικαιοσύνη, παιδεία! We τακε ονερ, join υς!

In somε decadεs from noω ωε ωill bε thε gearς of thε system. Wε arε noτ negoτiaτing, ωε don't makε dealς, ωε havε a plan.[1705]

With kind regards, me your son/daughter, of freedom and civilization.

Με εκτίμηση, Εγώ ο γιος σου/ κόρη σου, της Ελευθερίας και της Δημοκρατίας.

[1705] Στο συγκεκριμένο κείμενο και δη στα εν λόγω συνθήματα βλέπουμε π.χ. να χρησιμοποιείται από την GHS το ελληνικό γράμμα «ω» ως το αγγλικό γράμμα "w" και το ελληνικό γράμμα «ε» ως το αγγλικό γράμμα "e", ως ειδικό γλωσσικό μόρφωμα, όπως αναφέρεται διεξοδικά ανωτέρω στη σχετική με την υποκουλτούρα του hacking παράγραφο υπ' αρ. 2.8.

Άλλες σχετικές κινήσεις που συνέβαλε η οργάνωσε η Ελληνική Hacking Σκηνή, ενδεικτικά, το HackerzIr, Alliance Hacker Technology.

Το HackerzIr ήταν ένα δίκτυο βασισμένο στο Iran και με σκοπό την όσο πιο δυνατή εξάπλωση της Ελευθερίας και της Δημοκρατίας στην περιοχή. Μια κοινότητα οχτώ χιλιάδων μελών εκ των οποιων οι δυόμισι χιλιάδες ήταν ενεργά μέλη. Κατά την περίοδο 2008, το καθεστώς της χώρας συνέλαβε διαφορους με την πρόφαση ότι διαμοίραζαν stream εντός της χώρας από απαγορευμένα sites μέσω proxy. Έτσι πολλές τεχνολογικές κοινότητες έκλεισαν η διαλύθηκαν. Το ίδιο έγινε και με την παρόν κοινότητα. Μεγάλη εντύπωση έκανε η θέληση της νεολαίας για μάθηση και τεχνολογική ανάπτυξη. Οι περισσότεροι εκ των οποιων λένε πως η μεγαλύτερη γενιά που διήκουν τη χωρα τους κρατάνε πίσω. Άσχετα από τις αποφάσεις που λαμβάνει το καθεστώς, η νεολαία της χώρας είναι από αυτές που επιδιώκουν περισσότερο την ελευθερια από οποιαδήποτε άλλη στην περιοχή, μακρυά από θρησκευτικά και παραδοσιακά ταμπού. Πιστεύουν ότι όταν πάρουν την εξουσία στα χερια τους, θα αλλάξει και η χωρα ριζικά από αυτά που τους επιβάλλουν με το ζόρι. Παράδειγμα είναι δυο μέλη της σχετικής κοινότητας που διδάσκουν στο πανεπιστήμιο της Τεχεράνης.

Alliance Hacker Technology είναι μια κλειστή κοινότητα hacking βασισμένη στην Κίνα. Εκεί η Σκηνή εκπαιδεύει μεγάλο αριθμό κινέζων στο hacking με έμφαση την αντίθεση στα απολυταρχικά καθεστώτα ανά τον κόσμο, θέλοντας έτσι να δημιουργήσει ένα ισχυρό μπλόκο στην μακρινή ανατολή.

Η Greek Hacking Scene και οι Anonymous[1706]. Η GHS είναι anons, η Σκηνή οργάνωσε κομμάτια των anonymous και βελτίωσε διαφορα σημεία. Έτσι εντάχτηκε και η λέξει δημοκρατία. Σκοπός ήταν να περάσει μήνυμα στον πληθυσμό, έτσι αυθεντικοποιηθηκαν χτυπήματα των anons που δεν έγιναν ποτε, αναρωτηθείτε ποσα είναι τα χτυπήματα για τα οποια έχετε ακούσει και ποτε δεν έχετε δει άλλωστε, με σκοπό να στείλει μήνυμα στον πληθυσμό. Στη διάρκεια του χρόνου οι anons αντικαταστήθηκαν από τις αρχές και πλέον όλα είναι

[1706] Για την κολεκτίβα των "Anonymous" πρβλ. *του γράφοντος*, Anonymous - χακτιβισμός με "ονοματεπώνυμο"; ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 25, Νοέμβριος 2013, url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756.

υποκινούμενα, και εφόσον αλλοιώθηκε ο διαμορφωμένος χαρακτήρας και σκοπός, η GHS διέκοψε την υποστήριξη της. Τακτική των αρχων της Νέας Υόρκης εδώ και πολλά χρονια είναι να εισχωρούν δικοί της άνθρωποι σε διαφορες οργανώσεις και έτσι να τις ελέγχουν. Το ίδιο έγινε και με τους anons. Ήταν εξάλλου και μια ευκαιρία, δεν θα μπορούσαν να γίνουν νομοι που να περιορίζουν τις δικτυακές ελευθερίες επειδή οι κινέζοι hackers επιτίθονται στην αμερική εδώ και τόσα χρονια όπως συνεχώς διαμαρτύρονται. Έτσι οι anonymous ήταν χρυσή ευκαιρία για την θέσπιση νομων. Οι anonymous οι οποιοι και συνελήφθηκαν πριν καλά αρχίσει η δημοσιότητα, είχαν ήδη αντικατασταθεί από τις αρχές, οι οποιες ανάπτυξαν σε παγκόσμιο επίπεδο θέμα hacking το οποιο απειλή τις δικτυακές ελευθερίες των πολιτών. Έτσι πλέον έχουν ως πρόφαση κάτι υπαρκτό που απειλή την ασφάλεια, το οποιο οι ίδιοι φτιάξαν τεχνητά, για να δημιουργήσουν έτσι νομους για το διαδίκτυο. Έτσι πλέον οι anonymous που είναι εργαλείο των αρχων, υποκινούν τις μάζες που δεν έχουν επίγνωση του θέματος. Έτσι παρουσιάζουν το πλήθος να κερδίζει έναντι των κυβερνήσεων, ενώ στην ουσία υποκινούν τον κόσμο να προβεί σε πράξεις που αύριο θα θέσουν τέλος στις ελευθερίες των ιδιων. Σε διαφορες χώρες του κόσμου, πολιτικά κόμματα κυρίως, καπηλεύονται ανοιχτές ιδέες και τις βαφτίζουν με πολιτικο χρώμα για το συμφέρον τους. Το ίδιο συμβαίνει και στην Ελλάδα. Αυτός είναι και ο κυρίως λόγος που διαφορες ομάδες ανά των κόσμο που αποτέλεσαν τους anons, αποσύρουν την υποστήριξη τους εφόσον και ο σκοπός αλλοιώθηκε. Επίσης έγιναν και πολλές απόπειρες φίμωσης διαφορων groups από τις αρχές. Η GHS αποτέλεσε κομμάτι των Anonymous πριν ακόμα κανεις στην Ελλάδα έχει κάνει οποιαδήποτε ενέργεια η έχει προσπαθήσει να καπηλευτεί την ανοιχτεί ιδέα. Το #codehack αποτέλεσε ένα από τα μεγαλύτερα κανάλια του δικτύου των anons, και είναι ο κυρίως λόγος εισαγωγής της Δημοκρατίας στην γενική ιδεολογία, καθώς και πηγή διαφορων συνθημάτων. Η Greek Hacking Scene σταμάτησε την υποστήριξη της όταν ο σκοπός αλλοιώθηκε και διαπιστώθηκε ότι οι anonymous υποκινούνται πλέον από τις αρχές [1707]***. Κανεις δεν μπορεί να συμβάλει σε κάτι που σκοπό έχει πλέον να περιορίσει τις προσωπικές ελευθερίες του λαου, εν αγνοια των ιδιων.***

[1707] Για τη διάσταση που υπάρχει πλέον μεταξύ GHS και "Anonymous" πρβλ. url: http://thesecretrealtruth.blogspot.com/2012/09/greek-hacking-scene.html

Η Greek Hacking Scene και το DefCon. Το DefCon είναι ένα Hacking Convention, ένας θεσμός που υποστηρίζεται διαχρονικά από την ΕΧΣ. Διατηρούνται καλές επαφές και διαφορα μέλη της Σκηνής συνηθίζουν να παρευρίσκονται σε αυτά.

Οι επιθέσεις που πραγματοποιούνται γίνονται από groups της GHS, είτε από μεμονωμένα μέλη, είτε από την Ελεύθερη Πολιτεία. Για τον εσωτερικό χώρο, υπάρχει οδηγία να αποφεύγονται ενέργειες σε Ελληνικές ιστοσελίδες, εκτος και αν μπορεί να γίνει χρήση του άρθρου εκατόν-είκοσι του συντάγματος. Βεβαια πολλοί είναι και αυτοί που αναπτύσσουν τις ικανότητες τους και πειραματίζονται πάνω σε στόχους σε πραγματικό χρόνο. Τα δεδομένα που συλλέγονται, αξιολογούνται και στην συνεχεια όσα κριθούν ως σημαντικά στέλνονται σε έναν ποιο ευρύ κύκλο ατόμων που αγωνίζονται για την καταπολέμηση της διαφθοράς και άλλον θεμάτων που δυσκολεύουν τη ζωή του λαου. Στη συνεχεια εφόσον αποσπαστούν πληροφορίες και αξιολογηθούν, όχι πάντα, και εφόσον δεν έχει κάτι άλλο να προσφέρει το κάθε δίκτυο η ιστοσελίδα, τότε αλλοιώνεται με κάποιο μήνυμα της GHS. Οι επιθέσεις δεν πρέπει να γίνονται σε προσωπικό επίπεδο, η για προσωπικούς λόγους, και ούτε απασχολούν τα προσωπικά δεδομένα. Σημαντικά είναι τα δεδομένα που συλλέγονται από τα sites και δίκτυα και μπορούν να χρησιμοποιηθούν υπέρ του λαου, επίσης σημαντικά είναι και τα μηνύματα που ανεβαίνουν στην αλλοιωμένες σελίδες. Χτυπήματα γίνονται και σε σελίδες σε όλο το κόσμο, για διαφορους λόγους και σκοπούς, είτε ακόμα και για πειραματισμό σε πραγματικό χρόνο. Όπως μπορεί να παρατηρηθεί σε χρονική σειρά στις περισσότερες του συνόλου επιθέσεις, υπάρχει συνεχείς ροή.

Μερικά από τα χτυπήματα σε ιστοσελίδες αποτελούν ενδεικτικά τα: nasa.gov, navy.mil, mfa.gov.tr, telekom.gov.tr, ataturk.net, mil.tr, yeniparti.org.tr, metu.edu.tr, justice.gov.al, mete.gov.al, .mk, vmro-dpmne.org.mk, kultura.gov.mk, skopje.gov.mk, president.gov.mk, ukim.edu.mk, geodata.gov.gr, presidency.gr, minedu.gov.gr, in.gr ... κ.α. για τα οποια δεν θα μπορούσε να γίνει αναφορά.

Η παιδεία είναι μια βασική δομή για την εξέλιξη, όπως και για την ελευθερια. Η Σκηνή αντιτάσσεται σε απολυταρχικά καθεστώτα εκτος και αν είναι συνολική επιλογή του ιδιου του λαου. Τα απολυταρχικά καθεστώτα η συστήματα περιορίζουν την παιδεία και άρα και την εξέλιξη. Διαφυλάσσονται και επεκτείνονται όσο γίνετε τα γόνιμα εδάφη ως προς την καλλιέργεια της παιδείας που μπορούν να φέρουν εξελίξει και ανάπτυξη στον ίδιο τον άνθρωπο και το λαό.

Η Ελληνική Χάκινγκ Σκηνή κινείται με βάση ένα γενικό πλάνο που υλοποιείται την κάθε χρονική περίοδο και δημιουργεί έδαφος για το επόμενο στάδιο. Δεν αντιτίθεται μονο, αλλα έχει και προτάσεις-λύσεις. Όπως ο κόσμος μας μεταλλάσσεται και εξελίσσεται στην πάροδο του χρόνου, το ίδιο συμβαίνει και με την GHS. Η ενότητα είναι ένα από τα θεμελιώδεις συστατικά για την εξέλιξη του ανθρώπου. Αν ο άνθρωπος θέλει να εξελιχθεί σαν είδος, πρέπει να ενωθεί. Όλα δείχνουν ότι η παγκοσμιοποίηση θα επέλθει είτε με τον έναν είτε με τον άλλο τρόπο, είτε με κάποια άλλη μορφή. Και το σημαντικό είναι, ότι αν επέλθει αυτό, να γίνει σωστά. Η GHS αναζητεί εξέλιξη και διαγαλαξιακή εξερεύνηση. Για να γίνει κάτι τέτοιο πρώτα θα πρέπει να επέλθουν οι ισορροπίες και η ενότητα στην ανθρωπότητα. Πιστεύουμε πως όλοι μπορούμε να ζήσουμε αρμονικά και να κάνουμε τις ζωές μας καλύτερες.

Σήμερα, μια μεγάλη σκλαβιά σε παγκόσμια κλίμακα λαμβάνει μέρος στην ανθρωπότητα, διά μέσω της οικονομικής τρομοκρατίας. Οι κυβερνήσεις ψεύδονται και οι εταιρίες έχουν πάρει πλέον τον έλεγχο. Σύντομα η τεχνολογία θα ξεπεράσει τις ανάγκες μας γίαυτήν και τότε θα γίνουμε πλήρως ελεγχόμενοι χωρίς να μπορούμε να αντιδράσουμε.

Η Ελληνική Χάκινγκ Σκηνή θέλει να διαφυλάξει την Ελληνική γλώσσα και πολιτισμό από τα απολυταρχικά καθεστώτα, που την βλέπουν ως εμπόδιο στον απολυταρχισμό τους, καθώς επίσης και από το ίδιο το κράτος που μέρα με τη μέρα αλλοιώνει και υποβαθμίζει το χαρακτήρα της, όπως και τη ζωή του Έλληνα πολίτη. Για τι Σκηνή η Ελληνική γλώσσα θεωρείτε ουσιώδεις βάση για τις επιστήμες, καθώς είναι ήδη μια εξελιγμένη πλατφόρμα η οποια μπορεί να επιφέρει ευρύτερη σκέψη και ανάπτυξη στις επιστήμες. Πολλοί οροι είναι ήδη αυτονόητοι λόγο της γλωσσικής σύνθεσης που εννοεί ότι λέει, έτσι ένα από τα μέγιστα θετικά είναι ότι κατανοούνται οι επιστήμες γρηγορότερα διά μέσω της γλώσσας εφόσον υπάρχουν φυσικά και οι απαραίτητες δομές. Ο άνθρωπος μπορεί να εξελίχτηκε τεχνολογικά, να άλλαξαν τα πράγματα τριγύρω του είτε τεχνολογικά είτε στυλιστικά, αλλα ο πολιτισμός δεν κατάφερε να εξελιχτεί. Δεν είναι μυστικό ότι ο πολιτισμός εξελίχτηκε κυρίως σε δυο φάσεις, στην αρχαία Ελλάδα και επί του Βυζαντίου. Ο πολιτισμός που παρήγαγαν αυτές οι χρονικές εποχές, είναι διατυπωμένος και υιοθετημενος σε όλο το κόσμο χωρίς να επιβλήθηκε, και ιδιαιτερα τους τελευταίους αιώνες που ο Ελληνισμός ήταν απών, και πολλά μέρη

του πλανήτη έψαχναν ένα πιο δίκαιο τρόπο ζωής και διακυβέρνησης, πηγή ζωής και ελευθερίας.

Η ΕΧΣ καλλιεργεί μια νέα γενιά που να επιδιώκει την Ελευθερια, να θέλει το καλο του γενικού συνόλου και να έχει παιδεία. Μια γενιά που να μην νοσταλγεί ένα ένδοξο παρελθόν, αλλα μια γενιά που να γνωρίζει το παρελθόν και να θέλει να κάνει ακόμα περισσότερα. Μια γενιά που να έχει όραμα για το μέλλον, να έχει θέληση για ανάπτυξη και να επιδιώκει τις γνώσεις της στις επιστήμες.

Σήμερα, δυο δεκαετίες από την δημιουργία της Ελληνικής Hacking Σκηνής, έχει διαμορφώσει μια ιδεολογία την οποια προσπαθεί να βελτιώνει συνεχώς και να την κάνει καλύτερη.

Έχοντας υπόψιν τον κίνδυνο που μπορούν να προκαλέσουν οι εταιρίες, έναντι της Ελευθερίας και της εξέλιξης, η Σκηνή ετοιμάζει ένα παγκόσμιο κίνημα βασισμένο στην αλήθεια, ένα κίνημα που να μπορεί να κινηθεί διαχρονικά και να επιφέρει αν όχι μια ανατροπή, ίσως μια μελλοντική μετάβαση, διά μέσω των ανθρώπων που θα κυβερνήσουν στο μέλλον, γίαυτό είναι και σημαντική η παιδεία και τα συστήματα στα οποια μπορεί να υπάρξει έδαφος για την ελεύθερη παιδεία.

Στο μέλλον, η Greek Hacking Scene θα δώσει ιδιαίτερη προσοχή σε τεχνολογική ανάπτυξη, σε πρακτικό επίπεδο εφόσον υπάρχει η δυνατότητα. Θεωρεί ανάγκη να έχει δικά της ανεξάρτητα μέσα τηλεπικοινωνιών, και ως προς αυτή την πορεία κατευθύνεται. Η περίοδος της συλλογής πληροφοριών και τεχνογνωσίας έχει εξυπηρέτηση πολύ σε θεωρητικό επίπεδο, και ίσως θα μπορούσε να περάσει και στην πράξει. Η Greek Hacking Scene δεν διαθέτη οικονομικούς πόρους, και είναι φυσιολογικό να κινείται με αργούς ρυθμούς, κυρίως σε τέτοια θέματα, καθώς βασίζεται στις δυνατότητες των μελών της και στο χρόνο που μπορεί να διαθέσει ο καθένας από τον ελεύθερο του χρόνου για τις διαφορες δραστηριότητες. Πολλές από τις δραστηριότητες τυχαίνει να είναι και οι ασχολίες πολλών μελών στον ελεύθερο τους χρόνο. Όλα αυτά βασίζονται στην πιστη, εμπιστοσύνη και αγάπη των μελών για έναν καλύτερο κόσμο. Κάποια από τα μέλη ασχολούνται με την ρομποτική, συστήματα τηλεπικοινωνιών και εντοπισμού θέσεις, αλλα μέλη συμμετέχουν σε μετρήσεις με μετεωρολογικά μπαλόνια και άλλοι στέλνουν τα δικά τους. Η τεχνολογία είναι από τις πιο αγαπημένες ασχολίες όλων.

Το Hacking στο μέλλον θα έρθει σε απόλυτη σύγκρουση με την υπερβολική ανάπτυξη της τεχνολογίας, την μείωση των ελευθεριων και τον πλήρη έλεγχο και εξάρτηση του πληθυσμού από την τεχνολογία. Τότε, μονο ανεξάρτητες, οργανωμένες και ελεύθερες φωνές θα μπορέσουν να έρθουν σε αντιπαράθεση με αυτές τις εξελίξεις. Θα είναι μια σύντομη η μακράν σύγκρουση, ας ευχηθούμε όλοι να έχει καλο αποτέλεσμα.»

ΠΑΡΑΡΤΗΜΑ V: ΣΥΝΟΔΕΥΤΙΚΗ ΚΑΙ ΕΝΗΜΕΡΩΤΙΚΗ ΕΠΙΣΤΟΛΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ

Ως εισαγωγικό κείμενο κάθε ερωτηματολογίου χρησιμοποιήθηκε συνοδευτική επιστολή της οποίας το κείμενο έχει ως εξής:

«*Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών*

Σχολή Νομικών, Οικονομικών και Πολιτικών Επιστημών

Τμήμα Νομικής

Τομέας Ποινικών Επιστημών

υπ. Διδάκτωρ: Φώτιος Χ. Σπυρόπουλος

επιβλέπων Καθηγητής: Νέστωρ Ευαγ. Κουράκης

θέμα διδακτορικής διατριβής:

«Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα»

Το ερωτηματολόγιο που ακολουθεί αποτελεί τμήμα της διδακτορικής μου διατριβής με θέμα «Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα». Η συμμετοχή σας στην έρευνα θα συνδράμει στην πληρέστερη κατανόηση και τη διατύπωση σύγχρονων και βάσιμων επιστημονικών απόψεων αναφορικά με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα ειδικότερα, το φαινόμενο του hacking γενικότερα και τον σχετικό ρόλο της ποινικής νομοθεσίας.

Οι απαντήσεις θα χρησιμοποιηθούν μόνο για την εκπόνηση της διδακτορικής διατριβής και για ακαδημαϊκούς λόγους και καλύπτονται από πλήρη εχεμύθεια. Πρόσβαση στο υλικό θα έχει μόνο η ερευνητική ομάδα. Θα διατηρηθεί απολύτως η ανωνυμία των

συμμετεχόντων. Επίσης, η συμμετοχή σας είναι εθελοντική και παρακαλείστε να συμμετάσχετε μόνο μία φορά.

Με την «Υποβολή» πλήρως συμπληρωμένου ερωτηματολογίου αναγνωρίζετε ότι όλα τα ανωτέρω ισχύουν και ότι έχετε ενημερωθεί επαρκέστατα για αυτά. Σε περίπτωση απορίας σας αναφορικά με την έρευνα ή προβλήματος που προέκυψε σε εσάς από τη συμμετοχή σας σε αυτήν παρακαλώ επικοινωνήστε με τον επιβλέποντα της παρούσας διδακτορικής διατριβής Καθηγητή Νέστορα Κουράκη στο e-mail: nestor-courakis@jurisconsultus.gr.

Οι ερωτήσεις είναι ανοικτού τύπου ή πολλαπλής επιλογής και η συμπλήρωση του ερωτηματολογίου απαιτεί περίπου 15 λεπτά. Η απάντηση σε κάθε ερώτηση ανοικτού τύπου παρακαλώ να μην ξεπερνά τις εκατό (100) λέξεις.

Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο - ΕΚΤ) και από εθνικούς πόρους μέσω του "Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (ΕΣΠΑ) – Ερευνητικό Χρηματοδοτούμενο Έργο: Ηράκλειτος ΙΙ. Επένδυση στην κοινωνία της γνώσης μέσω του Ευρωπαϊκού Κοινωνικού Ταμείου".

Σας ευχαριστώ για τη συμμετοχή σας!

υπ. Δρ. Φώτης Σπυρόπουλος».

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ

Ελληνόγλωσση βιβλιογραφία και αρθρογραφία

Αγγελής, Ιωάννης «**Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης**», ΠοινΔικ 8-9/2005, σελ. 1062 επ.

Αγγελής, Ιωάννης, «**Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο**», ΠοινΔικ 12/2001, σελ. 1218 επ.

Αγγελής, Ιωάννης, «**Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο**», ΠοινΔικ 12/2001, 1293 επ.

Αγγελής, Ιωάννης, «**Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο**», ΠοινΧρ Ν/2000, σελ. 675 επ.

Αγγελόπουλος, Δημήτριος & *Πάσχος, Ιωάννης*, «**Κατάσχεση – ανάλυση ψηφιακών πειστηρίων**», ΠοινΔικ 4/2003, σελ. 438 επ.

Αλεξανδροπούλου – Αιγυπτιάδου, Ευγενία, «**Η νομική προστασία των προσωπικών δεδομένων κατά την πλοήγηση των ανηλίκων στο Διαδίκτυο»,** εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 141 επ.

Αλεξανδροπούλου – Αιγυπτιάδου, Ευγενία, «**Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών (Η ελληνική νομική ρύθμιση ενόψει και του πρόσφατου Ν. 3674/2008)**», ΔιΜΜΕ 4/2008, σελ. 446 επ.

Αλεξιάδης, Στέργιος, **Εγκληματολογία**, εκδ. Π. Ν. Σάκκουλα, 5η εκδ. Θεσσαλονίκη, 2011.

Αναστασιάδου, Σοφία, **Στατιστική και Μεθοδολογία έρευνας στις κοινωνικές επιστήμες**, εκδ. Κριτική, Αθήνα, 2012.

Αναστασόπουλος, Δημήτριος, «**Η προστασία της ιδιωτικότητας κατά το άρθρο 8 της ΕΣΔΑ στο ψηφιακό περιβάλλον**», ΔιΜΜΕ 3/2012, σελ. 325 επ.

Ανδρέου, Φίλιππος, **Ποινικός Κώδικας, κατ' άρθρο Ερμηνεία - Νομολογία - Βιβλιογραφία,** 4η έκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.

Ανδρουλάκης, Νικόλαος, **Ποινικό Δίκαιο – Γενικό Μέρος, Θεωρία για το έγκλημα**, **τομ. Α'**, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000.

Ανδρουλάκης, Νικόλαος, **Θεμελιώδεις έννοιες της ποινικής δίκης**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1994, σελ. 48 επ.

Αργυρόπουλος, Ανδρέας, **Ηλεκτρονική εγκληματικότητα**, σειρά Εγκληματολογικά, αρ. 19, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2001.

Αρμαμέντος, Παναγιώτης & Σωτηρόπουλος, Βασίλειος, **Προσωπικά δεδομένα – Ερμηνεία Ν. 2472/1997**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2005.

Αρτινοπούλου, Βάσω, **Επανορθωτική δικαιοσύνη: η πρόκληση των σύγχρονων δικαιικών συστημάτων**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2010.

Αρχιμανδρίτου, Μαρία, **Η διαχρονική εξέλιξη της προσέγγισης της ετικέτας**, εκδ. Σάκκουλα, Θεσσαλονίκη, 1996.

Απρογέρακας, Δημήτριος, «**Ποινική προστασία προγραμμάτων Η/Υ**», Πρακτικά ημερίδας για την «Πειρατεία Λογισμικού: Οικονομικές και Νομικές Επιπτώσεις», ΑΣΟΕΕ, 24.05.1999, σελ. 33-41.

Βαρλάμος, Ευάγγελος, «**Ασφάλεια Δεδομένων Ηλεκτρονικών Υπολογιστών**», Στρατιωτική Επιθεώρηση, Σεπτέμβριος – Οκτώβριος 2006, σελ. 116 επ.

*Βασιλάκη, Ειρήνη,***«Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών»**, σειρά Ποινικά, αρ. 40, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1993.

*Βασιλάκη, Ειρήνη,***«Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής τους καταστολής: Προετοιμάζοντας το Ποινικό Δίκαιο του 21ου αιώνα;»**, εις: *Ν. Κουράκη (εκδ. επιμ.)*, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2000 σελ. 23 επ.

Βιδάλη, Σοφία, **Αντεγκληματική πολιτική: από τη μικροεγκληματικότητα έως το οργανωμένο έγκλημα**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013.

Βλάχου, Βίκυ, «**Εγκληματολογική έρευνα: προκλήσεις, δυσχέρειες, προοπτικές»**, εις: *Ν. Κουράκη, Χρ. Ζαραφωνίτου, Χρ. Τσουραμάνη, Ε. Χαϊνά (επιστ. επιμ.)*, Εγκληματολογία: Διδασκαλία και Έρευνα στην Ελλάδα, Πρακτικά Επιστημονικού Συνεδρίου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2011, σελ. 69-80.

Βλάχου, Βίκυ, «**Η ιστορική προσέγγιση της εγκληματικής προσωπικότητας υπό το πρίσμα της αριστοτέλειας "συλλογιστικής": Η μετουσίωση της αρχαιοελληνικής εγκληματολογικής σκέψης στη σύγχρονη κοινωνία**», Εγκληματολογία, τευχ. 1, 2011, εκδ. Νομική Βιβλιοθήκη, σελ. 112-115.

Βολονάσης, Ηλίας, **«Ποινική προστασία προγραμμάτων Η/Υ»**, Πρακτικά ημερίδας της Ένωσης Δικαστών και Εισαγγελέων για την «Προστασία προγραμμάτων ηλεκτρονικών υπολογιστών», ΑΣΟΕΕ, 19.02.1999, σελ. 29-35.

Βουγιούκας, Κωνσταντίνος, **«Οι ανήλικοι ως δράστες εγκλημάτων και ως θύματα εγκληματικών πράξεων στους χώρους της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης και του Οργανισμού Ηνωμένων Εθνών. Οι συμβάσεις για τα δικαιώματα του παιδιού του Συμβουλίου της Ευρώπης και του Ο.Η.Ε.»**, εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. ΙΙ, σελ. 1487 επ.

Γαλανού, Μαρία, «**Ζητήματα ερμηνείας του δικαιώματος στην προσωπική ελευθερία και ασφάλεια στο κείμενο της ΕΣΔΑ**», εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 137 επ.

Γαλανού, Μαρία, «**Περί της οικονομικής ανάλυσης του συστήματος της ποινικής δικαιοσύνης**», ΠοινΔικ 1/2008, σελ. 76 επ.

Γεωργάτος, Γεράσιμος, **Ο θεσμός της έμπρακτης μετάνοιας και η δικαστηριακή πρακτική σε σχέση με αυτόν,** ΠΕΙΡΝ 2002/5, σελ. 5-8.

Γεωργούλας, Στράτος, **Η εγκληματολογία στην Ελλάδα σήμερα – Τιμητικός τόμος για τον Στέργιο Αλεξιάδη**, εκδ. ΚΨΜ, Αθήνα, 2007.

Γεωργούλας, Στράτος, «**Η παραβατικότητα ανηλίκων ως προβληματική κατάσταση**», ΠοινΔικ 8-9/2003, σελ. 986 επ.

Γιαννόπουλος, Γεώργιος, **Η ευθύνη των παρόχων υπηρεσιών στο internet**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2013.

Γιοβάνογλου, Σοφία, «**Η ενσωμάτωση της αποκαταστατικής δικαιοσύνης στα διεθνή κείμενα αντεγκληματικής πολιτικής για τους ανηλίκους**», ΠοινΔικ 11/2006, σελ. 1310 επ.

Γιωτοπούλου-Μαραγκοπούλου, Αλίκη, **Εγχειρίδιο Εγκληματολογίας**, μέρος Α', εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1984.

Γκρόζος, Κώστας, Σ., **Το άρθρο 379 ΠΚ μετά την τροποποίησή του με το άρθ. 14 παρ. 13 του ν. 2721/99**, Υπεράσπιση, 2000, σελ. 521 επ.

Δαγτόγλου, Πρόδρομος, **Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα, τομ. Α' και Β'**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, 2002.

Δασκαλάκης, Ηλίας, **Η εγκληματολογία της κοινωνικής αντίδρασης**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, 1985.

Δεληγιάννη, Έλσα, «**Πνευματική ιδιοκτησία και επικοινωνία την εποχή του διαδικτύου: νομικό πλαίσιο και προοπτικές για την διαδικτυακή ανταλλαγή μουσικών αρχείων**», ΔιΜΕΕ 4/2007, σελ. 480 επ.

Δελημάρης, Ιωάννης & Πιπεράκης, Στέλιος, «**Βιολογική θεώρηση της υπερβολικής χρήσης του Διαδικτύου σε παιδιά και εφήβους**», εις: *Κ. Σιώμου & Γ. Φλώρου (εκδ. επιμ.),* Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση

του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 219-222.

Δημητράτος, Νίκος, «**Ποινικό δίκαιο και κράτος δικαίου στη σύγχρονη εποχή**», ΠοινΔικ 5/2004, σελ. 598-599.

Δρόσος, Ιωάννης, «**Δημόσια τάξη και δημόσια ασφάλεια**», Επιθεώρησις Δημοσίου Δικαίου και Διοικητικού Δικαίου, τομ. 35, τ. Απρίλιος – Ιούνιος 1991, Αθήνα, σελ. 183-218.

Ζάννη, Αναστασία, **Το διαδικτυακό έγκλημα**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2005.

Ζαραφωνίτου, Χριστίνα, **(Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου,** Αθήνα-Κομοτηνή, εκδ. Αντ. Ν. Σάκκουλα, 2007.

Ζαραφωνίτου, Χριστίνα, «**Ανασφάλεια και επέκταση του κοινωνικού ελέγχου: Ποινικοποίηση των "αντικοινωνικοτήτων" και της "αταξίας"**», Ποινικός Λόγος, τεύχος 4, 2004, σελ. 2049-2059.

Ζαραφωνίτου, Χριστίνα, **Εμπειρική εγκληματολογία**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004.

Ζαραφωνίτου, Χριστίνα, **Πρόληψη της εγκληματικότητας σε τοπικό επίπεδο**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003.

Ζαραφωνίτου, Χριστίνα, **Ο φόβος του εγκλήματος, Εγκληματολογικές προσεγγίσεις και προβληματισμοί με βάση την εμπειρική διερεύνηση του φαινομένου στο εσωτερικό της Αθήνας**, Μελέτες Ευρωπαϊκής Νομικής Επιστήμης, τ. 3 εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2002.

Ιγγλεζάκης, Ιωάννης, **Δίκαιο της πληροφορικής**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, β' έκδοση, 2008.

Ιγγλεζάκης, Ιωάννης, **Ευαίσθητα προσωπικά δεδομένα**, εκδ. Π. Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2003.

Ιωσηφίδης, Θεόδωρος, **Ποσοτικές μέθοδοι έρευνας στις κοινωνικές επιστήμες**, εκδ. Κριτική, Αθήνα, 2008.

Καϊάφα – Γκμπάντι, Μαρία, **Ευρωπαϊκό ποινικό δίκαιο και Συνθήκη της Λισσαβώνας**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2011.

Καϊάφα-Γκμπάντι, Μαρία, «**Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη**», ΠοινΧρ ΞΑ/2011, σελ. 489-500.

Καϊάφα-Γκμπάντι, Μαρία, «**Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής**», Αρμενόπουλος 2007, σελ. 1058-1087.

Καϊάφα-Γκμπάντι, Μαρία, «**Προς μία νέα οριοθέτηση του αξιοποίνου του οργανωμένου εγκλήματος στην Ε.Ε. – Η σημασία της για την εθνική μας έννομη τάξη**», ΠοινΔικ 12/2005, σελ. 1435-1446.

Καϊάφα–Γκμπάντι, Μαρία, **«Συντονιστικά όργανα για την καταπολέμηση του οργανωμένου εγκλήματος στην ΕΕ: Από τον αστυνομικό (Europol) στον δικαστικό (Eurojust) συντονισμό – Η προοπτική της προστασίας των θεμελιωδών δικαιωμάτων»**, ΠοινΔικ 2/2003, σελ. 165 επ.

Καλλινίκου, Διονυσία,ν**Πνευματική ιδιοκτησία και συγγενικά δικαιώματα**, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000.

Κανελλοπούλου – Μπότη, Μαρία, **Νομική προστασία βάσεων δεδομένων**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004.

Καράκωστας, Ιωάννης, **Δίκαιο και Internet. Νομικά ζητήματα του Διαδικτύου**, εκδ. Δίκαιο & Οικονομία Π. Ν. Σάκκουλα, 3η έκδοση, Αθήνα, 2009.

Καρανικόλας, Σπυρίδων, **Η επίδραση του ευρωπαϊκού ποινικού δικαίου στην ελληνική ποινική έννομη τάξη**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2012.

Καρράς, Αργύριος, **Ποινικό Δικονομικό Δίκαιο**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1998, σελ. 306 επ.

Κατσής, Αθανάσιος & Σιδερίδης, Γεώργιος & Εμβαλωτής, Αναστάσιος, **Στατιστικές μέθοδοι στις κοινωνικές επιστήμες**, εκδ. Τόπος, Αθήνα, 2010.

Κιούπης, Δημήτριος & Παπαδοπούλου, Ρεβέκκα – Εμμανουέλα & Μουζάκης, Διονύσιος, **Το Ποινικό Δίκαιο μετά τη συνθήκη της Λισαβόνας**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011.

Κιούπης, Δημήτριος, «**Ηλεκτρονικά οικονομικά εγκλήματα»,** εις: *Ν. Κουράκης (εκδ. επιμ.)*, Τα οικονομικά εγκλήματα, τομος ΙΙ, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 2007, σελ. 405 επ.

Κιούπης, Δημήτριος, «**Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας**», Υπεράσπιση, 2000, σελ. 959-972.

Κιούπης, Δημήτριος, **Ποινικό Δίκαιο και Internet,** σειρά Ποινικά αρ. 57**,** εκδ. Αντ. Σάκκουλα, Αθήνα – Κομοτηνή, 1999.

Κιούπης, Δημήτριος, «**Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet**», ΠοινΧρ ΜΗ, 1998, σελ. 712 επ.

Κίτσιου, Αγγελική & Κουρούτζας, Χρήστος, «**Μελετώντας το ηλεκτρονικό έγκλημα στο πλαίσιο της κοινωνίας της πληροφορίας**. **Πιλοτική έρευνα αναπαραστάσεων σε φορείς του νομού Λέσβου**», εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τομ. Ι., σελ. 317 επ.

Κονταξής, Αθανάσιος, **Ποινικός Κώδικας [Συνδυασμός θεωρίας και πράξης]**, Τόμος Β', εκδ. Π. Ν. Σάκκουλα, γ' έκδοση, Αθήνα, 2000.

Κοτσαλής, Λεωνίδας, **Ποινικό Δίκαιο – Γενικό Μέρος**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.

Κοτσαλής, Λεωνίδας, «**Ποινική δογματική και αντεγκληματική πολιτική: σχέση τριβής;**», εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη

Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. Ι, σελ. 645 επ.

Κοτσαλής, Λεωνίδας & Τριανταφύλλου, Γεώργιος, **Ανθρώπινα δικαιώματα και ποινικό δίκαιο**, σειρά Ποινικά αρ. 75, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2007.

Κουράκης, Νέστωρ, **Δίκαιο παραβατικών ανηλίκων**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, β' εκδ., 2012.

Κουράκης, Νέστωρ, «**Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της**», ΠοινΧρ ΝΘ/2009, σελ. 865-871.

Κουράκης, Νέστωρ, **Ποινική Καταστολή**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2009.

Κουράκης, Νέστωρ, «**Ασφάλεια και ελευθερία – Τα μεταξύ τους στατικά και δυναμικά όρια**», εις: *Χ. Ζαραφωνίτου, (επιμ.)*, (Αν)ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του ανθρώπου, σειρά Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών αρ. 7, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2007, σελ. 7 επ.

Κουράκης, Νέστωρ, **Ποινική Καταστολή**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.

Κουράκης, Νέστωρ, **Εγκληματολογικοί Ορίζοντες**, **τομος Α': Ιστορική και θεωρητική προσέγγιση**, εκδ. Αντ. Ν. Σάκκουλα, Δεύτερη Ανανεωμένη Έκδοση, Αθήνα, 2005.

Κουράκης, Νέστωρ, **Εγκληματολογικοί Ορίζοντες, τόμος Β΄: Πραγματολογική προσέγγιση και επιμέρους ζητήματα**, εκδ. Αντ. Ν. Σάκκουλα, Δεύτερη Ανανεωμένη Έκδοση, Αθήνα, 2005.

Κουράκης, Νέστωρ, **Εισαγωγή στη θεωρία της ποινής**, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2000.

Κουράκης, Νέστωρ, «**Η πρόληψη της παραβατικότητας των ανηλίκων στην Ελλάδα**», εις: *Αγ. Τσήτσουρα (υπεύθυνη έκδοσης)*: Αντεγκληματική πολιτική και

δικαιώματα του Ανθρώπου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997, σελ. 63 επ.

Κουράκης, Νέστωρ, Ζαραφωνίτου, Χριστίνα, Τσουραμάνης, Χρήστος & Χαϊνάς, Ευάγγελος (εκδ. επιμ.), **Εγκληματολογία: Διδασκαλία και έρευνα στην Ελλάδα – Πρακτικά Επιστημονικού Συνεδρίου, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών Νομικής Αθηνών,** τόμος υπ' αρ. 22, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2011.

Κουράκης, Νέστωρ, Ζαγούρα, Παρασκευή & Γαλανού, Μαρία, «**Συμμορίες ανηλίκων στην Ελλάδα – Πορίσματα από τις αποφάσεις του Δικαστηρίου Ανηλίκων Αθηνών**», Ποινικός Λόγος 5/2003, σελ. 2205 – 2218.

Κορομηλάς, Ηλίας,«**Sensibilis modus operandi (?) – Οπτικός πολιτισμός και σύγχρονη εγκληματικότητα»,** εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τομ. Ι, σελ. 359 επ.

Κοφίνης, Στέργιος, Γ., «**Η συμμετοχή στην κοινωνία της πληροφορίας ως ένα νέο συνταγματικό δικαίωμα (ά. 5Α παρ. 2 Σ)**», ΔιΜΜΕ 2007. σελ. 515-522.

Κρανιδιώτη, Μαρία, **Η ολοκλήρωση – Μέθοδος ανάπτυξης θεωρίας στην εγκληματολογία**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2007.

Κυριαζή, Νότα, **Η κοινωνιολογική έρευνα: Κριτική επισκόπηση των μεθόδων και τεχνικών**, εκδ. Ελληνικά Γράμματα, Αθήνα, 2005.

Κωνσταντινίδης, Άγγελος, «**Παρατηρήσεις στην απόφαση ΑΠ 121/2003**», ΠοινΧρ ΝΓ/2003, σελ. 910 επ.

Κωστάρας, Αλέξανδρος, **Ποινικός Κώδικας και Ειδικοί Ποινικοί Νόμοι,** εκδ. Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, 2008.

Λαζαράκος, Γρηγόριος, «**Βιομετρία: Προστασία των προσωπικών δεδομένων μέσω της επεξεργασίας ευαισθήτων (σωματικών) πληροφοριών**», ΠοινΔικ 11/2001, σελ. 1165 επ.

Λάζος, Γρηγόρης, **Κριτική Εγκληματολογία**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2007.

Λάζος, Γρηγόρης, **Πληροφορική και έγκλημα**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2001.

*Λάζος, Γρηγόρης,*μ**Το πρόβλημα της ποιοτικής έρευνας στις κοινωνικές επιστήμες – θεωρία και πράξη**, εκδ. Παπαζήση, Αθήνα, 1998.

Λαμπίρη – Δημάκη, Ιωάννα, **Η Κοινωνιολογία και η Μεθοδολογία της**, Τόμος Α', Έβδομη συμπληρωμένη έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2003.

Λαμπίρη – Δημάκη, Ιωάννα, **Κοινωνικές έρευνες με στατιστικές μεθόδους**, εκδ. Αντ. Ν. Σάκκουλα, 1995.

Λαμπροπούλου, Έφη, **Κοινωνιολογία του ποινικού δικαίου και των θεσμών της ποινικής δικαιοσύνης**, εκδ. Ι. Σιδέρης, Αθήνα, 2012.

Λαμπροπούλου, Έφη, «**Κοινωνίες σε "κίνδυνο" και αίσθημα ανασφάλειας**», ΠοινΔικ 5/2002, σελ. 556 επ.

Λαμπροπούλου, Έφη, **Η κατασκευή της κοινωνικής πραγματικότητας και τα μέσα μαζικής επικοινωνίας: η περίπτωση της βίας και της εγκληματικότητας**, εκδ. Ελληνικά γράμματα, Αθήνα, 1999.

Λέανδρος, Νίκος, **Το Διαδίκτυο – Ανάπτυξη και αλλαγή**, εκδ. Καστανιώτη, Αθήνα, 2004.

Λίβος, Νικόλαος, «**Το πρόβλημα της ασφάλειας και η ασφάλεια ως πρόβλημα: Το παράδειγμα του ποινικού δικαίου**», εις: Τιμητικός Τόμος για τον Ιωάννη Μανωλεδάκη, εκδ. Π. Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2005, σελ. 185-207.

Λίβος, Νικόλαος, «**Η απαλλαγή από την ποινή επί ικανοποιήσεως του ζημιωθέντος μέχρι εκδόσεως της οριστικής αποφάσεως (Σκέψεις για την ποινική συνδιαλλαγή και την αποκατάσταση του θύματος στο ισχύον Ποινικό δίκαιο)»,** ΠοινΧρ 2000, σελ. 289 επ.

Λυδάκη, Άννα, **Ποιοτικές μέθοδοι της κοινωνικής έρευνας, εκδ. Καστανιώτη**, Αθήνα, 2001.

Μαγγανάς, Αντώνιος, **Το εγκληματικό φαινόμενο στην πράξη**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2004.

Μαγγανάς, Αντώνιος (εκδ. επιμ.), **Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου**, τομ. Ι και ΙΙ, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003.

Μαγγανάς, Αντώνιος, «**Η ιδιωτική ασφάλεια. Προβληματισμοί και επισημάνσεις**», ΠοινΔικ, 2001, σελ. 274-84.

Μαγγανάς, Αντώνιος, «**Το πρόβλημα της αποτίμησης του κινδύνου τέλεσης νέων εγκληματικών πράξεων**», ΠοινΔικ, 1999, σελ. 1008-1016.

Μαγγανάς, Αντώνιος, «**Οι δύο όψεις του κοινωνικού ελέγχου: καταστολή και εναλλακτικά μέτρα**», εις: *Αγ. Τσήτσουρα (υπεύθυνη έκδοσης)*: Αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997, σελ. 121 επ.

Μαγγανάς, Αντώνιος & Ζάννη, Μαρία & Παπαμιχαήλ, Στέλλα & Λάζος, Γρηγόριος, «**Εγκλήματα, ποινές και ελληνική κοινή γνώμη**», ΠοινΔικ 8-9/2002, σελ. 943 επ.

Μαλακάσης, Δημήτριος, **Η πνευματική ιδιοκτησία**, 2η εκδ. Αθήνα, 2002.

Μανωλεδάκης, Ιωάννης, **Ερμηνεία κατ' άρθρο των όρων του Ειδικού μέρους του Ποινικού Κώδικα**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 1996.

Μαργαρίτης, Μιχαήλ, **Ποινικός Κώδικας – Ερμηνεία και Εφαρμογή,** εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2003.

Μαρίνος, Μιχαήλ – Θεόδωρος, **Λογισμικό (software). Νομική προστασία και συμβάσεις**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1992.

Μαρίνος, Τάσος, **Οι ηλεκτρονικοί υπολογιστές και το Δίκαιο**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1991.

Μεταξάκης, Εμμανουήλ, «**Η ποινική προστασία της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος χρήστη, του κωδικού πρόσβασης και της διεύθυνσης διαδικτυακού πρωτοκόλλου**», ΠοινΧρ ΞΔ/ 2014, σελ. 8 επ.

Μηλιώνη, Φωτεινή, «**Το "φύλο" ως ιδιαίτερη παράμετρος στην εγκληματολογική έρευνα**», εις: *Αγγ. Πιτσελά (επιμ.),* Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 587-594.

Μήτρου, Λίλιαν, **Το δίκαιο στην κοινωνία της πληροφορίας,** εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002.

Μοσχοπούλου, Αλεξάνδρα, **Η εγκληματικότητα των Μεταναστών – Απεικόνιση του φαινομένου στον απογευματινό τύπο 1990-1999**, σειρά Ποινικά αρ. 69, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.

Μπόση, Μαίρη, **Ζητήματα Ασφάλειας στη Νέα Τάξη Πραγμάτων**, εκδ. Παπαζήση, Αθήνα, 1999.

Μυλωνόπουλος, Χρήστος, «**Το Ευρωπαϊκό Ποινικό Δίκαιο μετά τη Συνθήκη της Λισαβόνας**», ΠοινΧρ 2011, σελ. 81 επ.

Μυλωνόπουλος, Χρήστος, «**Κοινοτικό ποινικό δίκαιο και γενικές αρχές κοινοτικού δικαίου**», ΠοινΧρ 2011, σελ. 1 επ.

*Μυλωνόπουλος, Χρήστος, «***Ο ποινικός κώδικας ανάμεσα στο παρόν και στο μέλλον**», ΠοινΛογος 1/2002, σελ. 5-10.

Μυλωνόπουλος, Χρήστος, **Ποινικό Δίκαιο - Ειδικό μέρος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας**, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2001.

Μυλωνόπουλος, Χρήστος, **Εφαρμογές Ποινικού Δικαίου**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνη, 1997.

Μυλωνόπουλος, Χρήστος, **Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα, 1989.

Νικολόπουλος, Γεώργιος, **Η Ευρωπαϊκή Ένωση ως φορέας αντεγκληματικής πολιτικής**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2008.

Νικολόπουλος, Γεώργιος, **«"Ελευθερία, Ασφάλεια, Δικαιοσύνη": Οι προβληματικές οριοθετήσεις του Ευρωπαϊκού Κοινωνικού Ελέγχου»**, εις: *Χ. Ζαραφωνίτου (επιμ.)*, (Αν)Ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, υπ' αρ. 7 σειράς εκδόσεων Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2007, σελ. 73 επ.

Νικολούδης, Ηλίας, **ΑΡΙΣΤΟΤΕΛΗΣ – Άπαντα**, τομ. 25ος, Όργανον 3, ΤΟΠΙΚΩΝ Z, H, θ – Περί των σοφιστικών ελέγχων, Αρχαία ελληνική γραμματεία – οι Έλληνες, Νο 214, εκδ. Κάκτος.

Νούσκαλης, Γεώργιος, «**Η επεξεργασία των εξωτερικών τηλεπικοινωνιακών δεδομένων θέσης και κίνησης ως ανακριτική πράξη έρευνας κατά το Ν. 3917/2011»**, ΠοινΧρ ΞΒ/ 2012, σελ 246 επ.

Νούσκαλης, Γεώργιος, «**Απάτη με Ηλεκτρονικό Υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και της Ευρωπαϊκής Ένωσης»**, ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 178 επ.

Πανούσης, Ιωάννης, **«Ανασφάλεια – Το "σκιάχτρο" της παγκοσμιοποίησης»**, ΠοινΔικ 10/2004, σελ. 1153 επ.

Πανούσης, Ιωάννης, **«Ο εικονοποιημένος εγκληματίας. Ηλεκτρονικές απεικονίσεις και ψηφιακές διακαιικές κρίσεις»**, εις: *Ρ. Παναγιωτοπούλου (επιμ.)*, Η ψηφιακή πρόκληση: ΜΜΕ και Δημοκρατία, εκδ. Δαρδανός, Αθήνα, 2003.

Πανούσης, Ιωάννης, **Εγκληματολογία, εγκληματολογική έρευνα και ΜΜΕ**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1999.

Παπαδόπουλος, Μαρίνος, «**Wardriving, Warchalking & Wireless Hacking**», 2ο εθνικό συνέδριο με διεθνή συμμετοχή, ΕΒΕΑ, 16-17 Μαρτίου 2006, «Ηλεκτρονική Δημοκρατία, Προκλήσεις της ψηφιακής εποχής».

Παπαδοπούλου, Δέσποινα, **«Η νομική προστασία του δικαιώματος για ελεύθερη επικοινωνία»**, ΠοινΔικ 2/2009, σελ. 210 επ.

Παπαθανασόπουλος, Ευστράτιος, «**Διοικητισμός και ποινικότητα**», εις: *Αγγ. Πιτσελά (επιμ.)*, Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 723 επ.

Παπαθεοδώρου, Θεόδωρος, «**Κυβερνητική της Ασφάλειας και Αντεγκληματική πολιτική: η ποινική διαχείριση των δικαιωμάτων**», εις: *Χ. Ζαραφωνίτου (επιμ.)*, (Αν)Ασφάλεια, αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου, υπ' αρ. 7 σειράς εκδόσεων Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 2007, σελ. 59 επ.

Παπαθεοδώρου, Θεόδωρος, **Δημόσια ασφάλεια και αντεγκληματική πολιτική – συγκριτική προσέγγιση**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2002.

Παπαθεοδώρου, Θεόδωρος, **«Δικαιοσύνη ενηλίκων και ανήλικοι δράστες: Τα έσχατα όρια της "μηδενικής ανοχής" στις ΗΠΑ»**, ΠοινΔικ 1/2000, σελ. 77 επ.

Παπακωνσταντίνου, Απ., «**Το συνταγματικό δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας**», ΕΔΔΔ, 2006, σελ. 233 επ.

Παπανεοφύτου, Αγάπιος, «**Ποινική ευθύνη των νομικών προσώπων ή των υπολόγων για τη δράση τους φυσικών προσώπων**;», εις Ποινικό Δίκαιο-Ελευθερία-Κράτος Δικαίου, Τιμητικός Τόμος για τον Γ. Α. Μαγκάκη, εκδ. Αντ. Ν. Σάκκουλα, 1996, σελ. 195-223.

Παπάνης, Ευστράτιος, **Μεθοδολογία έρευνας και διαδίκτυο**, εκδ. Ι. Σιδέρης, β' εκδ., Αθήνα, 2012.

Παππάς, Θεόδωρος, **Η μεθοδολογία της επιστημονικής έρευνας στις ανθρωπιστικές επιστήμες**, εκδ. Καρδαμίτσα, Αθήνα, 2002.

Παύλου, Στέφανος, «**Ένας φαύλος κύκλος χωρίς τέλος: Οι τροποποιήσεις του ΠΚ (για την επιτάχυνση της δικαιοσύνης και την αποσυμφόρηση των φυλακών)**», ΠοινΔικ 10/2012, σελ. 921 επ.

Παύλου, Στέφανος, **Αποφάσεις - Πλαίσια/ Διεθνή και Ευρωπαϊκά Κείμενα Ποινικού Δικαίου**, εκδ. Δίκαιο και Οικονομία Π. Ν. Σάκκουλας, Αθήνα, 2005.

Πιτσελά, Αγγελική, **Η ποινική αντιμετώπιση της εγκληματικότητας των ανηλίκων**, εκδ. Π. Ν. Σάκκουλα, ζ' εκδ., Αθήνα-Θεσσαλονίκη, 2013.

Πιτσελά, Αγγελική (επιμ.), **Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη**, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010.

Σάμιος, Θωμάς, **Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο – Η de lege lata αξιολόγηση της αθέμιτης κτήσης και χρήσης καρτών αυτόματης συναλλαγής για ανάληψη μετρητών από ΑΤΜ**, Ποινικές Μελέτες, Τομέας Ποινικών και Εγκληματολογικών Επιστημών ΔΠΘ, εκδ. Π. Ν. Σάκκουλα, 2010.

Σιδηρόπουλος, Θεόδωρος, **Το Δίκαιο του Διαδικτύου**, εκδ. Π. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, β' έκδ., 2008.

Σιώμος, Κωνσταντίνος, παρουσίαση έρευνας της Ελληνικής Εταιρείας Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο στις 14/01/2014 με θέμα «**Ασφαλής πλοήγηση και κοινωνική δικτύωση στον Ελληνικό Στρατό**».

Σιώμος, Κωνσταντίνος & *Φλώρος, Γεώργιος & συν.* (εκδ. επιμ.), **Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου**, εκδ. Λιβάνης, 2012.

Σιώμος, Κωνσταντίνος & *Φλώρος, Γεώργιος* (εκδ. επιμ.), **Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου**, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011.

Σπινέλλη, Καλλιόπη, **Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις**, 2η εκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.

Σπινέλλη, Καλλιόπη, «**Κρατούμενοι χρήστες ή εξαρτημένοι: προς αναζήτηση των βέλτιστων θεραπευτικών πρακτικών**», σε: Τιμητικό Τόμο για τον Ιωάννη Μανωλεδάκη, Δημοκρατία - Ελευθερία – Ασφάλεια, Αθήνα – Θεσσαλονίκη 2005, σελ. 377-399.

Σπινέλλη, Καλλιόπη, **Προσβολές και προστασία της τρίτης ηλικίας – Εγκληματολογική, κοινωνιολογική και ποινική διερεύνηση του φαινομένου της κακοποίησης και παραμέλησης**, σειρά Ποινικά αρ. 34, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1991.

Σπινέλλη, Καλλιόπη & Κρανιδιώτη, Μαρία, «**Κανόνες δεοντολογίας για τους Έλληνες εγκληματολόγους: Πρόταγμα του 21ου αιώνα; /παράρτημα με σχέδιο κώδικα δεοντολογίας**», εις: Εγκληματολογία και Ευρωπαϊκή Αντεγκληματική Πολιτική, Προσφορά Τιμής στην Αγλαΐα Τσήτσουρα, εκδόσεις Π. Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2009, σελ. 549-589.

Σπυρόπουλος, Φώτιος, «**Digital και cyber bullying και αθέμιτη χρήση ηλεκτρονικών πληροφοριών ως το "bullying" του μέλλοντος – Γνώση και πρόληψη»,** πρακτικά 2ου συνεδρίου Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος ΕΛ.ΑΣ., 2013, σελ. 62 επ.

Σπυρόπουλος, Φώτιος, «**Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας**», εις: *Κ. Σιώμου* και *Γ. Φλώρου* (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

Σταλίκας, Αναστάσιος, **Μέθοδοι έρευνας στην ψυχολογία**, έκδ. Ελληνικά Γράμματα, Αθήνα, 2005.

Σφακιανάκης, Μιχάλης, **Εισαγωγή στην Πληροφορική σκέψη**, εκδ. Κλειδάριθμος, 2003.

Τάκης, Ανδρέας, «**Κοινωνία της Πληροφορίας και Σύνταγμα – μια πρώτη προσέγγιση**», ΝοΒ 2002, σελ. 28-44.

Τσήτσουρα, Αγλαΐα, **«Πρώιμη ψυχοκοινωνική επέμβαση για την πρόληψη της εγκληματικότητας των ανηλίκων»**, εις: *Αγγ. Πιτσελά* (επιμ.), Εγκληματολογικές αναζητήσεις – Τιμητικός Τόμος για τον Καθηγητή Στέργιο Αλεξιάδη, εκδ. Π. Ν. Σάκκκουλα, Αθήνα – Θεσσαλονική, 2010, σελ. 1033 επ.

Τσήτσουρα, Αγλαΐα, **«Εγκληματικότητα και αντεγκληματική πολιτική στην εποχή της παγκοσμιοποίησης»**, εις: *Αντ. Μαγγανά (εκδ. επιμ.)*, Τιμητικός τόμος για την Αλίκη Γιωτοπούλου – Μαραγκοπούλου, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003, τομ. ΙΙ, σελ. 1405 επ.

Τσήτσουρα, Αγλαΐα (υπεύθυνη έκδοσης), **Αντεγκληματική πολιτική και δικαιώματα του Ανθρώπου**, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1997.

Τσίγκανου, Ιωάννα, **Ανάλυση περιεχομένου**, Εθνικό Κέντρο Κοινωνικών Ερευνών.

Τσόλιας, Γρηγόριος, «**Επεξεργασία και προστασία των εξωτερικών στοιχείων της επικοινωνίας και των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών»**, εις: *Λ. Κοτσαλή & Γ. Τριανταφύλλου*, Ανθρώπινα δικαιώματα και ποινικό δίκαιο, σειρά Ποινικά αρ. 75, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2007, σελ. 441 επ.

Τσουραμάνης, Χρήστος, **«Η ψηφιακή (ηλεκτρονική) εγκληματικότητα στο πλαίσιο της "θεωρίας της καθημερινής δραστηριότητας" ("Routine Activity Theory")»**, εις: *Σ. Γεωργούλα*, Η εγκληματολογία στην Ελλάδα σήμερα – Τιμητικός τόμος για τον Στέργιο Αλεξιάδη, εκδ. ΚΨΜ, Αθήνα, 2007, σελ. 155 επ.

Τσουραμάνης, Χρήστος, **Ψηφιακή εγκληματικότητα – Η (αν)ασφαλής όψη του διαδικτύου**, εκδ. Κατσαρού, Αθήνα, 2005.

Τσουραμάνης, Χρήστος, «**Internet και Ποινική Δικαιοσύνη – Ασφάλεια πληροφοριών στο Διαδίκτυο**», ΠοινΔικ 2/2003, σελ. 160.

Τσουραμάνης, Χρήστος, **«Internet και Ποινική Δικαιοσύνη – Προστασία της πνευματικής ιδιοκτησίας στο Internet»**, ΠοινΔικ 11/2002, σελ. 1177.

Τσουραμάνης, Χρήστος, «**Εγκλήματα του κυβερνοχώρου και δικτυακοί τόποι (web sites) που αναφέρονται στην ασφαλεία των Η/Υ»,** ΠοινΔικ 12/2001.

Φαραντούρης, Νικόλαος, «**Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς**», ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 191 επ.

Φαρσεδάκης, Ιάκωβος, **Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011.

Φαρσεδάκης, Ιάκωβος, **Στοιχεία Εγκληματολογίας**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2005.

Φαρσεδάκης, Ιάκωβος, **Ηθική και εγκληματικότητα**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2000.

Φαρσεδάκης, Ιάκωβος, **Η κοινωνική αντίδραση στο έγκλημα και τα όριά της. Μερικές ιστορικές, συγκριτικές και θεωρητικές επισημάνσεις**, εκδ. Νομική Βιβλιοθήκη, Αθήνα 1991.

Φαρσεδάκης, Ιάκωβος & Σατλάνης, Χρήστος, **«Βαθμίδες, κριτήρια και μέθοδοι ερμηνείας και περαιτέρω διάπλασης του Ουσιαστικού Ποινικού Δικαίου»**, ΠοινΔικ 12/2012, σελ. 1118 επ.

Φίλιας, Βασίλειος, **Εισαγωγή στη μεθοδολογία και τις τεχνικές κοινωνικών ερευνών**, 2η εκδ., εκδ. Gutenberg, Αθήνα, 1996.

Χάιδου, Ανθοζωή, **Εγκληματολογικά κείμενα, Διεθνής αντεγκληματική πολιτική. Αποτελεσματικότητα των κυρώσεων και ανθρώπινα δικαιώματα. Ο ρόλος της σύγχρονης τεχνολογίας**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003.

Χάιδου, Ανθοζωή, **Θετικιστική εγκληματολογία. Αιτιολογικές προσεγγίσεις του εγκληματικού φαινομένου**, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996.

*Χάιδου, Ανθοζωή,***Σύγχρονη τεχνολογία και κοινωνικός έλεγχος**, Εγκληματολογικά κείμενα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2003.

Χαλκιά, Αναστασία, «**Σκέψεις για τη δόμηση και τη μελέτη των αντικειμένων έρευνας στην Εγκληματολογία**», ΠοινΔικ & Εγκληματολογία 1/2010, σελ. 41-47.

Χαραλαμπάκης, Αριστοτέλης, **Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο**, Τόμος Δεύτερος, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011.

Χαραλαμπάκης, Αριστοτέλης & Γιαννίδης, Ιωάννης, **Ποινικός Κώδικας και Νομολογία**, εκδ. Π. Ν. Σάκκουλα, Αθήνα, 2009.

Χρίστου, Γενοβέφα, **«Οι θετικές επιδράσεις των MMORPGs»,** εις: *Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.)*, Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 82 επ.

Χρυσόγονος, Κωνσταντίνος, «**Το θεμελιώδες δικαίωμα στην ασφάλεια**», εις: *Χ. Ανθόπουλου, Ξ. Κοντιάδη και Θ. Παπαθεοδώρου (επιμ.)*, Ασφάλεια και δικαιώματα στην κοινωνία της διακινδύνευσης, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005, σελ. 137-154.

Bottomley, Keith A., «**Έγκλημα και Ποινική Δικαιοσύνη στο ξεκίνημα του 21ου αιώνα: "Αυστηροί με το έγκλημα – Αυστηροί με τα αίτια του εγκλήματος";**», μετάφραση: *Γιώργος Καρανικόλας*, ΠοινΔικ 6/2002, ιδίως σελ. 640 επ.

Bourdieu, Pierre, **Επιστήμη της επιστήμης και αναστοχασμός**, μετάφραση: *Θ. Παραδέλλης*, εκδ. Πατάκη, Αθήνα, 2005.

Cohen, Louis & Manion, Lawrence & Morrison, Keith, **Μεθολογία εκπαιδευτικής έρευνας**, εκδ. Μεταίχμιο, 2007.

Delmas – Marty, Mireille, **Πρότυπα και τάσεις αντεγκληματικής πολιτικής**, Μετάφραση: *Χριστίνα Ζαραφωνίτου*, Βιβλιοθήκη εγκληματολογίας αρ. 8, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 1996.

Denning, Dorothy, **Πληροφοριακός πόλεμος και ασφάλεια πληροφοριών των επιχειρήσεων**, εκδ. Ίων, Αθήνα, 1999 (μετάφραση – επιμέλεια: *Χρ. Τσουραμάνης*).

Giddens, Anthony, **Κοινωνιολογία**, μετάφραση-επιμέλεια: *Δημήτρης Τσαούσης,* εκδ. Gutenberg, Αθήνα, 2002.

Feyerabend, Paul, **Ενάντια στη μέθοδο. Για μία αναρχική θεωρία της γνώσης**, μετάφραση: *Γ. Καυκαλάς & Γ. Γκουνταρούλης*, εκδ. Σύγχρονα θέματα, Αθήνα, 1991.

*Furnell, Steven,***Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας,** εκδ. Παπαζήση, 2006.

Haynes, Colin, **Τεχνικές προστασίας από τους ιούς υπολογιστών,** μετάφραση: *Ελένη Καλογήρου*, εκδ. Μ. Γκιούρδας, Αθήνα 1991.

Mansfield, Richard, **Οι Χάκερ Επιτίθενται**, απόδοση: *Ε. Γκαγκάτσιου*, 1η Αμερικάνικη Έκδοση, 2000, εκδότης Μ. Γκιούρδας.

Mason, Jennifer, **Η διεξαγωγή της ποιοτικής έρευνας**, μετάφραση: *Ελένη Δημητριάδου*, επιστημονική επιμέλεια: *Νότα Κυριαζή*, εκδ. Ελληνικά Γράμματα, Αθήνα, 2010.

Mearsheimer, John, **Η τραγωδία της πολιτικής των μεγάλων δυνάμεων**, μετάφραση: *Κωνσταντίνος Κολιόπουλος*, Επιστ. επιμέλεια: *Π. Ήφαιστος – Ηλ. Κουσκουβέλης*, εκδ. Ποιότητα, 5η εκδ., Αθήνα, 2009.

Mitnick, Kevin & Simmons, William, **Η τέχνη της απάτης**, μετάφραση: *Λ. Καρατζά*, εκδ. Ωκεανίδα, 2003.

Prittwitz, Cornelius, **Περίγραμμα του Ποινικού Δικαίου και της αντεγκληματικής πολιτικής στην εποχή της παγκοσμιοποίησης**, Υπερ/2000, σελ. 203-220.

Thio, Alex, **Παρεκκλίνουσα συμπεριφορά**, επιμέλεια: *Χρήστος Τσουραμάνης*, ίων, εκδ. έλλην, 2008.

Ξενόγλωσση βιβλιογραφία και αρθρογραφία

Baker, Estella, **Governing through crime – the case of the European Union**, European Journal of Criminology, vol. 7, n. 3, May 2010, pp. 187 f.

Barret, Neil, **Digital Crime – Policing the Cybernation**, Kogan Page eds., London, 1997.

Binder, Arnold & Geis, G., **Methods of Research in Criminology and Criminal Justice**, New York, 1983.

Bloombecker, Jay. J., **Computer Crime Update: The View as we exit 1984,** New England Law Review, 1985.

Brenner, Susan W. & Bert-Jaap Koops, **Appoaches to Cybercrime Jurisdiction**, 4 J. High Tech. L. 1, 2004.

*Brenner, Susan W.***Cybercrime jurisdiction**, Crime Law Soc Change (2006) 46:189–206.

Brown, Ian & Edwards, Lilian & and Marsden, Chris, **Information security and cybercrime**, University of Essex.

Calderoni, Francesco, **The European legal framework on cybercrime: striving for an effective implementation**, Crime Law Soc Change, 2010, 54, pp.: 339–357.

Chen, C. D., **Computer Crime and the Computer Fraud and Abuse Act of 1986**, Computer and Law Journal, 1990.

Cheng, Kristan T., **Identity Theft and the Case for a National Credit Report Freeze Law**, North Carolina Banking Institute, 12 N.C. Banking Inst. 239, March, 2008.

Chiesa, Raoul, Ducci, Stefania & Ciappi, Silvio, **Profiling hackers – The Science of Criminal Profiling as Applied to the World of Hacking**, Auerbach Publications - Taylor & Francis Group, 2009.

Clarke, Ronald V., **Technology, Criminology and Crime Science**, European Journal on Criminal Policy and Research 10: 55–63, 2004, Kluwer Academic Publishers.

Deflem, Mathieu, **Technology and the Internationalization of Policing: A Comparative-Historical Perspective**, Justice Quarterly 19(3), 2002, pp. 453-475.

D' Ovidio, Rob, **The Evolution of Computers and Crime: Complicating Security Practice**, Criminal Justice Program, Drexel University, Philadelphia, PA, U.S.A., Security Journal (2007).

Davidson, Julia & Gottschalk, Petter, **Characteristics of the Internet for criminal child sexual abuse by online groomers**, Criminal Justice Studies, Vol. 24, No. 1, March 2011, 23–36.

Denning, Dorothy & McDoran, P., **Location-Based System Delivers User Authentication Breakthrough**, Computer Security Alert, 1999.

Dreyfus, Suelette, **Computer hackers: Juvenile Deliquents or International Saboteurs?** εισήγηση η οποία παρουσιάστηκε στο συνέδριο "Internet Crime" το οποίο έλαβε χωρα στη Μελβούρνη της Αυστραλίας στις 16-17 Φεβρουαρίου 1998 και διοργανώθηκε από το Australian Institute of Criminology.

Eagleton,Terry, **Ideology: An Introduction,** Verso, London, 1991.

*Easttom, Chuck & Det. Jeff Taylor***, Computer Crime, Investigation and the Law, Course Technology PTR**, A part of Cengage Learning, 2011.

Flaherty, David, **Protecting Privacy in Surveillance Societies**, Chapel Hill: University of N. Carolina Press, 1989.

Gerruzzi, P.A., **A history of modern computing**, MIT Press, 1998.

Glenny, Misha, **Cyberthieves, Cybercops and You**, Alfred A. Knopf ed., New York, 2011.

Grabosky, Peter, **Security in the 21st Century**, Security Journal (2007) 20.

Grabosky, Peter, **Requirements of prosecution services to deal with cyber crime**, Crime Law Soc Change (2007) 47: 201-223.

Grabosky, Peter, **Computer Crime in a World Without Borders,** Platypus Magazine, The journal of the Australian Federal Police, June 2000.

Grabosky Peter & Smith, R. **Crime in the digital age**, Sydney: Federation Press, 1998, pp. 52-53.

Hagan, F. E., **Research Methods in Criminal Justice and Criminology**, McMillan Publ. Co., New York, 1982.

Harrington, Suzan J., **Software Piracy: Are Robin Hood & Responsibility Denial at Work?**, Ethical Issues of Information Systems, IRM Press, Hershey, USA 2002.

Himanen, Pekka, **The hacker ethic: A radical approach to the philosophy of business.** New York: Random House, 2001, p. 141.

Hollinger, R. C. & Lanza-Kaduce, L., **The process of criminalization: The case of computer crime laws**, Criminology, 1988.

Holtfreter, Kristy, Van Slyke, Shanna, & Blomberg, Thomas G. , **Sociolegal change in consumer fraud: From victim-offender interactions to global networks,** Crime, Law & Social Change (2005) 44: 251–275.

Hospers, John, **Utilitarian theory**, εις: *M. David Ermann, Mary B. William & Claudio Gutierrez*, Computer, ethics and society, Oxford University Press, Inc. New York, NY, USA,1990, pp. 26-34.

Jacobson, Michael, **Reply to Kevin D. Haggerty**, **Theoretical Criminology**, 2004, SAGE Publications, London, Thousand Oaks and New Delhi, Vol. 8(2): 233–238; 1362–4806.

Jackson, Jonathan, **A psychological perspective on Vulnerability in the Fear of Crime**, Psychology, Crime & Law, vol. 15(4), 2009.

Jackson, Jonathan & Allum, Nick & Gaskell, George, **Perceptions of risk in cyberspace,** London School of Economics and Politics, Cyber Trust & Crime Prevention Project, 04/06/2004.

Johnson, Paul & Williams, Robin, **Internationalizing New Technologies of Crime Control: Forensic DNA Databasing and Datasharing in the European Union**, Policing & Society, Vol. 17, No. 2, June 2007, pp. 103-118.

Jones, Richard, **Digital rule, Punishment, control and technology**, SAGE Publications, London, Thousand Oaks and New Delhi, Vol. 2(1): 5-22.

Jupp, Victor, **Methods of criminological research**, Routledge and Kegan Paul, London, 1995.

Innes, Martin & Fielding, Nige, & Cope, Nina, **The appliance of Science? The Theory and Practice of Crime Intelligence Analysis**, British Journal of Criminology (2005) 45, 39–57.

Kerr, Orin S., **Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes**, NYU Law Review, Vol. 78, No 5, 1646-1647.

Keyser, Mike, **The Council of Europe Convention of Cybercrime, Journal of Transnational Law & Policy**, 12 J. Transnat'l L. & Pol'y 287, Spring, 2003, lexisnexis database.

Killias, Martin, **Precis de criminology**, Staempfli Editions SA Berne, 2001.

Killias, Martin & Clerici, C. , **Different Measures of Vulnerability in their Relation to Different Dimensions of Fear of Crime**, British Journal of Criminology, vol. 40 (3), 2000.

Klang, Mathias & Murray, Andrew, **Human rights in the digital age**, eds. Glasshouse Press, 2005.

Kovacich, Gerald L., **Hackers: freedom fighters of the 21st century**, Computers & Security, v. 18, n. 7, p. 573-576.

Kyas, Othmar, **Internet Security: Risk Analysis, Strategies and Firewalls**, International Thomson Computer Press, London, 1997.

Lapsley, Phil, **Exploding the phone**, 2013.

Large, Peter, **The Micro Revolution,** Fontana, 1980.

Leary, Mary Lou & Rappaport, Mary, **Beyond the Beat Ethical Considerations for Community Policing in the digital age**, National Center for Victims of Crime, Washington DC, November 2008.

Levy, Steven, **Hackers – Heroes of the Computer Revolution**, ed. O'reilly, 1984.

Maruna, Shadd, **Mixed method research in Criminology: Why not go both ways,** published in: *A. Piquero & D. Weisburd* (ed.), Handbook of Quantitative Criminology, London: Springer 2010.

Marx, Gary T., **The Engineering of Social Control: The Search for the Silver Bullet**, published in *J. Hagan and R. Peterson*, Crime and Inequality, 1995, Stanford University Press.

McCusker, Rob, **Transnational organised cyber crime: distinguishing threat from reality,** Crime Law Soc Change (2006) 46:257–273.

Merton, Robert, **Social Theory and Social Structure**, New York: Free Press, 1968.

Microsoft Corporation with Andy Ruth & Kurt Hudson, **Security+ Certification, training kit,** Microsoft, 2003.

Moitra, Soumyo D., **Analysis and modeling of cybercrime: Prospects and potential,** Max Planck Institute for foreign and international criminal law.

Moitra, Soumyo D., **Developing Policies for Cybercrime - Some Empirical Issues**, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13/3, 2005, pp. 435-464.

Moore, Tyler, Clayton, Richard and Anderson, Ross, **The Economics of Online Crime, Journal of Economic Perspectives**—Volume 23, Number 3—Summer 2009 — p. 5.

Moustakas, C., **Phenomenological research methods**, Sage Publications, London, 1994.

Mueller-Gugenberger, Christian, **Wirtschaftsstrafrecht. Eine Gesamtdarstellung des deutschen Wirtschaftsstraf- und Ordnungswidrikeitenrechts**, 2nd ed., Muenster, 1992.

Nachmias, David & Nachmias, Chava, **Research methods in the social sciences**, St. Martin's Press, New York, 3rd edition, 1987.

Nelson, B. , **Straining the capacity of the law: The idea of computer crime in the age of the computer worm**, Computer and Law Journal, 1991.

Neuman, Peter, **Computer Related Risks**, Addison Wesley Publishing Company, 1995.

O'Brien, Martin & Yar, Majid, **Criminology – The key concepts**, Routledge ed., 2008.

Parker, Donn B., **Fighting Computer Crime**, Wiley pub., New York 1998.

Pastor-Satorras, Romualdo & Vespignani, Alessandro, **Evolution and Structure of the Internet – A statistical physics approach**, Cambridge University Press, 2004.

Penney, Steven, **Updating Canada's Communications surveillance laws: Privacy and security in the digital age**, 2008, 12 Canadian Criminal Law Review 115, 2008.

Pipkin, Donald, **Halting the Hacker: A Practical Guide to Computer Security**, Prentice Hall eds., New Jersey, 1997.

Pocar, Fausto, **New challenges for international rules against cyber-crime,** European Journal on Criminal Policy and Research 10: 27–37, Kluwer Academic Publishers, 2004.

Quarantiello, Laura, **Cyber Crime: How to Protect Yourself from Computer Criminals**, Limelight eds., New York, 1997.

Rachels, James, **Kantian theory the idea of human dignity,** published in: *M. D. Ermann, M. B. Williams, M. S. Schauf* (ed.)**: "Computer, ethics and society",** Oxford University Press, 1997.

Raymond Choo, Kim-Kwang, Smith, Russell G. & McCusker, Rob, **Future directions in technology-enabled crime**: 2007–09, Research and Public Policy Series No 78, Australian Institute of Criminology.

Raymond Choo, Kim-Kwang, Smith, Russell G. & McCusker, Rob, **The future of technology-enabled crime in Australia,** TRENDS & ISSUES in crime and criminal justice, Australian Institute of Criminology, No 341, July 2007.

Rege-Patwardhan, Aunshul, **Cybercrimes against critical infrastructures: a study of online criminal organization and techniques**, Rutgers School of Criminal Justice, Criminal Justice Studies, Vol. 22, No. 3, Routledge, September 2009.

Rose Gerry, **Deciphering Sociological Research**, published in: *Anthony Giddens* (ed.), Contemporary Social Theory, London School of Economics and Political Science, M 1982.

Russell, Deborah & Gangemi, G. , **Computer Security Basics,** O'Reilly and Associates, 1991.

Scelsi, Christina, **The i-phone hacking and cracking and copyright**, Entertainment and Sports Lawyer, Fall, 2008.

Schwabe, William, **Needs and prospects for crime-fighting technology**, RAND, Science and Technology Policy Institute, 1999.

Schneier, Bruce, **Beyond Fear: Thinking Sensibly about Security in an Uncertain World**, Copernicus Book, New York, 2003.

Shelley, Louise I., **Organized Crime, Terrorism and Cybercrime, Security Sector Reform: Institutions, Society and Good Governance**, Alan Bryden/Philipp Fluri (eds.), 2003, pp. 303-312.

Sieber, Ulrich, **Legal aspects of computer-related crime in the Information society**, January 1998, prepared for the European Commission.

Sieber, Ulrich, **Criminal Liability for the Transfer of Data in International Computer Networks: New Challenges of the Internet**, Juristenzeitung (JZ), 1996, p. 429-494.

Sieber, Ulrich, **The international handbook on computer crime: computer-related economic crime and the intifringements of privacy**, eds. J. Wiley and Sons, New York, 1986.

Smith, Russell G., **Identification systems: a risk assessment framework, TRENDS & ISSUES in crime and criminal justice**, Australian Institute of Criminology, No. 324, September 2006.

Smith, Russell G., **Travelling in Cyberspace on a False Passport: Controlling Transnational Identity related crime**, The British Criminology Conference: Selected Proceedings. Volume 5, Papers from the British Society of Criminology Conference, Keele, July 2002, published August 2003. Editor: Roger Tarling. ISSN 1464-4088.

Snoyer, Robert S. & Fischer, Glenn A., **Managing microcomputer security**, ed. Chantico Publishing Company, Inc., 1993.

Solove, J. Daniel, **The digital person – Technology and Privacy in the Information age**, New York University Press, 2004.

Sterling, Bruce, **The hacker crackdown : Law and Disorder on the Electronic Frontier**, Bantam Books, 1992.

Stohl, Michael, **Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games**?, Crime Law Soc Change, 2006.

Sutherland, Edwin, **White-Collar Crime**, Holt, Rinehart & Winston, New York, 1949.

Sykes, Gresham M. & Matza, David, **Techniques of Neutralization: A Theory of Delinquency**, American Sociological Review, Vol. 22, No. 6 (Dec., 1957), published by: American Sociological Association, pp. 664-670.

Taylor, Paul A., **Hackers: Crime in the Digital Sublime,** Routledge, 1999.

Taylor, Paul A., **Hackers**, distributed in Computer Underground Digest, Vol. 9 Issue 59.

Turgeman-Goldschmidt, Orly, **Between Hackers and White-Collar Offenders**, Bar-Ilan University, Israel, 2012.

Turgeman-Goldschmidt, Orly, **Identity construction among hackers,** εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011, pp. 31 f.

Turner, Jonathan H. **The Structure of Sociological Theory**, University of California, Riverside, The Dorsey Press Homewood, Illinois, Irwin-Dorsey Limited, Georgetown, Ontario, Revised Edition, 1978.

Urbas, Gregor & Raymond Choo, Kim-Kwang, **Resource materials on technology-enabled crime**, Australian Institute of Criminology, Technical and Background Paper, No. 28.

Vishnu Konoorayar, K., **Regulating Cyberspace: The Emerging Problems and Challenges**, Cochin University Law Review, 2003, pp. 413-435.

Wall, David S. , **Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime**, Information, Communication & Society Vol. 11, No. 6, pp. 861–884, 1st September 2008.

Wall, David S. , **Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime, International Review of Law**, Computers and Technology, vol. 22, nos. 1-2.

Wall, David S., **Digital Realism and the Governance of Spam as Cybercrime**, European Journal on Criminal Policy and Research, 10(4): 309 – 335.

Wall, David S., **Hunting, shooting and phising: new cybercrime challenges for cybercanadians in the 21st century**, British Library, 2008.

*Wall, David S. ,***Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace,** Police Practice and Research, 8:2, 183 205.

Wark, McKenzie, **A hacker manifesto**. Cambridge, Mass.: Harvard University Press, 2004.

Wasik, Martin, **Crime and the computer**, eds. Clarendon Press, Oxford, 1991.

Weber, Rolf H. & Weber, Romana, **Internet of Things - Legal Perspectives**, Springer Heidelberg Dordrecht London New York, Zurich – Basel – Geneva 2010.

Winn Peter A., **The Guilty Eye: Unauthorized access,** Trespass and Privacy. Business Lawyer, Vol. 62, 2007.

White, *Lynn Jr.,* **Medieval technology and Social Change**, Oxford: University Press, 1962.

Yar, *Majid,* **Computer Hacking: Just Another Case of Juvenile Delinquency?**, Howard Journal of Criminal Justice, Vol. 44, No. 4, pp. 387-399, September 2005.

Yar, *Majid,* **The Novelty of "Cybercrime" - An Assessment in Light of Routine Activity Theory**, European Journal of Criminology, Volume 2 (4): 407–427: 1477-3708, European Society of Criminology and SAGE Publications, London, Thousand Oaks CA, and New Delhi 2005.

ΔΙΑΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

Ελληνόγλωσσοι ιστότοποι

Αγγελής Ιωάννης, **Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη**, Νομική Επιθεώρηση, τεύχος 30 (url: http://www.eofn.gr/attachments/084_aggelis.pdf).

Αλάμπασης, Αθανάσιος, **iPhone vs Police. Η ψηφιοποίηση των στοιχείων που συνθέτουν την αντικειμενική υπόσταση του εγκλήματος. "Body-tracking wristbands", "tap n pay", "tap n vote" και "Wearable Democracy". Η επερχομένη έκρηξη των κοινωνικοπολιτικών apps (SoPol apps)** (url: http://alampasis.blogspot.gr/2014/05/iphone-vs-police-body-tracking.html).

Γεωργουσόπουλος, Σπύρος & Σπυρόπουλος, Φώτιος, **Ποιος είναι ο Jean Piaget**, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr, τεύχος 18, Απρίλιος 2011 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1303923164).

Διαμαντόπουλος, Επαμεινώνδας, **Σημειώσεις στατιστικής**, Ξάνθη, Νοέμβριος 2012 (url: http://users.sch.gr/epdiaman/images/stories/ergasies/biblia/statistics_with_calc_and_R_project.pdf).

Ζαραφωνίτου, Χριστίνα, **Τιμωρητικότητα: ανασφάλεια και κοσμοθεωρία**, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τεύχος 13, Φεβρουάριος 2010 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1263811765).

Ζαραφωνίτου, Χριστίνα και συν., **Θυματοποίηση και φόβος του εγκλήματος στο διαδίκτυο**, (url: http://criminology.panteion.gr/attachments/article/407/e-life%20ppt.pdf).

Ιωαννίδη-Καπόλου, Έλλη, **Κοινωνιολογική έρευνα – Μέθοδοι και τεχνικές** (url: www.nsph.gr/Files/006_Koinoniologias/Research_Stages.doc).

Κασκάλης, Θεόδωρος & Μαλέτσκος, Αθανάσιος & Ευαγγελίδης, Κωνσταντίνος, **«Χρήση και αξιοποίηση ηλεκτρονικών ερωτηματολογίων σε έναν εκπαιδευτικό δικτυακό τόπο»**, Τμήμα Νηπιαγωγών, Παιδαγωγική Σχολή, Πανεπιστήμιο Δυτικής Μακεδονίας (url: http://www.etpe.eu/new/custom/pdf/etpe43.pdf).

Κατσάνος, Χρήστος & Αβούρης, Νικόλαος, **Στατιστικές Μέθοδοι Ανάλυσης Πειραματικών Δεδομένων Συνεργασίας,** Πανεπιστήμιο Πατρών (url: http://karagian.users.uth.gr/cscl/22-Katsanos-Avouris.pdf).

Κεδρακά, Κατερίνα, **Μεθοδολογία λήψης συνέντευξης** (url: https://docs.google.com/document/d/1Ns81KOslEHm0PKruMXSgV-xe9gtye6Npp-x2KgROlBs/edit?hl=en).

Κουράκης, Νέστωρ, **Εθισμός στο διαδίκτυο**, ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 16, Νοέμβριος 2010 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1289401434).

Κουράκης, Νέστωρ, **Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της**, ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr (τεύχος 11, 2009) (url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1247152434).

Κουκουτσάκη, Αφροδίτη, **Νεολαία και «Ηθικοί Πανικοί»** (url: http://crimevssocialcontrol.blogspot.com/2009/10/blog-post_17.html).

Παππά, Αρτεμισία & Πανεζή, Αργυρή & Παναγιωτοπούλου, Σοφία, **Επιστημονική εκδήλωση με θέμα: «Κώδικας Δεοντολογίας για τους Εγκληματολόγους –**

Πρόταγμα του 21ου αιώνα;», ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 7 Φεβρουάριος 2008 (url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1207652324).

Παπάνης, Ευστράτιος, **Δημοκρατία και διαδίκτυο** (url: http://www.emprosnet.gr/emprosnet-archive/371b9acc-32b2-4af8-8a0d-da7162151531 και http://my.aegean.gr/web/article2985.html).

Παρασκευοπούλου-Κόλλια, Ευφροσύνη-Άλκηστη, **Μεθοδολογία ποιοτικής έρευνας στις κοινωνικές επιστήμες και συνεντεύξεις**, Open Education - The Journal for Open and Distance Education and Educational Technology, τεύχος 4, αρ. 1, 2008 / Section one (url:http://openworkshop.pbworks.com/w/file/fetch/64390800/poiotikh-ereyna-ekpaideysh.pdf).

Σπινέλλη, Καλλιόπη & Κρανιδιώτη, Μαρία, **Κώδικας Δεοντολογίας Εγκληματολόγων**, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 10, Φεβρουάριος 2009 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1237301236).

Σπυρόπουλος, Φώτιος, **Anonymous - χακτιβισμός με "ονοματεπώνυμο";** , ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τεύχ. 25, Νοέμβριος 2013 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1385808756).

Σπυρόπουλος, Φώτιος, **Οι "κατά παρέκκλιση" διαδικασίες και η αποκαταστατική-συμφιλιωτική δικαιοσύνη / Ιστορική και δογματική προσέγγιση**, ηλεκτρονικό εγκληματολογικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών τμήματος Νομικής Πανεπιστημίου Αθηνών www.theartofcrime.gr, τ. 7, Φεβρουάριος 2008 (url: http://theartofcrime.gr/index.php?pgtp=1&aid=1207246182).

Σωτηρόπουλος, Βασίλειος, **Εσφαλμένη και η τρίτη γνωμοδότηση Εισαγγελίας Αρείου Πάγου για την ανωνυμία,** νομικό ιστολόγιο "e-lawyer" (url: http://elawyer.blogspot.gr/2011/05/blog-post_31.html).

Σωτηρόπουλος, Βασίλειος, **Δωρεάν ασύρματη πρόσβαση πολιτών στο Διαδίκτυο**, νομικό ιστολόγιο "e-lawyer" (url: http://elawyer.blogspot.gr/2014/03/blog-post_7.html).

Τσόλιας, Γρηγόρης, **Η πρόταση Οδηγίας του ΕΚ και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών**, 2ο Πανελλήνιο Συνέδριο e ΘΕΜΙΣ, www.ethemis.gr.

Φαρσεδάκης, Ιάκωβος, **Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του**, Πάντειο Πανεπιστήμιο, 19/05/2009 (url: http://criminology.panteion.gr/attachments/article/386/j%20farsedakis%20%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BFs.pdf).

Χατζής, Αριστείδης & Φωκά – Καβαλιεράκη, Γιούλη, **Θεωρία ορθολογικής επιλογής – Πανεπιστημιακές σημειώσεις**, Τμήμα Μεθοδολογίας, Ιστορίας και Θεωρίας της Επιστήμης Ε.Κ.Π.Α., Αθήνα 2012 (url: http://www.aristideshatzis.net/2010/04/blog-post_2909.html).

Bartle, Phil, «**Τεχνικές ουδετεροποίησης – Μειώνοντας τη σοβαρότητα ενός εγκλήματος»,** Μετάφραση: Αποστολία Γουγούση (url: http://cec.vcn.bc.ca/mpfc/modules/cri-neug.htm).

Merritt, Marian, **Τα «Πρέπει» και τα «Μη» των κωδικών πρόσβασης** (url: http://gr.norton.com/dos-donts-passwords/article).

Raymond, Eric Steven, **Πώς να γίνεις Χάκερ**, Μετάφραση: Αριστοτέλης Μικρόπουλος, 2001 (url: http://earthlab.uoi.gr/indy/hacker-howto-gr/).

"ΓΕΕΘΑ: Ο κυβερνοπόλεμος είναι το νέο στρατηγικό όπλο" (url: http://www.onalert.gr/default.php?pname=Article&catid=20&art_id=1673).

Άρθρο με τίτλο «Ο Α' Παγκόσμιος Κυβερνοπόλεμος!», Τρίτη 10 Φεβρουαρίου 2009 (url: http://www.focusmag.gr/articles/view-article.rx?oid=410433).

Η χρήση του διαδικτύου από τους Έλληνες, Παρατηρητήριο για την κοινωνία της πληροφορίας, Μάιος 2011 (url: http://www.observatory.gr/files/meletes/A100526_%CE%A0%CF%81%CE%BF%CF%86%CE%AF%CE%BB%20%CF%87%CF%81%CE%B7%CF%83%CF%84%CF%8E%CE%BD%20internet%202010.pdf).

Λήμματα από ηλεκτρονική εγκυκλοπαίδεια «Βικιπαιδεία»

Λήμμα: Διακομιστές μεσολάβησης (url: http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%BA%CE%BF%CE%BC%CE%B9%CF%83%CF%84%CE%AE%CF%82_%CE%BC%CE%B5%CF%83%CE%BF%CE%BB%CE%AC%CE%B2%CE%B7%CF%83%CE%B7%CF%82).

Λήμμα: Εικονικό ιδιωτικό δίκτυο (url: http://el.wikipedia.org/wiki/%CE%95%CE%B9%CE%BA%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF).

Λήμμα: Σκάνδαλο τηλεφωνικών υποκλοπών 2004-2005 (url: http://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%AC%CE%BD%CE%B4%CE%B1%CE%BB%CE%BF_%CF%84%CE%B7%CE%BB%CE%B5%CF%86%CF%89%CE%BD%CE%B9%CE%BA%CF%8E%CE%BD_%CF%85%CF%80%CE%BF%CE%BA%CE%BB%CE%BF%CF%80%CF%8E%CE%BD_2004-2005).

Λήμμα: Internet Relay Chat (IRC), url: http://el.wikipedia.org/wiki/Internet_Relay_Chat.

Λήμμα: Έντουαρτ Σνόουντεν (url: http://el.wikipedia.org/wiki/%CE%88%CE%BD%CF%84%CE%BF%CF%85%CE%B1

%CF%81%CE%BD%CF%84_%CE%A3%CE%BD%CF%8C%CE%BF%CF%85%CE%BD%CF%84%CE%B5%CE%BD).

Ποιες μορφές διαδικτυακής απάτης συναντώνται συχνότερα; - ιστοσελίδα ελληνικής αστυνομίας (url: http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_content&perform=view).

«Εγκλήματα με την χρήση Η/Υ (ως βοηθητικό μέσο)» (url: https://sites.google.com/site/elektronikoenklema2012/morphes-tou-elektronikou-enklematos/enklemata-me-ten-chrese-e-y-os-boethetiko-meso).

Σχετικά με την *Ελληνική Χάκινγκ Σκηνή (Greek Hacking Scene)* (urls: https://www.facebook.com/groups/GreekHackScene/?fref=ts, https://www.facebook.com/pages/Greek-Hacking-Scene-%CE%95%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CE%AE-%CE%A7%CE%AC%CE%BA%CE%B9%CE%BD%CE%B3%CE%BA-%CE%A3%CE%BA%CE%B7%CE%BD%CE%AE/155940007782512, https://www.facebook.com/groups/GreekHackers/?ref=ts&fref=ts, http://www.digitallife.gr/tag/greek-hacking-scene

http://thesecretrealtruth.blogspot.com/2012/09/greek-hacking-scene.html

Φωτογραφίες από επιθέσεις της GHS στο url: http://antiparakmi.blogspot.com/search/label/Greek%20Hacking%20Scene).

Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο (url: http://www.hasiad.gr/).

Κέντρο Πληροφορικής & Νέων Τεχνολογιών Ηλείας (url: http://dide.ilei.sch.gr/keplinet/tech/virus.php).

Αιτιολογική έκθεση του ν. 3917/2011 (url: http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=In68q5jjdW0%3D&tabid=132).

Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, (url: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/RELATIVELAW/%CE%9F%CE%94%CE%97%CE%93%CE%8A%CE%912006-24-%CE%95%CE%9A.PDF).

Για την κοινωνική μηχανική (url: http://hellinikogenos.blogspot.gr/2013/11/blog-post_10.html).

Ιστότοπος με θέμα «Τρόποι και κόλπα των hackers!» (url: http://projecthackers-hacking.blogspot.gr/2012/10/blog-post_11.html).

«Οι 5 μεγαλύτεροι παράνομοι hackers όλων των εποχών», 22 Ιουνίου 2011, url: http://archive.today/20121127063559/hackingexperience.blogspot.com/2011/06/5-hackers.html)

Σχετικά με την τεχνική "Footprinting" (url: http://techtips.gr/how-to-tricks-tips/2015/i-texniki-tou-footprinting).

Σχετικά με τα προγράμματα Keylogger (urls: http://www.inout.gr/showthread.php?t=24288 και http://thanasaras13.blogspot.gr/2011/07/keylogger.html).

Για την ομάδα Hackerspace βλ. url: http://www.hackerspace.gr/wiki/Main_Page.

Ανοιχτή επιστολή καθηγητών ΑΕΙ και ΤΕΙ για το παράνομο hacking, 18/07/2014 (βλ. url: http://www.koutipandoras.gr/article/118505/anoihti-epistoli-kathigiton-aei-kai-tei-gia-paranomo-hacking).

Έρευνα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας με τίτλο «**Η χρήση του διαδικτύου από τους Έλληνες»**, url: (http://www.observatory.gr/files/meletes/A100526_%CE%A0%CF%81%CE%BF%CF%86%CE%AF%CE%BB%20%CF%87%CF%81%CE%B7%CF%83%CF%84%CF%8E%CE%BD%20internet%202010.pdf).

Έρευνα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας με θέμα: **«Διαδικτυακός Αλφαβητισμός στην Ελλάδα και στην ΕΕ των 27 (2007 – 2010)»** (url:

http://www.observatory.gr/files/meletes/INCL_%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CF%8C%CF%82_%CE%91%CE%BB%CF%86%CE%B1%CE%B2%CE%B7%CF%84%CE%B9%CF%83%CE%BC%CF%8C%CF%82_%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1_%CE%95%CE%95%202010.pdf.

Ξενόγλωσσοι ιστότοποι

Abbot, Kenneth W. & Snidal, Duncan, Hard and Soft Law in International Governance, International Organization, Vol. 54, p. 421, 2000 (url: file:///C:/Users/FSpyropoulos/Downloads/SSRN-id1402966.pdf).

Ali, Farha, **IP Spoofing**, Lander University (url: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html).

Arias, Martha, **Internet Law - Computer Hacking: A global Problem that Requires a Global Solution** (url: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2513).

Arief, Budi & Besnard, Denis, **Technical and Human Issues in Computer-Based Systems Security**, University of Newcastle upon Tyne, Μάρτιος 2003 (url: http://bscw.cs.ncl.ac.uk/pub/bscw.cgi/d48026/Arief%20and%20Besnard%20-%20Technical%20and%20Human%20Issues%20in%20Computer-Based%20Systems%20Security.pdf)

Ashton, Kevin, **That "Internet of Things" thing**, RFiD Journal, 22 Ιουνίου 2009 (url: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf).

Bachmann, Michael, **What makes them click?** Applying the rational choice perspective to the hacking underground, 2004 (url: http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf).

Bailey, Cynthia, Roedel, Lee Chris & Silenok, Elena, **Detection and Characterization of Port Scan Attacks**, Department of Computer Science & Engineering - University of California, San Diego (url: http://cseweb.ucsd.edu/~clbailey/PortScans.pdf).

Ball, Allen, **An empirical exploration of Neutralization Theory,** Criminology 7/4/2006 (url: http://onlinelibrary.wiley.com/subject).

Betancourt, Julio César & Zlatanska, Elina, **Online Dispute Resolution (ODR): What Is It, and Is It the Way Forward?**, 79 International Journal of Arbitration, Mediation and Dispute Management, Issue 3, 2013 (url: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325422).

Blobel, Volker, **Statistical and other errors**, University of Hamburg, March 2005 (url: http://www.desy.de/~blobel/blobel_errors.pdf).

Bossler, Adam M., & Holt, Thomas J. **Malware Victimization - A Routine Activities Framework.** εις: *K. Jaishankar (ed.)*, Cyber Criminology – Exploring Internet Crimes and Criminal Behavior, ed. CRC Press – Taylor and Francis Group, 2011 (url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf), pp. 317 f.

Crossman, Ashley, **Snowball Sample** (url: http://sociology.about.com/od/Types-of-Samples/a/Snowball-Sample.htm).

Crossman, Ashley, **Structural Strain Theory - An Overview** (url: http://sociology.about.com/od/Sociological-Theory/a/Structural-Strain-Theory.htm).

Denning, Dorothy, **Is Cyber Terror Next? In Understanding September 11**, edited by C. Calhoun, P. Price, and A. Timmer (2001) (url: http://www.ssrc.org/sept11/essays/denning.htm).

Denning, Dorothy, **Concerning hackers who break into computer systems**, 1990 (url: http://www.cpsr.org/prevsite/cpsr/privacy/crime/denning.hackers.html).

Donoghue, Andrew, **Cyberterror: Clear and present danger or phantom menace?,** ZDNet, 2004 (url: http://insight.zdnet.co.uk/specials/networksecurity/0,39025061,39118365-2,00.htm).

Fitch, Cynthia, **Crime and Punishment: The Psychology of Hacking in the New Millennium** (url: http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795).

Fötinger, Christian S. & Ziegler, Wolfgang, **Understanding a hacker's mind – A psychological insight into the hijacking of identities**, White Paper by the Danube-University Krems, Austria, pp. 2 f. (url: http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf).

Geis, Gilbert, **On the absence of self-control as the basis for a general theory of crime: A critique** (url: http://www.soc.umn.edu/~uggen/Geis_TC_00.pdf).

Gil, Paul, **"What is a 'Hacker'? Is that the same as a 'hax0r'?"** (url: http://netforbeginners.about.com/od/h/f/haxor.htm).

Graux, Hans, **New Directive on Attacks against Information Systems**, 16.10.2013, (url: http://www.timelex.eu/en/blog/detail/new-directive-on-attacks-against-information-systems).

Holt, Thomas & Schell, Bernadette, **Hackers and hacking: a reference handbook**, Contemporary World Issues – Science, Technology and Medicine, 2013 (url: http://books.google.gr/books?id=FZVfAQAAQBAJ&pg=PA149&lpg=PA149&dq=bossler+and+burruss&source=bl&ots=lL57-n6LHz&sig=0nOIvybIGJTRRSWsOEJWMxfHe3A&hl= el&sa=X&ei=OvsAU6TZI-O7ygO noLgCQ&ved=0CEwQ6AEwAw#v=onepage&q=subculture&f =false).

Hu, Qing & Xu, Zhengchuan & Yayla, Ali Alper, **Why college students commits computer hacks: Insights from a cross culture analysis** (url: http://www.pacis-net.org/file/2013/PACIS2013-104.pdf).

Jaishankar, Karuppannan, **Cyber Criminology – Exploring Internet Crimes and Criminal Behavior,** ed. CRC Press – Taylor and Francis Group, 2011 (url: http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf).

Jordan, Tim, **Hacking and power: Social and technological determinism in the digital age**, Journal "first Monday", vol. 14, n. 7, 06/07/2009 (url: http://firstmonday.org/ojs/index.php/fm/article/view/2417/2240).

Koops, Bert-Jaap, **Criteria for Normative Technology - An essay on the acceptability of 'code as law' in light of democratic and constitutional values**, TILT Law & Technology Working Paper No. 005/2007 Version 0.4 & Tilburg University Legal Studies Working Paper No. 007/2007, 7 December 2007 (url: http://ssrn.com/abstract=1071745).

Koops, Bert-Jaap, **Law, Technology, and Shifting Power Relations**, TILT Law & Technology Working Paper No. 014/2009, September 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 014/2009 (url: http://ssrn.com/abstract=1479819).

Koops, Bert-Jaap, **Technology and the Crime Society: Rethinking Legal Protection**, TILT Law & Technology Working Paper No. 010/2009, 23 March 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 006/2009 (url: http://ssrn.com/abstract=1367189).

Krone, Tony, **Hacking Motives**, January 2005 (url: http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb006.html).

Kumar Katyal, Neal, **Criminal Law in Cyberspace**, Georgetown University Law Center 2000 Working Paper Series in Business, Economics and Regulatory Policy and Public Law and Legal Theory, Working Paper No. 249030 (url: http://papers.ssrn.com/paper.taf?abstract_id=249030).

Kunz, Michael & Wilson, Patrick, **Computer Crime and Computer Fraud,** Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004 (url: http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf).

Kurbalija, Jovan, **Internet governance and international law**, Reforming Internet Governance: Perspectives from WGIG (url: http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf).

Leathers, Marilyn, **A Closer Look at Ethical Hacking and Hackers, East Carolina University** (url: http://www.infosecwriters.com/text_resources/pdf/MLeathers_Ethical_Hackers.pdf).

Lewis, James, **Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats**, Washington,DC: Center or Strategic and International Studies, December 2002, (url: http://www.csis.org/ tech/0211_lewis.pdf).

Licklider, Joseph Carl Robnett (J.C.R.), **Man – Computer Symbiosis** (url: http://groups.csail.mit.edu/medg/people/psz/Licklider.html/).

Long, Larisa April, **Profiling hackers,** January 2012 (url: http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864).

Loper, Kall D., **Digital Crime: Hackers,** Part 2, LETN (Law Enforcement Training Network) (url: http://www.twlk.com/law/tests/LETN1520009ct.pdf).

Lowman, Sarah, **Criminology of Computer Crime**, Μάιος 2010 (url: http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf).

Morris, Robert G., **Computer Hacking and the Techniques of Neutralization: An Empirical Assessment** (url: http://www.utdallas.edu/~rgm071000/index_files/Morris%20-%20Hacking%20and%20Neutralization. pdf).

Mizrach, Steven, **Is there a Hacker Ethic for 90s Hackers?** (url: http://www2.fiu.edu/~mizrachs/hackethic.html).

Newton, Andrew, Rogerson, Michelle & Alex Hirschfield, **Relating Target Hardening to Burglary Risk Experiences from Liverpool**, University of Huddersfield, 2008 (url: http://britsoccrim.org/volume8/10Newton08.pdf).

Palmer, C. C., **Ethical hacking**, (url: http://pdf.textfiles.com/security/palmer.pdf).

Parnell, Brid – Aine, **EU crackdown will see tougher sentences for stupid cyber-badhats**, The Register, 05.07.2013 (url: http://www.theregister.co.uk/2013/07/05/eu_tougher_sentences_for_hackers).

Pashel, Brian A., **Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level**, Kennesaw State University (url: http://cs.potsdam.edu/faculty/laddbc/Teaching/Ethics/StudentPapers/2006Pashel-TeachingStudentsToHack.pdf).

Phillips, Aemilia, **In And Around Language: "Hack",** The Harvard Crimson (url: http://www.thecrimson.com/article/2013/10/24/in-and-around-language-hack/).

Raab, Charles, **Beyond activism: Research perspectives on privacy**, The University of Edinburgh & Tilburg University, TILT Law & Technology Working Paper No. 007/2008, 22 February 2008, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 004/2008 (url: http://ssrn.com/abstract=1096562).

Rogers, Marc, **Psychological Theories of Crime and "Hacking"** (url: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.32.3697).

Schjolberg, Stein, **The Third Pillar for Cyberspace, An International Court or Tribunal for Cyberspace,** [Draft UN Treaty on an International Criminal Court or Tribunal for Cyberspace (9th edition, June 2014)], (url: http://www.cybercrimelaw.net/documents/140615_Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf).

Shim, Woohyun & Allodi, Luca & Massacci, Fabio, **Crime Pays If You Are Just an Average Hacker**, University of Trento, Povo, Italy (url: http://disi.unitn.it/~allodi/shim-12-cybersecurity.pdf).

Skogan, Wesley, **Fear of crime and neighborhood change** (url: http://www.skogan.org/files/Fear.of.Crime.and.Neighborhood.Change.1986.pdf).

Steel, Alex, **Vaguely Going Where No-One Has Gone: The expansive New Computer Offences** (url: file:///C:/Users/FSpyropoulos/Downloads/SSRN-id1030227.pdf).

Tafoya, William L., **Cyber terror** (url: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror).

Tanase, Matthew, **IP Spoofing: An introduction** (url: http://www.symantec.com/connect/articles/ip-spoofing-introduction).

Taylor, Paul A., **Hackers: Crime in the Digital Sublime**, Routledge, 1999 (url: http://www.google.gr/books?hl=el&lr=&id=V9VkmdYlvK4C&oi=fnd&pg=PP1&dq=Psychological+Theories+of+Crime+and+%E2%80%9CHacking&ots=1mWfjiP22v&sig=e98naWli9K0H0FTeYMwmVMqg4u8&redir_esc=y#v=onepage&q=Psychological%20Theories%20of%20Crime%20and%20%E2%80%9CHacking&f=false).

Turner, Mark, & Pantlin, Nick, Pugh Loretta & Young, Christine, **EU Cyber Crime Directive takes a tougher stance against attacks on information systems**, 17.10.2013 (url: http://cn.lexology.com/library/detail.aspx?g=d3863b21-3c3b-419e-8a8f-2b007acb3a10).

Tikk, Eneken, **Ten Rules for Cyber Security**, NATO Cooperative Cyber Defence Centre of Excellence, 2011 (url: http://citizenlab.org/cybernorms2011/rules.pdf).

Vishesh, Srivasta Tushar, **"Phishing and Pharming – The deadly duo"**, Sans Institute Reading Room site, January 2007 (url: http://www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil-twins_1731).

Wikström, Per-Olof H. & Treiber, Kyle H., **Violence as Situational action**, International Journal of Conflict and Violence (IJCV): Vol. 3 (1) 2009, pp. 75 – 96 (url: http://ijcv.org/index.php/ijcv/article/viewFile/49/49).

Wikström, Per-Olof H. & Treiber, Kyle, **The Role of Self-Control in Crime Causation**, European Journal of Criminology 2007; 4; 237 (url: http://www.sagepub.com/isw6/articles/ch6wikstrom.pdf).

Zavrsnik, Ales, **Cybercrime: Definitional challenges and criminological particularities,** Masaryk University Journal of Law and Technology (url: http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf).

Zittrain, Jonathan and *Edelman, Benjamin*, **Empirical Analysis of Internet Filtering in China**, Berkman Center for Internet & Society, Harvard Law School (url: http://cyber.law.harvard.edu/filtering/china/).

"Brief history of the internet" (url: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet).

"The birth of the web" (url: http://home.web.cern.ch/topics/birth-web).

"Tim Berners – Lee (biography)" (url: http://www.w3.org/People/Berners-Lee/).

"Dr. Vinton Cerf and Dr. Robert Kahn - Medal of Freedom Recipients" (url: http://georgewbush-whitehouse.archives.gov/government/cerf-kahn-bio.html).

"The social engineering framework" (url: http://www.social-engineer.org/).

"The conscience of a hacker" (url: https://web.archive.org/web/20050414161009/http://www.h2k2.net/display_grid.khtml?who=3).

Ποινικός Κώδικας της Νιγηρίας, url: http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm).

«13 Anonymous Hackers Plead Guilty To 2010 PayPal Attack» (url: http://www.redorbit.com/news/technology/1113023408/anonymous-hackers-plead-guilty-to-paypal-attack-120913/#7Uvfvofcvlbgmfds.99).

«Anonymous and WikiLeaks: Is it really a breakup?» (url: http://rt.com/news/anonymous-wikileaks-assange-paywall-572/).

Backdoor Shell (urls: http://en.wikipedia.org/wiki/Backdoor_Shell

http://www.hackforsecurity.net/2012/10/what-is-shell-and-how-to-use-it.html
http://www.go4expert.com/articles/shells-impressive-web-hacking-method-t19226/).

Biohacking (url: http://en.wikipedia.org/wiki/Biohacking).

"black hat hackers" (url: http://www.techopedia.com/definition/26342/black-hat-hacker).

"buffer overflow" (url: http://searchsecurity.techtarget.com/definition/buffer-overflow).

"Computer Misuse Act" (url: http://www.legislation.gov.uk/ukpga/1990/18/contents).

"Counterfeit Access Device and Computer Fraud and Abuse Act (Counterfeit Access Device Act)" (url: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA).

"Criminal Justice and Public Order Act" (url: http://www.legislation.gov.uk/ukpga/1994/33/contents).

«Cult of the Dead Cow» (url: http://www.cultdeadcow.com/tools/bo.html).

DIYbio (url: http://en.wikipedia.org/wiki/DIYbio).

"Dns spoofing" (url: http://www.menandmice.com/resources/dns-spoofing/).

"Elite hackers" (url: http://www.elite-hackers.com/).

Ethical hacker (urls: http://searchsecurity.techtarget.com/definition/ethical-hacker, http://www.computerhope.com/jargon/e/ethihack.htm).

Ethical hacking (urls: http://en.wikipedia.org/wiki/Certified_Ethical_Hacker, http://www.ethicalhacking.com).

"European Committee on Crime Problems (CDPC), Committee of Experts on Crime in Cyber – Space (PC-CY), Draft Convention on Cyber – crime (Draft No 22 REV.2)" (url: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm).

European Union Agency for Network and Information Security (url: http://www.enisa.europa.eu).

Exploit (computer security) (url: http://en.wikipedia.org/wiki/Exploit_(computer_security)).

Footprinting (url: http://searchsecurity.techtarget.com/definition/footprinting).

"Geek Rants: Why the Internet is Like the Wild West" (url: http://www.howtogeek.com/62135/geek-rants-why-the-internet-is-like-the-wild-west/).

"Good" hackers vs. Cyber-terrorists (url: http://www.cyberspacers.com/news/hackers4usa/).

gray ή grey hat hackers (url: http://searchsecurity.techtarget.com/definition/gray-hat).

"Hacker culture" (url: http://subcultureslist.com/hacker-culture/).

"Hackers language" (url: http://www.campusactivism.org/html-resource/hackers/section8.html).

hacking (url: http://www.iss.net/security_center/advice/Underground/Hacking/default.htm,

http://www.urbandictionary.com/define.php?term=hacking,
http://whatishacking.org/).

"Hacker slang and hacker culture" (url: http://www.catb.org/jargon/html/introduction.html).

Hacking Tutorials For Beginners (url: http://www.breakthesecurity.com/p/hacking-tutorials-for-beginners.html).

"How to avoid becoming a script kiddie" (url: http://www.wikihow.com/Avoid-Becoming-a-Script-Kiddie).

How to Hack (url: http://www.wikihow.com/Hack).

Internet Corporation for Assigned Names and Numbers (ICANN) (url: https://www.icann.org/resources/pages/udrp-2012-02-25-en).

"Internet 2012 in numbers" (url: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/).

Elf Qrin interviews the Mentor, 31/07/2000 (url: http://www.elfqrin.com/docs/hakref/interviews/eq-i-mentor.html).

IRC bouncer comparison (url: http://www.irc-junkie.org/2009-12-22/irc-bouncer-comparison/).

Simple Hack Threatens Outdated Joomla Sites, 12/08/2013 (url: http://krebsonsecurity.com/2013/08/simple-hack-threatens-oudated-joomla-sites/).

Keylogger (url: http://www.techopedia.com/definition/4000/keylogger, http://www.webopedia.com/TERM/K/keylogger.html).

Learn Hacking (url: http://learnhacking.in/).

"Leading questions lead to bad data", 18/12/2008 (url: http://survey.cvent.com/blog/cvent-survey-blog/leading-questions-lead-to-bad-data).

Logic bomb (url: http://www.techopedia.com/definition/4010/logic-bomb).

Neurohacking (url: http://en.wikipedia.org/wiki/Do_it_yourself).

NSFNet (url: http://www.nsfnet-legacy.org/about.php).

Password theft (urls: http://www.softstack.com/security/password-theft.html, http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Password_theft/default.htm).

"PHISHING AND PHARMING: A GUIDE TO UNDERSTANDING AND MANAGING THE RISKS", CPNI (Centre for the Protection of National Infrastructure), July 2010 (url: http://www.cpni.gov.uk/Documents/Publications/2010/2010019-Phishing_pharming_guide.pdf).

"Police Justice Act" (url: http://www.legislation.gov.uk/ukpga/2006/48/contents).

Resource mismatch (url: http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/resource_mismatch/default.htm).

rootkit (urls: http://en.wikipedia.org/wiki/Rootkit, http://www.webopedia.com/TERM/R/rootkit.html).

script kiddies, (urls: https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Script_kiddie.html, http://www.iss.net/security_center/advice/Underground/Hacking/Script-Kiddies/default.htm, http://www.techopedia.com/definition/4090/script-kiddie).

Shoulder surfing (url: http://searchsecurity.techtarget.com/definition/shoulder-surfing).

"SQL injection" (urls: http://en.wikipedia.org/wiki/SQL_injection, http://www.acunetix.com/websitesecurity/sql-injection/).

Source route (urls: http://linux.about.com/cs/linux101/g/source_route.htm, http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm).

"The Modus Operandi of Hacking" (url: http://www.drtomoconnor.com/3100/3100lect04.htm).

The Difference Between a Computer Virus, Worm and Trojan Horse (url: http://www.webopedia.com/DidYouKnow/Internet/virus.as).

"The conscience of a hacker" (Hacker manifesto) (url: http://www.phrack.org/archives/issues/7/3.txt).

Ορισμός "Internet of things" (url: http://www.techopedia.com/definition/28247/internet-of-things-iot).

"How to make aTrojan horse" (url: http://www.gohacking.com/make-trojan-horse/).

Virus (url: http://www.webopedia.com/TERM/V/virus.html).

Vulnerability Scanning (urls: http://www.techopedia.com/definition/4160/vulnerability-scanning, http://www.webopedia.com/TERM/V/vulnerability_scanning.html).

warez d00dz (url: http://dictionary.reference.com/browse/warez+d00dz).

Web 2.0 (url: http://www.techterms.com/definition/web20).

"What is a script kiddie?" (url: http://www.pctools.com/security-news/script-kiddie/).

"A history of hacking" (url: http://www.sptimes.com/Hackers/history.hacking.html).

«What are script kiddies" (url: http://www.wisegeek.com/what-are-script-kiddies.htm).

June 2014 Web Server Survey (url: http://news.netcraft.com/archives/category/web-server-survey/).

Internet pioneers – J. C. Licklider (url: http://www.ibiblio.org/pioneers/licklider.html).

Internet pioneers – Paul Baran (url: http://www.ibiblio.org/pioneers/baran.html.)

Black hat definition (url: http://searchsecurity.techtarget.com/definition/black-hat).

Cyber crime law (url: http://www.cybercrimelaw.net/Cybercrimelaw.html).

"Top 10 smartest hackers of all times" (url: http://thetoptenlisting.blogspot.gr/2013/11/top-10-smartest-hackers-of-all-times.html).

"Tips for hiring a hacker" (url: http://hackerforhirereview.com/tips-for-hiring-a-hacker/).

Hacker for hire (url: https://neighborhoodhacker.com/).

Hacker 1337 (url: http://www.hacker1337.com/).

Leonard Kleinrock (url: http://www.lk.cs.ucla.edu/index.html).

ΔΗΜΟΣΙΕΥΜΑΤΑ ΕΦΗΜΕΡΙΔΩΝ ΚΑΙ ΕΝΗΜΕΡΩΤΙΚΩΝ ΙΣΤΟΣΕΛΙΔΩΝ – ΔΕΛΤΙΑ ΤΥΠΟΥ (ΕΠΙΛΟΓΗ)

Booton, Jennifer, **From the Streets to Cyberspace: U.S. Gangs Turn to White-Collar Crime**, FoxBusiness, 28 Οκτωβρίου 2011 (url: http://www.foxbusiness.com/technology/2011/10/28/from-streets-to-cyberspace-us-gangs-turn-to-white-collar-crime/).

Brandom, Russell, **The NSA's elite hackers can hijack your Wi-Fi from 8 miles away**, 30 Δεκεμβρίου 2013 (url: http://www.theverge.com/2013/12/30/5256636/nsa-tailored-access-jacob-appelbaum-speech-30c3).

Cassell, Bryan – Low, **Hackers-for-Hire Are Easy to Find, The Wall Street Journal,** 23 Ιανουαρίου 2012 (url: http://online.wsj.com/news/articles/SB10001424052970203471004577145140543496380).

Chabrow, Eric, **"U.S., European Union Issue Cyber Accord - Cooperation on Data Protection, Promoting Online Human Rights"**, 27 Μαρτίου 2014 (url: http://www.bankinfosecurity.com/us-european-union-issue-cyber-accord-a-6684/op-1).

Feinstein, Ben, **Smart Shoe Takes on Wearable Technology Field**, 28 Ιουλίου 2014 (url: http://www.biznob.com/smart-shoe-takes-wearable-technology-field/3320#).

Green, Joshua, **The Myth of Cyberterrorism**, Washington Monthly, Νοέμβριος 2002 (url: http://www.washingtonmonthly.com/features/2001/0211.green.html).

Rusbridger, Alan & MacAskill, Ewen, **I, spy: Edward Snowden in exile**, συνέντευξη του Edward Snowden, εφημερίδα "The Guardian", Σάββατο 19 Ιουλίου 2014 (url:

http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill).

Riley, Michael, **"Is WikiLeaks Hacking for Secrets?"**, Bloomberg Business Week Magazine, 3 Φεβρουαρίου 2011 (url: http://www.businessweek.com/magazine/content/11_07/b4215046290051.htm).

Robertson, Jordan, "**Famous Hackers: Then and Now"**, 19 Απριλίου 2012 (url: http://www.bloomberg.com/slideshow/2012-04-18/famous-hackers-then-and-now.html#slide10).

Shell, Mary, **Fired employee admits to hacking Gucci**, 18 Ιουλίου 2012 (url: http://www.workforce.com/articles/fired-employee-admits-to-hacking-gucci).

Silvestrini, Elaine, **Ex-employee agrees to plead guilty in hacking of Tampa firm**, 3 Απριλίου 2014 (url: http://tbo.com/news/crime/ex-employee-guilty-of-hacking-tampa-firm-20140403/).

Smith, Dave, **"Computer Fraud And Abuse Act 2013: New CFAA Draft Aims To Expand, Not Reform, The 'Worst Law In Technology' "** (url: http://www.ibtimes.com/computer-fraud-abuse-act-2013-new-cfaa-draft-aims-expand-not-reform-worst-law-technology-1158515).

Smith, Gerry, **Matthew Keys Case Shows Rogue Employees Can Be Just As Dangerous As Hackers,** 19 Μαρτίου 2013 (url: http://www.huffingtonpost.com/2013/03/19/matthew-keys-rogue-employee-hackers_n_2903021.html).

Snyder, Michael, **Dumpster diving?, September 15th, 2011 (**url: http://theeconomiccollapseblog.com/archives/dumpster-diving).

Vegh, Sandor, **Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking** (url:http://firstmonday.org/ojs/index.php/fm/article/view/998/919).

Ανδριτσόπουλος, Γιάννης, **«Σκάνδαλο στο twitter - Χάκερ έκλεψαν τα δεδομένα χιλιάδων χρηστών»,** εφημερίδα «ΤΑ ΝΕΑ», Δευτέρα 4 Φεβρουαρίου 2013, σελ. 18.

Ανδριτσόπουλος, Γιάννης, **«Μαίνεται ο κυβερνοπόλεμος για τον Ασάνζ», εφημερίδα** «ΤΑ ΝΕΑ», 13 Δεκεμβρίου 2010 (url: http://www.tanea.gr/default.asp?pid=2&ct=2&artid=4608980).

Γιάνναρου, Λίνα, **Έλληνες... οι πιο καλοί οι μαθητές στο χάκινγκ,** εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 26 Φεβρουαρίου 2012 (url: http://www.kathimerini.gr/451545/article/epikairothta/ellada/ellhnes-oi-pio-kaloi-oi-ma8htes-sto-xakingk).

Δεληγιάννης, Κώστας, **«Τα 25α γενέθλιά του "γιορτάζει" σήμερα το World Wide Web»**, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 12 Μαρτίου 2014 (url: http://www.kathimerini.gr/757719/article/texnologia/diadiktyo/ta-25a-gene8lia-toy-giortazei-shmera-to-world-wide-web).

Δεληγιάννης, Κώστας, **Ο κόσμος του σκοτεινού Ίντερνετ,** εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 4 Μαΐου 2014, σελ. 29.

Λαμπρόπουλος, Βασίλειος, **«Ειρωνείες προς το θύμα στο Facebook μετά τη δολοφονία - Νέα στοιχεία για τη δολοφονία που έγινε για ένα like»**, εφημερίδα «Το Βήμα» (url: http://www.tovima.gr/society/article/?aid=405499).

Μανδραβέλης, Πάσχος, **«Ελευθερολογία πριν και μετά το Διαδίκτυο»**, εφημ. «Καθημερινή», 17 Δεκεμβρίου 2010 (url: http://www.medium.gr/internet-/3715-1659.html και http://www.kathimerini.gr/723205/opinion/epikairothta/arxeio-monimes-sthles/eley8erologia-prin-kai-meta-to-diadiktyo).

Μητροπούλου, Ειρήνη, **«"Διαρρέω", άρα υπάρχω!»**, εφημερίδα «ΤΟ ΒΗΜΑ», 24 Δεκεμβρίου 2010 (url: http://www.tovima.gr/society/article/?aid=374595).

Παπαδόπουλος, Γιάννης, **«Οι Ελληνες "πειρατές" του Διαδικτύου»**, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 10 Αυγούστου 2014 (url:

http://www.kathimerini.gr/778267/gallery/epikairothta/ereynes/oi-ellhnes-peirates-toy-diadiktyoy).

Σουλιώτης, Ιωάννης, **www.Ηλεκτρονικές απάτες.gr**, εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 26 Νοεμβρίου, 2004 (url: http://www.kathimerini.gr/201674/article/epikairothta/ellada/wwwhlektronikes-apatesgr).

Χαριτάτου, Μελίνα, **«Κυβερνο-πόλεμος ΗΠΑ-Κίνας»,** εφημερίδα «ΕΘΝΟΣ», 19/11/2010 (url: http://www.ethnos.gr/article.asp?catid=11381&subid=2&pubid=42240951).

«100.000 δολάρια η ανταμοιβή επαγγελματία χάκερ για κενό στα Windows 8.1», 11 Οκτωβρίου 2013 (url: http://tech.in.gr/news/article/?aid=1231268796).

«Η Ελληνική Χάκινγκ Σκηνή ανοίγει τα χαρτιά της», περιοδικό GADGET, αρ. τ. 129, εφημερίδα «Ελεύθερος Τύπος», Σάββατο 25 Αυγούστου 2012 (url: https://docs.google.com/viewer?url=http://www.e-typos.com/content/entheta_pdf/25hacker.pdf).

«Ελληνικό Γουοτεργκέιτ... Πολιτικός σεισμός από το σκάνδαλο παρακολούθησης κινητών τηλεφώνων», 2 Φεβρουαρίου 2006 (url: http://news.in.gr/greece/article/?aid=681341).

Hackers, Εφημερίδα «Τα ΝΕΑ – Πρόσωπα», Τεύχος 131, 08/09/2001, σελ. 14.

«Οι φυλές των χάκερ – Ένας άτυπος πόλεμος βρίσκεται σε εξέλιξη μεταξύ καλών και κακών», εφημερίδα «ΤΑ ΝΕΑ», Τετάρτη 10 Ιουλίου 2013, σελ. 30.

«**Ρώσοι χάκερς υπέκλεψαν 1,2 δισ. ονόματα χρηστών και κωδικούς πρόσβασης**», δημοσίευμα της ιστοσελίδας του τηλεοπτικού καναλιού alphatv, 6 Αυγούστου 2014 (url: http://www.alphatv.gr/news/international/rosoi-hakers-ypeklepsan-12-dis-onomata-hriston-kai-kodikoys-prosvasis).

Συνέντευξη του hacker Κέβιν Μίτνικ στο Θανάση Λάλα, ΒΗΜAgazino, 28 Νοεμβρίου 2004.

Συνέντευξη της Susan Greenfield, περιοδικό «Ε (έψιλον)», «Κυριακάτικη Ελευθεροτυπία», τ. 1037, 27 Φεβρουαρίου 2011 (συνέντευξη στον δημοσιογράφο Σπύρο Χατζηγιάννη).

«Σχετικά με το ποιόν (who is who) του μελλοντικού εγκληματία hacker», Εφημερίδα «Έθνος», 6 Απριλίου 2000, Ένθετο New Gen, σελ. 4.

Δελτίο τύπου European Commission - IP/14/129 10/02/2014 «Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο – ένας χρόνος μετά» (url: http://europa.eu/rapid/press-release_IP-14-129_el.htm).

«Η δημοκρατία του διαδικτύου κινδυνεύει - Σήμα κινδύνου από τον δημιουργό του, Τιμ Μπέρνερς- Λι», 22 Νοεμβρίου 2013 (url: http://www.newsbeast.gr/technology/arthro/611783/i-dimokratia-tou-diadiktuou-kinduneuei-/).

«Η Ελληνική Χάκινγκ Σκηνή GHS έχει αποκτήση πλήρης πρόσβαση σε όλα τα Πρωτοδικεία και Εφετεία!», 31 Οκτωβρίου 2012 (url: http://attikanea.blogspot.gr/2012/10/ghs.html).

«Η ιστορία του διαδικτύου», 11 Ιουνίου 2012 (url: http://tvxs.gr/news/internet-mme/i-istoria-toy-diadiktyoy).

«Πώς οι χάκερς «κλέβουν» τα προσωπικά μας δεδομένα από τα iPhone», ρεπορτάζ της εφημερίδας «Πρώτο Θέμα», 27 Ιουλίου 2014 (url: http://www.protothema.gr/technology/article/398146/iphone-allow-extraction-of-personal-data/)

«Διάτρητα τα συστήματα IT κυβερνητικών και αμυντικών οργανισμών, λέει η Kaspersky», 30 Αυγούστου 2013 (url: http://tech.in.gr/analysis/article/?aid=1231263192).

«Κυβερνοπόλεμος ακτιβιστών κατά της βιομηχανίας μουσικής και κινηματογράφου», ενημερωτική ιστοσελίδα www.in.gr, 20 Σεπτεμβρίου 2010 (url: http://news.in.gr/science-technology/article/?aid=1231059839).

«Κυβερνοτρομοκρατία» (url: http://www.eeei.gr/interbiz/articles/sarin.htm).

«Λογοκρισία και διαδίκτυο», 20 Δεκεμβρίου 2013 **(**url: http://www.euro2day.gr/news/highlights/article-news/1167473/logokrisia-sto-diadiktyo.html).

«Με τους Greek Hacking Scene... Δεκατριάχρονος κατηγορείται από την αστυνομία για συμμετοχή σε ομάδα χάκερ», ενημερωτική ιστοσελίδα www.in.gr, 27 Ιουνίου 2012 (url: http://news.in.gr/greece/article/?aid=1231202376).

«Μεγάλη επίθεση οργανώθηκε από την Ελληνική Χάκινγκ Σκηνή GHS!", 30 Ιανουαρίου 2013 (url: http://www.newsbomb.gr/politikh/story/275005/megali-epithesi-organothike-apo-tin-elliniki-hakingk-skini-ghs).

«Μέλη του «Greek Hacking Scene» - Σε τρεις μαθητές λυκείου αποδίδεται η κυβερνοεπίθεση στο υπουργείο Δικαιοσύνης», ενημερωτική ιστοσελίδα www.in.gr, 20 Φεβρουαρίου 2012 (url: http://news.in.gr/science-technology/article/?aid=1231182589).

«Ο Α' Παγκόσμιος Κυβερνοπόλεμος!», περιοδικό "Focus", Τρίτη 10 Φεβρουαρίου 2009 (url: http://www.focusmag.gr/articles/view-article.rx?oid=410433).

«Οι 10 καλύτεροι Έλληνες χάκερς», (url: http://www.youtube.com/watch?v=LxPlt1ImDaU).

«Ονοματεπώνυμο σε τρία ακόμα μέλη της Greek Hacking Scene», ενημερωτική ιστοσελίδα www.in.gr, 5 Μαρτίου 2012 (url: http://tech.in.gr/news/article/?aid=1231184730).

«Πώς δόθηκαν στη δημοσιότητα οι αποκαλύψεις του WikiLeaks», 29 Νοεμβρίου 2010 (url: http://tvxs.gr/news/%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5%CF%84-%CE%BC%CE%BC%CE%B5/%CF%80%CF%8E%CF%82-%CE%B4%CF%8C%CE%B8%CE%B7%CE%BA%CE%B1%CE%BD-%CF%83%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%BF%CF%83%CE%B9%CF%8C%CF%84%CE%B7%CF%84%CE%B1-%CE%BF%CE%B9-

%CE%B1%CF%80%CE%BF%CE%BA%CE%B1%CE%BB%CF%8D%CF%88%CE%B5%CE%B9%CF%82-%CF%84%CE%BF%CF%85-wikileaks).

«Στόχος ηλεκτρονικών επιθέσεων αμερικανικές εμπορικές αλυσίδες», εφημερίδα «ΚΑΘΗΜΕΡΙΝΗ», 25 Ιανουαρίου 2014 (url: http://www.kathimerini.gr/553853/article/oikonomia/die8nhs-oikonomia/stoxos-hlektronikwn-epi8esewn-amerikanikes-emporikes-alysides).

«Σοκ με την 17χρονη που δολοφονήθηκε από γνωριμία στο Facebook: Της χορήγησαν δια της βίας ηρωίνη», 30 Δεκεμβρίου 2013 (url: http://www.koolnews.gr/crime/sok-me-thn-17xronh-pou-dolofonithike-apo-gnwrimia-sto-facebook-ths-xorhghsan-dia-ths-vias-hrwinh/).

«Συνωμοσία της Πυρίτιδας: Remember, remember, the 5th of November», 5 Νοεμβρίου 2013 (url: http://tvxs.gr/news/%CF%83%CE%B1%CE%BD-%CF%83%CE%AE%CE%BC%CE%B5%CF%81%CE%B1/%CE%B8%CF%85%CE%BC%CE%AE%CF%83%CE%BF%CF%85-%CF%84%CE%B7%CE%BD-5%CE%B7-%CE%BD%CE%BF%CE%B5%CE%BC%CE%B2%CF%81%CE%AF%CE%BF%CF%85-%CF%84%CE%B7-%CF%83%CF%85%CE%BD%CF%89%CE%BC%CE%BF%CF%83%CE%AF%CE%B1-%CF%84%CE%B7%CF%82-%CF%80%CF%85%CF%81%CE%AF%CF%84%CE%B9%CE%B4%CE%B1%CF%82).

«Τζούλιαν Ασάνζ: από το χάκινγκ στα... βουλευτικά έδρανα;», 30 Ιανουαρίου 2013 (url: http://gr.euronews.com/2013/01/30/assange-wikileaks-elections-senate-australia-ekloges-ypopsifiotita/).

«Το Internet γίνεται 25 ετών», 12 Μαρτίου 2014 (url: http://tvxs.gr/news/internet-mme/internet-ginetai-25-eton).

«Χάκερς απειλούν…ψυγεία και οδοντόβουρτσες», εφημερίδα larissanet.gr, 15 Ιανουαρίου 2014 (url: http://www.larissanet.gr/2014/01/15/hackers-apeiloun-psygeia-kai-odontovourtses/).

"Αυτός είναι ο 17χρονος «ταλαντούχος» χάκερ που έγινε συνεργάτης της Δίωξης Ηλεκτρονικού Εγκλήματος", ενημερωτική ιστοσελίδα «Το κουτί της

Πανδώρας», 13 Ιουλίου 2014 (url: http://www.koutipandoras.gr/article/118088/aytos-einai-o-17hronos-talantoyhos-haker-poy-egine-synergatis-tis-dioxis-ilektronikoy).

«**WikiLeaks: Η 11η Σεπτεμβρίου της διπλωματίας**», 20 Νοεμβρίου 2010 (url: http://tvxs.gr/news/%CE%BA%CF%8C%CF%83%CE%BC%CE%BF%CF%82/wikileaks-%CE%B7-11%CE%B7-%CF%83%CE%B5%CF%80%CF%84%CE%B5%CE%BC%CE%B2%CF%81%CE%AF%CE%BF%CF%85-%CF%84%CE%B7%CF%82-%CE%B4%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%AF%CE%B1%CF%82).