ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
**Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών**

**ΝΟΜΙΚΗ ΣΧΟΛΗ**
**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**
**ΤΟΜΕΑ ΠΟΙΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΠΑΝΕΠΙΣΤΗΜΙΑΚΑ ΕΤΗ: 2015-2017**

## ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**της Σταυρούλας-Αντιγόνης Παναγιώτη Πριλή**
**Α.Μ.: 868/2015**

# Η παράνομη πρόσβαση σε πληροφοριακό σύστημα κατ' αρ. 370Γ §2 Ποινικού Κώδικα
# -
# *"Hacking"*

**Επιβλέπων:**
κ. Δημητράτος Νικόλαος, Λέκτορας Ποινικού Δικαίου-Ποινικής Δικονομίας

Αθήνα, Νοέμβριος 2017

# Πίνακας Περιεχομένων

## ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Σε παγκόσμια κλίμακα η τεχνολογία των ηλεκτρονικών υπολογιστών, η χρήση του διαδικτύου και η πληροφορική εν γένει εξελίσσεται με ραγδαίους ρυθμούς, εμφανίζοντας το παράδοξο αφενός μεν να κατακλύζει την διαδικασία παραγωγής και εξέλιξης άλλων τομέων και τεχνολογιών της καθημερινής ζωής του σύγχρονου ανθρώπου, και αφετέρου να καθιστά σχεδόν ανέφικτη την παρακολούθηση της εξέλιξης αυτής, με ό,τι τούτο συνεπάγεται, από τον ίδιο (!). Η δε εγκληματικότητα με μέσο τέλεσης ή αντικείμενο τον ηλεκτρονικό υπολογιστή έχει καταστεί η πλέον προσιτή και προτιμώμενη από τον μέσο δράστη επιλογή. Αξίζει να αναφερθεί στο σημείο αυτό ότι το ηλεκτρονικό έγκλημα εν γένει διαφέρει και υπερέχει από το «κοινό» κυρίως σε ταχύτητα, ευκολία και προσβασιμότητα.

Στο πλαίσιο αυτό δεν θα μπορούσε να μην έλξει το ενδιαφέρον του σύγχρονου νομικού το ισχύον πλαίσιο για την πρωταρχική, λογικά και δικαικά, πράξη: την πρόσβαση σε ένα πληροφοριακό σύστημα. Στο ελληνικό ποινικό δίκαιο, η επίμαχη πράξη ρυθμίζεται από τη διάταξη του αρ. 370 Γ παρ. 2 επ. του Ποινικού Κώδικα, η οποία μάλιστα έχει πολύ εύστοχα χαρακτηρισθεί ως *«ο πυρήνας του ελληνικού ποινικού δικαίου πληροφορικής»*[1]. Μάλιστα, έχει ειπωθεί ότι, μαζί με άλλες συναφείς θεματικά διατάξεις *«διακρίνεται από ευρεία διατύπωση και είναι τεχνολογικά ουδέτερη, έτσι ώστε να ελαχιστοποιείται ο κίνδυνος να καταστεί παρωχημένη λόγω των ραγδαίων εξελίξεων στο πεδίο της πληροφορικής»*[2].

Υπό το πρίσμα των ανωτέρω η παρούσα εργασία, εκπονηθείσα στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών του Τομέα Ποινικών Επιστημών της Νομικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, πραγματεύεται το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα. Ειδικότερα, στοχεύει να εκθέσει σύντομα το σχετικό νομοθετικό πλαίσιο σε διεθνές και ενωσιακό επίπεδο και να εξετάσει την ποινική διάταξη του αρ. 370Γ παρ. 2 επ., ως αυτή ισχύει σήμερα, κατόπιν της τροποποίησης που επέφερε ο Ν. 4411/2016[3]. Η γράφουσα θα αναφερθεί και στην προϊσχύουσα μορφή της διάταξης[4],

[1]Ιδ. Βασιλάκη Ε. «Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών» σελ. 83 επ.
[2]Ιδ. Φιλόπουλο Π. «Ποινική Προστασία Απορρήτου, Συστηματική Ερμηνεία άρθρων 370-371 ΠΚ», σελ. 167.
[3]Ιδ. ΦΕΚ Α' 142/ 03.08.2016 http://www.et.gr/index.php/2013-01-28-14-06-23/2013-01-29-08-13-13
[4]Η οποία εισήχθη με τον Ν. 1805/1988, κατά τα γερμανικά πρότυπα και συγκεκριμένα σύμφωνα με την διάταξη 202a StGB 1986 για την «χωρίς άδεια απόκτηση δεδομένων». Στον γερμανικό ΠΚ,

επισημαίνοντας αναλυτικά τις αλλαγές που έλαβαν χώρα, θα παραθέσει την συρροή της ισχύουσας διάταξης με άλλες ποινικές διατάξεις, καθώς και την νομολογιακή της αντιμετώπιση. Τέλος, αφού παρατεθούν συνοπτικά τα πορίσματα της έκθεσης αξιολόγησης της Ευρωπαϊκής Επιτροπής αναφορικά με την μεταφορά της Οδηγίας 2013/40/ΕΕ στο εθνικό δίκαιο, φιλοδοξείται όπως πραγματοποιηθεί μία κριτική αποτίμηση ως προς το κατά πόσον τελικά το ισχύον αρ. 370Γ §2 ΠΚ καλύπτει ή βελτιώνει τα «κενά» μιας ανέκαθεν ευρέος πεδίου εφαρμογής ποινικής διάταξης.

## ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

### Α. Διεθνές και Ευρωπαϊκό Νομοθετικό Πλαίσιο

Στις αρχές της δεύτερης χιλιετίας, με δεδομένες τις θεμελιώδεις αλλαγές που επέφερε η ψηφιοποίηση, η σύγκλιση και η συνεχιζόμενη παγκοσμιοποίηση των δικτύων υπολογιστών, το έντονο ενδιαφέρον της διεθνούς κοινότητας για την πρόληψη και την καταστολή του κυβερνοεγκλήματος αποτυπώθηκε **στις 23.11.2001 στην Σύμβαση του Συμβουλίου της Ευρώπης, στη Βουδαπέστη για το έγκλημα στον κυβερνοχώρο (εφεξής Σύμβαση)**. Συγκεκριμένα στο προοίμιο της εν λόγω σύμβασης ορίστηκε ρητά ότι: *«**είναι αναγκαία για να αποτρέψει τις ενέργειες που στρέφονται κατά του απορρήτου, της ακεραιότητας και της διαθεσιμότητας των συστημάτων υπολογιστών, των δικτύων υπολογιστών και των ηλεκτρονικών δεδομένων**, καθώς και την μη νόμιμη χρήση των συστημάτων, δικτύων και δεδομένων με την ποινικοποίηση αυτής ..{..} έχοντας κατά νου {..} και τις άλλες ισχύουσες συμβάσεις προστασίας των ανθρωπίνων δικαιωμάτων, οι οποίες επιβεβαιώνουν **το δικαίωμα κάθε ανθρώπου να έχει την γνώμη του** χωρίς παρεμβάσεις καθώς **και το δικαίωμα της ελευθερίας της έκφραση στο οποίο**, περιλαμβάνεται και η ελευθερία της αναζήτησης, λήψης και διανομής πληροφοριών και ιδεών παντός είδους, ανεξαρτήτως συνόρων, καθώς **και τα δικαιώματα που αφορούν τον σεβασμό απορρήτου**»*[5].

Επί τη βάσει αυτή και *«με σκοπό να επιτευχθεί προσέγγιση των διατάξεων των εγχώριων ποινικών δικαίων και να καταστεί δυνατή η χρήση αποτελεσματικών μέσων έρευνας των εγκλημάτων αυτών»*, μεταξύ άλλων, διατυπώθηκαν οι νέες νομοθετικά

ομοίως με τον ελληνικό, ο έγκλημα εντάσσεται στο κεφάλαιο της προσωπικής σφαίρας-απορρήτου. Ίδ. αναλυτικά Αργυρόπουλο «Ηλεκτρονική εγκληματικότητα» σελ. 58 επ.

[5]Ιδ. ΦΕΚ Α΄ 142/03.08.2016 σελ.7752.

έννοιες-ορισμοί: ***«σύστημα υπολογιστή», «δεδομένα υπολογιστών», «δεδομένα κίνησης***» και ως προς τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο, στο εθνικό δηλαδή ουσιαστικό ποινικό δίκαιο, θεσπίστηκε **στο Τμήμα Ι *«των εγκλημάτων κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών»*, το άρθρο 2 που αφορά το έγκλημα *«της παράνομης πρόσβασης»*[6].** Σύμφωνα με αυτό, αξιόποινη πράξη είναι η άνευ δικαιώματος πρόσβαση στο σύνολο ή σε μέρος ενός συστήματος υπολογιστή, όταν αυτή διαπράττεται από πρόθεση. Ένα συμβαλλόμενο μέρος μπορεί να θέσει ως προϋπόθεση διάπραξης του εγκλήματος την παραβίαση μέτρων ασφαλείας, με την πρόθεση να αποκτηθούν δεδομένα υπολογιστή, ή με άλλη αθέμιτη πρόθεση. Περαιτέρω**, στο άρθρο 6 της Σύμβασης με τίτλο *«κακή χρήση συσκευών»* ρητά προβλέφθηκε το έγκλημα της εκ προθέσεως διάπραξης προπαρασκευαστικών πράξεων** (δηλαδή της πώλησης, κατοχής κλπ συσκευών, προγραμμάτων Η/Υ, κωδικών πρόσβασης κλπ ), **μεταξύ άλλων εγκλημάτων, και του προαναφερομένου άρθρου 2,** και μάλιστα δόθηκε η δυνατότητα στα συμβαλλόμενα κράτη να θέσουν ως προϋπόθεση την κατοχή ενός ελάχιστου αριθμού τέτοιων αντικειμένων προκειμένου να θεμελιώσουν ποινική ευθύνη.

Λίγο αργότερα, σε ενωσιακό επίπεδο **το έτος 2005 το Συμβούλιο της Ευρωπαϊκής Ένωσης**, ερειδόμενο στον υπερεθνικό χαρακτήρα των σύγχρονων συστημάτων πληροφοριών, και ως εκ τούτου στην διασυνοριακή διάσταση των συναφών εγκλημάτων, τόνισε την ανάγκη να υπάρξει προσέγγιση των ποινικών δικαίων στο συγκεκριμένο τομέα (κοινοί ορισμοί και κοινή προσέγγιση για τα στοιχεία της αντικειμενικής υπόστασης των ποινικών αδικημάτων)[7], με σαφή μεν μνεία περί αποφυγής υπερβολικής ποινικοποίησης, αυστηρότερες δε κυρώσεις όταν τα σχετικά αδικήματα έχουν προκαλέσει σοβαρές ζημιές, έχουν θίξει θεμελιώδη συμφέροντα ή έχουν τελεστεί στο πλαίσιο εγκληματικής οργάνωσης.

Έτσι, υπό το πρίσμα των ανωτέρω, **εξεδόθη η Απόφαση-Πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της Ευρωπαϊκής Ένωσης της 24ης.02.2005 (εφεξής Απόφαση-Πλαίσιο)** για τις επιθέσεις κατά συστημάτων πληροφοριών, **στο άρθρο 1 της οποίας οριοθετήθηκαν οι έννοιες** του «συστήματος πληροφοριών», των «ηλεκτρονικών δεδομένων» και της «χωρίς δικαίωμα» πρόσβασης, **και στο άρθρο 2 θεσπίστηκε το αδίκημα της «παράνομης πρόσβασης σε σύστημα**

[6]Ιδ. προαναφερόμενο ΦΕΚ Α΄ 142/2016 σελ.7754.
[7]Ιδ. σκέψεις 10 και 11 Απόφασης-Πλαίσιο.

**πληροφοριών»,** με διακριτική ευχέρεια του κάθε κράτους μέλους να θεμελιώνει ή μη, σχετικό αξιόποινο μόνο όταν το αδίκημα διαπράττεται κατά παράβαση μέτρου ασφαλείας. Περαιτέρω, **στο άρθρο 5 ορίσθηκε** ότι κάθε κράτος μέλος θα τιμωρεί ως ποινικό αδίκημα την «ηθική αυτουργία, την υποβοήθηση και την συνέργεια» στην ανωτέρω πράξη, αφήνοντας ωστόσο αρρύθμιστη την ποινική αντιμετώπιση των συναφών προπαρασκευαστικών πράξεων.

Κάποια χρόνια αργότερα, και με ακόμη επιτακτικότερη την ανάγκη συνεργασίας μεταξύ κρατών-μελών, αρμοδίων αρχών και υπηρεσιών, **το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης** επαναπροσδιόρισε το νομοθετικό **πλαίσιο για τις επιθέσεις κατά συστημάτων πληροφοριών**, αντικαθιστώντας ρητά την Απόφαση-Πλαίσιο του Συμβουλίου της Ευρωπαϊκής Ένωσης **με την από 12.08.2013 Οδηγία 2013/40/ΕΕ (εφεξής Οδηγία)**, σύμφωνα με το άρθ. 83 παρ. 1 της Συνθήκης για την Λειτουργία της Ευρωπαϊκής Ένωσης, προβλέποντας ποινικές κυρώσεις **τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας**[8]. Στην **σκέψη 15** της Οδηγίας αποσαφηνίζεται ρητά ότι **η Σύμβαση του Συμβουλίου της Ευρώπης του 2001 για το έγκλημα στον κυβερνοχώρο** αποτελεί **το νομικό πλαίσιο αναφοράς** για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, (συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών) **και βάση της εν λόγω Οδηγίας,** ενώ λίγο παρακάτω **στην σκέψη 34, ο σκοπός της Οδηγίας συνίσταται στην τροποποίηση και επέκταση των διατάξεων της Απόφασης-Πλαίσιο παρέχοντας εξαρχής το κύριο ερμηνευτικό εργαλείο.** Και αυτό διότι, όπως εκτίθεται κυρίως στις σκέψεις 2, 4 και 6, τα συστήματα πληροφοριών είναι βασικό στοιχείο για την πολιτική, κοινωνική και οικονομική αλληλεπίδραση στην Ένωση και η κοινωνία εξαρτάται σε υψηλό και αυξανόμενο βαθμό από τέτοια συστήματα. Υπάρχουν δε στοιχεία, που δείχνουν μια τάση διάπραξης όλο πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη-μέλη ή για ειδικές δραστηριότητες του δημοσίου ή του ιδιωτικού τομέα. Ενώ τέλος, ιδιαίτερη μνεία γίνεται για τα εργαλεία που μπορούν να χρησιμοποιηθούν για την διάπραξη των αδικημάτων που αναφέρονται στην Οδηγία[9], με έμφαση στην αποφυγή της ποινικοποίησης μέσω απαίτησης συνδρομής στο

[8]Ιδ. σκέψη 11 της Οδηγίας
http://eur-lex.europa.eu/legacontent/EL/TXT/PDF/?uri=CELEX:32013L0040&from=EN
[9]Ιδ. σκέψη 16 της Οδηγίας.

πρόσωπο του δράστη άμεσης πρόθεσης χρησιμοποίησης των εργαλείων για την διάπραξη αυτών των αδικημάτων.

Υπό το πρίσμα συνεπώς των ανωτέρω σκέψεων, **στο άρθρο 2 της Οδηγίας** δόθηκαν εκ νέου **οι ορισμοί** των εννοιών *«σύστημα πληροφοριών», «ηλεκτρονικά δεδομένα»* και *«χωρίς δικαίωμα»*, **στο άρθρο 3** τυποποιήθηκε *«η παράνομη πρόσβαση σε συστήματα πληροφοριών»* και **στο άρθρο 7** με τίτλο *«εργαλεία που χρησιμοποιούνται για την διάπραξη των αδικημάτων»*, προβλέφθηκε η ποινικοποίηση των προπαρασκευαστικών πράξεων. Στο σημείο αυτό οφείλει να διασαφηνιστεί πως αναφορικά με το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα τόσο η προϊσχύουσα Απόφαση-Πλαίσιο όσο και η Οδηγία έχουν το ίδιο περιεχόμενο, με μόνη διαφορά ότι η Οδηγία απαιτεί ρητά παραβίαση μέτρου ασφαλείας για να θεμελιωθεί ποινικά ευθύνη για παράνομη πρόσβαση σε πληροφοριακό σύστημα και πλέον με την Οδηγία ποινικοποιώντας οι συναφείς προπαρασκευαστικές πράξεις. Έτσι, με αυτές τις ρυθμίσεις η Οδηγία πράγματι έχει ως νομικό πλαίσιο αναφοράς την Σύμβαση του Συμβουλίου της Ευρώπης[10], την οποία και ακολουθεί.

Τέλος, **στο άρθρο 16** προβλέφθηκε ως απώτατο χρονικό όριο μεταφοράς των ρυθμίσεων της Οδηγίας στα εθνικά δίκαια των κρατών-μελών η 4η.09.2015, και στο **άρθρο 17** προβλέφθηκε ως απώτατο χρονικό όριο η 4η.09.2017 προκειμένου η Επιτροπή να υποβάλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αναφορικά με την αξιολόγηση των επιμέρους μέτρων που έχουν λάβει τα κράτη-μέλη, και ως εκ τούτου την συμμόρφωση τους προς τις ρυθμίσεις της Οδηγίας, για τον οποία θα γίνει λόγος παρακάτω.

## Β.Αναγκαίες εθνικές νομοθετικές παρεμβάσεις με τον Ν. 4411/2016

Πράγματι, η από 23.11.2001 Σύμβαση για το έγκλημα στον κυβερνοχώρο σε συνδυασμό με την πρόσφατη ισχύουσα Οδηγία, παρέχουν στον εκάστοτε εθνικό νομοθέτη, και κατ' επέκταση στον εφαρμοστή του Δικαίου, ένα πλήρες ρυθμιστικό πλαίσιο αναφορικά με τις επιθέσεις κατά πληροφοριακών συστημάτων εκσυγχρονίζοντας έτσι το νομικό οπλοστάσιο. Με την θέσπιση της Οδηγίας, πέραν της υποχρέωσης που δημιουργήθηκε στα κράτη-μέλη, προκειμένου να υιοθετήσουν τους ελάχιστους κοινούς σχετικούς με το παρόν ζήτημα ποινικούς κανόνες, ρυθμίστηκε σε ευρωπαϊκό πλαίσιο: η αρρύθμιστη με την Απόφαση-Πλαίσιο

[10]Ιδ. σκέψη 15 της Οδηγίας.

περίπτωση των προπαρασκευαστικών πράξεων, εισήχθησαν ποινικές κυρώσεις για την δημιουργία των «botnets» (δίκτυα προγραμμάτων-ρομποτ)[11], παρασχέθηκε επαρκές υλικό μέσω των αρκετών σκέψεων της Οδηγίας για την επίλυση τυχόν ερμηνευτικών ζητημάτων, διευρύνθηκε το πεδίο εφαρμογής της Σύμβασης από σύστημα υπολογιστή σε σύστημα πληροφοριών. Επιπροσθέτως, αναγνωρίσθηκε ρητά ως **νομικό πλαίσιο-βάση για το έγκλημα στον κυβερνοχώρο** η Σύμβαση και προωθήθηκε η διευκόλυνση της πρόληψης της εγκληματικότητας στον Κυβερνοχώρο, με την βελτίωση της συνεργασίας μεταξύ των αρμοδίων εθνικών αρχών και υπηρεσιών.

Ο Έλληνας νομοθέτης με **τον Ν. 4411/2016 κύρωσε την** από 23.11.2001 Σύμβαση του Συμβουλίου της Ευρώπης, καθιστώντας την αναπόσπαστο μέρος του εσωτερικού ελληνικού δικαίου με αυξημένη μάλιστα τυπική ισχύ κατ' άρθρο 28 Σ.[12], **και μετέφερε** στο εθνικό δίκαιο **την Οδηγία**. Η δε Σύμβαση με την Οδηγία συμβαδίζουν όπως εκτέθηκε αναλυτικά παραπάνω συνεπώς δεν προκύπτουν ζητήματα αντινομίας. Ειδικότερα, ως προς το εξεταζόμενο στην παρούσα εργασία ποινικό αδίκημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα, η συμμόρφωση του ελληνικού ποινικού δικαίου με τις ρυθμίσεις της Σύμβασης και κυρίως της πλέον σύγχρονης Οδηγίας πραγματοποιήθηκε: **α)** με την εισαγωγή των όρων «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα» στο άρθρο 13 του ΠΚ, **β)** την αντικατάσταση της παρ. 2 του αρ. 370$^{Γ}$ ΠΚ και **γ)** την εισαγωγή του νέου άρ. 370$^{Ε}$ ΠΚ που ποινικοποιεί τις προπαρασκευαστικές πράξεις μεταξύ άλλων και του αρ. 370Γ παρ. 2 και 3.

Προτού εκτεθούν και εξεταστούν αναλυτικά τα επιμέρους στοιχεία της νέας ειδικής υποστάσεως του 370Γ παρ. 2 επ., πρέπει να επισημάνουμε ότι πρόκειται, όπως ήδη αναφέρθηκε, **για μία ποινική διάταξη με μεγάλο εύρος εφαρμογής** και αυτό διότι πλέον μετά τις ρυθμίσεις **του Ν. 4411/2016, ποινικοποιείται υπό συγκεκριμένες προϋποθέσεις κάθε παράνομη πρόσβαση, όχι απλά σε ηλεκτρονικό υπολογιστή, αλλά σε σύστημα πληροφοριών, είτε εν όλω είτε εν μέρει, δηλαδή το αποκαλούμενο στην γλώσσα των δραστών «hacking»[13],[14].**

[11]Δηλαδή την εξ' αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών δια της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο, η οποία περίπτωση αναφέρεται στο προοίμιο της Οδηγίας αρκετά ανησυχητική. Ίδ. Φιλόπουλο σελ. 171.
[12]Ιδ. Μαυριά Κ. «Συνταγματικό Δίκαιο» σελ. 275.
[13]Ιδ. σελ. 6 της αιτιολογ. έκθεσης Ν. 4411/2016 https://www.forin.gr/downloads/download/2867/n-4411-2016-aitiologikh-ekthesh .

Καίτοι θα αναπτυχθεί εκτενώς παρακάτω, αξίζει να αναφερθεί ότι η διεύρυνση αυτή ήταν επιτακτική, καθώς η διάδοση και επικράτηση του διαδικτύου δημιούργησε νέα «μορφώματα» αξιόποινης συμπεριφοράς, τα οποία δεν καλύπτονταν πλέον από τις υπάρχουσες ποινικές διατάξεις, όπως είχε επανειλημμένα επικριθεί από την Θεωρία[15].

Κι αυτή η ποινική απαξία που θέτει ο νομοθέτης υφίσταται χωρίς να παίζει ρόλο μία σειρά άλλων παραγόντων. Πιο συγκεκριμένα, αναφέρεται όλως συνοπτικά για τις ανάγκες καλύτερης κατανόησης του παρόντος κεφαλαίου, ότι **είναι ποινικά αδιάφορο στο πλαίσιο του αρ. 370Γ παρ. 2 επ.:** **1)** το «πράγματι απόρρητο» των πληροφοριών που περιλαμβάνει το εκάστοτε προσβληθέν πληροφοριακό σύστημα, **2)** η τυχόν πρόθεση τέλεσης ή η τέλεση οποιασδήποτε άλλης πράξης μετά την απόκτηση πρόσβασης, **3)** το πρόσωπο στο οποίο τυχόν αφορούν οι πληροφορίες-δεδομένα, **4)** η κυριότητα των υλικών φορέων του πληροφοριακού συστήματος, **5)** η τυχόν οικονομική αξία των υλικών φορέων του πληροφοριακού συστήματος και η τυχόν περιουσιακή ζημία που θα προκύψει από την παράνομη πρόσβαση. Αυτοί οι παράμετροι θα αναπτυχθούν μόνο στο πλαίσιο συρροής της διάταξης του αρ. 370 Γ παρ. 2 με άλλες ποινικές διατάξεις , ενώ το κατά πόσον ο εθνικός νομοθέτης συμμορφώθηκε αποτελεσματικά εν τοις πράγμασι στις επιταγές στις οποίες κλήθηκε, θα αναπτυχθεί εξίσου κατωτέρω.

## ΤΟ ΕΓΚΛΗΜΑ ΤΟΥ ΑΡΘΡΟΥ 370Γ § 1 Π.Κ.

Στο πλαίσιο εξέτασης του αδικήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα της παρ. 2 του 370Γ ΠΚ, είναι αναγκαίο να γίνει και μία σύντομη έκθεση των βασικών στοιχείων του αδικήματος της παρ. 1. Το σύντομο της αναφοράς αυτής, οφείλεται στην διαφορετικότητα του αδικήματος, το οποίο και έχει μείνει αυτούσιο από το έτος 1988 οπότε και εισήχθη, εν σχέσει με το αδίκημα της παρ. 2.

Πλέον ειδικά με την πρώτη κιόλας ανάγνωση της διάταξης, γίνεται αντιληπτό ότι η παρ.1 έχει **εξαιρετικά στενό υλικό αντικείμενο**, δεδομένου ότι θεμελιώνει αξιόποινο για όποιον χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί **προγράμματα**

[14]Οι εν λόγω δράστες ονομάζονται «hackers» και διακρίνονται από τους «crackers», καθώς οι πρώτοι είθισται να αποκτούν πρόσβαση κυρίως από ευχαρίστηση, ενώ οι δεύτεροι με σκοπό κυρίως οικονομικό όφελος. Ιδ. σχετικά με σκιαγράφηση προφίλ εγκληματία του κυβερνοχώρου. Ίδ. περισσότερα στο άρθρο του Αγγελή Ι. «Διαδίκτυο και ποινικό δίκαιο, Έγκλημα στον κυβερνοχώρο» ΠοινΧρον Ν 2000, σελ. 677 .

[15]Ιδ. Κιούπη « Αθέμιτη Πρόσβαση στα δεδομένα» Υπεράσπιση 2000, σελ. 972.

**ηλεκτρονικών υπολογιστών.** Προστατευόμενο λοιπόν έννομο αγαθό στην παράγραφο αυτή είναι **τα προγράμματα ηλεκτρονικών υπολογιστών** ως περιουσιακό αγαθό, **και μάλιστα η οικονομική αξία της πληροφορίας**[16], εκ διαμέτρου δηλαδή αντίθετο από το κατά την κρατούσα έως τώρα άποψη αγαθό του τυπικού απορρήτου των επόμενων παραγράφων του αρ. 370Γ ΠΚ. Στην εισηγητική έκθεση του Ν. 1805/1988 αναφέρεται σαφώς: *«κρίθηκε αναγκαία η θέσπιση της διάταξης αυτής **αν ληφθεί υπόψιν η μεγάλη δαπάνη** η οποία απαιτείται για την παραγωγή προγραμμάτων καθώς και ο οξύτατος ανταγωνισμός που έχει αναπτυχθεί στον κλάδο αυτό».*

Το αυτό έχει κριθεί μάλιστα και στην σχετική εισαγγελική πρόταση του υπ' αριθμ. 3204/1993 Βουλεύματος του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης[17], η οποία ενστερνιζόμενη την άποψη της Βασιλάκη και την προαναφερόμενη εισηγητική έκθεση αναφέρει επί λέξει : *« Η διάταξη λοιπόν αυτή προστατεύει τα προγράμματα των υπολογιστών **ως ένα ιδιαίτερο περιουσιακό αγαθό** **που εκφράζει κάποια οικονομική αξία ανάλογη με τη φύση του προγράμματος, το κόστος παραγωγής**».*

Εκτός των ανωτέρω επισημάνσεων, χρήζει ρητής αναφοράς πως με την παρούσα διάταξη δεν **προστατεύεται** το μηχανικό μέρος («hardware»[18]) του ηλεκτρονικού υπολογιστή, αλλά **το λογισμικό** («software»)**, δηλαδή τα προγράμματα και τα δεδομένα που έχουν αποθηκευθεί στην μνήμη του ηλεκτρονικού υπολογιστή ή των περιφερειακών συσκευών του**[19]. Αυτό θα μπορούσε να λεχθεί είναι ίσως και το μόνο κοινό σημείο της § 1 με την § 2 της διάταξης, καίτοι αφορούν διαφορετικά εγκλήματα, και τα δύο σχετίζονται με προγράμματα και δεδομένα, και όχι με το μηχανικό-υλικό μέρος (hardware) ενός πληροφοριακού συστήματος. **Προστατεύεται δε, οποιοδήποτε είδος προγράμματος, α)** ανεξαρτήτως του αν συγκεντρώνει τα χαρακτηριστικά του έργου πνευματικής ιδιοκτησίας, β) **ανεξαρτήτως** του **αν είναι απόρρητο** και γ) **ανεξαρτήτως συγκεκριμένης οικονομικής αξίας.**

---

[16]Ιδ. Βασιλάκη σελ. 103-104. Στο σημείο αυτό αξίζει να αναφέρουμε πως η άποψη αυτή περί της οικονομικής αξίας της πληροφορίας της παρ. 1, κατά την γνώμη της γράφουσας συνάδει και έρχεται να συμπληρώσει την άποψη της Βασιλάκη ότι προστατευόμενο αγαθό στην παρ. 2 του 370Γ είναι η πληροφορία αυτή καθεαυτή και το δικαίωμα εξουσίασης και διαθέσεως της σελ. 83, όπως θα αναλυθεί στο οικείο κεφάλαιο (προστατευόμενο έννομο αγαθό).

[17]Υπεράσπιση 1994, σελ. 1133 επ. με εισαγγελική πρόταση Κ. Χατζηπαζαρλή και Παρατηρήσεις Νούσκαλη.

[18]Ιδ. Βλαχόπουλο «Ηλεκτρονικό έγκλημα», Γλωσσάρι όρων πληροφορικής σελ. 217.

[19]Ιδ. ερμηνεία κατ' άρθρο Ποινικού Κώδικα Χαραλαμπάκη & Γιαννίδη, 2009, σελ. 1035.

**Ως Πρόγραμμα** ηλεκτρονικού υπολογιστή δε, νοείται μια ενότητα οδηγιών και κανονισμών που περιέχουν τα αναγκαία στοιχεία για την λύση ενός προβλήματος[20], και κατατάσσονται σε τρεις κατηγορίες α) ανάλογα με την βαθμίδα ανάπτυξης τους: σε πηγαία ή ή αντικειμενικά προγράμματα, β) ανάλογα με το ποιος είναι ο αποδέκτης τους υπολογιστής ή χρήστης σε: προγράμματα συστημάτων ή εφαρμογών αντίστοιχα και γ) ανάλογα με τον αριθμό των προσώπων που τα χρησιμοποιούν σε: ατομικά και προγράμματα για πολλούς χρήστες[21].

Η αξιόποινη συμπεριφορά του αρ. 370Γ παρ. 1 στοιχειοθετείται όταν **χωρίς δικαίωμα ο δράστης (εν όλω ή εν μέρει) αντιγράφει,** δηλαδή ενσωματώνει πιστά σε κάποιον υλικό φορέα το πρόγραμμα ώστε να μπορεί να γίνει κατανοητό άμεσα ή έμμεσα από τον άνθρωπο[22], **ή χρησιμοποιεί,** δηλαδή εκμεταλλεύεται-απολαμβάνει τις ωφέλειες των λειτουργιών του προγράμματος, το εκτελεί[23],[24]. Αξίζει να αναφερθεί στο σημείο αυτό, πως **την πράξη της παρ. 1 τελεί** και ο δράστης όπου χρησιμοποιεί τα προγράμματα του ηλεκτρονικού υπολογιστή για να διεκπεραιώσει υποθέσεις που δεν ανήκουν στον κύκλο εργασιών του εργοδότη του[25], πρόκειται για την κοινώς λεγόμενη **«κλοπή χρόνου ή time theft».**

Όσον αναφορά την έννοια του «**χωρίς δικαίωμα**», η σημασία της είναι αντίστοιχη αυτής που θα αναλυθεί εκτενώς στο πλαίσιο του 370Γ παρ. 2, ήτοι όλως επιγραμματικά αναφέρεται ότι νοείται η ενέργεια του δράστη που πραγματοποιείται **χωρίς την συγκατάθεση του νομίμου κατόχου του προγράμματος.**

## Κριτική της παρ. 1 ως προς την συστημική της τοποθέτηση

Έχοντας εκθέσει τα βασικά στοιχεία της παρ. 1 της διάταξης του αρ. 370Γ, και εν όψει των όσων θα παρατεθούν κατωτέρω σχετικά με την παρ. 2 επ., δέον όπως επιχειρηθεί η τοποθέτηση της γράφουσας **στην κριτική και τους προβληματισμούς περί εσωτερικών προβλημάτων συνοχής και συνάφειας[26]** της συγκεκριμένης

[20]Ιδ. Φιλόπουλο σελ. 174.
[21]Ιδ. Βασιλάκη σελ. 106 επ. κατηγορίες προγραμμάτων.
[22]Ιδ. αναλυτικότερα Βασιλάκη σελ. 115 .
[23]Ιδ. Κιούπη «Ποινικό Δίκαιο και Ίντερνετ», 1999, σελ. 141, όπου αναφέρει ότι σε κάποιες περιπτώσεις όταν ο δράστης αποστείλει ιό και αυτός ενεργοποιηθεί στον υπολογιστή του θύματος. ο αποστολέας του ιού χρησιμοποιεί χωρίς δικαίωμα κάποιο πρόγραμμα του θύματος πληρώντας το αρ. 370Γ παρ.1 .
[24]Ιδ. σχετικά με την έννοια και τα όρια της χρήσης του αρ. 370Γ παρ. 1 Βασιλάκη σελ 116-124.
[25]Ιδ. Μυλωνόπουλο «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», Σειρά Ποινικά σελ. 89.
[26]Ιδ. σχετικά Κιούπη «Το δίκαιο στην Ψηφιακή Εποχή, Προστασία Προσωπικότητας-Σύγχρονες Μορφές Εγκλήματος-Ηλεκτρονικό Επιχειρείν» συνέδριο e-θεμις, σελ. 158.

διάταξης, δεδομένου ότι τόσο το προστατευόμενο έννομο αγαθό όσο και η αξιόποινη συμπεριφορά των δύο παραγράφων καθ' ολοκληρία διαφέρουν.

**Η θέση της Βασιλάκη** ότι η παρ. 2 του 370Γ[27] αποτελεί το πυρήνα για την δημιουργία του ποινικού δικαίου πληροφορικής και συνεπώς είναι εμφανής η εξωτερική συνάφεια με την παρ. 1, οι οποίες αμφότερες αφορούν το χώρο της πληροφορικής, **κατά την γνώμη της γράφουσας** δεν είναι καθόλου πειστική υπό τα ισχύοντα σήμερα. Αν και θα μπορούσε να υποστηριχθεί, κατά την άποψη της (Βασιλάκη), πως ο ποινικός νομοθέτης κατά το χρόνο εισαγωγής της διάταξης το έτος 1988 με το τότε νεοεισαχθέν αρ. 370Γ προσπάθησε κατά το δυνατόν να ρυθμίσει τα βασικά ζητήματα που αφορούσαν τον ανερχόμενο τομέα της πληροφορικής και να δημιουργήσει μία νέα αυτόνομη διάταξη, εν τούτοις με την τροποποίηση της είκοσι εννέα (29) έτη μετά, με τον Ν. 4411/2016, τα προβλήματα συνοχής και συνάφειας του 370Γ όχι μόνο δεν φαίνεται να επιλύθηκαν, τουναντίον εντάθηκαν.

Κι αυτό διότι ο νομοθέτης **δεν επέφερε καμία μεταβολή** στην παρ. 1. (!) **αγνοώντας** όλα τα εκκρεμή ζητήματα, ήτοι: α) την γενικότητα της διατύπωσης της παρ. 1, β) την έλλειψη ορισμού στον ΠΚ του τεχνικού όρου «πρόγραμμα ηλεκτρονικού υπολογιστή», γ) την ύπαρξη σχετικών ειδικών ποινικών νόμων, δ) τα ζητήματα συρροής της με άλλες ποινικές διατάξεις όπως λόγου χάρη αυτές για την πνευματική ιδιοκτησία, **εξακολουθεί και διατηρεί την παρ. 1** που προστατεύει τα προγράμματα ως περιουσιακό αγαθό στο κεφάλαιο περί προστασίας απορρήτων του ΠΚ, και μάλιστα στην διάταξη που πλέον αφορά την πρόσβαση σε **πληροφοριακά συστήματα (!) προσθέτοντας έτσι ακόμη ένα.**

**Επιπροσθέτως δε,** με την εισαγωγή της περ.θ΄ στο άρθ. 13 (με τον Ν. 4411/2016) ενέταξε το «πρόγραμμα» στην έννοια των «ψηφιακών δεδομένων», τα δε ψηφιακά δεδομένα στην έννοια του «πληροφοριακού συστήματος» της περ. η΄, και ποινικοποίησε με το νεοεισαχθέν άρθρο 292Β την «παρακώλυση λειτουργίας πληροφοριακών συστημάτων» προκαλώντας εννοιολογική σύγχυση. Κατ' επέκταση προκλήθηκε και ζήτημα εφαρμογής των σχετικών διατάξεων μη καθιστώντας σαφές ποιο είναι το υλικό αντικείμενο της διάταξης. Ενδεικτικά αναφέρεται το εξής παράδειγμα: Επί τη βάσει των ανωτέρω, το πρόγραμμα αποτελεί μέρος του πληροφοριακού συστήματος σύμφωνα με τις περιπτώσεις των στ. η΄ & θ΄ του αρ. 13. Απορίας άξιον είναι τι σχέση θα έχει **η χωρίς δικαίωμα διαβίβαση προγραμμάτων**

[27]Ιδ. Βασιλάκη σελ. 93 επ.

(ψηφιακών δεδομένων πλέον) **του αρ. 292Β** παρ. 1 με την **χωρίς δικαίωμα αντιγραφή προγραμμάτων** του **370Γ παρ. 1** ;! Σε ποια διάταξη δηλαδή θα υπάγουμε την εν λόγω αξιόποινη συμπεριφορά **;!**

**Ως εκ τούτου, διαφαίνεται πως ο νομοθέτης άφησε αναλλοίωτη μία ρύθμιση η οποία τόσο από πλευράς υλικού αντικειμένου, όσο και από πλευράς συστημικής τοποθέτησης, καταλήγει να είναι ασύνδετη και ανεφάρμοστη για όλους τους προαναφερόμενους λόγους.**

## ΠΡΟΣΤΑΤΕΥΟΜΕΝΟ ΕΝΝΟΜΟ ΑΓΑΘΟ-ΝΟΜΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΑΡΘΡΟΥ 370 Γ § 2 Π.Κ.

Το ζήτημα του εννόμου αγαθού που προστατεύει το αρ. 370 Γ § 2 τείνει να είναι ένα από τα πλέον αμφιλεγόμενα ζητήματα στο πλαίσιο της παρούσας εκπονηθείσας εργασίας, ιδιαίτερα μετά τις αλλαγές που επέφερε ο Ν. 4411/2016. Η απόφανση δε, επ' αυτού είναι εξαιρετικά σημαντική καθότι θα σηματοδοτήσει καθοριστικό ρόλο στην κατάταξη του αδικήματος ως έγκλημα βλάβης ή διακινδύνευσης όπως θ' αναπτυχθεί παρακάτω.

Καταρχήν, κοινό τόπο αποτελεί πως **η παρ. 1 του αρ. 370Γ**, έχει ως προστατευόμενο έννομο αγαθό τα προγράμματα Η/Υ ως ένα περιουσιακό αγαθό που ενσωματώνει οικονομική αξία · αυτό προκύπτει και από την αιτιολογική έκθεση του Ν. 1508/1988, συνεπώς το παρόν δεν πρόκειται να μας απασχολήσει παραπάνω.

Προχωρώντας στην εξέταση της διάταξης του αρ. **370Γ παρ. 2, παρατηρείται πως** τιμωρείτο όποιος αποκτούσε πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, και πλέον μετά την τροποποίηση του Ν. 4411/2016, όποιος αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών.

Με δεδομένη την παραπάνω διατύπωση και λαμβάνοντας υπόψιν την συστημική θέση της διάταξης στο 22ο (εικοστό δεύτερο) κεφάλαιο του Ποινικού Κώδικα περί παραβίασης απορρήτων, έχουν διατυπωθεί διάφορες απόψεις αναφορικά με το έννομο αγαθό, δηλαδή την κοινωνική-ηθική αξία που σκοπεύει να προστατεύσει ο νόμος και η οποία προσβάλλεται κάθε φορά, όπου ο δράστης πλήττει

ένα συγκεκριμένο πρόσωπο ή ένα συγκεκριμένο αντικείμενο, το οποίο έχει επιλέξει ο νομοθέτης για να εξατομικεύσει το προστατευόμενο έννομο αγαθό[28].

Από την γραμματική και μόνο ερμηνεία, προκύπτει καταρχήν ότι πρόκειται **για ατομικό έννομο αγαθό** και όχι υπερατομικό, καθώς φορέας του δύναται να είναι κάποιο φυσικό πρόσωπο[29] και συγκεκριμένα το νόμιμο κάτοχο του πληροφοριακού συστήματος. Δεν αφήνεται δε, κανένα περιθώριο να γίνει λόγος για την **προστασία κάποιου περιουσιακού αγαθού, αλλά ούτε και την προστασία του απορρήτου εν στενή εννοία ή «ατομικό απόρρητο» όπως χαρακτηριστικά το ορίζει ο Μανωλεδάκης**, καθώς κάτι τέτοιο θα προϋπέθετε ρητή αναφορά στην αντικειμενική υπόσταση του εν λόγω αδικήματος, (όπως στο άρθρο 370Β), και κατ' επέκταση συνδρομή συγκεκριμένων κριτηρίων που θα έκριναν το απόρρητο αυτό[30]. Κατά τον Μανωλεδάκη[31], τα στοιχεία που αναφέρονται στα εγκλήματα του κεφαλαίου του ΠΚ περί απορρήτων δεν σχετίζονται πχ. με τις συναλλαγές ή την διακίνηση αγαθών, αλλά με ένα συγκεκριμένο κάτοχο και την προσωπική ελευθερία αυτού να έχει δικό του, απαραβίαστο χώρο. Υπό το πρίσμα των ανωτέρω απόψεων, ο ίδιος υποστηρίζει πως στην διάταξη του αρ. 370Γ παρ. 2 ως προστατευόμενο έννομο αγαθό δεν είναι το ατομικό απόρρητο-απόρρητο υπό ουσιαστική έννοια, διότι δεν τίθενται κάποιου είδους κριτήρια. Τα στοιχεία δε προστατεύονται ανεξάρτητα από τον αποδέκτη ή το πρόσωπο που αφορούν. **Συνεπώς δεν μπορεί να γίνει λόγος ούτε για προστασία δεδομένων προσωπικού χαρακτήρα.** Έτσι ο **Μανωλεδάκης** συντάσσεται με την κρατούσα μέχρι σήμερα θέση (που διέπει και τα υπόλοιπα εγκλήματα του συγκεκριμένου κεφαλαίου), σύμφωνα με την οποία προστατευόμενο με την διάταξη

[28]Ιδ. Κωστάρα, σχετικά με νομικό αντικείμενο σελ.77 & «Έννοιες και θεσμοί του ποινικού δικαίου», ανατύπωση 2008 σελ. 103.

[29]Με εξαίρεση το εδ. β' όπου η πράξη σχετίζεται με τις διεθνείς σχέσεις ή την ασφάλεια του κράτους.

[30]Κατά τον Μανωλεδάκη, τα «απόρρητα» υπηρετούν βασικά το αγαθό της προσωπικής ελευθερίας του ανθρώπου, ωστόσο ιδίως στη σύγχρονη εποχή , όπου με τα μέσα της τεχνολογίας συρρικνώνεται επικίνδυνα η ιδιωτική σφαίρα του ατόμου η αυτονόμηση των «απορρήτων» από την προσωπική ελευθερία προκειμένου να του παρασχεθεί καλύτερη προστασία κρίνεται εύλογη. Πρόκειται δηλαδή για σημαντικό αυτοτελές ατομικό έννομο αγαθό. Η αυτοτέλεια του «ατομικού απορρήτου» φαίνεται καθαρά, αφού το ίδιο υλικό αντικείμενο ως «πράγμα » που ανήκει, δηλαδή ως ιδιοκτησία μπορεί να έχει φορέα άλλο πρόσωπο, από αυτό που εμπεριέχει η εμπιστευτική πληροφορία η οποία συνδέεται με διαφορετικό άτομο. Ο φορέας του πρώτου αγαθού μπορεί να το διαθέσει ως ιδιοκτησία του, δεν μπορεί όμως να το διαθέσει το αγαθό του 'ατομικού απορρήτου', αφού αυτό έχει άλλον φορέα. Ίδ. περισσότερα στο έργο του «Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου», σελ. 359 επ.

[31]Ο Δημητράτος στο έργο του «Έννομο αγαθό και διδασκαλία περί εγκλήματος στο ποινικό δίκαιο», σελ. 280-287, παραθέτει την διαλεκτική έννοια του εννόμου αγαθού στη διδασκαλία του Μανωλεδάκη και υποστηρίζει πως συνιστά τη μόνη ολοκληρωμένη σχετική διδασκαλία που γνώρισε η ελληνική ποινική επιστήμη έως και σήμερα. Με όλες τις επιφυλάξεις που διατυπώνει στο εν λόγω έργο του, καταλήγει πως η θεωρία του Μανωλεδάκη δικαιωματικά αποτελεί «μία από τις αφετηρίες κάθε γόνιμου προβληματισμού για το ζήτημα αυτό, ακόμη κι όταν ο προβληματισμός οδηγεί κάποτε στην απόρριψη της».

του αρ. 370Γ παρ. 2 έννομο αγαθό είναι **το απόρρητο υπό τυπική έννοια ή «τυπικό απόρρητο», το οποίο υπηρετεί το απαραβίαστο της ιδιωτικής ζωής**[32]. Την ίδια ως άνω άποψη υιοθετεί και **ο Μυλωνόπουλος**[33]**,** δηλαδή το προστατευόμενο έννομο αγαθό συνίσταται στο τυπικό δικαίωμα του νομίμου κατόχου των στοιχείων-δεδομένων να αποκλείει άλλους από την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό ουσιαστική έννοια[34]. Στην ίδια κατεύθυνση φαίνεται να κινείται και **ο Φιλόπουλος** που θεωρεί ως προστατευόμενο έννομο αγαθό **τον ιδιωτικό βίο, και ειδικότερα το δικαίωμα διάθεσης του δικαιούχου-νομίμου κατόχου,** στην ιδιωτική σφαίρα του οποίου ανήκουν τα στοιχεία-δεδομένα ή προγράμματα Η/Υ. Κατ' αυτόν, το αντικείμενο προστασίας περιλαμβάνει από την μία την προστασία προσωπικών δεδομένων (ιδιωτική σφαίρα), καθόσον ποινικοποιείται η προσβολή του δικαιώματος στην πληροφοριακή αυτοδιάθεση-στον πληροφοριακό αυτοπροσδιορισμό, και από την άλλη προστατεύονται επίσης στοιχεία και προγράμματα τα οποία δεν ανήκουν πλέον στην ιδιωτική σφαίρα του δικαιούχου διάθεσης, έχουν όμως γι' αυτόν ιδεατή, οικονομική ή επιστημονική αξία.

Στο ίδιο πνεύμα, **ο Κιούπης και η Καϊάφα-Γκμπάντι**[35] θεωρούν ως αυτοτελές έννομο αγαθό **το απόρρητο των ηλεκτρονικών δεδομένων**, ως έκφανση της ιδιότητας τους να ανήκουν σε κάποιον. Έτσι λοιπόν, ο κάτοχος ανεξαρτήτως σε ποιον αφορούν τα δεδομένα αυτά, αν αποτελούν δημιουργήματα του έχει το δικαίωμα ν' αποκλείει την πρόσβαση σε αυτό. Γι' αυτό λοιπόν και η συγκατάθεση του κατόχου αποτελεί λόγο αποκλεισμού του καταρχήν αδίκου και όχι λόγο άρσης αδίκου αυτού. Διαπιστώνεται λοιπόν πως κατά την κρατούσα άποψη προστατευόμενο έννομο αγαθό της διάταξης είναι αυτό του τυπικού απορρήτου.

Ωστόσο, έχουν υποστηριχθεί και αντίθετες απόψεις όπως αυτή της Βασιλάκη και του Σπυρόπουλου. **Η Βασιλάκη** ρητά υιοθέτησε την άποψη πως η διάταξη του αρ. 370Γ παρ. 2 προστατεύει **την πληροφορία ως έννομο αγαθό**[36]. Μάλιστα, κατ' αυτήν η προστασία των στοιχείων ενός Η/Υ ή των στοιχείων που μεταδίδονται δεν είναι αυτοσκοπός, δεν μας ενδιαφέρουν δηλαδή τα στοιχεία αυτά καθεαυτά, παρά **μόνο η έκφραση της αξίας που προκύπτει απ' αυτά: της πληροφορίας**. Με αυτό τον τρόπο η πληροφορία και ειδικότερα το δικαίωμα εξουσίας και διάθεσης της,

[32]Ιδ. Χρυσόγονο Κ. «Ατομικά και Κοινωνικά Δικαιώματα», σελ. 251 επ.
[33]Ιδ. «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο» σελίδα 92.
[34]Ιδ. Συμβ.Πλημμ.Θεσσ. 3204/1993, Εισαγγ. Προτ Χατζηπαζαρλή, Υπερ. 1994, σελ.1136.
[35]Ιδ. Καιάφα-Γκμπάντι «Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής» Αρμενόπουλος, 2007 σελ. 1066.
[36]Ιδ. Βασιλάκη σελ. 83, 101-102.

συνιστούν ένα νέο έννομο αγαθό. Πρόκειται με άλλα λόγια, για το δικαίωμα του νόμιμου κατόχου να διαθέτει τις πληροφορίες που προκύπτουν από τα στοιχεία αυτά και να τις εξουσιάζει αξιώνοντας κανείς άλλος να μην αποκτά πρόσβαση σε αυτά, είτε στο φυσικό είτε στο τεχνικό χώρο που αυτός έχει οριοθετήσει. Έτσι προστατεύεται η πληροφορία υπό την έκφανση ενός δικαιώματος με θετικό περιεχόμενο και ενός άλλου δικαιώματος με αρνητικό περιεχόμενο. Δέον όπως σχολιασθεί , ότι η άποψη της Βασιλάκη ανάγει την πληροφορία ήδη από το έτος 1993, σ' ένα αυτοτελές έννομο αγαθό και πράγματι θα μπορούσε να υιοθετηθεί ως βάσιμη.

Ο **Σπυρόπουλος**[37], αφενός τονίζοντας ότι για να προσεγγίσουμε το προστατευόμενο έννομο αγαθό της διάταξης δεν πρέπει να στηριχθούμε μόνο στην γραμματική διατύπωση και την συστημική της θέση **και αφετέρου εμφανώς επηρεασμένος από τις σκέψεις της Οδηγίας[38]** θεωρεί πως με το αρ. 370Γ παρ. 2 προστατεύεται **ένα νέο έννομο αγαθό, η ασφάλεια των ηλεκτρονικών πληροφοριών και το δικαίωμα του έχοντος την εξουσία διάθεσης επ' αυτών στην άρτια και απεριόριστη δυνατότητα χρησιμοποίησης τους, η οποία εμπεριέχει την εμπιστευτικότητα[39], την ακεραιότητα[40] και την διαθεσιμότητα[41] των στοιχείων**.

Ωστόσο η θέση αυτή, η οποία άλλωστε επικαλύπτεται από την πληροφορία την οποία υιοθέτησε η Βασιλάκη, μοιάζει να δυσχεραίνει το ήδη θολό τοπίο και να γενικεύει την έννοια των εννόμων αγαθών, ενώ υπό το πρίσμα του αρ. 370 Γ παρ. 2 γίνεται αναφορά σε κάτι πολύ πιο οριοθετημένο, διότι η ασφάλεια των πληροφοριών και το δικαίωμα διάθεσης πάλι καταλήγουν στο τυπικό απόρρητο. Σε κάθε δε περίπτωση, θα μπορούσε να υποστηρίξει κανείς πως το απόρρητο-εμπιστευτικότητα των στοιχείων αποτελεί θεμέλια λίθο για την ακεραιότητα και διαθεσιμότητα αυτών, συνεπώς η ασφάλεια περιττεύει και καταλήγει να συνιστά μια έκφανση του εννόμου αγαθού του απορρήτου.

---

[37]Ιδ. Σπυρόπουλος Φ. «Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών», σελ. 180.

[39]δηλαδή το απόρρητο των πληροφοριών που ενσωματώνουν και η ιδιότητα τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες.

[40]δηλαδή την ιδιότητα τους να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, η αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας.

[41]δηλαδή την ιδιότητα τους να καθίστανται άμεσα προσπελάσιμα σε κάθε εξουσιοδοτημένο χρήστη του συστήματος.

**Κατά την γνώμη της γράφουσας,** δεδομένου ότι: 1) τα στοιχεία του πληροφοριακού συστήματος στα οποία αποκτά πρόσβαση ο δράστης προστατεύονται ανεξαρτήτως περιεχομένου χωρίς την συνδρομή χαρακτηριστικών που να τα καθιστούν απόρρητα υπό ουσιαστική έννοια και 2) οι υλικοί φορείς είναι ποινικά αδιάφοροι, καθίσταται πρόδηλο ότι κρίσιμη είναι η σύνδεση των στοιχείων με ένα συγκεκριμένο πρόσωπο. Το δε πρόσωπο αυτό, επιθυμεί ένα «προσωπικό πληροφοριακό» χώρο στον οποίο αποκλείει την πρόσβαση σε τρίτους. Αυτή του την βούληση την εξωτερικεύει μέσω απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει . Ως εκ τούτου, ακόμη και μετά τις τροποποιήσεις που επέφερε ο Ν. 4411/2016, **θεωρείται ορθότερο προστατευόμενο έννομο αγαθό της διάταξης να εξακολουθεί να είναι το τυπικό απόρρητο,** ειδικά αν λάβουμε υπόψιν την ρητή αξίωση του νομοθέτη **η χωρίς δικαίωμα πρόσβαση να λαμβάνει χώρα απαραιτήτως με την παραβίαση απαγορεύσεων ή μέτρων ασφαλείας (!).** Ορθά άλλωστε, ο Φιλόπουλος τονίζει την βαρύτητα των θυματολογικών εκτιμήσεων στο χώρο της ποινικής προστασίας των απορρήτων, όπου ο νομοθέτης επεμβαίνει **εφόσον** ο νόμιμος κάτοχος έχει λάβει τα απαραίτητα μέτρα και μέσω αυτών έχει εκφράσει σαφώς την βούληση του. Τέλος, το τυπικό απόρρητο ως προστατευόμενο έννομο αγαθό ενισχύεται και εκ του γεγονότος ότι τιμωρείται η χωρίς δικαίωμα πρόσβαση, χωρίς να απαιτείται κάποια άλλη προσβολή, η οποία τυχόν θα σχετιζόταν με την οικονομική ή άλλη αξία των στοιχείων του πληροφοριακού συστήματος κ.ο.κ. Συνεπώς, **ορθότερο είναι να θεωρηθεί ως έννομο αγαθό είναι το τυπικό απόρρητο εντασσόμενο στην έννοια της προστασίας του απαραβίαστου της ιδιωτικής ζωής.**

## ΦΟΡΕΑΣ ΕΝΝΟΜΟΥ ΑΓΑΘΟΥ: ΝΟΜΙΜΟΣ ΚΑΤΟΧΟΣ

Φορέας του εννόμου αγαθού, και ως εκ τούτου παθών σε περίπτωση τέλεσης του αδικήματος, είναι όπως σαφώς ορίζει η παρ. 2 του αρ. 370Γ **ο έχων την εξουσία διάθεσης** του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται, δηλαδή **ο νόμιμος κάτοχος τους**, είτε πρόκειται για φυσικό πρόσωπο είτε για νομικό πρόσωπο. Είναι δε ποινικά αδιάφορο για το υπό εξέταση ποινικό αδίκημα του αρ. 370Γ παρ. 2, ποιον αφορούν τα στοιχεία του πληροφοριακού συστήματος ή τα στοιχεία που μεταδίδονται, ή ποιος είναι κύριος των εκάστοτε υλικών φορέων. Τα ως άνω πρόσωπα προστατεύονται από έτερες ποινικές διατάξεις, όπως θα αναλυθεί στο

οικείο κεφάλαιο περί συρροής του εγκλήματος του αρ. 370Γ παρ. 2 με άλλα εγκλήματα.

**Ως κατοχή δε,** νοείται εκείνη η πραγματική κατάσταση που παρέχει σε κάποιον την δυνατότητα να απολαμβάνει κάθε είδους ωφέλεια του εννόμου αγαθού[42] όπως η φύση του το επιτρέπει. Εν προκειμένω, **νόμιμος κάτοχος** στο πλαίσιο του αρ. 370Γ παρ. 2 είναι αυτός που έχει την **δυνατότητα να ορίζει ποιος, με ποιες προϋποθέσεις και σε ποιο τμήμα του πληροφοριακού συστήματος** ή των στοιχείων που μεταδίδονται μπορεί να έχει πρόσβαση. Είναι δηλαδή αυτός που έχει την δυνατότητα πρόσβασης σ' αυτό **και** δικαίωμα διάθεσης. Μέσω των απαγορεύσεων και των ληφθέντων μέτρων ασφαλείας, εξωτερικεύει κατά τρόπο αντικειμενικό και διαγνώσιμο το ειδικό του ενδιαφέρον για την διαφύλαξη απορρήτου και «αποδεικνύει» συνεπώς την κατοχή του. Δέον όπως σημειωθεί σε αυτό το σημείο, πως τα μέτρα ασφαλείας δύνανται να μην έχουν ληφθεί από τον νόμιμο κάτοχο, αλλά από το δικαιοπάροχο του και αυτός να τα διατηρεί[43]. Σημασία έχει δηλαδή ποιου προσώπου την «σφαίρα διάθεσης» οριοθετούν και προστατεύονται και όχι ποιος τα έχει λάβει.

Σε περίπτωση δε, που πρόκειται για **πλείονα άτομα ως νόμιμους κατόχους,** όταν ένας εξ' αυτών ενεργεί και αποκτά πρόσβαση χωρίς την συναίνεση των υπολοίπων (δηλαδή χωρίς δικαίωμα) καθίσταται αυτουργός της πράξης της παράνομης πρόσβασης [44], καθότι ενεργεί καθ' υπέρβαση της εξουσίας διαθέσεως και του δικαιώματος που του αναλογεί ως προς τους λοιπούς συγκατόχους[45].

Εξ' ορισμού, **περίπτωση πλειόνων ατόμων έχουμε στην περίπτωση των στοιχείων που ήδη μεταδίδονται με συστήματα τηλεπικοινωνιών.** Ειδικότερα, νόμιμοι κάτοχοι εδώ και ως εκ τούτου φορείς του εννόμου αγαθού, τυγχάνουν τόσο ο «πομπός» που στέλνει τα δεδομένα-αποστολέας όσο και ο «δέκτης» αυτών-παραλήπτης. Χαρακτηριστικό παράδειγμα αποτελεί η παρακολούθηση εκπομπών από ηλεκτρονικό υπολογιστή μέσω ιντερνέτ. Έτσι, κάτοχος εδώ είναι όχι μόνο ο παραγωγός της εκπομπής αλλά και αυτός που αποκτά κατ' ορισμένο τρόπο τις πληροφορίες του συγκεκριμένου προγράμματος-εκπομπής.

[42]Ιδ. Α. Κονταξή Ερμηνεία Ποινικού Κώδικα, σελ. 3154-3155.
[43]Ιδ. Μυλωνόπουλο «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ ΚΑΙ 386 Α ΠΚ» Σειρά Ποινικά, σελ. 98.
[44]Ιδ. Φιλόπουλο σελ. 176.
[45]Ιδ. Βασιλάκη σελ. 91.

**Με τον νόμιμο κάτοχο είτε πρόκειται για ένα είτε για περισσότερα πρόσωπα δεν πρέπει να συγχέεται ο βοηθός ή ο φύλακας κατοχής. Αυτοί** δεν έχουν την δυνατότητα εξουσίας, έστω και αν έχουν πρόσβαση στην πληροφορία, αφού μόνο επικουρούν τον νόμιμο κάτοχο να επενεργεί στο έννομο αγαθό, ασκώντας την εξουσία διαθέσεως του.

Ξεχωριστή περίπτωση συνιστά αυτή που ο νόμιμος κάτοχος έχει δώσει σε κάποιον τρίτο την δυνατότητα να έχει πρόσβαση στο πληροφοριακό σύστημα μεταξύ τους **υφίσταται σχέση εργοδότη-εργαζομένου, η οποία θα εξετασθεί παρακάτω στο πλαίσιο του αρ. 370Γ παρ. 3,** που αφορά τέλεσης της πράξης από «υπόχρεο σε πίστη δράστη».

Τέλος για τις ανάγκες πληρότητας του παρόντος κεφαλαίου, αξίζει να αναφερθεί πως δύναται ν' αποκτηθεί νόμιμα πρόσβαση, πλην της συγκατάθεσης του νομίμου κατόχου, όταν αυτό προβλέπεται από διάταξη νόμου όπως πχ. στην περίπτωση του αρ. 253 ΚΠΔ, το οποίο αναπτυχθεί στην αντίστοιχη ενότητα.

## ΥΛΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΑΡΘΡΟΥ 370 Γ § 2 Π.Κ.

Η βασικότερη εκ των τροποποιήσεων που επέφερε ο Ν. 4411/2016, **ήταν η αλλαγή του νομικού αντικειμένου** της οικείας διάταξης, δηλαδή του πράγματος-ενσώματου αντικειμένου **επί του οποίου επενεργεί ο δράστης** και έτσι πληρεί την αντικειμενική υπόσταση του οικείου εγκλήματος. Ειδικότερα αυτό **διευρύνθηκε** από στοιχεία που έχουν εισαχθεί σε: «υπολογιστή ή περιφερειακή μνήμη ή μεταδίδονται με συστήματα τηλεπικοινωνιών **σε** «σύνολο ή τμήμα πληροφοριακού συστήματος» ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών. Προς τούτο εισήχθη **στο αρ. 13 ΠΚ ο όρος «πληροφοριακό σύστημα»** ο οποίος συνίσταται **σε συσκευή ή ομάδα** διασυνδεδεμένων ή σχετικών μεταξύ τους **συσκευών,** εκ των οποίων μία ή περισσότερες εκτελούν σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς **και τα ψηφιακά δεδομένα** που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται **από την εν λόγω συσκευή ή την ομάδα συσκευών** με σκοπό την λειτουργία, την χρήση, την προστασία και την συντήρηση των συσκευών αυτών. Εν συνεχεία, **ως έννοια ψηφιακών δεδομένων ορίστηκε** η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα,

συμπεριλαμβανομένου προγράμματος που παρέχει την δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.

Εκτός λοιπών των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών ως παραμένον υλικό αντικείμενο της διάταξης, τα στοιχεία που είναι αποθηκευμένα ή υφίστανται επεξεργασία από έναν ηλεκτρονικό υπολογιστή ή περιφερειακές του μνήμες (εσωτερικές η εξωτερικές, δισκέτες, usb, cd-roms μαγνητοταινίες κλπ.) αντικαταστάθηκαν **από τις συσκευές που εκτελούν επεξεργασία ψηφιακών δεδομένων** [πληροφοριακό σύστημα].

**Η αντικατάσταση αυτή, και συνεπώς η διεύρυνση του πεδίου εφαρμογής της διάταξης ήταν το λιγότερο επιτακτική**, δεδομένου ότι η επεξεργασία δεδομένων και η χρήση του διαδικτύου καθίσταται εφικτή σήμερα από σωρεία συσκευών, γνωστότερες των οποίων είναι: κινητά τηλέφωνα-smartphones, tablets, i-pads, laptops, notebooks, παιχνιδομηχανές που συνδέονται στο διαδίκτυο μέσω τεχνολογίας wi-fi (x-box, playstation) κλπ, μία μόνο εκ των οποίων είναι πλέον ο ηλεκτρονικός υπολογιστής. Η πράξη της παράνομης πρόσβασης σε πληροφοριακό σύστημα μπορεί λοιπόν να τελεστεί με μία εκ των ανωτέρω συσκευών. **Ως εκ τούτου, χωρίς την διεύρυνση του υλικού** της αντικειμένου η διάταξη του αρ. 370Γ παρ. 2 **θα ήταν σχεδόν ανεφάρμοστη**.

### Α. Ως προς το πρώτο σκέλος του υλικού αντικειμένου περί πληροφοριακού συστήματος :

Αν και πράγματι η θέσπιση της εν λόγω διάταξης ήταν αναγκαία για την προστασία των ψηφιακών-ηλεκτρονικών δεδομένων, είναι εν μέρει προβληματική καθώς δημιουργεί ένα κενό. Πιο συγκεκριμένα ως έχει διατυπωθεί η διάταξη, φαίνεται να προστατεύει τα ψηφιακά δεδομένα που βρίσκονται εντός ενός πληροφοριακού συστήματος (αρ. 13 στ.θ΄ ΠΚ), ήτοι όταν αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται η διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό την λειτουργία, την χρήση, την προστασία και την συντήρηση των συσκευών αυτών. Επί τη βάσει της γραμματικής ερμηνείας της διάταξης, δεν φαίνεται να προστατεύονται όσα βρίσκονται εκτός πληροφοριακού συστήματος όπως πχ. σε κάποια φορητή εξωτερική μνήμη, και δεν εκτελούν σύμφωνα με ένα πρόγραμμα αυτόματη επεξεργασία κλπ.

**Β. Ως προς το δεύτερο σκέλος του υλικού αντικειμένου περί στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών:**

Η μεταφορά των δεδομένων μπορεί να είναι είτε αναλογική είτε ψηφιακή, (ενσύρματη ή ασύρματη). Εδώ εμπίπτει η περίπτωση μετάδοσης ψηφιακών συστημάτων μέσω μιας κοινής (αναλογικής) τηλεφωνικής γραμμής. Όταν ο υπολογιστής-πομπός στέλνει ένα μήνυμα, το modem του μετατρέπει το μήνυμα από ψηφιακή σε αναλογική μορφή, κατάλληλη να μεταδοθεί μέσω της τηλεφωνικής γραμμής (διαμόρφωση) και να αναγνωριστεί έτσι από τον υπολογιστή-δέκτη το modem του οποίου μετατρέπει το αναλογικό σήμα που δέχεται από την τηλεφωνική γραμμή σε ψηφιακό. Με την διάταξη σκοπείται, λοιπόν, η ποινική καταστολή κάθε αυθαίρετης ακρόασης (λήψης) μεταδιδόμενων στοιχείων παγίδευσης δικτύων-αγωγών μετάδοσης δεδομένων, ακρόασης επικοινωνιών που μεταδίδονται ψηφιακά (digitally transmitted information), καθώς και κάθε περίπτωσης πρόσβασης σε ξένα συστήματα επεξεργασίας ή αποθήκευσης δεδομένων, όπως λ.χ. της χωρίς δικαίωμα πρόσβασης του δράστη σε τράπεζα πληροφοριών μέσω τηλεφωνικού δικτύου. Πρέπει να τονιστεί ότι, με την προκείμενη διάταξη προστατεύονται τα στοιχεία που ήδη μεταδίδονται με συστήματα τηλεπικοινωνιών και όχι ήδη αποθηκευμένα στο πληροφοριακό σύστημα ή σε κάποια περιφερειακή μνήμη, καθώς τα τελευταία εμπίπτουν στην πρώτη κατηγορία του υλικού αντικειμένου της διάταξης. Αυτός άλλωστε είναι ο λόγος που ο νομοθέτης τόσο κατά την εισαγωγή της διάταξης το έτος 1988, όσο και μετά την τροποποίηση της το έτος 2016, διαχώρισε τις δύο περιπτώσεις στοιχείων, καλύπτοντας έτσι επιτυχώς όλες τις δυνατές περιπτώσεις.

Προστατευόμενα είναι και τα μεταδιδόμενα δευτερογενή στοιχεία μιας σύνδεσης (ψηφιακής) μέσω τηλεπικοινωνιακών συστημάτων. Τέτοια δευτερογενή δεδομένα είναι λχ. η ταυτότητα του καλούντος και του καλουμένου[46]. Η προστασία λοιπόν που παρέχει, και παρείχε και προ του Ν. 4411, ο ποινικός νομοθέτης ως προς τα στοιχεία που μεταδίδονται είναι ολοκληρωτική.

Η μετάδοση των στοιχείων διαμέσου συστημάτων τηλεπικοινωνιών μπορεί να σημαίνει τρεις διαφορετικές λειτουργίες μιας συσκευής πληροφοριακού συστήματος, οι οποίες και παρατίθενται αμέσως: 1) απομακρυσμένη επεξεργασία στοιχείων, 2) απόκτηση στοιχείων από Τράπεζες στοιχείων και 3) επικοινωνία μέσω ηλεκτρονικών συστημάτων επικοινωνιών.

1) απομακρυσμένη επεξεργασία στοιχείων

[46]Ιδ. Λίβο Ποιν.Χρον ΜΔ΄ σελ.564-565.

Σε αυτή την περίπτωση μεταφέρονται τα στοιχεία από ένα τερματικό σ' ένα υπολογιστή που βρίσκεται σε διαφορετικό από αυτό χώρο, ο οποίος και τα επεξεργάζεται. Τα αποτελέσματα είτε επαναφέρονται στην αρχική μονάδα αποστολής, είτε παραμένουν στο κεντρικό υπολογιστή. Σημαντική τεχνική προϋπόθεση για την απομακρυσμένη επεξεργασία στοιχείων αποτελεί το σύστημα διαμοιρασμού χρόνου που μπορεί να εξυπηρετήσει πολλούς χειριστές συγχρόνως. Σε κάθε απομακρυσμένη επεξεργασία στοιχείων από ένα τερματικό γίνεται προς έναν κεντρικό επεξεργαστή που ευρίσκεται στο διπλανό δωμάτιο ή σε απόσταση πολλών εκατοντάδων χιλιομέτρων[47].

2) απόκτηση στοιχείων από Τράπεζες στοιχείων

Σε αυτή την περίπτωση η πρόσβαση στα στοιχεία γίνεται μέσω ενός δικτύου επικοινωνίας ενώ απαιτείται και διαδικασία ελέγχου («αυθεντικοποίηση»), η οποία συνήθως είναι η αναφορά ενός κλειδάριθμου και η εισαγωγή ενός κωδικού για την αναγνώριση του δικαιώματος εισόδου σε ένα 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. Παραδείγματα τέτοιων τραπεζών αποτελούν οι τράπεζες νομικός πληροφοριών NOMOS και ΙΣΟΚΡΑΤΗΣ του δικηγορικού Συλλόγου Αθηνών.

3) Επικοινωνία μέσω ηλεκτρονικών συστημάτων

Η περίπτωση αυτή αφορά την 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 και πληροφοριών. Στην τρίτη αυτή κατηγορία εντάσσονται πλέον και τα νεφελοειδή συστήματα αποθήκευσης (cloud computing)[48].

Τέλος, στην προστασία των στοιχείων που μεταδίδονται εντάσσεται χαρακτηριστικά και ο προγραμματιστικός κώδικας (γλώσσα προγραμματισμού) των λειτουργικών προγραμμάτων του ηλεκτρονικού υπολογιστή. Σε όλες τις ως άνω κατηγορίες στοιχείων, ο νόμιμος κάτοχος δύναται να δημιουργήσει ένα είδος κυριαρχίας και μία δυνατότητα απαγορεύσεως πρόσβασης σε αυτά, αυτός που

[47]Ιδ. Βασιλακη σελ.85
[48]Ιδ. Σπυρόπουλο «Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking)» σελ. 187

αποκτά δε πρόσβαση κατά παράβαση των μέτρων ασφαλείας καθίσταται φυσικός αυτουργός του εγκλήματος.

## ΠΕΡΙΒΑΛΛΟΝ ΤΕΛΕΣΗΣ ΤΟΥ ΑΡ. 370Γ § 2: ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ή ΠΛΗΡΟΦΟΡΙΚΟ ΕΓΚΛΗΜΑ;

Με την ραγδαία εξέλιξη και καθιέρωση των ηλεκτρονικών υπολογιστών και της τεχνολογίας εν γένει, μεταβλήθηκε ουσιωδώς και η ειδική υπόσταση-ποιότητα ορισμένων αξιοποίνων πράξεων, καθιστώντας ως εκ τούτου εμφανή την ανάγκη εισαγωγής νέων εννοιών και στην νομική επιστήμη. Έτσι λοιπόν, το λεγόμενο *«κοινό-συμβατικό έγκλημα»* άρχιζε να υποχωρεί αισθητά έναντι του *«ηλεκτρονικού εγκλήματος»*, δηλαδή του τελούμενου **με ή σε** περιβάλλον ηλεκτρονικών υπολογιστών. Το δε τελευταίο με την χρήση του διαδικτύου εξειδικεύθηκε ακόμα περισσότερο, φτάνοντας στο σημείο σήμερα να γίνεται λόγος κατά κόρον για *«κυβερνοεγκλήματα»* (άλλως «διαδικτυακά εγκλήματα»).

Όπως εύστοχα έχει παρατηρηθεί από την πλειοψηφία της θεωρίας, οι έννοιες «ηλεκτρονικό έγκλημα», «έγκλημα με υπολογιστή», «διαδικτυακό έγκλημα», και η περαιτέρω κατηγοριοποίηση τών, χρησιμοποιούνται αδιάκριτα και μάλιστα σε νομικά κείμενα, χωρίς να ορίζονται σαφώς δημιουργώντας έτσι σύγχυση τόσο στον νομοθέτη όσο και στον εκάστοτε εφαρμοστή του δικαίου[49]. Η δε φτωχή γνώση και εξοικείωση με τα συναφή τεχνικά ζητήματα, καθώς και η έλλειψη σχετικής βιβλιογραφίας κατά τις προηγούμενες δεκαετίες επιδείνωνε ακόμη περισσότερο το τότε θολό τοπίο[50]. Προς τούτο χρήζουν έκθεσης και επισήμανσης ορισμένοι βασικοί ορισμοί, προκειμένου να μπορέσουμε να προβούμε σε όσο το δυνατόν ασφαλέστερο χαρακτηρισμό της διάταξης του αρ. 370Γ παρ. 2 ΠΚ ως κυβερνοεγκλήματος ή μη.

Στο πλαίσιο ενασχόλησης με τα ως άνω ζητήματα, πέραν των πολλών επιμέρους κατηγοριοποιήσεων που έχουν επιχειρηθεί κατά καιρούς[51], υπάρχει μία βασική-αποδεκτή ταξινόμηση των εγκλημάτων ως εξής[52]:

[49]Ιδ. σχετικά Δ. Κιούπη «Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα», σελ. 151 επ. «3ο Πανελλήνιο Συνέδριο e-Θέμις, Το δίκαιο στην ψηφιακή εποχή»

[50]Ιδ. σχετικά «Διαδίκτυο και ποινικό δίκαιο, έγκλημα στον Κυβερνοχώρο» Ι. Αγγελής, ΠοινΧρον Ν 2000, σελ. 675 επ.

[51]Ιδ. Ζαννή «Το διαδικτυακό έγκλημα» σελ. 59, επιμέρους κατηγοριοποιήσεις από Interpol κ.ο.κ. αλλά και Ι. Αγγελή σελ. 676+677 **&** Δ. Ζημιανίτη «Το δίκαιο στην ψηφιακή εποχή,3ο ,Πανελλήνιο Συνέδριο e-Θέμις», Η τεχνολογία ως το περιβάλλον εκδήλωσης και ανάδειξης συμπεριφορών ως εγκληματικών: ηλεκτρονικό έγκλημα, παθόντες, έννομα αγαθά και δυνατότητα αντίδρασης.

α) **<u>το «κοινό ή συμβατικό» έγκλημα</u>** το οποίο μπορεί να τελεστεί από το δράστη τόσο **σε κοινό περιβάλλον-φυσικό χώρο όσο και με την χρήση διαδικτύου** όπως πχ. η συκοφαντική δυσφήμηση μπορεί να τελεστεί διαζευκτικά με όλους τους ανωτέρω τρόπους.

β) **<u>το «ηλεκτρονικό έγκλημα ή έγκλημα με υπολογιστή» computer related crime)</u>** ορίζεται ως αυτό στο οποίο ο δράστης παρεμβαίνει σε έναν μην συνδεδεμένο υπολογιστή ή σε υπολογιστές συνδεδεμένους σε τοπικά δίκτυα, δηλαδή διαπράττεται μόνο σε περιβάλλον υπολογιστή, **χωρίς την χρήση του διαδικτύου** όπως πχ. η χωρίς δικαίωμα αντιγραφή ή η χρησιμοποίηση ενός προγράμματος ηλεκτρονικού υπολογιστή κατά το άρθρο 370Γ παρ. 1 από τον σκληρό δίσκο όπου είναι αποθηκευμένο σε μία εξωτερική περιφερειακή μνήμη usb.

γ) **<u>το «διαδικτυακό έγκλημα ή κυβερνοέγκλημα» (internet crime-cybercrime)</u>** αποτελεί την πλέον εξειδικευμένη και εξελιγμένη νομικά και τεχνολογικά εκδοχή, κατά την οποία **ο δράστης αποκτά πρόσβαση μέσω του διαδικτύου-ιντερνετ**[53], και όχι μόνο σε ηλεκτρονικούς υπολογιστές, αλλά σε υπολογιστικά-πληροφοριακά συστήματα εν γένει. Με άλλα λόγια, **<u>ο δράστης αποκτά εξ' αποστάσεως πρόσβαση μέσω του διαδικτύου (γνήσια διαδικτυακά εγκλήματα</u>**[54]-διαδικτυακά εγκλήματα stricto sensu[55]) <u>σε συσκευές ή ομάδα διασυνδεδεμένων</u> ή σχετικών μεταξύ τους συσκευών, και μια ή περισσότερες εξ αυτών σύμφωνα <u>με ένα πρόγραμμα αποθηκεύουν, εκτελούν αυτόματη επεξεργασία στοιχείων και δεδομένων, και στην συνέχεια μπορεί να προχωρήσει στην τέλεση</u> άλλων εγκλημάτων όπως φθορά, αντιγραφή, αλλοίωση δεδομένων κλπ., όπως πχ. η

[52]Ιδ. Ν. Φαραντούρη «Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο-Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του hacking και του φαινομένου της μόλυνσης με ιούς» ΠοινΔικ 2/2003, σελ. 191 επ.

[53]Η Ζαννή, ίδετε σελ. 192 προβαίνει σε σαφή διαχωρισμό μεταξύ διαδικτύου (ιντερνετ) και κυβερνοχώρου συμφώνως με τους ορισμούς που προέρχονται από την τεχνολογία. Ως διαδίκτυο μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ τους, ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδίκτυο στο οποίο οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών και η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση.

[54]Ιδ. Ζημιανίτη σελ. 162 συνέδριο e-θεμις 2012, και Αγγελή σελ. 677 Ποιν Χρον.2000.

[55]Ιδ. σχετικά και Κιούπης σελ. 152 συνέδριο e-θεμις 2012.ο οποίος αναφέρει ότι τα «διαδικτυακά εγκλήματα stricto sensu», περιλαμβάνουν ως στοιχείο της ειδικής υπόστασης είτε τον υπολογιστή είτε το διαδίκτυο είτε ως μέσο τέλεσης, είτε ως υλικό ή νομικό αντικείμενο του εγκλήματος. Κατά την γνώμη της γράφουσας, ο διαχωρισμός αυτός τείνει πιο γενικός και προκαλεί σύγχυση, καθώς έγκλημα τελούμενο σε περιβάλλον υπολογιστή δεν προϋποθέτει την χρήση διαδικτύου για την πλήρωση της ειδικής υπόστασης. Η κατηγοριοποίηση α, β ,γ τείνει πιο σαφής και οριοθετημένη. Άλλωστε πλέον δεν μιλάμε για Η/Υ και για άλλες συσκευές, δηλαδή κατηγορίας β, όπως ήταν το αρ. 370Γ παρ. 2 προ του Ν. 4411.

μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή διάδοση πορνογραφικού υλικού δια του κυβερνοχώρου.

Κοινό τόπο αποτελεί πως δεν πρέπει αυθαιρέτως να εκλαμβάνεται ότι το κοινό-συμβατικό έγκλημα διαφέρει από το διαδικτυακό μόνο ως προς την χρήση του περιβάλλοντος διαδικτύου, καθότι ακριβώς αυτό το στοιχείο θέτει μια σειρά παραμέτρων που του προσδίδουν χαρακτηριστικά, τα οποία ως επί το πλείστον δεν έχει το κοινό [56].

Στο σημείο αυτό αξίζει να αναφερθεί ο ιδιαίτερα εύστοχος και «ανθεκτικός» στις ραγδαίες τεχνολογικές εξελίξεις που ακολούθησαν τις επόμενες δεκαετίες, ορισμός που δόθηκε μόλις το έτος 1986 ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), κατά τον οποίο «*πληροφορικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή και μετάδοση δεδομένων*»[57].

Αν και έχει επικριθεί για την γενικότητα της διατύπωσης του, εν τούτοις **κατά την γνώμη της γράφουσας ο όρος «πληροφορικό έγκλημα»** εμπεριέχει εντός του τόσο το ηλεκτρονικό όσο και το διαδικτυακό έγκλημα κατά πως διαμορφώθηκε, δημιουργώντας έτσι μια ευρύτερη και πιο αντιπροσωπευτική κατηγορία αξιοποίνων προσβολών[58].

Κατόπιν των παραπάνω τοποθετήσεων, είναι αδιαμφισβήτητο **ότι η παράνομη πρόσβαση σε πληροφοριακό σύστημα του αρ. 370 Γ. παρ. 2, ως αυτό αντικαταστάθηκε με τον Ν. 4411/2016**, δεν συνιστά πλέον κοινό-συμβατικό έγκλημα. Ορθότερο είναι να χαρακτηρισθεί ως **αμιγώς πληροφορικό έγκλημα[59] ως αυτό εκτέθηκε ανωτέρω, δεδομένου ότι** όταν α) η **απόκτηση πρόσβασης γίνεται** με την φυσική πρόσβαση-επαφή του δράστη με τους υλικούς φορείς-τις συσκευές του πληροφοριακού συστήματος (πχ. με τον Η/Υ, i-pad ) ή με τους υλικούς φορείς που μεταδίδονται στοιχεία με συστήματα τηλεπικοινωνιών (πχ. το modem, την τηλεφωνική γραμμή) **χωρίς την χρήση του διαδικτύου** συνιστά ηλεκτρονικό έγκλημα [με την παραβίαση μέτρων ασφαλείας και απαγορεύσεων που αφορούν τον φυσικό χώρο ή τους υλικούς φορείς], β) **όταν δε ο δράστης αποκτά εξ' αποστάσεως πρόσβαση στα ανωτέρω μέσω του διαδικτύου** συνιστά διαδικτυακό έγκλημα [με

[56]Ιδ. σχετικά Αγγελή σελ. 677 **&** Ζημιανίτη πρακτικά συνεδρίου e-θεμις σελ. 166.
[57]Ιδ. Ζαννή σελ. 58.
[58]Ιδ. Μ. Καιάφα-Γκμπάντι «Ποινικό Δίκαιο και Καταχρήσεις της Πληροφορικής» Αρμεν. 2007, σελ. 1061-1062.
[59]Άλλως έγκλημα πληροφορικής, ίδ. σχετικά Νούσκαλη «Ψηφιακή Τεχνολογία και Δίκαιο», σελ. 123.

την παραβίαση μέτρων ασφαλείας ή απαγορεύσεων]. Η διατύπωση άλλωστε της διάταξης του αρ. 370Γ παρ. 2 δεν οριοθετεί ρητά τον τρόπο της χωρίς δικαίωμα πρόσβασης, καλύπτοντας έτσι αμφότερες τις περιπτώσεις όλων των συσκευών που μπορούν να απαρτίζουν ένα πληροφοριακό σύστημα αλλά και τις περιπτώσεις των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών, με ή χωρίς χρήση διαδικτύου. Ας μη λησμονείται ότι οι αλλαγές που επέφερε ο Ν. 4411/2016 με την διεύρυνση του πεδίου εφαρμογής της προγενέστερης παρωχημένης πλέον διάταξης, στόχευε ακριβώς να συμπεριλάβει κάθε είδους παράνομη πρόσβαση προκειμένου να ποινικοποιήσει πλήθος προσβολών που μέχρι τότε ήταν μη αξιόποινες. Ωστόσο αναμένεται ότι η πλειονότητα των τελούμενων πράξεων του αρ. 370Γ παρ. 2 θα πραγματοποιείται στον κυβερνοχώρο-διαδίκτυο, για τους λόγους που εκτίθενται στο σύνολο της παρούσας εργασίας (ταχύτητα-ευκολία-ποικιλομορφία).

## ΔΙΑΚΡΙΣΕΙΣ-ΧΑΡΑΚΤΗΡΙΣΜΟΙ ΤΟΥ ΑΡΘΡΟΥ 370Γ § 2

Η διάταξη του αρ. 370 Γ παρ. 2 συνιστά **κυρωτικό ποινικό κανόνα** ο οποίος εμπεριέχει προστακτικό-απαγορευτικό κανόνα[60], καθόσον ο νομοθέτης απαγορεύει την χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα ή στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών. Η πράξη της παράνομης πρόσβασης της παρ. 2 συνιστά **κοινό έγκλημα** αφού υποκείμενο μπορεί να είναι οποιοδήποτε πρόσωπο («όποιος»), ενώ **η παρ. 3** του αρ. 370Γ συνιστά μη γνήσιο ιδιαίτερο έγκλημα, καθώς ο δράστης απαιτείται να είναι στην υπηρεσία του νομίμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων. Πρόκειται δε για **έγκλημα ενέργειας**, καθώς το προστατευόμενο έννομο αγαθό πλήττεται με κάποια μυϊκή κίνηση του δράστη αντιληπτή με τις αισθήσεις η οποία επιφέρει ως μεταβολή στον εξωτερικό κόσμο την πρόσβαση στο πληροφοριακό σύστημα ή στα στοιχεία που μεταδίδονται[61]. Η παραβίαση του εν λόγω απαγορευτικού πρωτεύοντος κανόνα («μην αποκτήσεις χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα») μπορεί να παραβιαστεί αποκλειστικά και μόνο με θετική συμπεριφορά εκείνου που παραβιάζει το πληροφοριακό σύστημα, **και ποτέ με παράλειψη**. Το αυτό ερείδεται στην ρητά απαιτούμενη εκ της ισχύουσας διατάξεως σωρευτική συνδρομή παραβίασης (εκ μέρους του δράστη) απαγορεύσεων ή μέτρων ασφαλείας, η οποία ασφαλώς δεν μπορεί να λάβει χώρα με παράλειψη του δράστη (!). Ωστόσο, η σωρευτική αυτή

[60]Ιδ. Κωστάρα .σχετικά με είδη και διακρίσεις των κανόνων του Ποινικού δικαίου, σελ.69 επ.
[61]Ιδ. σχετικά με εγκλήματα ενεργείας και εγκλήματα παραλείψεως Μυλωνόπουλο Χ. «Ποινικό Δίκαιο-Γενικό Μέρος Ι», σελ. 153 .

συνδρομή δεν πρέπει να οδηγήσει στην εσφαλμένη άποψη ότι πρόκειται για σύνθετο έγκλημα, αλλά για **απλό** αφού μία πράξη τυποποιείται αυτοτελώς ως έγκλημα, η δε παραβίαση μέτρων ασφαλείας και απαγορεύσεων δεν συνιστούν αυτοτελή εγκλήματα, αλλά η συνδρομή τους καθιστά το έγκλημα **πολύτροπο**, δυνάμενο να πραγματωθεί με πλείονες τρόπους που προβλέπονται στην ειδική υπόσταση διαζευκτικά. Ειδικότερα, το υπό εξέταση έγκλημα είναι υπαλλακτικώς μικτό, καθότι όσοι τρόποι τέλεσης και αν πραγματωθούν μόνο ένα αδίκημα στοιχειοθετείται[62].

Περαιτέρω, εξόχως σημαντικός είναι και ο χαρακτηρισμός του εγκλήματος ως συμπεριφοράς ή αποτελέσματος, διάκριση η οποία έχει μεγάλη πρακτική σημασία αναφορικά με τον τόπο τέλεσης, τον χρόνο τέλεσης, την αρμοδιότητα των ποινικών αρχών, την ύπαρξη ή μη αντικειμενικού αιτιώδους συνδέσμου[63].

Με γνώμονα την αντικειμενική υπόσταση του αδικήματος, προκύπτει πως πρόκειται για **τυπικό έγκλημα-συμπεριφοράς**, καθότι η αντικειμενική του υπόσταση εξαντλείται στην περιγραφή της ορισμένης συμπεριφοράς, ήτοι της χωρίς δικαίωμα πρόσβασης, χωρίς να ενδιαφέρει στο πλαίσιο της συγκεκριμένης διάταξης το τυχόν αποτέλεσμα αυτής της πρόσβασης. Ο νομοθέτης δηλαδή, **έχει εξοπλίσει την χωρίς δικαίωμα πρόσβαση με αυτοτελές άδικο** χωρίς να το εξαρτά από οιαδήποτε άλλη πράξη-αποτέλεσμα στην ειδική υπόσταση στοιχείο. Δέον όπως τονισθεί πως δεν θα πρέπει εσφαλμένως να εκληφθεί ως έγκλημα αποτελέσματος, καθώς κάτι τέτοιο θα συνεπαγόταν μια μεταβολή ξεχωριστή κατά χώρο και χρόνο απ' την συμπεριφορά, ήτοι το αποτέλεσμα. Τουναντίον στο υπό εξέταση έγκλημα η μεταβολή της κατάστασης στον εξωτερικό κόσμο, ήτοι η απόκτηση παράνομης πρόσβασης συνδέεται άρρηκτα με την συμπεριφορά του δράστη[64].

Προχωρώντας στην διάκριση του εγκλήματος με βάση την διαμόρφωση της αντικειμενικής υπόστασης, ιδιαίτερο ενδιαφέρον παρουσιάζει η κατάταξη του εγκλήματος σε έγκλημα βλάβης ή διακινδύνευσης.

**Ως βλάβη νοείται** η άμεση, πραγματική και οριστική τρώση του εννόμου αγαθού ανεξαρτήτως του αν αυτή είναι ολική ή μερική, υλική ή άυλη[65]. Στον κίνδυνο

[62]Ιδ. εγκλήματα απλότροπα και μικτά Μυλωνόπολο Χ. «Ποινικό Δίκαιο-Γενικό Μέρος Ι», σελ. 160.
[63]Ιδ. Στα εγκλήματα συμπεριφοράς τόπος τελέσεως είναι πάντοτε ο τόπος στον οποίο ο δράστης συμπεριφέρθηκε, δηλαδή προέβη ολικά στην εγκληματική του ενέργεια, και είναι αδιάφορος ο τόπος που τυχόν επήλθαν, αν επήλθαν οι συνέπειες αυτής εν αντιθέσει με τα εγκλήματα αποτελέσματος στα οποία τόπος τέλεσης κατ' αρ. 16 ΠΚ είναι τόσο ο τόπος εκδήλωσης της πράξης-ενέργειας του δράστη όσο και ο τόπος επέλευσης του αποτελέσματος.
[64]Ιδ. σχετικά με διακρίσεις εγκλημάτων συμπεριφοράς και αποτελέσματος Ν. Ανδρουλάκη «Ποινικό Δίκαιο-Γενικό Μέρος», σελ. 170.
[65]Ιδ. Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος Ι» σελ. 149.

δε, ο νομοθέτης τρόπο τινά *«μεταθέτει προς τα εμπρός το όριο της ποινικής προστασίας και δεν περιμένει την επέλευση της βλάβης»* όπως χαρακτηριστικά υποστηρίζει ο Ανδρουλάκης[66]. Έτσι ο κίνδυνος είναι μια ασυνήθιστη, μη κανονική κατάσταση που δρομολογεί την επέλευση βλάβης ενός αγαθού προκαλώντας αβεβαιότητα και ανασφάλεια.

Τα ως άνω σε συνδυασμό με το δεδομένο ότι η αντικειμενική του υπόσταση του αδικήματος εξαντλείται στην περιγραφή της χωρίς δικαίωμα πρόσβασης σε πληροφοριακό σύστημα ή στα στοιχεία που μεταδίδονται, χωρίς να τυποποιείται και να ενδιαφέρει τυχόν αποτέλεσμα αυτής της πρόσβασης συνιστά **έγκλημα διακινδύνευσης[67]** ως άλλωστε θεσπίστηκε σύμφωνα με την αιτιολογική έκθεση του Ν. 1805/1988, καθώς αποτελεί *«στο χώρο της επεξεργασίας και μετάδοσης στοιχείων[..]το πρώτο βήμα εξέλιξης μιας επικίνδυνης προσωπικότητας για την κοινωνία»[68]*. Η αξιόποινη συμπεριφορά της απόκτησης πρόσβασης σε στοιχεία πληροφοριακού συστήματος, δημιουργεί αναντίρρητα την δυνατότητα άπειρων περαιτέρω καταχρήσεων-βλαβών, χωρίς ακόμα όμως να έχει επέλθει αυτή η βλάβη, και χωρίς να τυποποιείται η επέλευση συγκεκριμένου κινδύνου ως προς κάποιο υλικό αντικείμενο ως στοιχείο της αντικειμενικής υποστάσεως αποτελώντας ως εκ τούτου **έγκλημα αφηρημένης διακινδύνευσης[69]**. Η διείσδυση λοιπόν στο εκάστοτε πληροφοριακό σύστημα ή τα στοιχεία που μεταδίδονται είναι φορέας αυτοτελούς αδίκου με την μορφή έντονης διακινδύνευσης περαιτέρω εννόμων αγαθών, πριν την επέλευση οιασδήποτε βλάβης.

Στην παρούσα προβληματική κεντρίζει το ενδιαφέρον και η **άποψη του Σπυρόπουλου, περί ενδεχόμενης στοιχειοθέτησης εγκλήματος βλάβης[70]** στην εν λόγω διάταξη του αρ. 370Γ παρ. 2[71]. Η άποψη αυτή ερείδεται στο απόρρητο ως έννομο αγαθό το οποίο έχει τρωθεί-βλαφτεί με μόνη την πρόσβαση, χωρίς καμιά περαιτέρω πράξη. Ωστόσο, ο Σπυρόπουλος σπεύδει να πάρει θέση πως η εν λόγω

[66]Ιδ. του ιδίου «Ποινικό Δίκαιο-Γενικό Μέρος Ι» σελ. 171.
[67]και μάλιστα έντονης, όπως έχει επισημάνει ο Μυλωνόπουλος στο έργο του «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο» σελ. 93.
[68]Ιδ. Βασιλάκη σελ. 8, Φιλόπουλο σελ. 168 και Ιγγλεζάκη «Δίκαιο της Πληροφορικής» σελ. 279.
[69]Ιδ. Αλ. Κωστάρα «Ποινικό Δίκαιο-Επιτομή Ειδικού Μέρους αρ. 134-410 ΠΚ» σελ. 1133 το χαρακτηρίζει συγκεκριμένης διακινδύνευσης.
[70]Την άποψη του Weissenberger παραθέτει στο έργο του ο Σπυρόπουλος (σελ. 185), όπου ο πρώτος θεωρεί ότι η σχετική διάταξη έχει στοιχεία εγκλήματος βλάβη, διότι η διείσδυση του δράστη στο πληροφοριακό σύστημα του νομίμου κατόχου προκαλεί εξ' ορισμού βλάβη στο δικαίωμα στο «computer», αλλά και στοιχεία εγκλήματος διακινδύνευσης διότι προστατεύονται οι απασχολούμενοι με Η/Υ και οι κάτοχοι Η/Υ από πχ. κλοπή στοιχείων κλπ. (ίδετε Σπυρόπουλο σελ. 185.
[71]Ιδ. σχετικά Σπυρόπουλος σελ. 184.

άποψη συγχέει την προσβολή του εννόμου αγαθού με τον κίνδυνο που ενέχει η πρόσβαση για προσβολή άλλων εννόμων αγαθών.

**Εκτός των ανωτέρω διαλαμβανομένων,** με δεδομένο την γραμματική διατύπωση της διάταξης η οποία δεν περιλαμβάνει καμία αναφορά, αλλά και το ήδη ευρύ λογικό πεδίο της έννοιας της πρόσβασης, ορθότερο θα ήταν κατά την γνώμη της γράφουσας, να μην αυστηροποιηθεί και άλλο η φύση της ποινικής διάταξης και με την εκδοχή της βλάβης. Αυτό ενισχύεται άλλωστε και από το γεγονός ότι για περαιτέρω επενέργεια στο πληροφοριακό σύστημα ή στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών υπάρχουν αυτοτελείς ποινικές διατάξεις όπως αυτές του αρ. 370 Β όταν πρόκειται για απόρρητα επιστημονικά κλπ, οι νέες διατάξεις των άρθρων 292 Α και Β, καθώς και η φθορά ψηφιακών δεδομένων του αρ. 381Β. Σε επίπεδο δε αντεγκληματικής πολιτικής, με την αυτοτελή ποινική απαξία και τιμώρηση μόνης της απόκτησης πρόσβασης, δίνεται μεγαλύτερη έμφαση και ο εν δυνάμει δράστης-κοινωνός του δικαίου αντιλαμβάνεται ότι δεν μένει ατιμώρητος στην προσπάθεια του ν' αποκτήσει πρόσβαση. Εδώ μπορούμε ενισχυτικώς του παρόντος επιχειρήματος να ανατρέξουμε και στην προσομοίωση που θα παρατεθεί παρακάτω με την διάταξη περί διατάραξης οικιακής ειρήνης, η οποία φέρει (ορθώς και δικαίως κατά το κοινό αίσθημα) αυτοτελές άδικο, καθώς η πολιτεία δεν θα τιμωρήσει μόνο τον δράστη που εισήλθε στο σπίτι και έκλεψε, αλλά και το δράστη που μόνο εισήλθε ανεξαρτήτως της βουλήσεως ή της δυνατότητας του να προβεί σε οποιαδήποτε περαιτέρω ενέργεια. Τα αντίστοιχα ισχύουν και για το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα.

**Την υπερβολική διεύρυνση του αξιοποίνου** που θεμελιώνεται φροντίζει να αντισταθμίσει ο νομοθέτης στο ίδιο κιόλας εδάφιο με την **ρητή αξίωση <u>σωρευτικής συνδρομής 2 επιπλέον στοιχείων τα οποία εντάσσονται στην αντικειμενική υπόσταση:</u>** <u>«παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του» και «χωρίς δικαίωμα</u>.» Υπενθυμίζεται ότι στην προϊσχύουσα διάταξη του αρ. 370Γ παρ. 2, η παραβίαση απαγορεύσεων –μέτρων ασφαλείας αποτελούσε ενδεικτική αναφορά τρόπων τέλεσης της πράξης.. Ωστόσο ο ν. 4411/2016, εναρμονιζόμενος με τις επιταγές της Οδηγίας θεσπίζει το στοιχείο αυτό σωρευτικά και όχι ενδεικτικά.

Σημαντική, είναι και η διάκριση του εν λόγω αδικήματος σε διαρκές ή στιγμιαίο έγκλημα, καθόσον αυτό καθορίζει τον χρόνο τέλεσης και κατ' επέκταση τον χρόνο παραγραφής, αλλά και τυχόν ζητήματα άμυνας εφόσον συντρέχει άδικη

και παρούσα επίθεση. Συμφώνως με τα όσα εκτέθηκαν, προκύπτει ότι το έγκλημα της χωρίς δικαίωμα πρόσβασης είναι **στιγμιαίο,** διότι η αντικειμενική υπόσταση ολοκληρώνεται σε μία μεμονωμένη χρονική στιγμή και δεν παρατείνεται αυτοβούλως από τον δράστη, και δεν ενδιαφέρει αν και για πόσο χρονικό διάστημα διατηρείται η παράνομη κατάσταση που έχει δημιουργηθεί[72] · αρκεί η απόκτησης παράνομης πρόσβασης.

Τέλος, η υπό κρίση διάταξη–**βασικό έγκλημα** με κριτήριο την απειλούμενη ποινή συνιστά **πλημμέλημα** (ποινή φυλάκισης), ενώ στην περίπτωση της **διακεκριμένης εγκληματικής παραλλαγής** που η πράξη αφορά στις διεθνείς σχέσεις ή την ασφάλεια του κράτους συνιστά **κακούργημα** (ποινή κάθειρξης).

## ΕΙΔΙΚΗ ΥΠΟΣΤΑΣΗ : ΑΝΤΙΚΕΙΜΕΝΙΚΗ ΥΠΟΣΤΑΣΗ

### Α. Απόκτηση πρόσβασης

Σπεύδεται εξαρχής να τονιστεί ότι στο παρόν κεφάλαιο εκτίθεται η πρόσβαση εν στενή εννοία, σε ό,τι αφορά τα στοιχεία του πληροφοριακού συστήματος και τα στοιχεία που μεταδίδονται.

Η πράξη η οποία έχει επιλέξει ο ποινικός νομοθέτης να κολάσει στην διάταξη του αρ. 370Γ παρ. 2 είναι η απόκτηση πρόσβασης στο σύνολο ή τμήμα του πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών[73]. Η έννοια της απόκτησης πρόσβασης καίτοι με μία πρώτη ματιά φαίνεται ευκόλως αντιληπτή, με μία ενδελεχέστερη δημιουργεί ερωτηματικά και ως προς το ποιες πράξεις στοιχειοθετούν πράγματι την πράξη της πρόσβασης, αλλά και ως προς το πότε κατ' επέκταση γίνεται λόγος για έγκλημα στην ολοκληρωμένη-τετελεσμένη μορφή του και πότε γίνεται λόγος για απόπειρα τέλεσης ή μη.

Καταρχήν, προκειμένου να απαντήσουμε στα ανωτέρω, οφείλουμε να τονίσουμε ότι **η ποινική απαξία του νομοθέτη (ως προς την αντικειμενική υπόσταση) εξαντλείται στην απόκτηση πρόσβασης αυτοτελώς[74],** πράγμα το οποίο σημαίνει πως στην υπό κρίση διάταξη του αρ. 370 Γ παρ. 2 **είναι ποινικά αδιάφορη**

[72]Ιδ. Α. Χαραλαμπάκη, «Ποινικός κώδικας ερμηνεία κατ' άρθρο» 2011, σελ.1711.
[73]Ο Έλληνας νομοθέτης ποινικοποιεί τις αντίστοιχες συμπεριφορές όπως προβλέπει και η Σύμβαση του Συμβουλίου της Ευρώπης στο άρθρο 2 και όπως καθορίζουν και αρκετές αλλοδαπές έννομες τάξεις. Ίδ. σχετικά με ρυθμίσεις αλλοδαπών εννόμων τάξεων Δ. Κιούπη, Υπεράσπιση 2000, «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, κενά και αδυναμίες της ποινικής νομοθεσίας», σελ. 959επ. Β. «Αθέμιτη πρόσβαση σε δεδομένα» σελ. 969, υποσημείωση No 32.
[74] Ίδ. Καράκωστας σελ. 164 σχετικά με αυτοτελή απαξία.

**οποιαδήποτε ενέργεια-πράξη ακολουθήσει της πρόσβασης**[75], πχ. χρησιμοποίηση, αλλοίωση, μεταβίβαση των στοιχείων κλπ. **Ποινικά αδιάφορος είναι εν προκειμένω και ο σκοπός για τον οποίο ο δράστης θέλησε την πρόσβαση** αυτή. Αυτό συνάδει άλλωστε αφενός με το χαρακτήρα του Ποινικού μας Δικαίου ως δίκαιο της πράξης και όχι δίκαιο της σκέψης, και αφετέρου με την ρητή διατύπωση της διάταξης στην οποία απουσιάζει ο περαιτέρω σκοπός · δεν πρόκειται δηλαδή για έγκλημα υπερχειλούς υποκειμενικής υποστάσεως όπως θα αναλύσουμε και στο οικείο κεφάλαιο.

**Με τον όρο απόκτηση πρόσβασης νοείται** η απόκτηση δυνατότητας, είτε φυσικής είτε τεχνητής επίδρασης στα στοιχεία ή στο πληροφοριακό σύστημα του νομίμου κατόχου, πρόκειται δηλαδή για κάθε διείσδυση ή εισβολή του δράστη η οποία του εξασφαλίζει την εν δυνάμει γνώση αυτών και την δυνατότητα να προχωρήσει σε οποιαδήποτε περαιτέρω ενέργεια επιθυμεί. Επαναλαμβάνεται πως η πρόσβαση αφορά τα στοιχεία του πληροφοριακού συστήματος και τα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών με την στενή έννοια στο οποίο αποκτά πρόσβαση ο δράστης, και δεν πρέπει να συγχέεται στο συγκεκριμένο πλαίσιο ,κατά την γνώμη της γράφουσας, με απόκτηση πρόσβασης σε ένα φυσικό χώρο όπου βρίσκονται υλικοί φορείς.

Για να γίνει πιο κατανοητή η απόκτηση πρόσβασης αναγκαία φαίνεται η σύντομη περιγραφή της διαδικασίας σύνδεσης σε ένα σύστημα πληροφοριών από κάποιον υλικό φορέα, πχ. ηλεκτρονικό υπολογιστή ή κινητό τηλέφωνο. Αρχικά, κατά την προσπάθεια εισόδου ζητείται η κωδική ονομασία-κλειδάριθμος του χρήστη και ένας κωδικός **[1ο στάδιο].** Αφού ο χρήστης συμπληρώσει αυτά τα δύο ζητούμενα πεδία και επιβεβαιωθούν από το σύστημα **[2ο στάδιο**] αποκτά πλέον πλήρη πρόσβαση, καθώς εμφανίζεται μπροστά του το οικείο μενού επιλογών, προκειμένου να προβεί στην εκτέλεση οποιαδήποτε άλλης λειτουργίας του συστήματος **[3ο στάδιο].** Στο δεύτερο δηλαδή στάδιο, η αντικειμενική υπόσταση του αδικήματος έχει πληρωθεί, διότι ο δράστης έχει πλέον την δυνατότητα να ενεργήσει ό,τι άλλο επιθυμεί στο πληροφοριακό σύστημα.

Τετελεσμένο είναι το έγκλημα και στην περίπτωση που κατά το 1ο προπεριγραφέν στάδιο, αντί για αίτημα συμπλήρωσης κωδικής ονομασίας χρήστη και

[75]Ιδ. σχετικά Δ. Κιούπη, Υπερ. 2000, «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, κενά και αδυναμίες της ποινικής νομοθεσίας», σελ. 959επ. Β. «Αθέμιτη πρόσβαση σε δεδομένα» σελ. 968.

κωδικού εισόδου (δηλαδή αντί ύπαρξης μέτρων ασφαλείας) υπάρχει η σαφής προειδοποίηση ότι απαγορεύεται η πρόσβαση (δηλαδή η ύπαρξη απαγορεύσεων) στο μη νόμιμο κάτοχο -χρήστη των στοιχείων του πληροφοριακού συστήματος. Και υπ' αυτά τα πραγματικά περιστατικά, όταν ο δράστης παρά την ως άνω απαγόρευση προχωρήσει στο 2ο στάδιο είναι τετελεσμένο το έγκλημα καθώς έχει αποκτήσει πλέον πλήρη πρόσβαση.

Η απόκτηση πρόσβασης σε πληροφοριακό σύστημα κατά πως περιγράφηκε ανωτέρω, προσιδιάζει αρκετά στο έγκλημα της διατάραξης οικιακής ειρήνης του αρ. 334 ΠΚ[76]. Σύμφωνα με την ειδική υπόσταση αυτού, το έγκλημα είναι τετελεσμένο με την παράνομη είσοδο του δράστη ή παραμονή του στο χώρο μετά την πρόσκληση του παθόντος[77], ανεξαρτήτως οιασδήποτε μεταγενέστερης πράξης του δράστη κατά λογική αντιστοιχία με την ειδική υπόσταση του αρ. 370Γ παρ. 2. Ομοίως, ο σκοπός παράνομης εισόδου ή παραμονής είναι ποινικά αδιάφορος, όπως και ο σκοπός απόκτησης πρόσβασης στο πληροφοριακό σύστημα. Πρόκειται συνεπώς για αμφότερα τυπικά-εγκλήματα συμπεριφοράς.

Γίνεται λοιπόν αμέσως αντιληπτό πως το αξιόποινο της εν λόγω πράξης του αρ. 370Γ παρ.2 είναι ιδιαίτερα ευρύ, καθότι αρκείται στην απόκτηση πρόσβασης και μόνο, η οποία δίνει την δυνατότητα για σωρεία μεταγενεστέρων πράξεων-προσβολών του πληροφοριακού συστήματος.

## Β. Ειδικές περιπτώσεις πρόσβασης

**Λαμβάνοντας ως δεδομένο ότι ο δράστης παραβιάζει απαγορεύσεις ή μέτρα ασφαλείας του νομίμου κατόχου, και δεν έχει φυσική πρόσβαση στους χώρους και στους υλικούς φορείς του πληροφοριακού συστήματος, δηλαδή δρα εξ' αποστάσεως μέσω διαδικτύου, μπορεί να αποκτήσει πρόσβαση με ποικίλους τρόπους,** οι συνηθέστεροι από τους οποίους εκτίθενται κατωτέρω.

**1.**Αρκετά διαδεδομένο είναι το φαινόμενο **«pharmimg»**[78] η ονομασία του οποίου προέρχεται από την αγγλική λέξη farming και την μετατροπή στους κύκλους των δραστών hackers του γράμματος «f» se «ph». Η μέθοδος αυτή αφορά ένα μεγάλο αριθμό υπολογιστών συνδεδεμένων στο διαδίκτυο που μπορούν να συγκριθούν με μία φάρμα ζώων (farm) και συντηρούνται από τους δράστες. Ένα ειδικό πρόγραμμα

[76]Ιδ. Κιούπη, Υπεράσπιση σελ. 970, όπου κάνει λόγο για «διατάραξη ηλεκτρονικής οικιακής ειρήνης».
[77]Ιδ. σχετικά Μ. Μαργαρίτης Ποινικός Κώδικας, Ερμηνεία-Εφαρμογή, 2009, σελ. 902 επ.
[78]Δεν θα πρέπει να συγχέεται το φαινόμενο του pharming με αυτό του phising, καθώς το τελευταίο προσιδιάζει στην απάτη του αρ . 386 ΠΚ ίδ. σχετικά Ιγγλεζάκη, σελ. 282

εκμεταλλεύεται κενά ασφαλείας του προσβαλλόμενου πληροφοριακού συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο ώστε να μπορεί να επισκέπτεται πλαστές ιστοσελίδες, ακόμη και αν ο χρήστης πληκτρολογεί την σωστή διεύθυνση της ιστοσελίδας που επιθυμεί να φορτώσει. Στην οθόνη του χρήστη-θύματος εμφανίζεται η πλαστή ιστοσελίδα πανομοιότυπη με την αυθεντική, στην οποία εκτελεί διάφορες λειτουργίες θεωρώντας ότι βρίσκεται σε ασφαλές διαδικτυακό περιβάλλον. Εάν δε πρόκειται πχ. για ιστοσελίδα τράπεζας, η προσπάθεια του θύματος να πραγματοποιεί συναλλαγές μέσω online-banking καταλήγει στην μεταφορά των κεφαλαίων στους λογαριασμούς των δραστών farmers. Έτσι λοιπόν οι δράστες αποκτούν παρανόμως πρόσβαση και τελούν την ειδική υπόσταση του αρ. 370Γ παρ. 2[79]. (στο εν λόγω παράδειγμα η μεταφορά των κεφαλαίων στους λογαριασμούς των δραστών συνιστά έτερη-αυτοτελή εγκληματική πράξη).

**2.**Άλλος εξίσου γνωστός τρόπος παράνομης απόκτησης πρόσβασης σε πληροφοριακό σύστημα είναι εκείνος μέσω της χρησιμοποίησης προγραμμάτων δούρειων ίππων. Ο δούρειος ίππος είναι αυτοτελές πρόγραμμα το οποίο συνήθως προσφέρεται στο δράστη ως ένα βοηθητικό πρόγραμμα είτε ως ένα πρόγραμμα εφαρμογής ή συνημμένο σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου. Όσο ο χρήστης εκτελεί το δούρειο ίππο, «φωλιάζει» το κατασκοπευτικό πρόγραμμα στον υπολογιστή χωρίς να προκαλεί βλάβη στο σύστημα. Αποθηκεύει όμως απαρατήρητα, είτε ανακαλούμενα από τον χρήστη έγγραφα είτε εισερχόμενους κωδικούς ή αριθμούς πιστωτικών καρτών και άλλα στοιχεία που στην συνέχεια διαβιβάζονται σε μία προκαθορισμένη διεύθυνση ηλεκτρονικού ταχυδρομείου.

**3.**Ακόμη πιο επικίνδυνα είναι και τα προγράμματα της πίσω πόρτας («backdoor programmes»), τα οποία επιτρέπουν την λειτουργία του μολυσμένου υπολογιστή από απόσταση.

**4.** Τα προγράμματα ιών επίσης αποτελούν ένα τρόπο πρόσβασης στο πληροφοριακό σύστημα, καθώς έχουν την ιδιότητα να πολλαπλασιάζονται και έχουν ως σκοπό να παρενοχλούν την λειτουργία του υπολογιστή με διάφορους τρόπους, ειδικότερα σβήνουν δεδομένα ή στοιχεία υπολογιστών[80]. Οι ιοί των Η/Υ είναι μη αυτόνομα προγράμματα ή τμήματα προγραμμάτων τα οποία «κολλάνε» σε άλλα

[79]Ιδ. Βασιλάκη Ε. «Τα φαινόμενα phising, pharming και η ποινική τους αξιολόγηση», Ποινικά Χρονικά ΝΖ 2007, σελ. 860 σχετικά με περίπτωση επιθέσεων κατά πληροφοριακών συστημάτων.
[80]Ιδ. σχετικά Ν. Φαραντούρη σελ. 191 επ.

«μητρικά» προγράμματα. Σκοπός των Makro-ιών είναι η μόλυνση του περιβάλλοντος προγραμμάτων, των αρχείων και των στοιχείων, καθώς και η περαιτέρω μετάδοση των μολυσμένων στοιχείων. Τα αρχεία του χρήστη δεν μεταδίδονται αυτόματα. Προκειμένου οι δράστες «hackers» να πετύχουν την συλλογή στοιχείων ανατρέχουν στα κενά ασφαλείας των προγραμμάτων, τα οποία σε σύνδεση με το διαδίκτυο επιτρέπουν την αθέατη εισβολή σε ένα ξένο υπολογιστή, καθώς και την κατασκόπευση στοιχείων.

**5.** Η χωρίς δικαίωμα παρακολούθηση εκπομπών από ηλεκτρονικό υπολογιστή της επί πληρωμή τηλεόρασης μέσω ιντερνετ συνιστά χωρίς δικαίωμα πρόσβαση σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών[81].

Τέλος, για λόγους πληρότητας του παρόντος κεφαλαίου, πέραν των ανωτέρω ενδεικτικών τρόπων απόκτησης πρόσβασης σε ένα πληροφοριακό σύστημα, πρόσβαση δύναται να αποκτηθεί και μέσω των υλικών φορέων του, στο φυσικό χώρο του νομίμου κατόχου στον οποίο εισέρχεται ο δράστης.

## Γ. «παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του» -- Εξωτερικοί όροι του αξιοποίνου

Ήδη, από το άρθρο 2 της Σύμβασης του Συμβουλίου της Ευρώπης (2001) μνημονευόταν η παραβίαση μέτρου ασφαλείας ως προϋπόθεση διάπραξης του εν λόγω εγκλήματος, και εναπόκειτο σε έκαστο συμβαλλόμενο μέρος να την θέση ως τέτοια. Το ίδιο υιοθετήθηκε και στο άρθρο 2 της Απόφασης-Πλαίσιο (2005) του Συμβουλίου της Ευρωπαϊκής Ένωσης.

**Με τις τροποποιήσεις που επέφερε ο Ν. 4411/2016, απαιτείται πλέον η χωρίς δικαίωμα πρόσβαση να τελείται με την σωρευτική συνδρομή παραβίασης απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών[82]**. Τα ληφθέντα μέτρα ασφαλείας και απαγορεύσεις αποτελούν ακριβώς την με αντικειμενικά διαγνώσιμο τρόπο εξωτερίκευση της βούλησης του νομίμου κατόχου να μην καθίστανται προσιτά (τα στοιχεία του πληροφοριακού συστήματος και τα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών) σε

[81]Ιδ. Φιλόπουλος σελ. 186-188 σχετικά με ειδικές περιπτώσεις πρόσβασης σε Η/Υ, αλλά και Κιούπη «Ποινικό Δίκαιο και Ίντερνετ» σελ. 121 επ.
[82]Σωρευτική συνδρομή απαιτεί και η Οδηγία για το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα.

οποιονδήποτε[83]. Πρόκειται λοιπόν, **για συνδρομή αντικειμενικών στοιχείων, και δη πρόσθετων,** αφού δεν τιμωρείται απλά η χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα, αλλά αυτή που λαμβάνει χώρα με την προαναφερόμενη παραβίαση, προσδίδοντας στην εν λόγω διάταξη το χαρακτηρισμό της ως ***«εγκλήματος με υπερχειλή αντικειμενική υπόσταση»***[84]. Ως εκ τούτου, οι αντικειμενικές αυτές περιστάσεις **συνιστούν εξωτερικούς όρους του αξιοποίνου**[85]**, οι οποίοι ανήκουν στην με ευρεία εννοία αντικειμενική υπόσταση του εγκλήματος** και δεν απαιτείται να καλύπτονται από την υπαιτιότητα του δράστη, καθώς δεν **θεμελιώνουν** το άδικο της πράξης, αλλά **το αξιόποινο αυτής.**

Δέον όπως τονισθεί ότι ως απορριπτέα, κατά την γνώμη της γράφουσας, θα πρέπει να κριθεί η τυχόν άποψη που θεωρεί την παραβίαση μέτρων ασφαλείας ως αντικειμενικό στοιχείο αντί για εξωτερικό όρο του αξιοποίνου, και αυτό διότι **το άδικο της πράξης του δράστη του αρ. 370 Γ παρ. 2 εξαντλείται στην συμπεριφορά του** (ήτοι στην χωρίς δικαίωμα πρόσβαση)[86], και δεν προϋπάρχει αυτής.

Σε περίπτωση δηλαδή, που δεν συντρέχει παραβίαση μέτρων ασφαλείας και απαγορεύσεων, ο δράστης παρά το γεγονός ότι τελεί εν μέρει την άδικη πράξη της χωρίς δικαίωμα πρόσβασης, παραμένει ατιμώρητος σύμφωνα με την ισχύουσα διάταξη του αρ. 370Γ παρ. 2, ακριβώς γιατί δεν συντρέχει ο ως άνω **εξωτερικός όρος του αξιοποίνου**[87]**. Καθίσταται λοιπόν αντιληπτό, ότι αυτός ο όρος- όπως και κατά την κρατούσα άποψη όλοι οι εξωτερικοί όροι του αξιοποίνου- δεν θεμελιώνει, αλλά περιορίζει το αξιόποινο στην με ευρύ πεδίο εφαρμογής διάταξη του αρ. 370 Γ παρ. 2, ως αυτή ίσχυε προ των αλλαγών του Ν. 4411/2016.**

**Κατά την γνώμη της γράφουσας**, η έννοια των απαγορεύσεων και μέτρων ασφαλείας είναι αρκετά επιτυχής τοποθέτηση, καθώς πέραν του περιορισμού του αξιοποίνου ως εκτέθηκε αμέσως παραπάνω συμβάλλει και σε άλλα θέματα. Ειδικότερα: α) προσδιορίζει τι πρέπει να έχει προηγηθεί από πλευράς του νομίμου κατόχου κατά περιεχόμενο,(και όχι κατά αποτελεσματικότητα), χωρίς να συνοδεύεται

[83]Ιδ. Καράκωστας σελ. 163.
[84]Ιδ. σχετικά Ν. Ανδρουλάκης «Ποινικό Δίκαιο –Γενικό Μέρος, Θεωρία για το Έγκλημα», σελ. 244
[85]Ολοένα και περισσότεροι αμφισβητείται η ύπαρξη και η φύση αυτών των στοιχείων, ίδ. σχετικά Κοτσαλή «Ποινικό Δίκαιο-Γενικό Μέρος Ι », 2005 σελ. 78.
[86]Ιδ. για αμφισβητούμενες περιπτώσεις Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος Ι», σελ. 135
[87]ενώ με την προϊσχύουσα διάταξη ήταν σίγουρη η τιμώρηση του.

από εξωνομικά-αξιολογικά στοιχεία[88] όπως πχ. «ιδιαίτερα αυστηρά μέτρα ασφαλείας» ή «αποτελεσματικά μέτρα ασφαλείας», τα οποία θα δυσχέραιναν την κρίση του Δικαστηρίου της Ουσίας που θα αποφαινόταν ανελέγκτως μεταξύ άλλων, και για τεχνικά ζητήματα πληροφορικής αλλά και λόγω της ραγδαίας εξέλιξης της τεχνολογίας θα άλλαζαν διαρκώς τα κριτήρια των μέτρων ασφαλείας, καθιστώντας την διάταξη διάτρητη. Ας μην παραμερίζεται ότι μια τέτοια οριοθέτηση θα εξαρτούσε την προστασία του δικαιούχου από τυχόν τεχνικές γνώσεις του περί τα μέτρα ασφαλείας που να δεν γνώριζε, ούτε ενδεχομένως μπορούσε να γνωρίζει κλπ. **Έτσι, ο νομοθέτης απαιτεί απλά και όχι ιδιαίτερα μέτρα ασφαλείας και απαγορεύσεις**, αρκούμενος στο να εκφράζεται κατά τρόπο αντικειμενικά διαγνώσιμο το ειδικό-συγκεκριμένο ενδιαφέρον του νομίμου κατόχου για διαφύλαξη του απορρήτου των στοιχείων ή του πληροφοριακού συστήματος. Συνεπώς, η βαρύτητα και η απαξία της ενέργειας του δράστη δεν αλλάζει, αλλά ούτε και συνιστά επιβαρυντική περίσταση η παραβίαση τυχόν αυστηρότερων μέτρων ασφαλείας · η ποινική αντιμετώπιση του δράστη περί το άδικο που έθεσε με την πράξη του παραμένει η ίδια. Η δε συνδρομή των εξωτερικών όρων του αξιοποίνου ερευνάται αυτεπαγγέλτως από το δικάζον Δικαστήριο.

Στο σημείο αυτό λοιπόν της εξέτασης των στοιχείων της με ευρείας εννοίας αντικειμενικής υπόστασης του αρ. 370Γ παρ. 2, τίθεται ο καθοριστικός **παράγων των θυματολογικών εκτιμήσεων**, ο οποίος είναι χαρακτηριστικός της ποινικής προστασίας των απορρήτων.[89] **Δηλαδή ο ποινικός νομοθέτης παρεμβαίνει στη σφαίρα απορρήτου του θύματος, εφόσον** το τελευταίο καίτοι την έχει οριοθετήσει και την έχει εξωτερικεύσει ως τέτοια λαμβάνοντας τα απαραίτητα κατ' αυτό μέτρα προστασίας[90], αυτή τελικά παραβιάζεται από τον δράστη και αποκτάται πρόσβαση σ' αυτή. Κατά τη γνώμη της γράφουσας, εδώ διαφαίνεται μία πολύ ευέλικτη και προστατευτική όψη και λειτουργία του δικαίου, αφού στη συγκεκριμένη διάταξη ο νομοθέτης «αφήνει» τον φορέα του εννόμου αγαθού-θύμα να οριοθετήσει την σφαίρα του απορρήτου του κατά τι νομίζει, χωρίς να κρίνει καθόλο το περιεχόμενο. Εν συνεχεία, αφήνει τον δικαιούχο να λάβει όποια μέτρα προστασίας ή έστω

[88]Ιδ. σχετικά με αξιολογικά στοιχεία της αντικειμενικής υπόστασης σχετικά Μυλωνόπουλος «Ποινικό Δίκαιο-Γενικό Μέρος Ι», σελ. 130.
[89]Ιδ. Φιλόπουλο, σελ. 27.
[90]Ιδ. Ανν. Ψαρούδα-Μπενάκη, Πρακτικά Β, ΠανΣυνΕΕΠΔ, «Η θέση του θύματος στο ποινικό σύστημα και ο θεσμός της πολιτικής αγωγής» 1989, σελ. 18, όπου η προβληματική της συμβολής του θύματος στην πραγμάτωση του εγκλήματος αρνητικά με την παράλειψη του να λάβει όλα τα ενδεικνυόμενα, γενικώς πρόσφορα και δυνατά σε αυτό μέτρα αυτοπροστασίας.

απαγορεύσεις-προειδοποιήσεις ως καταλληλότερα εξειδικεύοντας την βούληση του και μόνο όταν αυτά αποδεικνύονται διάτρητα επεμβαίνει. Η δε επέμβαση αυτή λαμβάνει χώρα με μόνη την απόπειρα ή την απόκτηση πρόσβασης και δεν απαιτείται ο δράστης να έχει προχωρήσει σε βαρύτερες προσβολές (!) Οι απαγορεύσεις και τα μέτρα ασφαλείας που έχει λάβει το θύμα εξωτερικεύουν την θέληση του νομίμου κατόχου περί μη απόκτησης πρόσβασης[91]. Ας μην λησμονείται άλλωστε ότι **πρόκειται κατ' άρθρο 370Γ παρ. 4, για ένα απολύτως κατ' έγκληση διωκόμενο έγκλημα, εύλογα λοιπόν ο νόμιμος κάτοχος έχει «κομβικό ρόλο».**

## Έννοια απαγορεύσεων και μέτρων ασφαλείας

**Ο όρος «απαγορεύσεις»** περιλαμβάνει σαφείς δηλώσεις βουλήσεως του νομίμου κατόχου, είτε γραπτές είτε προφορικές που ενημερώνουν και αποτρέπουν οποιονδήποτε τρίτο να αποκτήσει πρόσβαση στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών ή εν γένει στο πληροφοριακό σύστημα. Αυτές δε οι απαγορεύσεις, **μπορεί να είναι είτε στο φυσικό χώρο** πχ. να είναι εμφανώς αναρτημένες στο χώρο όπου βρίσκονται οι υλικοί φορείς, είτε **να εμφανίζονται ως ηλεκτρονικές ειδοποιήσεις** σε κάποιο στάδιο κατά την προσπάθεια εισόδου του δράστη στο πληροφοριακό σύστημα, πχ. κατά την προσπάθεια του δράστη να εισέλθει στην επιφάνεια εργασίας του Η/Υ του θύματος μπορεί να εμφανίζεται στην οθόνη ότι το περιεχόμενο και το λογισμικό του εν λόγω Η/Υ είναι απόρρητο. Αυτονόητο είναι δε, ότι λαμβάνει χώρα παραβίαση των απαγορεύσεων όταν αυτές είναι σε γλώσσα όπου ο δράστης αντιλαμβάνεται και σε χώρο εμφανή, προκειμένου πράγματι το θύμα να έχει προβεί σε εξωτερίκευση της βούλησης του.

**Ο όρος «μέτρα ασφαλείας»** αφορά μέτρα που κατατείνουν στην μη απόκτησης πρόσβασης από τρίτο πρόσωπο, είτε αυτά αφορούν την μη απόκτηση πρόσβασης **στο φυσικό χώρο** όπως πχ. κλειδαριές, σιδεριές, εγκαταστημένο σύστημα συναγερμού, βιομετρικά μέτρα ασφαλείας. κλπ., είτε πρόκειται για **μέτρα ασφαλείας του λογισμικού** ή του πληροφοριακού συστήματος πχ. η ύπαρξη κωδικού πρόσβασης, η κρυπτογράφηση στοιχείων η οποία συνίσταται στη μέσω μαθηματικών αλγορίθμων μετατροπή ενός προσιτού σε όλους κειμένου σε μια κωδικοποιημένη μορφή που μπορεί να αποκωδικοποιήσει μόνο όποιος διαθέτει το ειδικό μυστικό κλειδί[92], η χρήση συνθηματικών ερωτήσεων η απάντηση των οποίων παρέχει

[91]Το αυτό τονίζει και ο Νούσκαλης, ίδ. Υπερ. 1994 σελ. 1142, Παρατηρήσεις.
[92]Ιδ. σχετικά .Καράκωστα σελ. 175 επ., για το ζήτημα της κρυπτογραφίας.

πρόσβαση στο χρήστη, ή βιομετρικά μέτρα ασφαλείας (αναγνώριση δακτυλικού αποτυπώματος, ίριδας του οφθαλμού κλπ.).

Βέβαια πέραν των όσο προεκτέθηκαν, ορθότερο είναι η παραβίαση των απαγορεύσεων ή των μέτρων ασφαλείας να κρίνεται in concreto κάθε φορά, με αξιολόγηση όλων των συνθηκών τέλεσης ( συνολικό modus operandi του δράστη), ειδικά όταν πρόκειται για παραβίαση απαγορεύσεων ή μέτρων ασφαλείας του φυσικού χώρου διότι εκεί ελλοχεύει ο κίνδυνος να καταλογιστεί στον δράστη και πράξη για την οποία δεν έχει τελέσει την οικεία αντικειμενική και υποκειμενική υπόσταση (!). Για παράδειγμα, ο δράστης που εισέρχεται σε οικία για να κλέψει χρήματα δεν μπορεί να του καταλογισθεί άκριτα, άνευ άλλου τινός, ότι αποπειράθηκε να αποκτήσει πρόσβαση σε ηλεκτρονικό υπολογιστή που βρισκόταν εντός της οικίας.

Όσον αφορά τα ζητήματα της επίδρασης των ως άνω εξωτερικών όρων του αξιοποίνου στον χρόνο και στο τόπο τέλεσης του εγκλήματος, για αυτά γίνεται λόγος εκτενώς στο αντίστοιχο κεφάλαιο.

### Δ. «χωρίς δικαίωμα»

Η παραβίαση των απαγορεύσεων ή των μέτρων ασφαλείας του νομίμου κατόχου δεν αρκεί για την πλήρωση της αντικειμενικής υπόστασης του αδικήματος αν η πρόσβαση δεν αποκτάται **και «χωρίς δικαίωμα»,** όπως ήδη αναφέρθηκε. Και αυτό διότι, μπορεί κάποιος να αποκτήσει πρόσβαση σε πληροφοριακό σύστημα με παραβίαση μέτρων ασφαλείας, όχι απλά σε γνώση αλλά και **κατ' εντολήν του νομίμου κατόχου του.** Συνεπώς στην περίπτωση αυτή δεν διαπράττει καμία αξιόποινη πράξη.

Η φράση ***«χωρίς δικαίωμα»*** ταυτίζεται εννοιολογικά με τις έννοιες «αθέμιτα» ή «άνευ εξουσιοδοτήσεως» ή **«χωρίς την συγκατάθεση»** του νομίμου κατόχου. Συζήτηση έχει προκαλέσει στη θεωρία, η φύση της έννοιας αυτής, ως προς το αν συνιστά στοιχείο της αντικειμενικής υποστάσεως, που ως εκ τούτου θα πρέπει να καλύπτεται από το δόλο του δράστη, ή αν πρόκειται για λόγο άρσης του αδίκου που ερευνάται μετά την πλήρωση του καταρχήν αδίκου.

Ειδικότερα**, η Βασιλάκη** εκκινεί από την βάση ότι πρόκειται για αξιολογικό στοιχείο, εφόσον ως έννοια δεν αποδίδει μια κατάσταση του πραγματικού κόσμου[93], και προχωρά το συλλογισμό της ερευνώντας το αν η φράση «χωρίς δικαίωμα»

[93]Ιδ. Βασιλάκη σελ. 89. Εδώ συμφωνεί με την κρατούσα άποψη που θέλει την συγκατάθεση να έχει πραγματικό χαρακτήρα, καθότι δεν λαμβάνουν χώρα νομικές αξιολογήσεις για την κρίση περί κατάφασης της ή μη.

χαρακτηρίζει την πρόσβαση, οπότε και αποτελεί στοιχείο της αντικειμενικής υποστάσεως, ή το καταρχήν άδικο οπότε η συνδρομή του θα αίρει το τελικά άδικο. Πράγματι, ο **νομοθέτης** δεν **θέλησε να ποινικοποιήσει** την κάθε είδους πρόσβαση σε πληροφοριακό σύστημα με μόνη την παραβίαση μέτρων ασφαλείας, αλλά **αυτή που διαπράττεται χωρίς δικαίωμα, χωρίς την συγκατάθεση [=φυσική βούληση[94]] του** νομίμου κατόχου με την οποία υφίσταται προσβολή του εννόμου αγαθού του τυπικού απορρήτου. Κι **αυτό για να αποκλειστεί η περίπτωση της υπερβολικής ποινικοποίησης όπου** πχ. ένας τεχνικός ηλεκτρονικών συσκευών και πληροφοριακών συστημάτων παραβιάζει κατ' εντολή του νομίμου κατόχου της συσκευής τον κωδικό πρόσβασης που ο ίδιος είχε θέσει και δεν θυμάται.

Για την στοιχειοθέτηση της αντικειμενικής υπόστασης του εγκλήματος απαιτείται ρητά να τελείται η πράξη ενάντια ή χωρίς την βούληση του παθόντος-φορέα του εννόμου αγαθού-νομίμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται. **Εάν λοιπόν δεν συντρέχει η βούληση του παθόντος, τότε η πρόσβαση αποκτάται χωρίς δικαίωμα και πληρείται η αντικειμενική υπόσταση, και συνεπώς το καταρχήν άδικο του εγκλήματος.**

**Επομένως, το «χωρίς δικαίωμα»** συνιστά στοιχείο της αντικειμενικής υποστάσεως του αρ. 370Γ παρ. 2 και ουχί λόγο άρσης του αδίκου. Εν προκειμένω, δεν θα πρέπει τυχόν να συγχέεται το στοιχείο αυτό με τον λόγο άρσης του αδίκου του αρ. 20 ΠΚ περί «ενάσκησης δικαιώματος», όπου το άδικο αίρεται όταν η πράξη που πληροί την ειδική υπόσταση συνιστά αυτή καθ' αυτή περιεχόμενο του δικαιώματος, και όχι μέσω αυτής να σκοπείται η ενάσκηση δικαιώματος συνιστάμενη με άλλη πράξη. Το δικαίωμα πάντα αφορά στην συγκατάθεση του κατόχου. Όταν ελλείπει αυτή και η πρόσβαση αποκτάται χωρίς δικαίωμα, οπότε καταφάσκεται το καταρχήν άδικο αυτό δύναται να αρθεί αν συντρέχουν οι προϋποθέσεις κάποιου λόγου άρσης του αδίκου, όπως πχ. του αρ. 25 ΠΚ ή του αρ. 253 ΚΠΔ, όπου η ανακριτική πράξη συνιστά εκπλήρωση καθήκοντος που επιβάλλεται από το νόμο, από τα αρμόδια όργανα και σύμφωνα με τους προβλεπόμενους όρους[95].

[94]Ο Μυλωνόπουλος (Ποινικό Δίκαιο-Γενικό Μέρος Ι) ισχυρίζεται πως δεν χρειάζεται εξωτερίκευση ρητή ή σιωπηρή της συγκατάθεσης, ούτε γνώση εκ μέρους του δράστη κλπ. σελ 516 , ο Ανδρουλάκης σελ. 353 την αντιμετωπίζει ως ένα απλό πραγματικό γεγονός.
[95] Ίδ. σχετικά Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος Ι», σελ. 254.

## Ε. Διάκριση συγκατάθεσης και συναίνεσης

Καίτοι με μία πρώτη σκέψη δεν τίθεται προβληματισμός, πρέπει ωστόσο σε αυτό το σημείο να δώσουμε προσοχή στην διάκριση της έννοιας της συγκατάθεσης απ' αυτήν της συναίνεσης, η οποία έχει βαρύνουσα πρακτική σημασία[96]. Όπως ήδη εκτέθηκε, **ο νομοθέτης αξιώνει ρητά ως στοιχείο της αντικειμενικής υπόστασης του αρ. 370Γ παρ. 2 την τέλεση της πράξης χωρίς την βούληση του παθόντος-νομίμου κατόχου, η οποία εξωτερικεύεται από την λήψη μέτρων ασφαλείας ή απαγορεύσεων.** Το πραγματικό γεγονός της με βούληση του νομίμου κατόχου απόκτησης πρόσβασης από το δράστη, αίρει την αντικειμενική υπόσταση του εγκλήματος ανεξάρτητα από οιαδήποτε περαιτέρω νομική αξιολόγηση, και δεν υφίσταται προσβολή του εννόμου αγαθού. Γι' αυτό και συμπεραίνεται ότι πρόκειται για συγκατάθεση, διότι η συνδρομή της αποκλείει εννοιολογικά την παράνομη πρόσβαση, ήτοι έχει αμιγώς πραγματικό χαρακτήρα.

Στην περίπτωση τώρα της συναίνεσης, υπάρχει έτσι και αλλιώς προσβολή του εννόμου αγαθού[97] την οποία και δέχεται ο φορέας- έχων την εξουσία διάθεσης (του εννόμου αγαθού) και καταφάσκεται το καταρχήν άδικο. Η τυχόν όμως συναίνεση ερευνάται ως προς το αν πληροί συγκεκριμένες προϋποθέσεις ώστε να άρει ή όχι το τελικά άδικο, γι αυτό και υποστηρίζεται ότι έχει νομικό χαρακτήρα σε αντίθεση με την συγκατάθεση που έχει πραγματικό. Υπό το πρίσμα των ανωτέρω, αναμφίβολα προκύπτει ότι το στοιχείο «χωρίς δικαίωμα» νοείται ως «χωρίς την συγκατάθεση» του παθόντος-νομίμου κατόχου, η συνδρομή της οποίας καθιστά την υπό διερεύνηση πράξη άνευ ποινικού ενδιαφέροντος, θέση η οποία μάλιστα είναι αποδεκτή και από την νομολογία των δικαστηρίων μας[98].

Δέον όπως τονισθεί η σκέψη 17[99], η διάταξη του αρ. 3 της Οδηγίας, και κυρίως η διάταξη του αρ. 2, οι οποίες συνάδουν απόλυτα με τα όσα προελέχθησαν για την ισοδυναμία του όρου «χωρίς δικαίωμα» με την μη ύπαρξη συγκατάθεσης (και όχι συναίνεσης), ως ενός εκ των σωρευτικών στοιχείων της αντικειμενικής υπόστασης που απαιτούνται, την οποία και η προαναφερθείσα διάταξη (της Οδηγίας)

---

[96]Βέβαια, έχει υποστηριχθεί από πολλούς ότι η διάκριση αυτών των δύο εννοιών δεν έχει ουσιαστικό αντίκρισμα και η συγκατάθεση εμπεριέχεται στην ευρύτερη έννοια της συναίνεσης, Ίδετε σχετικά Ανδρουλάκη «Ποινικό Δίκαιο –Γενικό Μέρος-Θεωρία για το έγκλημα», σελ.336.

[97]Τόσο ο Μυλωνόπουλος όσο και ο Ανδρουλάκης διαφωνούν με την άποψη του Roxin ότι η συναίνεση αποκλείει την αντικειμενική υπόσταση του και θεωρούν εσφαλμένη την σύλληψη του εννόμου αγαθού ως «φιλελεύθερη έννοια», καθότι η προσβολή του ή μη συνιστά αντικειμενικό γεγονός. Ίδ. σχετικά Ανδρουλάκης σελ. 337 & 338.

[98]Ιδ. απόφαση 530/2003 ΝαυτΠειρ ΠοινΧρον. ΝΔ/2004, σελ. 76.

[99]*«ή στην περίπτωση εξουσιοδοτημένης δοκιμής».*

αποδίδει ως «*μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο*» του συστήματος ή μέρους του ή «*μη επιτρεπόμενη δυνάμει του εθνικού δικαίου*».

## ΣΤ. Η συναίνεση του νομίμου κατόχου ως ειδικός λόγος άρσης του αδίκου του αρ. 370Γ § 2;

Η συναίνεση του παθόντος ως γενικός λόγος άρσης του αδίκου δεν προβλέπεται στον Ποινικό μας Κώδικα, παρά μόνο ως ειδικός στο άρθρο 308 παρ.2 όπου αίρει το άδικο *(«δεν είναι άδικη»)* στην αξιόποινη πράξη της απλής σωματικής βλάβης, με την ρητή προϋπόθεση ότι δεν προσκρούει στα χρηστά ήθη. Η κρατούσα άποψη[100] θέλει την συναίνεση του παθόντος ως λόγο άρσης του αδίκου να μπορεί να εφαρμοστεί αναλογικά και σε άλλες αξιόποινες πράξεις αίροντας το τελικό άδικο αυτών, και μάλιστα ανεξαρτήτως του αν προσκρούει στα χρηστά ήθη, με μοναδικά κριτήρια εκ μέρους του συναινούντος: την εξουσία διάθεσης του εννόμου αγαθού, την ικανότητα διάκρισης και αξιολόγησης της συναίνεσης ως προς την συγκεκριμένη πράξη, σαφούς αποδοχής της προσβολής, βούλησης απαλλαγμένης ελαττωμάτων, εξωτερίκευση της συναίνεσης και προϋφιστάμενη της πράξης.

Η αναλογική εφαρμογή βέβαια δεν μπορεί να λάβει χώρα απεριορίστως, αλλά in bonam partem σε πράξεις που παρουσιάζουν αξιολογική ομοιότητα με την διάταξη του αρ. 308, δηλαδή σε πράξεις όπου ο πράτων έχει την εξουσία διάθεσης του εννόμου αγαθού, άρα μόνον σε ατομικά έννομα αγαθά. **Ως εκ τούτου, δεδομένου ότι στην διάταξη του αρ. 370Γ παρ. 2 προστατευόμενο έννομο αγαθό τυγχάνει έως την μέχρι σήμερα κρατούσα άποψη το τυπικό απόρρητο, ήτοι ατομικό έννομο αγαθό**, θα μπορούσε να υποστηριχθεί ότι η συναίνεση του νομίμου κατόχου-έχοντος την εξουσία διαθέσεως του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται, μπορεί να άρει το τελικά άδικο της παράνομης πρόσβασης ως ενάσκηση του δικαιώματος του προς ανάπτυξη της ιδίας προσωπικότητας, εφόσον πρόκειται για ελαφρές προσβολές απ' τις οποίες δεν θίγεται στον πυρήνα της η ανθρώπινη αξιοπρέπεια. Η δε συναίνεση στο πλαίσιο του αρ. 370Γ παρ. 2, δεδομένου ότι πρόκειται για έγκλημα διακινδύνευσης και όχι βλάβης, θα πρέπει να θεωρηθεί ότι εξαντλείται στην αναδοχή του κινδύνου, όχι και στην πραγμάτωση αυτού[101].

**Ωστόσο, ληφθέντος του ότι η μη ύπαρξη φυσικής βούλησης του νομίμου κατόχου να αποκτήσει κάποιος τρίτος πρόσβαση στο πληροφοριακό σύστημα συνιστά στοιχείο της αντικειμενικής υπόστασης («χωρίς δικαίωμα»), όπου η**

[100] Ιδ. Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος Ι» σελ. 512 και Ανδρουλάκης σελ. 335.
[101] Ιδ. σχετικά με συναίνεση στην διακινδύνευση Ανδρουλάκη σελ. 344-345.

**συνδρομή της αποκλείει την στοιχειοθέτηση της, η συναίνεση δεν μπορεί να άρει το άδικο του αρ. 370 Γ παρ. 2 ως ειδικός λόγος άρσης του αδίκου[102], αφού σε αυτήν την περίπτωση δεν υφίσταται ούτε καν καταρχήν άδικο (!).** Εάν ο νόμιμος κάτοχος επιθυμεί κάποιο άλλο πρόσωπο να αποκτήσει πρόσβαση σε στοιχεία του πληροφοριακού συστήματος που έχει την εξουσία να διαθέτει, με παραβίαση απαγορεύσεων-μέτρων ασφαλείας που έχει λάβει, δεν υφίσταται αξιόποινη πράξη παράνομης πρόσβασης · η πρόσβαση είναι νόμιμη αφού δεν συντρέχουν τα απαιτούμενα του αρ. 370Γ παρ. 2 συνεπώς σε ποια «ανύπαρκτη» προσβολή του τυπικού απορρήτου του δύναται «λογικά» και κατ' επέκταση νομικά συναινεί τελικά ο νόμιμος κάτοχος ο οποίος μόνος του έχει καταργήσει τον χαρακτήρα του πληροφοριακού συστήματος ως τυπικά απορρήτου; Σε καμία ασφαλώς! Οπότε, ως λόγοι άρσης του αδίκου θα εξετασθούν οι γενικοί των άρθρων 20-25 ΠΚ, καθώς και ειδικοί, όπου τέτοιοι προβλέπονται σε ποινικές διατάξεις.

## ΑΡΘΡΟ 370Γ § 2 εδ. β΄: ΠΕΡΙΠΤΩΣΗ ΤΕΛΕΣΗΣ ΠΟΥ ΑΦΟΡΑ ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ΄Η ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΚΡΑΤΟΥΣ

Η παρούσα περίπτωση, πέραν των όσων ρητά περιλαμβάνει η ειδική υπόσταση του εγκλήματος στο εδ. α΄ της παρ. 2 του αρ.370 Γ, θέτει ένα επιπλέον στοιχείο: αυτό των διεθνών σχέσεων και της ασφάλειας του κράτους, το οποίο την καθιστά μάλιστα κακούργημα με απειλούμενη ποινή κάθειρξης, κατ' ευθεία παραπομπή στο άρθρο 148 ΠΚ. Περαιτέρω τα στοιχεία της ασφάλειας του κράτους και των διεθνών σχέσεων καθιστούν τον χαρακτήρα του προστατευόμενου έννομου αγαθού από ατομικό σε υπερατομικό.

Ως στοιχείο που αφορά την ασφάλεια του κράτους είναι συνήθως μυστικό που αφορά στην εξωτερική ασφάλεια του κράτους, δηλαδή το σχετικά «αδιακινδύνευτο» αυτής απέναντι σε ξένα κράτη. Ενώ, στοιχείο που αναφέρεται στις διεθνείς σχέσεις του κράτους είναι συνήθως μυστικό που αφορά στις μεταξύ των Κυβερνήσεων των διαφόρων χωρών αναπτυσσόμενες επαφές[103]. Καίτοι αναφέρεται στην ενότητα των δικονομικών ζητημάτων, **ορθότερο είναι** όταν η παράνομη πρόσβαση σε πληροφοριακό σύστημα αφορά την ασφάλεια του κράτους και τις διεθνείς σχέσεις η **ποινική δίωξη να ασκείται αυτεπαγγέλτως και όχι κατόπιν εγκλήσεως**, καθώς η διάταξη αυτή δεν έχει θεσπιστεί για την προστασία του ιδιωτικού συμφέροντος, αλλά του γενικού συνόλου.

[102]Ιδ. Μυλωνόπουλο σελ. 514-515.
[103]Ιδ. Φιλόπουλο σελ. 190.

## ΑΡΘΡΟ 370Γ §3 : ΠΕΡΙΠΤΩΣΗ ΤΕΛΕΣΗΣ ΑΠΟ ΔΡΑΣΤΗ ΠΟΥ ΕΙΝΑΙ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΤΟΥ ΝΟΜΙΜΟΥ ΚΑΤΟΧΟΥ

Η αξιόποινη συμπεριφορά της παρ. 3 του αρ. 370Γ ΠΚ συνιστά **ιδιαίτερο έγκλημα**, καθότι δράστης μπορεί να είναι μόνο «**υπόχρεος σε πίστη» λόγω της εργασιακής σχέσης** που τον συνδέει με τον εργοδότη του-νόμιμο κάτοχο του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών.

Η εν λόγω περίπτωση συνδέεται με την προβληματική του στοιχείου «χωρίς δικαίωμα», και αποκλείει το καταρχήν άδικο συνιστώντας έναν ειδικό περιορισμό της αντικειμενικής υπόστασης και ως εκ τούτου περιορισμό του κινδύνου υπερβολικής ποινικοποίησης που εγκυμονεί το ευρύ πεδίο εφαρμογής της παρ. 2, ακριβώς για τις περιπτώσεις κατά τις οποίες ο εργαζόμενος λόγω της ιδιότητας του αποκτά de facto πρόσβαση στο πληροφοριακό σύστημα του εργοδότη του, προκειμένου να εκτελέσει τα καθήκοντα του. Η διασφάλιση αυτή πραγματοποιείται από το γεγονός ότι η πράξη της πρόσβασης είναι τιμωρητέα **όταν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του εργοδότη-νομίμου κατόχου**[104]**,** η οποία ασφαλώς έχει περιέλθει σε γνώση του εργαζομένου-δράστη. Σημειωτέον, ότι ο εργαζόμενος-υπάλληλος πρέπει να εκτελεί εξαρτημένη εργασία («είναι στην υπηρεσία του νομίμου κατόχου» ακόμη και σε επιχείρηση του δημοσίου τομέα), γιατί τότε μόνο η απαγόρευση είναι δεσμευτική γι' αυτόν, δεν έχει δε δικαίωμα να εξετάσει την νομιμότητα του εσωτερικού κανονισμού ή της έγγραφης απόφασης του κατόχου ή αρμοδίου υπαλλήλου του.

Ιδιαίτερης διερεύνησης χρήζουν οι περιπτώσεις κατά τις οποίες ο εργαζόμενος αποκτά πρόσβαση στο πληροφοριακό σύστημα καθ' όν μέρος που δεν έχει δικαίωμα, ή για σκοπό που δεν άπτεται της εργασιακής σχέσης, αλλά για ιδιωτικούς σκοπούς όπως πχ. απόκτηση πρόσβασης σε προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου του εργοδότη-νομίμου κατόχου αντί του επαγγελματικού λογαριασμού στο οποίο έχει πρόσβαση. Σε αυτές τις περιπτώσεις ο εργαζόμενος διαπράττει το αδίκημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα.

Πρέπει δε να επισημανθεί ότι, τυχόν σχετικές συμβατικές υποχρεώσεις δεν δημιουργούν άνευ άλλου τινός ποινική ευθύνη του εργαζομένου, αλλά αυτό θα κρίνεται πάντα in concreto, μετά από εκτίμηση των πραγματικών περιστατικών. Το

[104]Η Βασιλάκη κάνει λόγο για καθορισμό των ορίων πρόσβασης του εργαζομένου σε στοιχεία του εργοδότη και από το συμβόλαιο εργασίας- συναφθείσα σύμβαση εργασίας, το οποίο πράγματι θα ξεκαθάριζε εξαρχής το τοπίο.

καθοριστικό στοιχείο στην παρ. 3 είναι η ρητή απαγόρευση πρόσβασης από εσωτερικό κανονισμό ή από έγγραφη απόφαση του νομίμου κατόχου ή αρμοδίου υπαλλήλου του. Η υπό κρίση περίπτωση λοιπόν κινούμενη στο ίδιο πνεύμα με την Οδηγία και συγκεκριμένα με τις σκέψεις 17 και 18, όπου προβλέπεται διαφορετική ποινική αντιμετώπιση του προσώπου που έχει πρόσβαση στο πληροφοριακό σύστημα μέσα στο πλαίσιο των καθηκόντων του, απ' αυτόν που προσπαθεί για πρώτη φορά να την αποκτήσει.

## ΕΙΔΙΚΗ ΥΠΟΣΤΑΣΗ: ΥΠΟΚΕΙΜΕΝΙΚΗ ΥΠΟΣΤΑΣΗ του αρ. 370 Γ §2

### Ενδεχόμενος ή άμεσος δόλος;

Η αξιόποινη πράξη της παράνομης πρόσβασης σε πληροφοριακό σύστημα ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, επί τη βάσει του ανωτάτου ορίου του απειλούμενου πλαισίου ποινής της φυλάκισης συνιστούσε πλημμέλημα (αρ. 18 ΠΚ) και απαιτείτο επικάλυψη της αντικειμενικής υπόστασης με οποιουδήποτε είδος δόλου (κατά άρθρο 26 ΠΚ). **Συνεπώς, κατά την κρατούσα, μέχρι και τις τροποποιήσεις του Ν. 4411/2016, άποψη** η υπαιτιότητα που απαιτεί το αρ. 370Γ παρ. 2 συνίστατο σε **ενδεχόμενο δόλο**, δεδομένου ότι στην ειδική υπόσταση του εγκλήματος δεν αξιώνεται η τέλεση της πράξης εν γνώσει ορισμένων στοιχείων από τον δράστη[105], πολλώ δε μάλλον η επιδίωξη συγκεκριμένου σκοπού («με σκοπό να» ή «προκειμένου να»).

Ο ποινικός νομοθέτης δηλαδή, **αρκείτο στο ότι ο δράστης γνωρίζει με την συμπεριφορά του ότι ενδέχεται να προκαλέσει** την αξιόποινη συμπεριφορά, ήτοι να αποκτήσει χωρίς δικαίωμα πρόσβαση (γνωστικό στοιχείο) **και το αποδέχεται** (βουλητικό στοιχείο) . Καίτοι το ζήτημα της υπαιτιότητας φαίνεται να επιλύεται απλά κατά τα ανωτέρω, χωρίς περαιτέρω προβληματισμούς, η Βασιλάκη[106] έχει πάρει ρητά αντίθετη θέση, υποστηρίζοντας πως ο ποινικός νομοθέτης απαιτεί την συνδρομή άμεσου δόλου (α΄ ή β΄ βαθμού), διότι η παράνομη πράξη πρέπει να γίνεται χωρίς δικαίωμα, δηλαδή απαιτείται η γνώση ορισμένου περιστατικού. Η ως άνω άποψη δεν αναλύεται από την ίδια και γι' αυτό συμπεραίνεται πως ερείδεται στον εξής συλλογισμό: το στοιχείο της αντικειμενικής υπόστασης «*χωρίς δικαίωμα*» όπως αναλύθηκε στο οικείο κεφάλαιο, νοείται ως χωρίς την συναίνεση του νομίμου

[105]Ιδ. Φιλόπουλο σελ. 191.
[106]Ιδ. Βασιλάκη σελ. 93 για υποκειμενική υπόσταση του αρ. 370Γ παρ. 2.

κατόχου του πληροφοριακού συστήματος, συνεπώς κατά την προδιατυπωθείσα άποψη, ο εν λόγω δράστης γνωρίζει ότι ούτε νόμιμος κάτοχος του πληροφοριακού συστήματος είναι ούτε έχει την απαιτούμενη εξουσιοδότηση για να αποκτήσει πρόσβαση, και το επιδιώκει ή έστω το αποδέχεται.

**Την ανωτέρω άποψη της Βασιλάκη αποδυναμώνει, κατά την γνώμη της γράφουσας, το γεγονός** ότι καίτοι η ίδια εντάσσει το στοιχείο 'χωρίς δικαίωμα' στην αντικειμενική υπόσταση του αρ. 370Γ παρ. 2 χαρακτηρίζοντας-προσδιορίζοντας την πρόσβαση, εν τούτοις προκαλεί σύγχυση προσπαθώντας να του προσδώσει, και όχι να το επικαλύψει με το στοιχείο της υπαιτιότητας. Υπ' αυτή την λογική λόγου χάρη στο έγκλημα της κλοπής του αρ. 372 ΠΚ θα έπρεπε να θεωρήσουμε ότι δεν αρκεί ο ενδεχόμενος δόλος, αλλά απαιτείται άμεσος δόλος γιατί η πράξη της αφαίρεσης τελεί σε γνώση ότι το κινητό πράγμα είναι ξένο (!). Όπως γίνεται αντιληπτό η άποψη αυτή οδηγεί σε άτοπα.

Σε κάθε δε περίπτωση, η απαίτηση συνδρομής ενδεχόμενου δόλου επιβεβαιώνεται και από το άρθρο 3 της Οδηγίας η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 4411/2016 και το τροποποιημένο άρθρο 370Γ παρ. 2, η οποία ρητά απαιτεί την «εκ προθέσεως και χωρίς δικαίωμα πρόσβαση», μην απαιτώντας «βαρύτερη» μορφή δόλου.

Τέλος, σε περίπτωση που δεν συντρέχει ενδεχόμενος δόλος στο πρόσωπο του δράστη αλλά αμέλεια, η πράξη θα παραμείνει ατιμώρητη, καθώς η παράνομη πρόσβαση δεν τυποποιείται και ως έγκλημα από αμέλεια[107].

## Πραγματική Πλάνη

Όταν ο δράστης αγνοεί ή πλανάται ως προς την λήψη (από το νόμιμο κάτοχο) απαγορεύσεων και μέτρων ασφαλείας, αγνοεί στοιχεία της εν ευρεία εννοία αντικειμενικής υποστάσεως της διάταξης[108], συνεπώς έχουμε πραγματική πλάνη και δεν στοιχειοθετείται το έγκλημα του αρ. 370Γ παρ. 2. Ωστόσο, επισημαίνεται εκ νέου ότι είναι εξαιρετικά δύσκολο να λάβει χώρα τέτοιου είδους πλάνη, αφού η ισχύουσα διάταξη απαιτεί ρητά την απόκτηση πρόσβασης με την σωρευτική συνδρομή παραβίασης απαγορεύσεων ή μέτρων ασφαλείας.

[107]Ιδ. Φιλόπουλο σελ. 191 για επιμέρους περιπτώσεις, όπου ο φυσικός αυτουργός της πράξης παραμένει ατιμώρητος.
[108]καθότι όπως παρατέθηκε, τα ως άνω συνιστούν εξωτερικούς όρους του αξιοποίνου και εντάσσονται στην αντικειμενική υπόσταση της διάταξης εν ευρεία εννοία.

Η δε πλάνη ως προς την ύπαρξη μερικής ή ολικής συγκατάθεσης του νομίμου κατόχου να αποκτήσει ο δράστης πρόσβαση στο πληροφοριακό σύστημα είναι πραγματική διότι έχει αμιγώς πραγματικό χαρακτήρα (η συγκατάθεση δηλαδή) και αποκλείει το δόλο[109], όπως εκτέθηκε ανωτέρω.

## Νομική Πλάνη

Διαφορετική περίπτωση με την αμέσως προαναφερθείσα, συνιστά αυτή στην οποία ο δράστης πλανάται ως προς το γεγονός ότι η ανάκληση του δικαιώματος από τον νόμιμο κάτοχο περί απόκτησης πρόσβασης στο πληροφοριακό σύστημα είναι ανίσχυρη ως προς το πρόσωπο του. Στην εν λόγω περίπτωση πρόκειται για νομική πλάνη[110].

## ΑΠΟΠΕΙΡΑ

Στο ζήτημα της απόπειρας τέλεσης του εγκλήματος του αρ. 370Γ παρ. 2, η μη πλήρωση του εξωτερικού όρου του αξιοποίνου (η οποία και ερευνάται αυτεπαγγέλτως από το δικαστήριο), ήτοι η απόκτηση πρόσβασης χωρίς την παραβίαση μέτρων ασφαλείας ή απαγορεύσεων, ασκεί καταλυτική επίδραση, αφού χωρίς την συνδρομή αυτών δεν υφίσταται αξιόποινη πράξη και δεν είναι δυνατή η τιμώρηση για απόπειρα, για συμμετοχή, ούτε και για επιβολή μέτρου ασφαλείας[111].

Επιστρέφοντας στο σχηματικό παράδειγμα των τριών (3) σταδίων[112], για απόπειρα μπορεί να γίνει λόγος μόνο στο 1ο στάδιο, όπου ακόμα ο δράστης «παρενοχλεί» το σύστημα προσπαθώντας να παραβιάσει απαγορεύσεις ή μέτρα ασφαλείας. Από την στιγμή όμως που έχει ολοκληρωθεί η παραβίαση και εμφανίζεται το μενού λειτουργιών δίνεται στο δράστη η δυνατότητα να εκτελέσει οποιαδήποτε (!) λειτουργία ή πρόγραμμα του πληροφοριακού συστήματος, (είτε ολικά είτε μερικά), το εν λόγω έγκλημα συμπεριφοράς είναι τετελεσμένο και δεν ευρίσκεται πλέον στο στάδιο της απόπειρας · έχει ήδη τεθεί ο κίνδυνος του εννόμου αγαθού. Είναι αδιάφορο δε, εάν ο δράστης μπορεί να «διαβάσει» ή να «κατανοήσει» το περιεχόμενο των στοιχείων του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται. Η πρόσβαση αυτή καθεαυτή θεμελιώνει αυτοτελές άδικο.

---

[109]Ιδ. Μυλωνόπουλο "Ποινικό Δίκαιο-Γενικό Μέρος ΙΙ", σελ. 517.
[110]Ιδ. Φιλόπουλο σελ. 192.
[111]Ιδ. Κωστάρα σελ. 83 & Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος» σελ. 135
[112]Ιδ. κεφάλαιο της παρούσης εργασίας «Ειδική υπόσταση: Αντικειμενική Υπόσταση, Α. Απόκτηση πρόσβασης»

**Η Οδηγία** ωστόσο δεν προβλέπει, πολλώ δε μάλλον δεν απαιτεί, από τα κράτη-μέλη την τιμώρηση της απόπειρας τέλεσης της παράνομης πρόσβασης σε συστήματα πληροφοριών, παρά μόνο υποχρεώνει την τιμώρηση όλων των μορφών συμμετοχής στο εν λόγω έγκλημα (άρθρο 8). Παράλληλα, προβλέπεται το αυτοτελές ποινικό αδίκημα των προπαρασκευαστικών πράξεων (άρθρο 7), που θα εκτεθεί εν συνεχεία.

Ολοκληρώνοντας το παρόν κεφάλαιο χρήζει αναφοράς, πως μετά την ισχύ του Ν. 4411/2016, η απόπειρα τελέσεως του αρ. 370Γ παρ. 2 **δεν μπορεί να κριθεί πλέον ατιμώρητη σύμφωνα με τον προβλεπόμενο στο άρθρο 42 παρ. 3 ΠΚ λόγο δικαστικής άφεσης της ποινής, καθώς προβλεπόμενη ποινή είναι εφεξής η φυλάκιση (10 ημέρες -5 έτη, και όχι 3 μήνες όπως ίσχυε προ του Ν. 4411/2016).**

## ΤΟΠΟΣ ΤΕΛΕΣΗΣ

Από το σύνολο θεωρίας και νομολογίας, και εξ' όσων ήδη παρατέθηκαν στο κεφάλαιο περί διεθνούς και ενωσιακού νομοθετικού πλαισίου, τονίζεται επανειλημμένως **ο διασυνοριακός χαρακτήρας του εγκλήματος της παράνομης πρόσβασης όταν αυτό τελείται με την χρήση του διαδικτύου**, και της ανάγκης συνεργασίας τουλάχιστον δύο κρατών σχετικά με την εξιχνίαση και εντοπισμό του δράστη. Εξαιρετικά εύστοχα, **το έγκλημα στον κυβερνοχώρο εν γένει** έχει χαρακτηρισθεί από την Ζάννη[113] ως έγκλημα ***«χωρίς πατρίδα»***, παρότι τα αποτελέσματα του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους.

Όπως δε είναι γνωστό, ο **τόπος τελέσεως του αδικήματος** έχει εξαιρετικά βαρύνουσα σημασία, καθότι σύμφωνα με τον γενικά αναγνωρισμένο κανόνα διεθνούς δικαίου της **αρχής της εδαφικότητας,** καθορίζει την ποινική δικαιοδοσία ενός κράτους για τις πράξεις που τελούνται στο έδαφος του (αρ. 5 ΠΚ)**. Περαιτέρω, ο Έλληνας νομοθέτης υιοθετεί στο άρθρο 16 ΠΚ την «θεωρία της ενότητας»** σύμφωνα με την οποία, τόπος τέλεσης της πράξης θεωρείται τόσο ο τόπος όπου ενήργησε ή όφειλε να ενεργήσει ο δράστης, όσο και ο τόπος όπου επήλθε το αξιόποινο αποτέλεσμα[114].

Προκειμένου λοιπόν να αποφανθούμε για τον τόπο τέλεσης του αδικήματος του αρ. 370Γ παρ. 2, και κατ' επέκταση την θεμελίωση ή μη ποινικής δικαιοδοσίας

[113]Ιδ. Ζάννη, σελ. 63.
[114]Ιδ. Μυλωνόπουλο «Διεθνές Ποινικό Δίκαιο, Τα τοπικά όρια των ποινικών νόμων» σελ. 151 επ.

από τις αρμόδιες ελληνικές αρχές και τα ποινικά δικαστήρια, **οφείλουμε να λάβουμε υπόψιν κάποια χαρακτηριστικά της αξιόποινης αυτής πράξης.** Ως ήδη εκτέθηκε στο οικείο κεφάλαιο, πρόκειται για ένα **έγκλημα ενέργειας, διακινδύνευσης και συμπεριφοράς,** καθόσον η μεταβολή που επέρχεται στον εξωτερικό κόσμο, δεν διακρίνεται της συμπεριφοράς. Με άλλα λόγια, η συμπεριφορά του δράστη (απόκτηση πρόσβασης σε πληροφοριακό σύστημα) συνδέεται αναπόσπαστα με το υλικό αντικείμενο στο οποίο επενεργεί και το έγκλημα συντελείται με την απόκτηση πρόσβασης. Ως εκ τούτου, εφαρμόζοντας το αρ. 16 ΠΚ και εφόσον πρόκειται για έγκλημα συμπεριφοράς, θα εμφανίζεται το παράδοξο σε πράξη παράνομης πρόσβασης που έχει πραγματοποιηθεί από πχ. Ισραηλινό σε πληροφοριακό σύστημα Έλληνα κατόχου να μην έχει η Ελλάδα καμία ποινική δικαιοδοσία, και να τυχόν το Ισραήλ δεν ποινικοποιεί την εν λόγω πράξη ο δράστης να μείνει τελικά ακαταδίωκτος ατιμώρητος (!). Υπό το πρίσμα αντιστοίχων πιθανών περιπτώσεων και συναφών προβληματισμών **ο Κιούπης** έχει εύστοχα επισημάνει πως η διάταξη του αρ. 16 ΠΚ εφαρμόζεται λίαν αποτελεσματικά στα «παραδοσιακά- κοινά εγκλήματα», δεν μπορεί όμως να τύχει εφαρμογής στα κυβερνοεγκλήματα[115]. Εκεί τα πράγματα γίνονται ιδιαίτερα πολύπλοκα, καθώς ο δράστης μπορεί να εισέρχεται στο Διαδίκτυο από οποιοδήποτε κράτος ανά την υφήλιο, ο δε server του παρόχου πρόσβασης μπορεί να είναι εγκατεστημένος σε κάποιον άλλο κράτος και ο χρήστης του οποίου «χακάρεται» το πληροφοριακό σύστημα να βρίσκεται στην Ελλάδα.

Ο ποινικός νομοθέτης προσπαθώντας να επιλύσει συναφή ζητήματα και να θεμελιώσει ελληνική ποινική δικαιοδοσία τροποποίησε με τον **Ν. 4267/2014[116] το άρθρο 5 του ΠΚ προσθέτοντας την εξής παράγραφο :** «*3. Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και* ***η ελληνική επικράτεια, εφόσον στο έδαφός της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους»*.** Ωστόσο, με την διάταξη αυτή επεκτείνεται υπερβολικά το αξιόποινο, και εμφανίζεται το παράδοξο η Ελλάδα να μπορεί να θεμελιώσει ποινική δικαιοδοσία για οποιοδήποτε κυβερνοέγκλημα[117] και κατ' επέκταση τίθενται ζητήματα παραβίασης της αρχής ne bis in idem.

Επομένως, ούτε αυτή η πρόσφατη νομοθετική τροποποίηση μπορεί να επιλύσει το ζήτημα του τόπου τελέσεως του αρ. 370Γ παρ. 2 και έτερων

[115]Ιδ. Κιούπη «Ποινικό Δίκαιο και Ίντερνετ», σελ. 79-81.
[116] http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=CC0Lu-vKzI0%3D&tabid=132 .
[117]Ιδ. Σπυρόπουλο για τη κριτική για τη νέα διάταξη, σελ. 158.

κυβερνοεγκλημάτων. Η δε Οδηγία καίτοι περιλαμβάνει άρθρο περί ζητημάτων δικαιοδοσίας[118], δεν επιλύει τα προβλήματα. **Δέον όπως επισημανθεί σε αυτό το σημείο ότι για την τοποθέτηση επί του τόπου τελέσεως του εν λόγω αδικήματος,** πέραν του τόπου όπου αποκτά πρόσβαση ο δράστης, **έννομη σημασία έχει και ο τόπος όπου παραβιάζονται οι απαγορεύσεις ή τα μέτρα ασφαλείας (όταν φυσικά αυτοί οι τόποι διαφέρουν, όπου στο πλαίσιο του αρ. 370Γ παρ. 2 είναι αδύνατο να συμβεί διότι με την παραβίαση των μέτρων ασφαλείας αποκτάται η πρόσβαση), δηλαδή που λαμβάνουν χώρα οι εξωτερικοί όροι του αξιοποίνου, η συνδρομή των οποίων θεμελιώνει αξιόποινο.**

**Ομοίως, ο Κριθαράς[119]** με αφετηρία την θεωρία της ενότητας θεωρεί ως τόπο τέλεσης τόσο τον τόπο που είναι εγκατεστημένος ο server που φιλοξενεί την ιστοσελίδα του δράστη (που εκδηλώνεται η παράνομη συμπεριφορά ) όσο και τους τόπους όπου οι χρήστες του διαδικτύου αποκτούν πρόσβαση στο περιεχόμενο της ιστοσελίδας (ιδιωτικός ψηφιακός χώρος απορρήτου του χρήστη-θύματος). **Ο Καράκωστας[120]** δε υιοθετώντας την **θεωρία του βαρύνοντος τόπου** υποστηρίζει πως τόπος τέλεσης των κυβερνοεγκλημάτων είναι το κράτος στο οποίο εκδηλώνεται η κύρια σημασία του αδικήματος. Τέλος, **ο Μυλωνόπουλος** σχετικά με τα διεθνή όρια των ποινικών νόμων έχει υποστηρίξει πως στα εγκλήματα αφηρημένης διακινδύνευσης, όπου ο κίνδυνος δεν είναι στοιχείο της αντικειμενικής υπόστασης ότι τόπος τέλεσης είναι μόνο ο τόπος που εκδηλώθηκε η έκνομη συμπεριφορά ρου δράστη.

Έχοντας ανατρέξει σε διάφορες απόψεις που έχουν υποστηριχθεί σχετικά στην θεωρία, **ο Κιούπης[121] πρότεινε –την ορθότερη κατά την γνώμη της γράφουσας-** θέση σύμφωνα με την οποία τόποι τέλεσης των διαδικτυακών εγκλημάτων να θεωρούνται αυτοί στους οποίους οι χρήστες «κάλεσαν» την ψηφιακή

[118]**Άρθρο 12 Δικαιοδοσία** *« 1. Τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, εφόσον το αδίκημα έχει διαπραχθεί: α) εν όλω ή εν μέρει στο έδαφος τους· ή β) από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί. 2. Κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμφωνα με την παράγραφο 1 στοιχείο α), εξασφαλίζει ότι διαθέτει δικαιοδοσία, οσάκις: α) ο δράστης διέπραξε το αδίκημα, όταν ευρίσκετο στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του· ή β) το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός του ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα ευρίσκετο στο έδαφός του. 3. Το κράτος μέλος ενημερώνει σχετικά την Επιτροπή οσάκις αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8, το οποίο διαπράττεται εκτός του εδάφους του, οσάκις, μεταξύ άλλων: α) ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή β) το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του».*

[119]Ιδ. Κριθαρά σελ. 44.

[120]Ιδ. Καρακώστα σελ. 265-267.

[121]Ιδ. Κιούπη σελ. 92-94.

σελίδα[122], «κατέβασαν» δηλαδή τα δεδομένα και απέκτησαν πρόσβαση στο διαδίκτυο. Έτσι δεν υπέχει καμία ποινική ευθύνη ο παραγωγός δεδομένων όπου παράγει και αποθηκεύει δεδομένα στο server, καθώς η συμπεριφορά του εξαντλείται εδώ· αλλά η συμπεριφορά των χρηστών όπου εισάγουν τα δεδομένα στο χώρο της αντίστοιχης έννομης τάξης. Πράγματι, αυτή η θεώρηση μειώνει δραστικά τους πιθανούς τόπους τέλεσης του εγκλήματος, τοποθετώντας στο ποινικό επίκεντρο τους πραγματικά ενδιαφέροντες.

## ΕΥΘΥΝΗ ΠΑΡΟΧΟΥ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το ζήτημα της τυχόν ποινικής ευθύνης των νομίμων εκπροσώπων του παρόχου πρόσβασης στο διαδίκτυο για αξιόποινες πράξεις που έχουν τελέσει οι χρήστες του, έχει απασχολήσει τον νομικό κόσμο τόσο για άλλα αδικήματα, όσο και γι' αυτό της χωρίς δικαίωμα πρόσβασης σε πληροφοριακό σύστημα. Δέον όπως διευκρινιστεί ευθύς εξαρχής πως στην ελληνική έννομη τάξη δεν έχει θεσπιστεί κανένα νομοθέτημα και καμία διάταξη μέχρι στιγμής που να θεμελιώνει ποινική ευθύνη του παρόχου πρόσβασης για χρήστες που αποκτούν παράνομη πρόσβαση σε πληροφοριακό σύστημα ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών[123].

Έτσι, στην υπό κρίση ενότητα εξετάζεται λίαν συντόμως εάν και σε ποια έκταση και υπό ποιες προϋποθέσεις θα μπορούσε να θεμελιωθεί ποινική ευθύνη του παρόχου για τις περιπτώσεις όπου η χωρίς δικαίωμα πρόσβαση επιτυγχάνεται εξ' αποστάσεως μέσω διαδικτύου[124], δεδομένου εκτός των άλλων ότι η πρόσβαση και περιήγηση στο διαδίκτυο γίνεται υπ' ευθύνη των ίδιων των χρηστών. Ο πάροχος πρόσβασης στο διαδίκτυο έχει τις δικές του ιστοσελίδες, όπου παρουσιάζει μέσω αυτών διάφορα στοιχεία και δεδομένα κλπ (ενεργεί δηλαδή ως παραγωγός δεδομένων και ευθύνεται σχετικά), συνάπτει δε «συμβάσεις» με χρήστες στους οποίους επιτρέπει την πρόσβαση στο διαδίκτυο. Ειδικότερα επί τη βάσει αυτών των συμβάσεων «ανοίγει τον δίαυλο» του χρήστη με το διαδίκτυο προκειμένου ο τελευταίος να αποκτήσει πρόσβαση αφενός, και αφετέρου υποστηρίζει τεχνικά την σύνδεση του

[122]Όπως έχει αναφερθεί ανωτέρω, το Διαδίκτυο-Ίντερνετ συνιστά μία πολύ εξελιγμένη μορφή τηλεφωνικής επικοινωνίας.
[123]Υπάρχει όμως σχετικά το Προεδρικό Διάταγμα υπ' αριθμ. 131/2003 που αφορά το ηλεκτρονικό εμπόριο.
[124]Αυτονόητο είναι ότι όταν η πράξη τελείται με φυσική πρόσβαση στο χώρο όπου βρίσκονται οι υλικοί φορείς, ο πάροχος πρόσβασης στο διαδίκτυο δεν μπορεί να έχει γνώση (!).

χρήστη με την υποδομή του ίδιου του παρόχου και διοχετεύει ψηφιακά δεδομένα που αντιστοιχούν σε διαδικτυακές ενέργειες στις οποίες προβαίνει ο χρήστης.

Τυχόν ευθύνη του παρόχου μπορεί να γεννηθεί μόνο κατά το τελευταίο αυτό στάδιο της διοχέτευσης δεδομένων, καθώς οι προαναφερόμενες ενέργειες του παρόχου συνιστούν νόμιμη εκπλήρωση των όρων της μεταξύ τους συμβατικής του σχέσης. Ωστόσο η διοχέτευση δεδομένων δεν συνιστά «ανθρώπινη συμπεριφορά» και δεν εκτελείται «συνειδητά» κατ΄ εντολή του παρόχου, αλλά αυτόματα, χωρίς καμία ανθρώπινη επέμβαση, και μάλιστα όχι προς ένα συγκεκριμένο χρήστη, αλλά προς αναρίθμητους ταυτόχρονα. Ως εκ τούτου χρήζει διερεύνησης αν ο πάροχος «παραλείπει» να διακόψει την διοχέτευση δεδομένων στο χρήστη που προσπαθεί παρανόμως να αποκτήσει πρόσβαση σε ένα πληροφοριακό σύστημα, καίτοι έχει νομική υποχρέωση, και φυσικά με την προϋπόθεση ότι γνωρίζει και έχει την δυνατότητα να το πράξει.

Σε απάντηση του εν λόγω ερωτήματος ο Κιούπης έχοντας εξετάσει επιμέρους περιπτώσεις[125], ορθά και κατά την γνώμη της γράφουσας, δίνει αρνητική απάντηση σε αυτό το ζήτημα διότι πέραν των τεχνικών δυσκολιών ελέγχου εκ μέρους του παρόχου τόσων χρηστών και κατ΄ επέκταση των διαδικτυακών τους ενεργειών (κάτι το οποίο αν συνέβαινε θα δημιουργούσε αυτοτελή ποινική ευθύνη του παρόχου) είναι πολύ δύσκολη η θεμελίωση ποινικής ευθύνης νομικής υποχρέωσης η μη συμμόρφωση στην οποία συνιστά έγκλημα τελούμενο δια παραλείψεως[126]. Ο δε Σιδηρόπουλος, έρχεται και προσθέτει στο ανωτέρω επιχείρημα, ακόμα ένα σοβαρό παράγοντα μιας τέτοια τυχόν ρύθμισης: ότι η τυχόν επιβολή στους παρόχους της υποχρέωσης άμεσης απόσυρσης ή διακοπής της πρόσβασης σε πληροφορίες ή δραστηριότητες με παράνομο περιεχόμενο συνεπάγεται την επιφόρτιση τους με αρμοδιότητες ανακριτικής και δικαστικής φύσης δημιουργώντας πλήθος προβλημάτων[127]. Ως εκ τούτου, συνάγεται πως καίτοι η πρόβλεψη ποινικής ευθύνης του παρόχου πρόσβασης στο διαδίκτυο να περιόριζε ενδεχομένως τον αριθμό των αξιοποίνων πράξεων που τελούνται μέσω αυτού, σχεδόν βέβαιο είναι ότι θα δημιουργήσει πολλά περισσότερα ζητήματα απ' αυτά που στόχευσε να επιλύσει.

[125]Ιδ. Κιούπη «Ποινικό Δίκαιο και Ίντερνετ» σελ. 49 επ.
[126]Ιδ. Κιούπη σελ. 73.
[127]Ιδ. Σπυρόπουλο σελ. 161.

## ΣΥΡΡΟΗ ΤΟΥ ΑΡΘΡΟΥ 370 Γ § 2 ΜΕ ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ ΤΟΥ Π.Κ. & ΕΙΔΙΚΟΥΣ ΠΟΙΝΙΚΟΥΣ ΝΟΜΟΥΣ

### Α. Συρροή με άλλες διατάξεις του Ποινικού Κώδικα

→Άρθρο 372 περί Κλοπής

Η διάταξη του αρ. 372[128], συμπεριλαμβανόμενη στο 23ο κεφάλαιο του Ποινικού Κώδικα για τα εγκλήματα κατά της ιδιοκτησίας, ποινικοποιεί την ολική ή μερική αφαίρεση ξένου κινητού πράγματος. Ειδικότερα, κατά την κρατούσα άποψη, προστατευόμενο έννομο αγαθό είναι **η κυριότητα αλλά και η κατοχή**, και υλικό αντικείμενο ξένο κινητό πράγμα[129]. Όταν λοιπόν ο δράστης του αρ. 370Γ παρ. 2 αποκτά χωρίς δικαίωμα πρόσβαση σε στοιχεία πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών και αφαιρεί τους υλικούς φορείς των στοιχείων αυτών, διαπράττει και κλοπή κατ' άρθρο 372 ΠΚ, η οποία τελεί σε αληθινή συρροή με την διάταξη του αρ. 370Γ παρ. 2 λόγω της ετερότητας των εννόμων αγαθών που προσβάλλονται, και μάλιστα πραγματική διότι πρόκειται για πλείονες πράξεις.

→Άρθρο 381 περί Φθοράς ξένης ιδιοκτησίας

Η διάταξη του αρ. 381[130], ανήκουσα συστημικά ομοίως με το αρ. 372 στο 23ο κεφάλαιο του Ποινικού Κώδικα για τα εγκλήματα κατά της ιδιοκτησίας, τιμωρεί την καταστροφή ή βλάβη ξένου πράγματος, και ως εκ τούτου προστατευόμενο έννομο αγαθό της διάταξης είναι **η ιδιοκτησία**, αφού με την φθορά καταλύεται εν όλω ή εν μέρει η κυριότητα. Όταν λοιπόν ο δράστης του αρ. 370Γ παρ. 2 αποκτά χωρίς δικαίωμα πρόσβαση σε στοιχεία πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών και βλάπτει ή καταστρέφει τους υλικούς φορείς των ως άνω στοιχείων πρόκειται για περίπτωση αληθινής πραγματικής συρροής, γιατί εξ' ορισμού τα εγκλήματα αυτά τελούνται με περισσότερες πράξεις.

→Άρθρο 381Α περί Φθοράς ηλεκτρονικών δεδομένων

---

[128] **αρ. 372 παρ. 1-Κλοπή** *«Όποιος αφαιρεί ξένο (ολικά ή εν μέρει) κινητό πράγμα από την κατοχή άλλου με σκοπό να το ιδιοποιηθεί παράνομα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών, και αν το αντικείμενο της κλοπής είναι ιδιαίτερα μεγάλης αξίας με φυλάκιση τουλάχιστον δύο ετών».*

[129] ίδετε Μαργαρίτης Μ. «Ποινικός Κώδικας Ερμηνεία-Εφαρμογή», 2η έκδοση 2009, σελ. 1043

[130] **αρ.381 παρ. 1-Φθορά ξένης ιδιοκτησίας** *«Όποιος με πρόθεση καταστρέφει ή βλάπτει ξένο (ολικά ή εν μέρει) πράγμα ή με άλλον τρόπο καθιστά ανέφικτη τη χρήση του τιμωρείται με φυλάκιση μέχρι δύο ετών».*

Η διάταξη του αρ. 381$^{A}$ [131], εισήχθη στον Ποινικό κώδικα με τον Ν. 4411/2016 και συγκεκριμένα εντάχθηκε στο 23ο κεφάλαιο του Ποινικού Κώδικα για τα εγκλήματα κατά της ιδιοκτησίας. Με την θέσπιση αυτής της διάταξης ο Έλληνας νομοθέτης εναρμονίστηκε με το άρθρο 4 της Σύμβασης για το έγκλημα στον κυβερνοχώρο και το άρθρο 5 της Οδηγίας 2013/40/ΕΕ[132], προκειμένου πλέον να προστατεύονται αυτοτελώς τα ηλεκτρονικά-ψηφιακά δεδομένα από πράξεις καταστροφής, αλλοίωσης κλπ[133]. Πρόκειται για ένα έγκλημα που στρέφεται αμιγώς κατά της ακεραιότητας και της διαθεσιμότητας τόσο των δεδομένων όσο και των πληροφοριακών συστημάτων, καθότι κατά το στ. θ΄ του άρθρου 13, τα πρώτα (ήτοι τα ψηφιακά-ηλεκτρονικά δεδομένα) εντάσσονται στην έννοια του πληροφοριακού συστήματος αφενός, και διαφοροποιείται ως προς τις ρυθμίσεις της Σύμβασης και της Οδηγίας ως προς το ότι δεν αρκείται σε «παρεμβολές σε δεδομένα» αλλά αφορά βαρύτερες προσβολές αφετέρου. **Προστατευόμενο έννομο αγαθό συνεπώς, είναι η ιδιοκτησία-τα ψηφιακά δεδομένα** αυτοτελώς, ανεξαρτήτως του υλικού τους φορέα, ως ένα ιδιαίτερο ιδιοκτησιακό-περιουσιακό αγαθό που εκφράζει κάποια οικονομική αξία, δεδομένων των ανωτέρω επιλογών του νομοθέτη[134].

Ο δράστης λοιπόν του αρ. 370Γ παρ. 2, ο οποίος αποκτά παράνομα πρόσβαση σε πληροφοριακό σύστημα και στη συνέχεια προβαίνει σε διαγραφή-καταστροφή

---

[131] **αρ. 381$^{A}$ –Φθορά ηλεκτρονικών δεδομένων** *« 1. Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη. 2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια. 3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών. 4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».*

[132] **Αρ. 5 Παράνομη παρεμβολή σε δεδομένα** *«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις» .*

[133] Ιδ. αιτιολογική έκθεση Ν. 4411/2016, σελ. 6.

[134] Ιδ. Κιούπη, Υπεράσπιση 2000 σελ.962 σχετικά με σκέψεις του και κριτική περί μη ύπαρξης διάταξης για αυτοτελή προστασία κα προβληματική εφαρμογή του αρ. 381 ΠΚ..

αλλοίωση ψηφιακών δεδομένων-στοιχείων διαπράττει τις αντικειμενικές υποστάσεις τόσο της διάταξης του αρ. 370 Γ παρ. 2 όσο και αυτής του αρ. 381$^{A}$, λόγω δε της ετερότητας των προσβαλλόμενων εννόμων αγαθών πρόκειται για αληθινή συρροή, και μάλιστα πραγματική γιατί απαιτούνται περισσότερες πράξεις

→Άρθρο 334 § 1 περί Διατάραξης οικιακής ειρήνης

Η διάταξη του 334[135], ανήκουσα στο 18ο κεφάλαιο του Ποινικού Κώδικα για τα εγκλήματα κατά της προσωπικής ελευθερίας, όπου τιμωρεί την παράνομη είσοδο και παραμονή σε ιδιωτικό χώρο με διάφορες μορφές, έχει ως προστατευόμενο έννομο αγαθό **το δικαίωμα της «κατοικίας»**. Ειδικότερα, πρόκειται για εγκληματική συμπεριφορά που προσβάλλει **την προσωπική ελευθερία του ατόμου**, η οποία εξειδικεύεται στο απαραβίαστο της ιδιωτικής σφαίρας[136].

Όταν ο δράστης παραβιάζει το προσωπικό χώρο-κατοικία του παθόντος και εξασφαλίζει πρόσβαση σε στοιχεία του πληροφοριακού συστήματος του ίδιου προσώπου τελεί τόσο το έγκλημα του αρ. 334 όσο και αυτό του αρ. 370Γ παρ. 2, τα οποία συρρέουν αληθινά και μάλιστα πραγματικά, διότι έχουμε περισσότερες πράξεις, όταν το θύμα του αρ. 370Γ παρ. 2 έχει λάβει μέτρα ασφαλείας που αφορούν το πληροφοριακό σύστημα καθεαυτό (πχ. κωδικούς πρόσβασης), και όχι απλά μέτρα ασφαλείας που αφορούν τον φυσικό χώρο όπως ύπαρξη κλειδαριών, συναγερμών κλπ. Ωστόσο, αρκετά προβληματική φαίνεται η τελευταία προπεριγραφείσα περίπτωση, καθότι όταν ο δράστης εισέρχεται παρανόμως στην κατοικία τρίτου όπου ευρίσκονται πχ. φορητοί ηλεκτρονικοί υπολογιστές και ipad για τα οποία ο νόμιμος κάτοχος δεν έχει λάβει μέτρα ασφαλείας που αφορούν αποκλειστικά τις προαναφερόμενες συσκευές, ελλοχεύει ο κίνδυνος να καταλογισθεί στο δράστη η αξιόποινη πράξη του αρ. 334 σωρευτικά με τουλάχιστον απόπειρα του αρ. 370Γ παρ. 2. Ως εκ τούτου θα πρέπει να κρίνεται in concreto κάθε φορά αν υφίσταται εν προκειμένω η απόπειρα ή τετελεσμένο το έγκλημα του αρ. 370Γ παρ. 2, με εκτίμηση του συνόλου των διδομένων πραγματικών περιστατικών.

→Άρθρο 370 Γ §1 περί αντιγραφής ή χρησιμοποίησης προγραμμάτων υπολογιστών

[135]**αρ. 334 παρ. 1- Διατάραξη οικιακής ειρήνης**- *«1. Όποιος εισέρχεται παράνομα ή παραμένει παρά τη θέληση 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.*

[136]Ιδ. ΣυμβΔιαρκΣτρΘεσσ 298/1995, Υπερ. 1995 σελ. 872 με εισαγγελική πρόταση Α. Παπαδαμάκη, από Χαραλαμπάκη-Γιαννίδη «Ποινικός Κώδικας και Νομολογία» 2009, σελ. 1425.

Η παρ. 1 της διάταξης του αρ. 370Γ[137], καίτοι εμπεριέχεται στο αδίκημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα είναι διαμετρικά αντίθετη με την παρ. 2 επ όπως ήδη αναπτύχθηκε, καθώς προστατεύει τα προγράμματα των ηλεκτρονικών υπολογιστών ως ένα ιδιαίτερο περιουσιακό αγαθό που εκφράζει κάποια οικονομική αξία, ανάλογη με την φύση του προγράμματος, το κόστος παραγωγής κλπ.[138]. Ενώ στην παρ. 2 του ιδίου άρθρου κατά την κρατούσα μέχρι σήμερα άποψη, προστατευόμενο έννομο αγαθό είναι το απόρρητο υπό τυπική έννοια. Ως εκ τούτου, ο δράστης που αποκτά παρανόμως πρόσβαση σε πληροφοριακό σύστημα και κατόπιν αντιγράφει ή χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών τελεί τόσο το έγκλημα της παρ. 1, όσο και της παρ. 2 του αρ. 370Γ, τα οποία συρρέουν αληθινά πραγματικά.

→Άρθρο 370Β ΠΚ περί παράνομης αντιγραφής ή χρήσης απόρρητων δεδομένων

Με την διάταξη του αρ. 370Β[139] ο νομοθέτης σκοπεύει να προστατεύσει το κρατικό-επιστημονικό-επαγγελματικό απόρρητο ή απόρρητα επιχείρησης με την μορφή στοιχείου ή προγράμματος ηλεκτρονικού υπολογιστή. Αντιθέτως, στο αρ. 370Γ παρ. 2 ο νομοθέτης προστατεύει το τυπικό απόρρητο, χωρίς να αξιώνει επιπλέον χαρακτηριστικά.

Όταν λοιπόν ο δράστης αποκτά πρόσβαση σε πληροφοριακά συστήματα ή στοιχεία που μεταδίδονται, τα οποία συνιστούν κρατικά, επιστημονικά, επαγγελματικά απόρρητα ή επιχειρησιακά απόρρητα υφίσταται κατ' ιδέαν συρροή μεταξύ του αρ. 370Β και 370Γ παρ. 2, η οποία θα επιλυθεί με την αρχή της ειδικότητας και συνεπώς ο δράστης θα τιμωρηθεί τελικώς με το αρ. 370Β ως ειδικότερη.

Όταν δε, ο δράστης κατόπιν της παράνομης πρόσβασης προβαίνει στις πράξεις της αντιγραφής, αποτύπωσης, χρήσης και αποκάλυψης σε τρίτα πρόσωπα στοιχείων τα οποία ασφαλώς συνιστούν κρατικά, επιστημονικά, επαγγελματικά

[137] **αρ. 370Γ παρ. 1** «*Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ* ».

[138] ίδετε ΣυμβΠλημΘεσσ 3204/1993 Υπερ. 1994, σελ. 1133.

[139] **αρ. 370Β παρ. 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.*»

απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, εφαρμογή θα έχει ως ελέχθη ανωτέρω η διάταξη του άρθρου 370Β ως ειδικότερη.

Ζήτημα έχει ανακύψει αναφορικά με την παρ. 1 εδ. β΄ του αρ. 370Β όπου αναφέρεται σε «*απόρρητα που 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»,* και την σχέση αυτού του εδαφίου με την παρ. 2 του αρ. 370Γ. Σε αυτήν την περίπτωση ορθότερο είναι να εφαρμοσθεί η παρ. 2 του αρ. 370 Γ ως ειδικότερη καθόσον αφορά την παράνομη πρόσβαση αυτή καθεαυτή. Ενώ το έγκλημα του αρ. 370Β τελείται μόνο στην περίπτωση που τα στοιχεία συνιστούν κρατικά, επιστημονικά, επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα και σκοπεύει να τιμωρήσει τις πράξεις της αντιγραφής, αποτύπωσης των εν λόγω στοιχείων και συμπληρωματικά, επικουρικά της πρόσβασης («οπωσδήποτε παραβιάζει»), άλλως η παρ. 2 του αρ. 370Γ δεν θα έβρισκε ουδέποτε εφαρμογή[140] (!).

→Άρθρο 292[Α] περί εγκλημάτων κατά της ασφάλειας των τηλεφωνικών επικοινωνιών

Το άρθρο 292Α[141] ανήκει στο 14ο Κεφάλαιο ΠΚ σχετικά με τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών και κατά των κοινωφελών εγκαταστάσεων, και εισήχθη με τον Ν. 3674/2008, ο οποίος αφορούσε την διασφάλιση του απορρήτου της τηλεφωνικής επικοινωνίας. Προστατευόμενο έννομο αγαθό με την υπό κρίση διάταξη είναι το υπερατομικό έννομο αγαθό του απορρήτου των τηλεπικοινωνιών[142].

Ζήτημα συρροής της διάταξης του αρ. 292[Α] με αυτήν του αρ. 370Γ παρ. 2, υφίσταται αποκλειστικά όταν η πράξη του δράστη αφορά πρόσβαση σε λογισμικό πληροφοριακού συστήματος παροχής υπηρεσιών τηλεφωνίας. Σε αυτήν την περίπτωση ορθότερη είναι η άποψη περί φαινομενικής συρροής και υπερίσχυσης της

[140] Ιδ. σχετικά Κιούπη «Ποινικό Δίκαιο και Ίντερντετ» σελ. 132.

[141] **αρ. 292[Α] παρ. 1- Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών** *«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».*

[142] Για την σχέση των άρθρων 292[Α] και 370[Α] ίδετε Φ. Σπυρόπουλου σελ. 219.

διάταξης του αρ. 292$^{A}$ ως ειδικότερης ρύθμισης αναφορικά με τις υπηρεσίες τηλεφωνίας.

→Άρθρο 292$^{B}$ περί παρακώλυσης λειτουργίας πληροφοριακών συστημάτων

Το άρθρο 292Β[143] ανήκει ομοίως στο 14ο Κεφάλαιο ΠΚ σχετικά με τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών και κατά των κοινωφελών εγκαταστάσεων, και εισήχθη με τον Ν. 4411/2016. Δεδομένης της συστημικής τοποθέτησης της διάταξης στο 14ο κεφάλαιο που τα προστατευόμενα έννομα αγαθά είναι υπερατομικά αφενός και των τρόπων τέλεσης που περιλαμβάνει η ειδική υπόσταση του αρ. 292Β αφετέρου, εξάγεται το συμπέρασμα πως η διάταξη του αρ. 370Γ παρ. 2 συρρέει αληθώς και πραγματικώς. Κι αυτό διότι πρόκειται για διαφορετικά προστατευόμενα έννομα αγαθά και διότι η διάταξη του αρ. 292Β δεν τιμωρεί την απόκτηση πρόσβασης, αλλά διαφορετικές πράξεις.

Χρήζει ιδιαίτερης προσοχής προς αποφυγή σύγχυσης, το γεγονός ότι η αντικειμενική υπόσταση του αρ. 292Β αναφέρεται σε παρεμπόδιση λειτουργίας με [..μεταξύ άλλων τρόπων…] αποκλεισμό πρόσβασης σε δεδομένα πληροφοριακού συστήματος. Άραγε, το έγκλημα που θέλει να τιμωρήσει εδώ ο ποινικός νομοθέτης είναι η παρεμπόδιση λειτουργίας, ενώ στο αρ. 370Γ παρ. 2 η παράνομη πρόσβαση. Είναι ωστόσο, λογικά και εννοιολογικά έκδηλο ότι παρεμπόδιση λειτουργίας ενός πληροφοριακού συστήματος, δύναται να λάβει χώρα συνήθως αφού ο δράστης αποκτήσει πρόσβαση (!), αφού δηλαδή αποκτήσει την φυσική-τεχνική δυνατότητα να παρέμβει με οιοδήποτε τρόπο στις λειτουργίες ενός πληροφοριακού συστήματος. Συνεπώς, αληθινή πραγματική συρροή των δύο εγκλημάτων υφίσταται στην

[143]*αρ.* ***292Β –παρακώλυση λειτουργίας πληροφοριακών συστημάτων*** *«1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών. 2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια. 3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών. 4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».*

περίπτωση κατά την οποία σ' ένα πληροφοριακό σύστημα παρεμποδίζεται ή διακόπτεται η λειτουργία του, χωρίς προηγουμένως να έχει αποκτηθεί παρανόμως πρόσβαση, ειδάλλως εφαρμόζεται η διάταξη του αρ. 292 Β ΠΚ.

## Β. Συρροή με άλλες διατάξεις ειδικών ποινικών νόμων

→Άρθρο 22 § 4 Ν. 2472/1997

Ζήτημα συρροής της διάταξης του αρ. 370Γ παρ. 2 με το Ν. 2472/97 περί προστασίες δεδομένων προσωπικού χαρακτήρα τίθεται, όταν τα στοιχεία του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται συνιστούν ταυτόχρονα δεδομένα προσωπικού χαρακτήρα[144] ή ευαίσθητα δεδομένα[145] κατά τις έννοιες του προαναφερόμενου νόμου.

Όταν το πρόσωπο του νομίμου κατόχου του πληροφοριακού συστήματος στο οποίο παρανόμως αποκτά πρόσβαση ο δράστης και το πρόσωπο στο οποίο αφορούν τα στοιχεία αυτά, δεν ταυτίζεται πρόκειται για αληθινή κατ' ιδέαν συρροή, δεδομένου ότι με μία πράξη του δράστη προσβάλλονται ατομικά-προσωποπαγή έννομα αγαθά διαφορετικών προσώπων.

Πολυπλοκότερο είναι το ζήτημα όταν υπάρχει ταυτοπροσωπία νομίμου κατόχου-δικαιούχου διάθεσης των στοιχείων του πληροφοριακού συστήματος και υποκειμένου των δεδομένων αφετέρου κατά την έννοια της παρ. 1 στ. γ του αρ. 2 του Ν. 2472/97[146]. Σε αυτήν την περίπτωση η κατ' ιδέαν συρροή θα επιλύεται και η τιμώρηση του δράστη θα λαμβάνει χώρα δυνάμει του αρ. 22 παρ. 4 του ν. 2472/1997 το οποίο απειλεί βαρύτερη ποινή έναντι του 370Γ παρ. 2.

→Άρθρο 15 Ν. 3471/2006

---

[144] **Αρ. 2 παρ. 1 στ. α΄ Ν. 2472/1997** *"Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.*

[145] **Αρ. 2 παρ. 1 στ. β΄ Ν. 2472/1997** *«Ευαίσθητα δεδομένα», τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Ειδικά για τα σχετικά με ποινικές διώξεις ή καταδίκες δύναται να επιτραπεί η δημοσιοποίηση μόνον από την εισαγγελική αρχή για τα αδικήματα που αναφέρονται στο εδάφιο β' της παρ. 2 του άρθρου 3 με διάταξη του αρμόδιου Εισαγγελέα Πρωτοδικών ή του Εισαγγελέα Εφετών, εάν η υπόθεση εκκρεμεί στο Εφετείο.*

[146] **Άρθρο 2 παρ. 1 στ. γ΄ Ν. 2472/1997** *"Υποκείμενο των δεδομένων", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική»*

Με το άρθρο 15 του Ν. 3471/2006[147] περί προστασίας δεδομένων προσωπικού χαρακτήρα θεσπίζονται ποινικές κυρώσεις αφορώσες την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ωστόσο πρέπει σε αυτό το σημείο να επισημανθεί, ότι ο νομοθέτης δεν τιμωρεί στο αρ. 15 του Ν. 3471/2006 την απόκτηση πρόσβασης, αλλά την περιέλευση σε γνώση *(«τα καθιστά προσιτά {…} επιτρέπει να λάβουν γνώση»)* και έτερες πράξεις. Επομένως, στην περίπτωση που ο δράστης ο οποίος αποκτά παράνομη πρόσβαση σε πληροφοριακό σύστημα και εν συνεχεία προβαίνει σε ανακοίνωση δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα συνδρομητών ή χρηστών στο πλαίσιο ηλεκτρονικών επικοινωνιών, διαπράττει με περισσότερες πράξεις και το αδίκημα του αρ. 370Γ παρ. 2, αλλά και αυτό του αρ. 15 του Ν. 3471/2006, τα οποία συρρέουν αληθινά πραγματικά. Σε περίπτωση όμως, που ο δράστης λαμβάνει γνώση των προσωπικών δεδομένων συνδρομητών ή χρηστών στο πλαίσιο δημοσίων δικτύων ηλεκτρονικών επικοινωνιών τιμωρείται πάντα με το αρ. του Ν. 3471/2006[148] το οποίο προβλέπει βαρύτερη ποινή.

→Άρθρο 11 Ν. 3917/2011

Ο νόμος 3917/2011, αφορά τις τηλεπικοινωνιακές υπηρεσίες και τα τηλεπικοινωνιακά δίκτυα, και ειδικότερα τα δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και τα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη. Ρητά αναφέρεται ωστόσο, στο άρθρο 1 περί πεδίου εφαρμογής, ότι οι διατάξεις του δεν εφαρμόζονται

[147]*«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 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)»*

[148]Ιδ. Καιάφα-Γκμπάντι, Αρμενόπουλος 2007, σελ. 1070.

στο περιεχόμενο των ηλεκτρονικών επικοινωνιών, καθώς και στις πληροφορίες, στις οποίες η πρόσβαση πραγματοποιείται με τη χρήση δικτύου ηλεκτρονικών επικοινωνιών.

Περαιτέρω, στο άρθρο 11 προβλέπονται ποινικές κυρώσεις, καμία όμως εξ' αυτών δεν αφορά την απόκτηση πρόσβασης, αλλά την περιέλευση σε γνώση *(«τα καθιστά προσιτά {...} επιτρέπει να λάβουν γνώση»)* και έτερες πράξεις. Οπότε μεταξύ του αρ. 370Γ παρ. 2 και του αρ. 11 του ν. 3917/2011 υφίσταται σχέση αληθινής πραγματικής συρροής, κατ' αντιστοιχία με όσα αναπτύχθηκαν προηγουμένως για το αρ. 15 του Ν. 3471/2006.

Στο σημείο αυτό δέον όπως αναφερθεί ο προβληματισμός που έχει εκφραστεί αναφορικά με την πραγματική ταύτιση της απόκτησης πρόσβασης με την λήψη γνώσης[149] τόσο σχετικά με το αρ. 11 του Ν. 3917/2011 όσο και με το άρθρο 15 του Ν. 3471/2006 . Ωστόσο, υπό το πρίσμα των όσων αναφέρθηκαν στο σχετικό κεφάλαιο της παρούσας εργασίας για την έννοια της πρόσβασης, ως φυσικής και τεχνικής δυνατότητας εκτέλεσης οποιασδήποτε λειτουργίας του πληροφοριακού συστήματος, κατά την γνώμη της γράφουσας η λήψη γνώσης συνιστά ένα περαιτέρω στάδιο το οποίο δεν προϋποθέτει ότι οπωσδήποτε έχει λάβει χώρα αφής στιγμής ο δράστης αποκτήσει παρανόμως πρόσβαση. Μπορεί με άλλα λόγια, ο δράστης να σπάσει τον κωδικό ενός πληροφοριακού συστήματος έχοντας πλέον την δυνατότητα να προβεί σε εκτέλεση οποιασδήποτε λειτουργίας του (δυνητικά), αλλά δεν έχει περιέλθει σε γνώση του εν τοις πράγμασι στοιχείο του πληροφοριακού συστήματος. Σε περιπτώσεις δε, που η διάκριση είναι δυσχερής και δεν μπορεί να διαπιστωθεί μέχρι ποίου σημείου έφθασε η συμπεριφορά του δράστη, βάσει της αρχής in dubio pro reo, πρέπει να γίνει δεκτή η απόκτηση πρόσβασης και όχι η λήψη γνώσης.

## ΑΡΘΡΟ 370Ε Π.Κ. : ΑΞΙΟΠΟΙΝΟ ΠΡΟΠΑΡΑΣΚΕΥΑΣΤΙΚΩΝ ΠΡΑΞΕΩΝ

Η νεοεισαχθείσα διάταξη του άρθρου 370 Ε αποτελεί ενσωμάτωση του άρθρου 7 της Οδηγίας με τίτλο *«εργαλεία που χρησιμοποιούνται για την διάπραξη των αδικημάτων»*[150], και κατ' επέκταση του αρ. 6 της Σύμβασης, και αφορά αμιγώς

[149]Ιδ. Σπυρόπουλος σελ. 224.

[150]«*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*

προπαρασκευαστικές πράξεις, μεταξύ άλλων και της παράνομης πρόσβασης του αρ. 370Γ παρ. 2. Πρωτίστως, δέον όπως αναφερθεί η ιδιαίτερη απαξία που θέτει ο νομοθέτης μέσω αυτής της διάταξης, καθότι δεν αρκείται στην τιμώρηση μόνο του αδικήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα, αλλά και στις προπαρασκευαστικές αυτής πράξεις, όπως προκύπτει ρητά από τη διατύπωση της διάταξης, και μάλιστα θέτει επαπειλούμενο πλαίσιο ποινής φυλάκιση έως 2 έτη-, αυστηρότερη ποινή ανάλογη της κύριας πράξης του τροποποιηθέντος αρ. 370 Γ παρ. 2 (η προγενέστερη διάταξη προέβλεπε για την κύρια πράξη φυλάκιση έως 3 μήνες ή χρηματική ποινή). Πρόκειται για πολύτροπο έγκλημα, δηλαδή όποιος τρόπος και αν έχει επιλεχθεί από τον δράστη: παραγωγή, πώληση, προμήθεια προς χρήση εισαγωγή, κατοχή, διανομή και με οιοδήποτε τρόπο διακίνηση, ένα έγκλημα θα έχει τελεστεί, εφόσον βέβαια δεν έχει επέλθει ειρήνευση του εννόμου αγαθού ασφαλώς.

Ως προς την υποκειμενική υπόσταση του αδικήματος του αρ. 370 Ε, απαιτείται τουλάχιστον ενδεχόμενος δόλος[151] , αλλά και *«σκοπός διάπραξης κάποιου από τα εγκλήματα [..] 370Γ παρ. 2 [..]»*, συνεπώς συνιστά έγκλημα υπερχειλούς υποκειμενικής υποστάσεως όπου όταν ελλείπει ο σκοπός διάπραξης, ο δράστης θα είναι ατιμώρητος. Έτσι ο Έλληνας νομοθέτης αποφεύγει την περίπτωση της υπερβολικής ποινικοποίησης, η οποία θα στοιχειοθετούσε εγκλήματα και θα εμπόδιζε την προαγωγή και εξέλιξη της έρευνας και της επιστήμης στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Στο σημείο αυτό, χρήζει αναφοράς το προβληματικό της διατύπωσης της ειδικής υπόστασης αναφορικά με τον σκοπό διάπραξης κάποιων εκ των κυρίων πράξεων. Πλέον ειδικά, **από την μία αναφέρεται ως ρητά προαπαιτούμενος ο σκοπός διάπραξης, και από την άλλη στο στοιχείο α΄** περί των συσκευών ή προγραμμάτων υπολογιστή **απαιτείται αυτά να είναι σχεδιασμένα ή προσαρμοσμένα «*κυρίως για το σκοπό της διάπραξη*ς** *κάποιου από τα εγκλήματα των άρθρων {..} 370Γ παρ. 2 {..}»*.

Κατά την γνώμη της γράφουσας, η σώρευση των φράσεων «*με σκοπό την διάπραξη κάποιου από τα εγκλήματα*» και *«κυρίως για το σκοπό της διάπραξης»* πλεονάζει και προκαλεί σύγχυση, διότι ο δράστης ο οποίος έχει σκοπό να διαπράξει το έγκλημα της παράνομης πρόσβασης χρησιμοποιώντας στοιχεία, προγράμματα και κωδικούς με έναν από τους αναφερόμενους στο αρ.370[Ε] τρόπους (πώληση,

*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.»*
[151]Ιδ. Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος» σελ. 237 επ.

προμήθεια, παραγωγή κλπ.), θα τιμωρηθεί ανεξαρτήτως του αν αυτά είναι σχεδιασμένα ή προορισμένα για τέτοιο σκοπό. Αυτή η αστοχία άλλωστε του νομοθέτη ενισχύεται και από το γεγονός ότι αν απομονώσουμε μερικώς την ειδική υπόσταση, «μοιάζει» σαν να αξιολογείται ποινικώς ο σκοπός σχεδίασης των επίμαχων στοιχείων, ενώ το ουσιώδες και νομικά κρίσιμο είναι ο σκοπός διάπραξης εκ μέρους του δράστη της πράξης της παράνομης πρόσβασης, ο οποίος και καθιστά το αδίκημα του αρ. 370$^{E}$ ως υπερχειλούς υποκειμενικής υπόστασης. Περαιτέρω, προβληματική φαίνεται και η διατύπωση των συσκευών ή προγραμμάτων υπολογιστή ως *«σχεδιασμένων ή προσαρμοσμένων για το σκοπό διάπραξης κάποιων εκ των εγκλημάτων»*, καθώς κάτι τέτοιο είναι δυσαπόδεικτο και ελλοχεύει κίνδυνο πολλών σφαλμάτων.

Προβληματισμό δημιουργεί και το στοιχείο «χωρίς δικαίωμα», το οποίο κατά αναλογική εφαρμογή των όσων αναπτύχθηκαν ανωτέρω, συνιστά στοιχείο της αντικειμενικής υπόστασης, καθόσον ο νομοθέτης δεν τιμωρεί κάθε πώληση, παραγωγή, προμήθεια κλπ. αλλά αυτή που διαπράττεται χωρίς δικαίωμα. Βέβαια, ζήτημα ανακύπτει ως προς το ποιος νομιμοποιείται να δώσει την συγκατάθεση του, όπως στο αρ. 370Γ παρ. 2 γίνεται λόγος ρητά για νόμιμο κάτοχο. Άραγε, γιατί εδώ ο νομοθέτης παραλείπει αυτή την αναφορά; Λόγω του ανωτέρω ατόπου, κατά την γνώμη της γράφουσας το στοιχείο «χωρίς δικαίωμα» θα πρέπει να απαλειφθεί ολοκληρωτικά, η δε διατύπωση του αρ. 370 Ε λόγω και των όσων εκτέθηκαν ανωτέρω θα μπορούσε de lege ferenda να διαμορφωθεί ως εξής:

*« Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος ~~χωρίς δικαίωμα~~ και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, ~~σχεδιασμένα ή προσαρμοσμένα κυρίως~~ για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα, ~~σχεδιασμένα ή προσαρμοσμένα~~ για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος ».*

Τέλος, καίτοι αναφέρθηκε παραπάνω, ότι η εν λόγω διάταξη αποτελεί ενσωμάτωση της αντίστοιχης ρύθμισης της Οδηγίας, εν τούτοις παρατηρείται απόκλιση ως προς τους τρόπους τέλεσης, η οποία προκαλεί απορία. Πλέον ειδικά,

πρόκειται για πολύτροπο[152] έγκλημα, δηλαδή όποιος τρόπος και αν έχει επιλεχθεί από τον δράστη: παραγωγή, πώληση, προμήθεια προς χρήση εισαγωγή, κατοχή, διανομή, με οιοδήποτε τρόπο διακίνηση, ένα έγκλημα θα έχει τελεστεί, εφόσον δεν έχει επέλθει ειρήνευση του εννόμου αγαθού. Ωστόσο, ο Έλληνας νομοθέτης επιλέγει να εισάγει στην ειδική υπόσταση του 370 Ε και την πράξη της κατοχής, αν και η Οδηγία δεν κάνει λόγο γι' αυτή (!!). Έτσι, φαίνεται ότι τιμωρείται κάθε δυνατή πράξη που μπορεί να σχετιστεί με την διάπραξη της παράνομης πρόσβασης σε πληροφοριακό σύστημα, παρόλο που η Οδηγία θεσπίζει στο άρθρο 9 υποχρέωση (!) των κρατών-μελών να λαμβάνουν τα αναγκαία μέτρα για την τιμώρηση των περιπτώσεων που δεν είναι ήσσονος σημασίας.

Σε κάθε πάντως περίπτωση, η εισαγωγή του αρ. 370$^{E}$ συντελεί καθοριστικά στην πραγμάτωση του σκοπού της Οδηγίας, όπως αυτός περιγράφεται στην σκέψη 1, ήτοι στην προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, και τονίζει την έντονη απαξία τόσο του Ευρωπαίου όσο και του Έλληνα νομοθέτη, αναφορικά με την πράξη της παράνομης πρόσβασης ως ιδιαίτερα επικίνδυνου εγκλήματος που μπορεί να τελεστεί με εξελιγμένες και περίπλοκες μεθόδους.

## ΕΠΑΠΕΙΛΟΥΜΕΝΗ ΠΟΙΝΗ ΤΟΥ ΑΡΘΡΟΥ 370Γ § 2

### Προβλέψεις Σύμβασης-Απόφασης Πλαίσιο-Οδηγίας

Αναφέρεται ρητά στην Οδηγία ότι η **Σύμβαση του Συμβουλίου της Ευρώπης του 2001** συνιστά το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Εν τούτοις στο σχετικό άρθρο 2 της Σύμβασης, η υποχρέωση του εκάστου συμβαλλόμενου κράτους που προσχωρεί και υπογράφει την Σύμβαση έγκειται στην λήψη των αναγκαίων νομοθετικών μέτρων για την ποινικοποίηση των συγκεκριμένων πράξεων, χωρίς καμία αναφορά σε πλαίσιο ποινής για την πράξη της παράνομης πρόσβασης, ούτε και σε κανένα άλλο άρθρο. Στο άρθρο 13 δε, με τίτλο «κυρώσεις και μέτρα» προβλέπεται η αυτή υποχρέωση του συμβαλλόμενου κράτους να τιμωρεί **με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές ή μη κυρώσεις ή μέτρα, περιλαμβανομένων των χρηματικών κυρώσεων.**

[152]Ιδ. σχετικά με εγκλήματα απλότροπα και μικτά Μυλωνόπουλο «Ποινικό Δίκαιο-Γενικό Μέρος» σελ. 160.

Η ως άνω μνεία περί του χαρακτήρα των κυρώσεων εμπεριέχεται αυτούσια και στην **Απόφαση-Πλαίσιο,** χωρίς επίσης ρητή αναφορά πλαισίου ποινής για την πράξη της παράνομης πρόσβασης σε σύστημα πληροφοριών με ρητή απαίτηση ύπαρξης ποινικής κύρωσης, με την διαφορά αφενός ότι πρέπει να αποφευχθεί η υπερβολική ποινικοποίηση εισάγοντας την έννοια των υποθέσεων «ήσσονος σημασίας» και αφετέρου με σαφή πρόβλεψη περί αυστηρότερων κυρώσεων όταν η διάπραξη αδικημάτων τελείται στο πλαίσιο εγκληματικής οργάνωσης ή σε περιπτώσεις πρόκλησης σοβαρών ζημιών ή βλάβης θεμελιωδών συμφερόντων[153].

Περαιτέρω, στις σκέψεις της **Οδηγίας διατηρείται το ίδιο ως άνω σκεπτικό της Απόφασης-Πλαίσιο,** είναι όμως ιδιαίτερη εμφανής η επανειλημμένη έμφαση που δίδεται στις απειλές και τους κινδύνους που προκύπτουν από επιθέσεις στον κυβερνοχώρο[154], ώστε είναι επιτακτική η πρόβλεψη αυστηρών ποινικών κυρώσεων στις περιπτώσεις που οι πράξεις πλήττουν υποδομές ζωτικής σημασίας για την Ένωση[155]. Τα δε κράτη-μέλη, έχουν την ευχέρεια σύμφωνα με το εθνικό δίκαιο να ορίσουν τι συνιστά *σοβαρή ζημία* και τι συνιστά περίπτωση *ήσσονος σημασίας,* με ενδεικτική αναφορά κάποιων περιπτώσεων. Έτσι, υπό το ανωτέρω πλαίσιο **της Οδηγίας ορίζεται στην παρ. 2 του άρθρου 9** ότι η αξιόποινη πράξη της παράνομης πρόσβασης σε σύστημα πληροφοριών **τιμωρείται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται** σε τουλάχιστον 2 έτη και τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας, ενώ στο άρθρο 11 προβλέπονται συγκεκριμένες κυρώσεις κατά νομικών προσώπων.

## Εθνικό Δίκαιο

Το πλαίσιο της επαπειλούμενης ποινής του άρθρου 370Γ παρ. 2 προ των τροποποιήσεων που επέφερε ο Ν. 4411/2016 **συνίστατο σε στερητική της ελευθερίας ποινή, και συγκεκριμένα σε φυλάκιση μέχρι τρεις μήνες (δηλαδή από 10 ημέρες[156] έως 3 μήνες) ή διαζευκτικά χρηματική ποινή τουλάχιστον 29 ευρώ (δηλαδή από 29 ευρώ έως 15.000 ευρώ)[157]**. Αν δε, κατά το εδάφιο γ΄ της διάταξης, η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους τιμωρείται

[153]Ιδ. σκέψη 14 και 15 της Απόφασης-πλαίσιο.
[154]Με ρητή αναφορά στα δίκτυα "botnets".
[155]Ιδ. σκέψεις 4,5 και 6 της Οδηγίας .
[156]Ιδ. άρθρο 53 Π.Κ. σχετικά με διάρκεια της ποινής φυλάκισης.
[157]Ιδ. άρθρο 57 Π.Κ. σχετικά με το ύψος της χρηματικής ποινής.

κατά το άρθρο 148 Π.Κ., ήτοι με φυλάκιση τουλάχιστον ενός έτους (παρ. 1) ή με ισόβια κάθειρξη ή θάνατο (παρ. 2) .

Πλέον, **μετά τον Ν. 4411 επαπειλούμενη ποινή του πλημμελήματος του 370Γ παρ. 2 είναι** και πάλι η στερητική της ελευθερίας φυλάκιση, χωρίς αυτή την φορά να τίθενται από τον νομοθέτη κάποιος περιορισμός. Ως εκ τούτου το πλαίσιο διαμορφώνεται από 10 ημέρες έως 5 έτη φυλάκισης και **δεν δίδεται πλέον η δυνατότητα επιβολής χρηματικής ποινής**, αντ' αυτής της φυλακίσεως όπως στο προϊσχύον δίκαιο. Βέβαια, ναι μεν ο Έλληνας νομοθέτης ακολουθεί τα οριζόμενα στο άρθρο 9 παρ. 2 της Οδηγίας, ωστόσο προβληματικό είναι το ζήτημα της μετατροπής της στερητικής της ελευθερίας ποινής σε χρηματική κατά το άρθρο 82 ΠΚ, σύμφωνα με το οποίο δύναται να μετατραπεί σε χρηματική ποινή έως 5 ετών κάθειρξη κατά την νομολογία[158]. Όποτε ο Έλληνας νομοθέτης συμμορφώνεται με τις επιταγές της Οδηγίας κατ' αποτέλεσμα όμως την αθετεί ευθύς εξαρχής.

Πράγματι με την πρώτη κιόλας ανάγνωση της νεότερης, όσο και της προγενέστερης διάταξης προκύπτει αδιαμφισβήτητα η βούληση του εμφανώς συμμορφούμενου με την Οδηγία Έλληνα νομοθέτη περί αυστηρότερου πλαισίου ποινής, απατώντας εμμέσως στην κριτική που είχε δεχθεί περί ηπιότερης έως τώρα ποινικής μεταχείρισης του δράστη.

Ειδικότερα, **ο Κιούπης είχε ασκήσει επανειλημμένα δριμεία κριτική[159] ως προς το ζήτημα της απειλουμένης ποινής της επίμαχης διάταξης**, συγκρίνοντας την με αυτές που προβλέπουν τα άρθρα που συμπεριλαμβάνονται στο κεφάλαιο περί παραβίασης απορρήτων του Ποινικού Κώδικα. Όντως, στις βασικές τουλάχιστον μορφές των αδικημάτων των άρθρων 370, 370$^{A}$, 370Β και 371, (δηλαδή εξαιρουμένων των περιπτώσεων που οι πράξεις αφορούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου και ως προς την τιμώρηση εφαρμογή βρίσκουν τα αρ. 146-148ΠΚ ) προβλεπόταν και προβλέπεται ως ελάχιστο φυλάκιση τουλάχιστον 3 μηνών[160] ή κάθειρξη μέχρι δέκα ετών[161]. Αντιστοίχως, και στο νεοεισαχθέν αρ. 370 Δ

[158]Ιδ. υπ' αριθμ 728/2017 απόφαση ΑΠ. ΠοινΧρον 2017, ΞΖ σελ. 514-516 σχετικά με την προβληματική μετατροπής της πενταετούς καθείρξεως σε χρηματική.
[159]Ιδ. σχετικά Κιούπη, Υπερ. 2000, «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, κενά και αδυναμίες της ποινικής νομοθεσίας», σελ. 959 επ. Β. «Αθέμιτη πρόσβαση σε δεδομένα» σελ.969, αλλά και σελ 971 όπου κάνει λόγο για τις ποινικές κυρώσεις σε αλλοδαπές έννομες τάξεις **&** 3ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ «Το δίκαιο στην ψηφιακή εποχή» Νομική Βιβλιοθήκη 2012, σελ. 158 **&** του Ιδίου «Ποινικό Δίκαιο και Ίντερνετ» σελ. 133.
[160]Ιδ. άρθρο. 370Β παρ. 1 ΠΚ.
[161]Ιδ. άρθρο 370 Α παρ.1 ΠΚ.

ΠΚ προβλέπεται κάθειρξη έως 10 ετών, αλλά και στο νεοεισαχθέν αρ. 370 Ε ΠΚ προβλέπεται φυλάκιση έως 2 ετών.

Συγκεκριμένα ο Κιούπης, είχε συγκρίνει την διάταξη του αρ. 370Γ παρ. 2 ως προς το απαξιολογικό της περιεχόμενο με αυτήν του αρ. $370^{A}$ ΠΚ αφορώσα παρακολούθηση τηλεφωνικών συνδιαλέξεων, τονίζοντας πως μόνο το χρησιμοποιούμενο από τον δράστη τεχνικό μέσο διαφέρει εν προκειμένω και ασφαλώς δεν υπάρχει καμία δικαιολογητική βάση τέτοιας διαφοροποίησης, αλλά και το γεγονός ότι η εξάπλωση του υπολογιστή και του διαδικτύου είναι ευρέως διαδεδομένη, ειδικά συγκριτικά με την χρήση του τηλεφώνου. Μάλιστα, είχε αναφερθεί σχετικά και σε κυρώσεις αλλοδαπών εννόμων τάξεων αναφορικά με το προβληματισμό περί απαίτησης ή μη κάποιου πρόσθετου στοιχείου (πχ. γνώση, αλλοίωση δεδομένων κλπ.) για την στοιχειοθέτηση του αδικήματος της παράνομης πρόσβασης. Βέβαια, κατά την κρατούσα γνώμη, δεν τίθεται ζήτημα· ο ημεδαπός νομοθέτης θεσπίζει αυτοτελή ποινική απαξία για την χωρίς δικαίωμα πρόσβαση χωρίς να απαιτεί κανένα άλλο πρόσθετο στοιχείο ή πράξη για την θεμελίωση ποινικής ευθύνης[162] (!)

Κλείνοντας το ζήτημα της θέσης αυτής, ιδιαιτέρως εύστοχη ήταν και η επιχειρηματολογία του (Κιούπη) πως μια τέτοια επιλογή ποινής απαξιώνει εξαρχής την διάταξη και την θέτει στο περιθώριο, ειδικά στην Ελλάδα όπου φημίζεται για το υψηλό πλαίσιο απειλούμενων ποινών και την σωρεία κακουργημάτων (!) Και αυτό δικαιολογημένα, καθώς υπό την προϊσχύουσα διάταξη, σε περιπτώσεις συρροής της με άλλες διατάξεις του Ποινικού Κώδικα, αλλά και ειδικών ποινικών νόμων, μόνη η αρχή της απορρόφησης την καθιστούσε ανενεργή και ανεφάρμοστη, αφού κάθε άλλη διάταξη προέβλεπε μεγαλύτερο πλαίσιο ποινής από αυτό των 3 μηνών φυλάκισης (!!).

Επί τη βάσει όλων όσων εκτέθηκαν στο οικείο κεφάλαιο περί απόκτησης πρόσβασης, **το πλέον μετά τον Ν. 4411/2016 αυστηρότερο πλαίσιο ποινής, υπακούει στην Οδηγία** και **συνάδει τόσο με την κρίσιμη πράξη της απόκτησης πρόσβασης**, αφού ο «hacker» που καταφέρνει να «μπει» σε έναν υπολογιστή- εφεξής σε ένα πληροφοριακό σύστημα-, είναι πλέον σε θέση να κάνει ακριβώς όσα και ο νόμιμος χρήστης του, μπορεί συνεπώς, μεταξύ άλλων, να αντιγράψει ή να αλλοιώσει αρχεία, ακόμα και να καταστρέψει ολόκληρο το σύστημα[163] αφενός, και **αφετέρου το**

[162]Ιδ. Κιούπη, αλλά και το οικείο κεφάλαιο της παρούσας «ειδική υπόσταση-αντικειμενική υπόσταση-απόκτηση πρόσβασης» σελ 972.
[163]Ιδ. Αργυρόπουλο «Ηλεκτρονική εγκληματικότητα», σελ. 36.

**ευρύτερο πεδίο εφαρμογής της διάταξης μετά την εισαγωγή των όρων** η) «πληροφοριακό σύστημα» θ) «ψηφιακά δεδομένα» του άρθρου 13 ΠΚ δικαιολογεί ευλόγως θα λέγαμε και αυστηρότερο πλαίσιο ποινής αφετέρου.

Τέλος, **το αυστηρότερο αυτό πλαίσιο ποινής συμβαδίζει και με αυτό της νέας διάταξης περί τιμώρησης των προπαρασκευαστικών πράξεων του νεοεισαχθέντος άρθρου 370Ε** με απειλούμενη ποινή φυλάκισης μέχρι δύο έτη, διότι διαφορετικά θα εμφανιζόταν το παράδοξο να τιμωρούνται βαρύτερα οι προπαρασκευαστικές πράξεις από την κύρια (!).

## ΕΠΑΠΕΙΛΟΥΜΕΝΗ ΠΟΙΝΗ ΤΟΥ ΑΡΘΡΟΥ 370Ε Π.Κ.

Πλέον με τον Ν. 4411/2016 θεσπίστηκε το αξιόποινο των προπαρασκευαστικών των άρθρων 370 Β, 370Γ παρ. 2 και 3 και 370Δ πράξεων. Ως προς την διαμόρφωση του πλαισίου ποινής από την Σύμβαση του Συμβουλίου της Ευρώπης το 2001 ισχύουν αντιστοίχως τα όσα αναφέρθηκαν ανωτέρω για το πλαίσιο ποινής του αρ. 370 Γ παρ. 2. Δέον όπως σημειωθεί, ότι στην Απόφαση-Πλαίσιο δεν προβλέφθηκε καθόλου η τιμώρηση των προπαρασκευαστικών πράξεων και συνεπώς ούτε πλαίσιο ποινής αυτών. Στην **Οδηγία όμως το άρθρο 7** ρητά θεμελιώνει αξιόποινο με τίτλο «Εργαλεία που χρησιμοποιούνται για την διάπραξη των αδικημάτων» και ο δράστης **τιμωρείται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται** σε τουλάχιστον 2 έτη και τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας. Έτσι, και το άρθρο 370$^{Ε}$ ΠΚ υιοθετεί τις επιταγές της Οδηγίας και προβλέπει ποινή φυλάκισης 2 ετών, χωρίς όμως να διαχωρίζει τις ήσσονος σημασίας περιπτώσεις, συνεπώς είναι αυστηρότερη η ποινική μεταχείριση του δράστη από τον Έλληνα νομοθέτη. Τέλος όπως ήδη εκτέθηκε και ανωτέρω, αυτό το πλαίσιο ποινής φαίνεται εύλογο με το πλαίσιο ποινής που τίθεται στο αρ. 370Γ παρ. 2 για την κύρια πράξη της παράνομης πρόσβασης.

## ΔΙΚΟΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ

Όπως έχει ήδη αναπτυχθεί, όποια θέση και αν πάρει κανείς για το προστατευόμενο έννομο αγαθό, η διάταξη του αρ. 370Γ παρ. 2 έχει θεσπιστεί για την προστασία του ιδιωτικού και όχι του κοινωνικού συμφέροντος. Δικαιολογημένα λοιπόν, η αξιόποινη πράξη της παράνομης πρόσβασης σε πληροφοριακό σύστημα αποτελεί ένα απολύτως κατ' έγκληση διωκόμενο έγκλημα, όπως ορίζεται ρητά στην

παρ. 4, και η ποινική δίωξη μπορεί να ασκηθεί μόνο αν έχει υποβληθεί έγκληση εντός τριμήνου από την τέλεση της πράξης ή της λήψης γνώσης της από τον παθόντα. Δικαιούχος υποβολής της εγκλήσεως, και κατ' επέκταση ενεργητικά νομιμοποιούμενος σε δήλωσης παράστασης πολιτικής αγωγής για χρηματική ικανοποίηση λόγω άμεσης ηθικής βλάβης ή λόγω της άμεσης υλικής ζημίας που υπέστη[164], είναι κατ' άρθρο 118 ΠΚ ο άμεσα παθών από την παράνομη πρόσβαση, ήτοι ο νόμιμος κάτοχος του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών- φορέας του προσβληθέντος εννόμου αγαθού (είτε πρόκειται για φυσικό πρόσωπο ως νόμιμο κάτοχο του πληροφοριακού συστήματος είτε για νομικό πρόσωπο, όπως πχ. μια ανώνυμη εταιρεία που θα εκπροσωπηθεί και θα υποβληθεί έγκληση από τον οριζόμενο νόμιμο εκπρόσωπο της).

Το ζήτημα της εγκλήσεως έχει στην υπό κρίση περίπτωση ακόμη μεγαλύτερη σημασία, δεδομένου ότι πρόκειται για ένα κατά κόρον διασυνοριακό έγκλημα, και η θεμελίωση ποινικής δικαιοδοσίας των ελληνικών δικαστηρίων επί πλημμελημάτων που τελέστηκαν στην αλλοδαπή από ημεδαπό ή κατά ημεδαπού, **προϋποθέτει έγκληση του παθόντος**[165].

Δέον όπως επισημανθεί **η αυτοτέλεια του δικαιώματος της έγκλησης, στις περιπτώσεις,** όπου παθόντες από την παράνομη πρόσβαση είναι πλείονα πρόσωπα πχ. στην περίπτωση που είναι τρεις οι νόμιμοι κάτοχοι του πληροφοριακού συστήματος, στην περίπτωση που η παράνομη πρόσβαση αφορά στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών όπου έχουμε τουλάχιστον έναν αποστολέα-πομπό και ένα παραλήπτη-δέκτη των στοιχείων. Σε κάθε μία εξ' αυτών των περιπτώσεων η τρίμηνη προθεσμία υποβολής της εγκλήσεως ξεκινά ξεχωριστά για τον καθένα, η δε τυχόν παραίτηση ή ανάκληση της εγκλήσεως εκ μέρους ενός εκ των εγκαλούντων δεν επηρεάζει το δικαίωμα των λοιπών[166].

Δεδομένης της θέσπισης της διάταξης για την προστασία του ιδιωτικού συμφέροντος, εξόχως προβληματική ως προς τον φορέα του εννόμου αγαθού και κατ' επέκταση τον δικαιούχο υποβολής έγκλησης και δήλωσης παράστασης πολιτικής αγωγής η περίπτωση του εδάφιου β΄ της παρ. 2 του αρ. 370Γ, όταν η πράξη

[164]Βέβαια, το δικαίωμα της έγκλησης δεν ταυτίζεται με αυτό της παράστασης πολιτικής αγωγής που είναι ευρύτερο του πρώτου, αλλά ως επί το πλείστον συμπίπτουν τα πρόσωπα των φορέων τους, ίδετε Μαργαρίτης Μ. «Ποινικός Κώδικας, Ερμηνεία-Εφαρμογή» 2η έκδοση 2009, σελ. 310.
[165]Ιδ. σχετικά και άρθρο 12 παρ. 1 της Οδηγίας.
[166]Ιδ. σχετικά «Ποινικός Κώδικας και Νομολογία» Α. Χαραλαμπάκης-Ι. Γιαννίδης, 2009, σελ. 523.

αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους. **Η διάταξη παραπέμπει ρητά ως προς την τιμώρηση του δράστη στο άρθρο 148ΠΚ,** διάταξη που υπάγεται στις διατάξεις για την προδοσία της χώρας και ποινικοποιεί την κατασκοπεία. Ωστόσο, στο αρ. 370Γ θα έπρεπε να μην απαιτείται η υποβολή έγκλησης όταν η παράνομη πρόσβαση βάλλεται κατά του κράτους. Κατά την κρατούσα άποψη, **στο άρθρο 148 ΠΚ το προβλεπόμενο έγκλημα της** κατασκοπείας είναι έγκλημα κατά της εξωτερικής Υποστάσεως-Ασφάλειας του Κράτους[167], ήτοι στρέφεται κατά του προστατευομένου εννόμου αγαθού της κρατικής εξουσίας εν γένει υπό τις διάφορες εκφάνσεις της[168], και ελλείψει σχετικής μνείας, διώκεται αυτεπαγγέλτως. Ομοίως, εγκλήματα που αφορούν διεθνείς σχέσεις και ασφάλεια του κράτους βάλλουν κατά υπερατομικών εννόμων αγαθών.

Σ' αυτά τα εγκλήματα που **πλήττουν αποκλειστικά το γενικό συμφέρον** και όχι ιδιωτικά συμφέροντα, τυχόν ζημία ιδιώτη ασφαλώς δεν θεμελιώνει αξίωση αποζημίωσης ή χρηματικής ικανοποίησης και αντίστοιχα δικαίωμα παράστασης πολιτικής αγωγής[169]. Συνεπώς μια τέτοια δηλωθείσα παράσταση πολιτικής αγωγής θα τύχει απορριπτέα ως απαράδεκτη. Συμφώνως με τα προαναφερθέντα, **η διάταξη του αρ. 370Γ ΠΚ έχει θεσπιστεί για την προστασία του ιδιωτικού συμφέροντος και όχι του κοινωνικού, και δεν γεννάται αξίωση αποζημίωσης ή χρηματικής ικανοποίησης λόγω ηθικής βλάβης του Δημοσίου[170], παρά μόνο στην περίπτωση που το Κράτος ενεργεί ως fiscus.**

## ΝΟΜΟΛΟΓΙΑΚΗ ΕΦΑΡΜΟΓΗ

Το παρωχημένο των ρυθμίσεων της διάταξης του αρ. 370Γ, ως αυτή ίσχυε πριν τις τροποποιήσεις που επέφερε ο Ν. 4411/2016, αποδεικνύεται αναμφισβήτητα από την εξαιρετικά φτωχή έως ανύπαρκτη νομολογιακή της εφαρμογή, παρά το γεγονός ότι η προϊσχύουσα διάταξη είχε αρκετά διευρυμένο πεδίο περιπτώσεων για θεμελίωση του αξιόποινου, αφού αρκούνταν στην χωρίς δικαίωμα πρόσβαση με ενδεικτική και όχι σωρευτική συνδρομή παραβίασης απαγορεύσεων ή μέτρων ασφαλείας. **Πιο συγκεκριμένα, η μόνη -δημοσιευμένη τουλάχιστον- απόφαση**

[167]Ιδ. σχετικά με ερμηνεία διάταξης 148 ΠΚ «Ποινικός Κώδικας και Νομολογία» Α. Χαραλαμπάκης-Ι. Γιαννίδης, 2009, σελ. 565 επ. και Φ. Ανδρέου Ποινικός Κώδικας, 2005, σελ. 617 .
[168]Ιδ. σχετικά Ψαρούδα-Μπενάκη Α. «Η πολιτική αγωγή στην ποινική δίκη» σελ. 109 επ.
[169]Ιδ. σχετικά «Ποινικός Κώδικας Ερμηνεία κατ' αρθρο» Χαραλαμπάκη, 2014 σελ. 2989 περί πολιτικής αγωγής.
[170]Ιδ. σχετικά Ψαρούδα-Μπενάκη Α. «Η πολιτική αγωγή στην ποινική δίκη» σελ. 99 και Τριμ.Ναυτ Πειραιά 530/2003, ΠοινΧρον. 2004, 75, όπου απορρίφθηκε η δηλωθείσα παράσταση πολιτικής αγωγής του Ελληνικού Δημοσίου λόγω έλλειψης ενεργητικής νομιμοποίησης.

**είναι η υπ' αριθμ. 530/2003 του Ναυτοδικείου Πειραιώς**, στην οποία θα αναφερθούμε αναλυτικά κατωτέρω, ενώ λόγος για την διάταξη του αρ. 370Γ, χωρίς εφαρμογή αυτής ή εκτενέστερη αναφορά, έχει γίνει στην υπ' αριθμ. 1227/1990 ΑΠ[171] και στην υπ' αριθμ. 643/2012 του Μονομελούς Πλημμελειοδικείου Σάμου[172]. Επιπλέον, όπως ήδη αναφέρθηκε σε άλλο κεφάλαιο της παρούσας μελέτης, προσέγγιση των ρυθμίσεων του αρ. 370Γ παρ. 1 για την περίπτωση της χωρίς δικαίωμα αντιγραφής προγράμματος ηλεκτρονικού υπολογιστή, έχει επιχειρηθεί και με το υπ' αριθμ. 3204/1993 Βούλευμα του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης[173], το οποίο παρέπεμψε τον κατηγορούμενο στο ακροατήριο, ωστόσο δεν έχει δημοσιευτεί η έκβαση της εν λόγω ποινικής διαδικασίας.

Στην υπ' αριθμ. **530/2003 απόφαση του Ναυτοδικείου Πειραιώς**[174] γίνεται δεκτό πως η διάταξη του αρ. 370Γ έχει θεσπιστεί για την προστασία του ιδιωτικού συμφέροντος και όχι του κοινωνικού, και *«προστατευόμενο έννομο αγαθό είναι το απόρρητο υπό τυπική έννοια, δηλαδή το τυπικό δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό τυπική έννοια [..] Προστατεύεται η ίδια η πληροφορία, καθόσον προσλαμβάνει υπόσταση και αξία κατόπιν αξιολογήσεως από τον φορεά της»* Στην εν λόγω απόφαση περαιτέρω, παρουσιάζεται η περίπτωση της «χωρίς δικαίωμα πρόσβασης» από κελευστή, ο οποίος παρόλο που άνηκε εν γένει στο προσωπικό του πολεμικού πλοίου, εν τούτοις **«δεν είχε εξουσιοδότηση»,** να βρίσκεται στο συγκεκριμένο χώρο όπου βρισκόταν ο ηλεκτρονικός υπολογιστής, **τον οποίο αφού έθεσε σε λειτουργία προέβη σε χρησιμοποίηση εγκατεστημένου ηλεκτρονικού προγράμματος και σε εκτύπωση συγκεκριμένων εγγράφων**.

Ο ως ανω δράστης-κελευστής **χωρίς δικαίωμα**, δηλαδή **χωρίς την συγκατάθεση του Κυβερνήτη του πολεμικού πλοίου (νομίμου κατόχου Η/Υ),** αφού **απέκτησε πρόσβαση** στο φυσικό χώρο όπου βρισκόταν ο υπολογιστής αλλά και στον ίδιο τον υλικό φορέα, **προέβη σε χρησιμοποίηση προγράμματος του.**

---

[171]υπ'αριθμ. 1227/1990 ΑΠ, ΤΝΠ Ισοκράτης, στην οποία προσβάλλεται βούλευμα δια αναιρέσεως, μεταξύ άλλων λόγων και για εσφαλμένη εφαρμογή της διάταξης του αρ. 386 παρ. 1, έναντι της ορθής, κατά τον αναιρεσείοντα του αρ. 370Γ. Ωστόσο, το Ακυρωτικό μας Δικαστήριο δεχόμενο ότι *«ορθώς δεν υπήχθησαν τα δεκτά υπό του βουλεύματος γενόμενα, κατά τ' ανωτέρω πραγματικά περιστατικά στην διάταξη του αρ. 370Γ»* απορρίπτει τον συγκεκριμένο λόγο αναίρεσης ως αβάσιμο.

[172]υπ' αριθμ. 634/2012 ΜονΠλημμΣάμου, ΤΝΠ Ισοκράτης, στην οποία απλά αναφέρεται ότι «*Από πλευράς συνταγματικού δικαίου, η προστασία της ιδιωτικής ζωής, όπως είναι οι διατάξεις των άρθρων $5^{A}$, 9, $9^{A}$ και 19 του Συντάγματος. Υπάρχουν όμως και από πλευράς ποινικού δικαίου διατάξεις προστασίας της ιδιωτικής ζωής, όπως είναι οι διατάξεις των άρθρων 370-370Γ ΠΚ [..]»*

[173] δ. Υπερ. 1994, σελ. 1133 επ.

[174]υπ' αριθμ. 530/2003 Ναυτοδικείο Πειραιώς, ΠοινΧρον ΝΔ 2004, σελ.75.

Από τα πραγματικά περιστατικά δεν αναφέρεται, ούτε προκύπτει ότι υπήρχαν και παραβιάσθηκαν μέτρα ασφαλείας που αφορούσαν είτε τον φυσικό χώρο είτε τον ηλεκτρονικό υπολογιστή, καθότι κατά τον χρόνο τέλεσης της αξιόποινης πράξης η διάταξη του αρ. 370Γ παρ. 2 στοιχειοθετούσε αξιόποινο **για την χωρίς δικαίωμα πρόσβαση,** με ενδεικτική *{'ιδίως'}*, και όχι σωρευτική συνδρομή απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχος.

Ωστόσο, παρά το γεγονός ότι στην περί ου ο λόγος απόφαση εκτίθεται λίαν αντιπροσωπευτικά η περίπτωση της χωρίς δικαίωμα πρόσβασης σε υπολογιστή και χωρίς δικαίωμα χρησιμοποίησης προγράμματος από τον δράστη, το Ναυτοδικείο Πειραιώς **ομοφώνως κηρύσσει ένοχο τον δράστη** για την παράνομη χρήση προγράμματος ηλεκτρονικού υπολογιστή, **ήτοι για το έγκλημα του αρ. 370Γ παρ. 1**, ενώ κατά την γνώμη της γράφουσας θα έπρεπε να τον κηρύξει ένοχο αμφοτέρων των αδικημάτων λόγω της ετερότητας των προσβαλλόμενων εννόμων αγαθών και των πλειόνων πράξεων που συνιστούν αληθινή πραγματική συρροή.

Διαπιστώνεται λοιπόν, πως δεν υφίσταται νομολογιακή εφαρμογή (!) του αρ. 370Γ παρ. 2 για παράνομη πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ως προβλεπόταν πριν τις αλλαγές της διάταξης, πρωτίστως λόγω των εξελιγμένων μορφών του εγκλήματος που η προϊσχύουσα διάταξη αδυνατούσε να καλύψει και δευτερευόντως λόγω της δυσκολίας να αντιληφθεί κάποιος ότι έχει πέσει θύμα παράνομης πρόσβασης από τρίτο, πολλώ δε μάλλον να τον εντοπίσει.

Ωστόσο, μετά τις τροποποιήσεις του Ν. 4411/2016, η διάταξη του αρ. 370Γ παρ. 2 τιμωρεί σχεδόν όλες τις δυνατές μορφές τέλεσης της παράνομης πρόσβασης, καθότι υλικό αντικείμενο πλέον δεν είναι μόνο ο ηλεκτρονικός υπολογιστής, αλλά πληροφοριακά συστήματα και στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, στις οποίες μπορεί κάποιος χωρίς δικαίωμα να αποκτήσει πρόσβαση **είτε με την χρήση διαδικτύου, είτε χωρίς αυτήν**. Την υπέρμετρη διεύρυνση της αντικειμενικής υπόστασης μέσω του υλικού αντικειμένου, έρχεται να περιορίσει η υποχρεωτική συνδρομή παραβίασης απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχος. Έτσι κατόπιν των ανωτέρω, και λαμβανομένης υπόψιν της νεοεισαχθείσας διάταξης του αρ. $370^{E}$ περί τιμώρησης των προπαρασκευαστικών πράξεων του αρ. 370Γ παρ. 2, προσδοκάται να τύχει εφαρμογής η τροποποιημένη διάταξη περί παράνομης πρόσβασης σε πληροφοριακά συστήματα. Αναμένεται ωστόσο με ενδιαφέρον η αντιμετώπιση από το σύστημα

απονομής της ποινικής δικαιοσύνης στο σύνολο του, ήτοι από την κίνηση της ποινικής δίωξης, έως και την καταδίκη του δράστη.

Εκφράζεται στο σημείο αυτό, και ο προβληματισμός της γράφουσας περί μεγάλου ενδεχομένου μη εφαρμογής της εν λόγω διάταξης, παρά τις τροποποιήσεις που την εκσυγχρόνισαν. Και τούτο διότι οι σύγχρονοι «hackers», δεν δρουν με σκοπό την επίδειξη των τεχνικών τους ικανοτήτων να «σπάσουν ένα πληροφοριακό σύστημα», αλλά ως επί το πλείστον αποσκοπούν στην αξιοποίηση των πληροφοριών και στοιχείων περισσοτέρων εγκληματικών πράξεων.

## ΣΚΕΨΕΙΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

### Α. Σε ενωσιακό επίπεδο

Η Ευρωπαϊκή Επιτροπή (εφεξής Επιτροπή) έχει δεσμευτεί να διασφαλίσει την ολοκλήρωση της μεταφοράς των διατάξεων της Οδηγίας στο εθνικό δίκαιο όλων των κρατών μελών της Ευρωπαϊκής Ένωσης και την ορθή εφαρμογή τους. Στα πλαίσια αυτών των δύο σκοπών, η Επιτροπή υπέβαλε την από 13.09.2017 **έκθεση αξιολόγησης**[175] προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, **με αντικείμενο** το κατά πόσον τα κράτη-μέλη έχουν λάβει τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την Οδηγία, και σαφή υπόμνηση (μέσω της έκθεσης), ότι θα συνεχίσει να παρέχει στήριξη στα κράτη-μέλη για την εφαρμογή της. Η Επιτροπή κατέστησε σαφές ότι η περιγραφή και η ανάλυση της έκθεσης της βασίζονται σε πληροφορίες που υπέβαλαν τα κράτη-μέλη έως τις 31.05.2017. Ό,τι υπεβλήθη αργότερα δεν λήφθηκε υπόψιν, ενώ συνεκτιμήθηκαν όλα τα κοινοποιηθέντα μέτρα που αφορούν τις εθνικές νομοθεσίες, αποφάσεις δικαστηρίων, η κοινή νομική θεωρία και επιπρόσθετες πληροφορίες-διευκρινίσεις που λήφθηκαν, κατόπιν άμεσης επικοινωνίας με τα κράτη-μέλη. Μάλιστα, τον Νοέμβριο του έτους 2015, η Επιτροπή κίνησε δικαστικές διαδικασίες, μεταξύ και άλλων κρατών-μελών, και κατά της Ελλάδας διότι δεν της κοινοποίησε τα εθνικά μέτρα μεταφοράς της Οδηγίας στο εθνικό μας δίκαιο, ως όφειλε να είχε θεσπίσει έως τις 04.09.2015[176].

---

[175]Ιδ. https://ec.europa.eu/transparency/regdoc/rep/1/2017/EL/COM-2017-474-F1-EL-MAIN-PART-1.PDF Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στην οποία αξιολογείται κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

[176]Ιδ. http://europa.eu/rapid/press-release_MEMO-16-4211_EL.htm *: «Ένωση ασφάλειας - οδηγία της ΕΕ για το ηλεκτρονικό έγκλημα: Η Επιτροπή ζητά από 3 κράτη μέλη να εξασφαλίσουν πλήρη εφαρμογή και περατώνει 2 υποθέσεις {..} Η οδηγία, η οποία εκδόθηκε στις 12 Αυγούστου 2013, θα έπρεπε να είχε μεταφερθεί από τα κράτη μέλη έως τις 4 Σεπτεμβρίου 2015. Η οδηγία για τις επιθέσεις κατά συστημάτων*

Ειδικότερα, με αφετηρία τους στόχους και το πεδίο εφαρμογής της Οδηγίας, η Επιτροπή σε ό,τι αφορά το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα, αναφέρει πως η Ελλάδα έχει πλέον θεσπίσει νομικές διατάξεις με τον ορισμό των όρων «σύστημα πληροφοριών» και «ψηφιακά δεδομένα». Εν συνεχεία, ως προς τον ορισμό του όρου «χωρίς δικαίωμα» αναφέρεται ότι σε όλα τα κράτη-μέλη (συμπεριλαμβανομένης και της Ελλάδας) ισχύει η γενική αρχή της μη ποινικής ευθύνης για οποιαδήποτε ενέργεια, εφόσον αυτή η ενέργεια λαμβάνει χώρα βάσει παρεχόμενων δικαιωμάτων. Αντιστοίχως, και για τον όρο «νομικό πρόσωπο» προβλέπεται ορισμός στο αστικό μας δίκαιο, καθώς και επιμέρους ποινικές διατάξεις για ευθύνη νομικών προσώπων. Ως προς δε τους γενικούς κανόνες για τα σχετικά αδικήματα της Οδηγίας (άρθρα 8 -12) αφορώντες ηθική αυτουργία, συνέργεια και απόπειρα, αυτοί καλύπτονται από διατάξεις του γενικού μέρους του ελληνικού ποινικού κώδικα (αρ. 42 περί απόπειρας, αρ. 46 επ. περί συμμετοχής κλπ), χωρίς να είναι απαραίτητη καμία ειδικότερη νομοθετική πρόβλεψη. Τέλος, ως προς το ζήτημα των κυρώσεων, η Ελλάδα κατά τα διαλαμβανόμενα στην Οδηγία, «φαίνεται» να προβλέπει αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις, αφού καλύπτει τόσο για το έγκλημα της παράνομης πρόσβασης (αρ. 370Γ παρ. 2) όσο και γι' αυτό των προπαρασκευαστικών πράξεων (άρ. 370Ε), το ελάχιστο επίπεδο του ανωτάτου ορίου κυρώσεων, ήτοι: στερητική της ελευθερίας ποινή τουλάχιστον για δύο έτη. Ως εκ των ανωτέρω συνάγεται ότι η Ελλάδα έχει ενσωματώσει πράγματι τις σχετικές ρυθμίσεις και έχει συμμορφωθεί με την Οδηγία.

## Β. Σε εθνικό επίπεδο

Εξ' όσων παρατέθηκαν ανωτέρω, αλλά και από το σύνολο της παρούσας μελέτης, είναι έκδηλο ότι με το Ν. 4411/2016 ενσωματώθηκε η Οδηγία **που «εκσυγχρόνισε» την μέχρι τότε παρωχημένη ειδική υπόσταση** του «χωρίς

---

*πληροφοριών ποινικοποιεί τη χρήση εργαλείων που χρησιμοποιούνται σε επιθέσεις στον κυβερνοχώρο, όπως είναι το κακόβουλο λογισμικό, ενισχύει το πλαίσιο για την ανταλλαγή πληροφοριών όταν συμβαίνουν επιθέσεις και παρέχει ένα κοινό ευρωπαϊκό πλαίσιο ποινικού δικαίου στον τομέα αυτό. Η Επιτροπή θεωρεί ότι τα μέτρα που κοινοποιήθηκαν από το Βέλγιο, τη Βουλγαρία και την Ιρλανδία δεν έχουν ακόμη μεταφέρει πλήρως όλες τις διατάξεις της οδηγίας στο εθνικό δίκαιο των οικείων χωρών. Το Βέλγιο, η Βουλγαρία και η Ιρλανδία έχουν πλέον στη διάθεσή τους δύο μήνες για να κοινοποιήσουν στην Επιτροπή όλα τα μέτρα που έλαβαν προκειμένου να εξασφαλίσουν την πλήρη εφαρμογή της οδηγίας· διαφορετικά, η Επιτροπή μπορεί να αποφασίσει να παραπέμψει αυτές τις υποθέσεις στο Δικαστήριο της ΕΕ. Επιπλέον, αφού εξέτασε τα μέτρα που κοινοποίησαν οι ελληνικές και σλοβενικές αρχές, η Επιτροπή αποφάσισε να περατώσει τις διαδικασίες επί παραβάσει κατά της Ελλάδας και της Σλοβενίας.»*

πατρίδα» αδικήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα, **ποινικοποιώντας σχεδόν όλες τις δυνατές περιπτώσεις τέλεσης** του αδικήματος, τόσο με όσο και χωρίς την χρήση διαδικτύου, **διευρύνοντας έτσι το εύρος της ποινικής προστασίας** που απολαμβάνει ο νόμιμος κάτοχος.

Την ευρεία αυτή διεύρυνση του υλικού αντικειμένου της διάταξης, εξισορρόπησε ο ίδιος ο ποινικός νομοθέτης με την **ρητή απαίτηση** του, **η χωρίς δικαίωμα πρόσβαση να λαμβάνει χώρα σωρευτικά με την παραβίαση απαγορεύσεων ή μέτρων ασφαλείας** (εξωτερικοί όροι του αξιοποίνου). Με αυτήν την απαίτηση του «ενδυνάμωσε», κατά την γνώμη της γράφουσας, **το τυπικό απόρρητο ως προστατευόμενο έννομο αγαθό της διάταξης**. Και τούτο διότι με την σαφή και εξωτερικευμένη, μέσω των ληφθέντων μέτρων ασφαλείας βούληση του, ο νόμιμος κάτοχος οριοθετεί τον δικό του αυστηρά ιδιωτικό πληροφοριακό «χώρο»· ο χαρακτήρας του «χώρου» αυτού ως πληροφοριακού ή ψηφιακού κλπ., δεν θα πρέπει να οδηγεί στην υιοθέτηση της εσφαλμένης άποψης ότι προστατευόμενο έννομο αγαθό είναι η πληροφορία ή τα πληροφοριακά συστήματα. Το αυτό άλλωστε αποκλείεται και εκ του γεγονότος θέσπισης με τον ίδιο νόμο συναφών, ωστόσο αυτοτελών εγκληματικών πράξεων, όπως πχ. τα αρ. 292Β και 381Α. Ως εκ τούτου, ορθότερο είναι να θεωρήσουμε ότι προστατευόμενο έννομο αγαθό της διάταξης παραμένει το τυπικό απόρρητο, με την μόνη διαφοροποίηση (ως προς το ζήτημα του εννόμου αγαθού) να είναι το πεδίο προστασίας του τυπικού απορρήτου, απ' αυτό του συστήματος υπολογιστή σε αυτό του πληροφοριακού συστήματος.

Κατ' επέκταση, με την πρόβλεψη του λίαν **αυστηρότερου του προϊσχύοντος πλαισίου ποινής της φυλάκισης** καθώς και την **θεμελίωση αξιόποινου των προπαρασκευαστικών της παράνομης πρόσβασης πράξεων**, ο νομοθέτης κατέστησε σαφή πλέον στους κοινωνούς του δικαίου την έντονη απαξία της έννομης τάξης, για μία πράξη η οποία δίνει την δυνατότητα στο δράστη για σωρεία τέλεσης άλλων ποινικών αδικημάτων (!). Ας μη παραβλέπεται άλλωστε, πως η άυλη φύση της πληροφορίας και των ψηφιακών δεδομένων δημιουργεί **σοβαρές τεχνικές δυσχέρειες στην ανακάλυψη και βεβαίωση των σχετικών εγκλημάτων αυξάνοντας τα ποσοστά αφανούς εγκληματικότητας.** Προς τούτο τόσο η Σύμβαση όσο και η Οδηγία τονίζουν την επιτακτική **ανάγκη διακρατικής συνεργασίας** των αρμοδίων αρχών των κρατών-μελών, την **ανάγκη κοινής προσέγγισης-αντιμετώπισης των σχετικών εγκλημάτων από τους εθνικούς νομοθέτες, και την**

**ανάγκη θέσπισης επιχειρησιακών εθνικών σημείων επαφής με σκοπό την ανταλλαγή πληροφοριών σχετικά με τα επίμαχα αδικήματα· Όλα αυτά επισημαίνονται εκ νέου επισημαίνονται και αξιολογούνται θεσμικά για πρώτη φορά στην προαναφερόμενη έκθεση της Επιτροπής.**

Δεδομένου ότι πρόκειται για μια εξαιρετικά πρόσφατη τροποποίηση δεν υπάρχει μέχρι στιγμής κάποιο δείγμα νομολογίας για να διαπιστωθεί πως οι αλλαγές στην ειδική υπόσταση της διάταξης έχουν λάβει χώρα εν τοις πράγμασι. Εκφράζεται στο σημείο αυτό ο έντονος προβληματισμός της γράφουσας, περί του αν τελικά η «νέα» διάταξη θα τύχει εφαρμογής από τους εφαρμοστές του δικαίου στην ελληνική έννομη τάξη, δεδομένων τριών, κατά τη γνώμη της, σοβαρών παραγόντων-κωλυμάτων: 1) της έλλειψης σχετικής τεχνογνωσίας και της δυσκολίας εξιχνίασης εγκλημάτων και εντοπισμού των δραστών, 2) του προσδιορισμού του τόπου τέλεσης της πράξης και κατ' επέκταση την θεμελίωση ποινικής δικαιοδοσίας και 3) της τέλεσης ως επί το πλείστον κάποιας άλλης αξιόποινης πράξης μετά την απόκτηση πρόσβασης στο πληροφοριακό σύστημα, δυνάμει της οποίας θα καταλήγει να διώκεται τελικά ο δράστης, σύμφωνα με τους κανόνες περί συρροής

Για την αντιμετώπιση του πρώτου ζητήματος, απαραίτητη κρίνεται η στελέχωση των αρμοδίων αρχών και υπηρεσιών με καταλλήλως εκπαιδευμένο σε τέτοιας φύσεως αδικήματα ανθρώπινο δυναμικό (όπως πχ. στο Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος), καθώς και η σχετική επιμόρφωση των δικαστικών και εισαγγελικών λειτουργών που θα επιλαμβάνονται τις σχετικές δικογραφίες. Εν συνεχεία, για την επίλυση του θέματος του τόπου τελέσεως έχει ήδη προκριθεί αιτιολογημένα ως συνεπέστερη η θέση του Κιούπη[177] περί επιλογής των τόπων όπου οι χρήστες «κάλεσαν-κατέβασαν» τα δεδομένα και απέκτησαν πρόσβαση στο διαδίκτυο. Για την αντιμετώπιση δε, του τελευταίου ζητήματος χρειάζεται αυξημένη προσοχή από τον εκάστοτε εφαρμοστή του δικαίου, αν θα υφίσταται τελικά πραγματική ή φαινομένη συρροή ποινικών διατάξεων, καθότι τελευταία θα καθιστά την διάταξη του αρ. 370 Γ παρ. 2 ανεφάρμοστη λόγω της αρχής της ειδικότητας.

Σε κάθε όμως περίπτωση, ανεξαρτήτως των προαναφερθέντων αλλά και άλλων τυχόν ζητημάτων που θα ανακύψουν κατά την εφαρμογή της διάταξης, οι τροποποιήσεις που έγιναν ήταν τουλάχιστον επιτακτικές για την κάλυψη νομοθετικών κενών, καθώς δεν νοείται μία σύγχρονη έννομη τάξη, κατά το έτος 2017 να μην

[177] Ιδ. αναλυτικά την τοποθέτηση του Κιούπη σελ 52 της παρούσας εργασίας.

προβλέπει μία ικανή ουσιαστικά και νομικά διάταξη για ένα έγκλημα που μαζί με όσα άλλα έπονται, πλήττει κατά κόρον τον κυβερνοχώρο και θέτει σε κίνδυνους φυσικά πρόσωπα, νομικά πρόσωπα, αλλά και υποδομές ζωτικής σημασίας. Έτσι μπορεί κάλλιστα να ειπωθεί ότι η Ελλάδα πέραν του ενωσιακού πεδίου, συμμορφώθηκε και προς την «άγραφη επιταγή» της σύγχρονης ημεδαπής έννομης τάξης. Αναμένεται λοιπόν με εξαιρετικά μεγάλο ενδιαφέρον να διαγραφεί η πορεία της ισχύουσας διάταξης και η εφαρμογή της, η αποτελεσματικότητα της διακρατικής συνεργασίας καθώς και τυχόν νέες κατευθυντήριες γραμμές της Ευρωπαϊκής Επιτροπής προς τα κράτη-μέλη της ένωσης

. _____ .

## ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

| | |
|---|---|
| ΑΚ | Αστικός Κώδικας |
| Αριθμ. | Αριθμός |
| Αρ. | Άρθρο |
| Αρμ. | Αρμενόπουλος |
| Βλ. | Βλέπε |
| Εδ. | Εδάφιο |
| Εκδ. | Εκδόσεις |
| Επ. | Επόμενα |
| Η/Υ | Ηλεκτρονικός Υπολογιστής |
| Ιδ. | Ίδετε |
| κλπ. | Και λοιπά |
| ΚΠΔ | Κώδικα Ποινικής Δικονομίας |
| Ν. | Νόμος |
| Παρ. | Παράγραφος |
| Περ. | Περίπτωση |
| ΠΚ | Ποινικός Κώδικας |

| | |
|---|---|
| Ποιν. Δικ. | Ποινική Δικαιοσύνη |
| Ποιν. Χρον. | Ποινικά Χρονικά |
| Σελ. | Σελίδα |
| Στ. | Στοιχείο |
| Σ | Σύνταγμα |
| Υπερ. | Υπεράσπιση |

## ΑΡΘΡΟΓΡΑΦΙΑ-ΒΙΒΛΙΟΓΡΑΦΙΑ

### Α. Αρθρογραφία :

**Αγγελής Ι.**, «Διαδίκτυο (internet) και ποινικό δίκαιο, έγκλημα στον Κυβερνοχώρο (Cybercrime-Internet crime)», Ποιν Χρον. Ν 2000, σελ. 675 επ.

**Βασιλάκη Ε.** «Τα φαινόμενα phising, pharming και η ποινική τους αξιολόγηση», Ποινικά Χρονικά ΝΖ 2007, σελ. 860

**Καιάφα-Γκμπάντι Μ.** «Ποινικό Δίκαιο και Καταχρήσεις Πληροφορικής», Αρμενόπουλος 2007, σελ. 1058 επ.

**Κιούπης Δ.** «Ποινική ευθύνη παρόχων πρόσβασης», Ποινικά Χρονικά ΜΗ 1993, σελ. 720 επ.

**Κιούπης Δ**. «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας», Υπεράσπιση 2000, σελ. 959 επ.

**Κιούπης Δ.** «Το δίκαιο στην Ψηφιακή Εποχή, Προστασία Προσωπικότητας-Σύγχρονες Μορφές Εγκλήματος-Ηλεκτρονικό Επιχειρείν», 3ο Πανελλήνιο Συνέδριο Ένωση Ελλήνων Νομικών **e-ΘΕΜΙΣ**, Νομική Βιβλιοθήκη 2012

**Λίβος Ν.** «Ποινικοδικονομικές επεμβάσεις σε δεδομένα τηλεπικοινωνιών» ΠοινΧρον ΜΔ σελ. 564-565

**Φαραντούρης Ν.** «Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο- Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς», ΠοινΔικ 2/2003, σελ. 191 επ.

## Β. Βιβλιογραφία :


**Ανδρουλάκης Ν.** «Ποινικό Δίκαιο, Γενικό Μέρος, Θεωρία για το Έγκλημα», Π. Ν. Σάκκουλας 2000

**Αργυρόπουλος Α.** «Ηλεκτρονική Εγκληματικότητα», Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή 2001

**Βασιλάκη Ε.** «Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών», Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή, 1993

**Βλαχόπουλος Κ.** «Ηλεκτρονικό έγκλημα, Μορφές-Πρόληψη-Αντιμετώπιση», Νομική Βιβλιοθήκη, έκδοση 2007

**Γεωργιάδης Α.** «Εμπράγματο Δίκαιο», Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη, 2η έκδοση, 2010

**Δημητράτος Ν. «**Έννομο αγαθό και διδασκαλία περί εγκλήματος στο ποινικό δίκαιο,» εκδόσεις Αντ. Ν. Σάκκουλα 1998

**Ζάννη Α.** «Το διαδικτυακό έγκλημα», Σειρά Media και έγκλημα, εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή 2005

**Ιγγλεζάκης Ι.** «Δίκαιο της Πληροφορικής», Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη, 2008

**Καράκωστας Ι**. «Δίκαιο και Ίντερνετ, Νομικά ζητήματα του διαδικτύου», Π.Ν. Σάκκουλας, 3η έκδοση 2009

**Κιούπης Δ.** «Ποινικό Δίκαιο και Ίντερνετ», Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή 1999

**Κονταξής Α.** «Ποινικός Κώδικας» Τόμος ΙΙ, Π.Ν. Σάκκουλας 2000

**Κοτσαλής Λ.** «Ποινικό Δίκαιο, Γενικό Μέρος Ι», εκδόσεις Αντ. Ν. Σάκκουλα 2005

**Κριθαράς Θ.** «Ποινικό Δίκαιο & Διαδίκτυο», Νομική Βιβλιοθήκη, έκδοση 2009

**Κωστάρας Α.** «Έννοιες και Θεσμοί του Ποινικού Δικαίου», εκδόσεις Αντ. Ν. Σάκκουλα, ανατύπωση 2008

**Κωστάρας** «Ποινικό Δίκαιο-Επιτομή Ειδικού Μέρους (άρθρα 134-410 ΠΚ)», Νομική Βιβλιοθήκη, 4η έκδοση, 2014

**Λάζος** «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, 2001

**Μαυριάς Κ**. «Συνταγματικό Δίκαιο», Εκδ. Αντ. Ν. Σάκκουλας,, 2005

**Μαργαρίτης Μ.** «Ποινικός Κώδικας, Ερμηνεία-Εφαρμογή» Π.Ν. Σάκκουλας, 2η έκδοση 2009

**Μανωλεδάκης Ι.** «Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου», εκδόσεις Σάκκουλα, Θεσσαλονίκη 1998

**Μυλωνόπουλος Χ.** «Ηλεκτρονικοί υπολογιστές και Ποινικό δίκαιο, Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386Α ΠΚ», εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή 1991

**Μυλωνόπουλος Χ**. «Διεθνές Ποινικό Δίκαιο, τα τοπικά όρια των ποινικών νόμων», Τεύχος Α΄ Εισαγωγή-Θεμελιώδεις έννοιες, Έκδοση Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή, 1990

**Μυλωνόπουλος Χ.** «Ποινικό Δίκαιο» Γενικό Μέρος Ι, εκδόσεις Π.Ν. Σάκκουλας, 2007

**Σπυρόπουλος Φ.** «Χωρίς Δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking)» Έκδοση Αντ. Ν. Σάκκουλα Ε.Ε. 2016

**Φιλόπουλος Π.** «Ποινική Προστασία Απορρήτου, συστηματική Ερμηνεία άρθρων 370-371 ΠΚ», Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη 2015

**Χαραλαμπάκης-Γιαννίδης** «Ποινικός Κώδικας και Νομολογία» Π.Ν. Σάκκουλας Αθήνα 2009

**Χαραλαμπάκης** «Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο» Τόμος δεύτερος, Νομική Βιβλιοθήκη, 2014

**Χρυσόγονος Κ.** «Ατομικά και Κοινωνικά Δικαιώματα» Νομική Βιβλιοθήκη, 2006

**Ψαρούδα-Μπενάκη Α.** «Η πολιτική αγωγή στην ποινική δίκη», εκδόσεις Π.Ν. Σάκκουλας 2015

## ΝΟΜΟΛΟΓΙΑ

-Τριμελές Ναυτοδικείο Πειραιά 530/2003, ΠοινΧρον. ΝΔ 2004, σελ. 75

-Μονομελές Πλημμελειοδικείο Σάμου 634/2012, ΤΝΠ Ισοκράτης

-Άρειος Πάγος 1227/1990 (σε Συμβούλιο), ΤΝΠ Ισοκράτης

-Βούλευμα Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης 3204/1993, Υπεράσπιση 1994, σελ. 1133

## ΝΟΜΟΘΕΣΙΑ

-Νόμος 4411/2016, ΦΕΚ Α΄142/03.08.2016

-Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρώπης

-Απόφαση-Πλαίσιο 2005/222/ΔΕΥ

-Σύμβαση της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, Βουδαπέστη 2001

**********