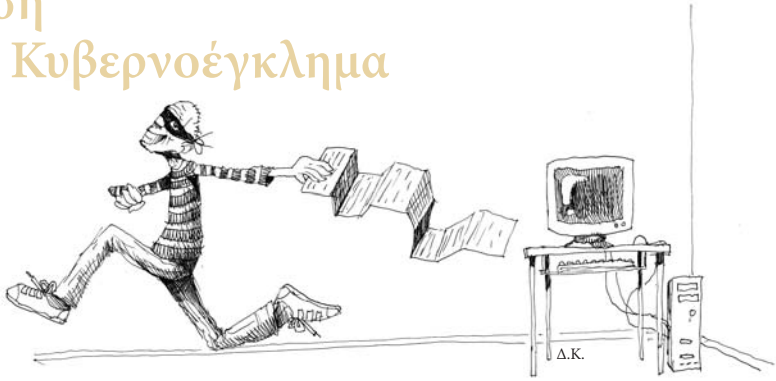
Η Σύμβαση για το Κυβερνοέγκλημα



της Παγώνας Μαρκοπούλου

Οι αξιόποινες πράξεις που λαμβάνουν χώρα στο διαδίκτυο δημιουργούν πλήθος νομικών προβλημάτων λόγω της περίπλοκης λειτουργίας των υπολογιστών καθώς και λόγω των ιδιαιτεροτήτων του διαδικτύου. Ακριβώς τα προβλήματα αυτά επιχειρεί να επιλύσει και η Σύμβαση για το Κυβερνοέγκλημα που αναλύεται στο παρόν άρθρο και η οποία δεν έχει κυρωθεί ακόμη από την Ελλάδα [σελ. 43-52]

Εισαγωγή

Οι ραγδαίες εξελίξεις στον τομέα της πληροφορικής επιστήμης οδήγησαν σε μια σειρά τεχνολογικών επιτευγμάτων που έχουν πολλαπλές συνέπειες. Από τη μια πλευρά διευκολύνουν πολλές πτυχές του κοινωνικού βίου, απ' την άλλη πλευρά όμως παρέχουν τις αναγκαίες προϋποθέσεις για την εμφάνιση μιας νέας μορφής εγκληματικής δραστηριότητας. Για την περιγραφή αυτής της νέας μορφής εγκλήματος χρησιμοποιούνται ποικίλοι όροι[1], όπως ηλεκτρονικό έγκλημα, πληροφορικό έγκλημα, έγκλημα στον κυβερνοχώρο, έγκλημα με Η/Υ, έγκλημα υψηλής τεχνολογίας (hi-tech crime), κ.λπ.

Οι αξιόποινες πράξεις που περιγράφονται μ' αυτούς τους όρους συγκεντρώνουν μια σειρά από ιδιαίτερα γνωρίσματα λόγω της άμεσης σχέσης τους με τεχνικά ζητήματα.

Τα μέσα διάδοσης και ανταλλαγής πληροφοριών, κατά κύριο λόγο ο Η/Υ, που άλλοτε αποτελούν μέσα τέλεσης κι άλλοτε στόχους της εγκληματικής δραστηριότητας,

είναι περίπλοκα στη λειτουργία τους. Αποτέλεσμα είναι τα εγκλήματα που σχετίζονται με την πληροφορική επιστήμη να αντιμετωπίζονται συχνά με αμηχανία από το νομικό κόσμο, επειδή απαιτούν από το μελετητή του δικαίου μία στοιχειώδη, έστω, εξοικείωση με την τεχνολογία των Η/Υ.

Από την άλλη πλευρά οι Η/Υ, κυρίως μέσω του διαδικτύου, επιτρέπουν τη μετάδοση πληροφοριών σε παγκόσμια κλίμακα μέσα σε δευτερόλεπτα. Το γεγονός αυτό δημιουργεί ποικίλα προβλήματα, αφού απροσδιόριστος παραμένει ο τόπος τέλεσης του εγκλήματος και η δωσιδικία των δικαστηρίων, ενώ εφαρμογή διεκδικούν οι κανόνες δικαίου διαφορετικών εννόμων τάξεων. Το σκηνικό της τέλεσης αξιόποινων πράξεων, όπως το ξέρουμε σήμερα, αλλάζει, και προβάλλει πιο επιτακτική από ποτέ η ανάγκη για διεθνή συνεργασία.

Σε μια προσπάθεια επίλυσης των ζητημάτων που ανακύπτουν στο χώρο του ηλεκτρονικού εγκλήματος, κι αναγνωρίζοντας ότι ο τομέας αυτός χρήζει διεθνούς συνεννόησης, το Συμβούλιο της Ευρώπης συνέταξε τη Σύμβαση για το Κυβερνοέγκλημα[2] η οποία υπογράφηκε[3] από την πλειοψηφία των μελών του Συμβουλίου, μεταξύ των οποίων η Ελλάδα, αλλά κι από τις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Νότιο Αφρική, στις 23/11/2001. Η Ελλάδα δεν έχει μέχρι στιγμής κυρώσει τη Σύμβαση.

Η Σύμβαση για το Κυβερνοέγκλημα κινείται σε τρεις κατευθύνσεις: εναρμόνιση του Ουσιαστικού Ποινικού Δικαίου, εναρμόνιση του Δικονομικού Ποινικού Δικαίου και θέσπιση κανόνων Διεθνούς Δικαστικής Συνεργασίας. Οι ουσιαστικού δικαίου διατάξεις βρίσκονται στην 1η Ενότητα του 2ου Κεφαλαίου της Σύμβασης και περιλαμβάνουν τις εξής κατηγορίες εγκλημάτων:

1. Εγκλήματα κατά της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των Δεδομένων και Συστημάτων. (άρ.2-6)
2. Εγκλήματα που σχετίζονται με Η/Υ. (άρ.7-8)
3. Εγκλήματα που σχετίζονται με το Περιεχόμενο των Δεδομένων. (άρ.9)
4. Εγκλήματα κατά της Πνευματικής Ιδιοκτησίας και των Συγγενών Δικαιωμάτων. (άρ.10)

Με το παρόν άρθρο θα επιχειρηθεί η παρουσίαση ενός μέρους των ουσιαστικού δικαίου διατάξεων που θέτει η Σύμβαση, καθώς και των υποχρεώσεων της Ελλά-

δας προς συμμόρφωση σ' αυτές. Συγκεκριμένα, θα γίνει αναφορά στα εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων και στα εγκλήματα που σχετίζονται με Η/Υ.

Ι. Εγκλήματα κατά της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των Δεδομένων και Συστημάτων

Άρθρο 2: Παράνομη Πρόσβαση σε Σύστημα Πληροφοριών

Οι χώρες που υπέγραψαν τη Σύμβαση καλούνται να ποινικοποιήσουν την εκ προθέσεως και χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα συστήματος πληροφοριών. Σκοπός της διάταξης είναι η προστασία του δικαιώματος κάθε προσώπου να διατηρεί κάποια δεδομένα απόρρητα, μακριά από τη δημόσια θέα.[4]

Στην ελληνική έννομη τάξη υπάρχουν ήδη πολλές διατάξεις για την προστασία του απορρήτου:

- Το άρθρο 4 σε συνδυασμό με το άρθρο 15 του ν. 3471/2006 που τροποποίησε το ν. 2472/1997 για τα προσωπικά δεδομένα, με την προϋπόθεση ότι το απόρρητο προστατεύει προσωπικά δεδομένα.
- Το άρθρο 370Β ΠΚ που τιμωρεί την πρόσβαση σε απόρρητα συγκεκριμένου είδους (κρατικά, επιστημονικά, επαγγελματικά ή επιχείρησης του δημόσιου ή ιδιωτικού τομέα) ή σε δεδομένα που ο ίδιος ο κάτοχός τους μεταχειρίζεται ως απόρρητα.
- Το άρθρο 370Γ§2 ΠΚ που τιμωρεί την απλή πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ, χωρίς περαιτέρω προϋποθέσεις κι άρα είναι αρκετά ευρεία διάταξη που περιλαμβάνει κι όλες τις περιπτώσεις που δεν καλύπτουν οι ανωτέρω διατάξεις.[5]

Ενόψει των προαναφερθέντων, φαίνεται ότι η Ελλάδα ανταποκρίνεται ήδη στην υποχρέωσή της να συμμορφωθεί με το άρ. 2 της Σύμβασης.

Άρθρο 3: Παράνομη Υποκλοπή Δεδομένων

Το άρθρο 3 καλεί τις χώρες που υπέγραψαν τη Σύμβαση να ποινικοποιήσουν τη παράνομη υποκλοπή δεδομένων σε περιπτώσεις μη δημόσιας μεταφοράς τους από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύ-

Το γεγονός της μετάδοσης πληροφοριών μέσα σε δευτερόλεπτα δημιουργεί ποικίλα προβλήματα, αφού απροσδιόριστος παραμένει ο τόπος τέλεσης του εγκλήματος και η δωσιδικία των δικαστηρίων

στημα που περιέχει δεδομένα. Η διάταξη έχει σκοπό την προστασία του απορρήτου των επικοινωνιών μέσω συστημάτων πληροφοριών, και ιδίως μέσω Η/Υ.

Η υποκλοπή δεδομένων καλύπτεται εν μέρει μόνο από το ελληνικό δίκαιο, και συγκεκριμένα όταν πρόκειται για προσωπικά δεδομένα από τον αντίστοιχο ειδικό ποινικό νόμο.[6] Δεδομένης όμως της συνεχώς αυξανόμενης διάδοσης της επικοινωνίας μέσω ηλεκτρονικών μηνυμάτων (e-mails) καθίσταται εμφανής η ανάγκη δημιουργίας μιας διάταξης συμβατής με το άρθρο 3 της Σύμβασης, που θα αποτελεί το αναγκαίο συμπλήρωμα του άρθρου 370Α ΠΚ για την παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής επικοινωνίας.

Αξίζει να σημειωθεί εδώ ότι το μη δημόσιο της μεταφοράς στο άρθρο 3 της Σύμβασης αφορά το είδος της επικοινωνίας κι όχι τα δεδομένα. Αυτό, δηλαδή, που δεν πρέπει να είναι δημόσιο είναι ο τρόπος με τον οποίο τα μέρη επέλεξαν να επικοινωνήσουν. Είναι αδιάφορο αν οι πληροφορίες που μεταφέρονται είναι απόρρητες ή αν είναι ελεύθερα προσβάσιμες από άλλη πηγή, για παράδειγμα από τον Τύπο ή από κάποια ιστοσελίδα.[7]

Άρθρο 4: Παράνομη Παρεμβολή σε Δεδομένα

Το άρθρο 4 της Σύμβασης για το Κυβερνοέγκλημα αφορά την παράνομη παρεμβολή σε δεδομένα. Μέχρι σήμερα η φθορά, αλλοίωση, διαγραφή ή άλλη επέμβαση σε δεδομένα δεν τιμωρείται διότι τα δεδομένα δεν αποτελούν «πράγμα» με την έννοια του άρθρου 381 ΠΚ, δηλαδή της φθοράς ξένης ιδιοκτησίας.[8] Τιμωρητέα είναι μόνο η φθορά στον υλικό φορέα των δεδομένων.

Ως προς την αλλοίωση αυτών καθαυτών των δεδομένων υπάρχουν στο ελληνικό δίκαιο, υπό προϋποθέσεις, δύο δρόμοι προστασίας. Αν πρόκειται για προσωπικά δεδομένα, μέσω του νόμου προστασίας προσωπικών δεδομένων κι αν πρόκειται για «έγγραφο» με την έννοια του άρθρου 13περ.γ ΠΚ, μέσω της υπεξαγωγής εγγράφου (222 ΠΚ). Η έννοια του εγγράφου όμως είναι ιδιαιτέρως στενή, διότι απαιτεί να έχουν τα δεδομένα διαιωνιστική, εγγυητική και αποδεικτική λειτουργία.[9] Έτσι, παρεμβάσεις σε δεδομένα που δεν συγκεντρώνουν τα στοιχεία του εγγράφου, ούτε αποτελούν προσωπικά δεδομένα, μένουν ατιμώρητες, παρόλο που προκαλούν σημαντικής αξίας ζημίες στους νό-

μιμους κατόχους των δεδομένων. Με τη δημιουργία ενός άρθρου που θα προστατεύει ως αυτοτελές έννομο αγαθό τα ηλεκτρονικά δεδομένα, ανεξάρτητα από τη φθορά του υλικού φορέα και θα τιμωρεί οποιαδήποτε παρέμβαση σ' αυτά, όπως για παράδειγμα η αρκετά συνηθισμένη μετάδοση «ιών», αυτό το κενό θα καλυφθεί.

Άρθρο 5: Παράνομη Παρεμβολή σε Σύστημα

Το άρθρο 5 καλεί τις χώρες που υπέγραψαν τη Σύμβαση να ποινικοποιήσουν την παράνομη παρεμβολή σε σύστημα, δηλαδή την παρεμπόδιση λειτουργίας συστήματος. Συμπεριφορές που μπορούν να υπαχθούν σ' αυτή τη νομοτυπική μορφή είναι, ενδεικτικά, το «mail bombing», δηλαδή η αποστολή τεράστιου όγκου ηλεκτρονικών μηνυμάτων με σκοπό να υπερφορτωθεί το σύστημα και να καταρρεύσει και το «denial of service», δηλαδή η παρεμπόδιση της λειτουργίας του συστήματος προσωρινά ή μόνιμα, συνήθως με τη χρήση κωδικών που το «μπλοκάρουν».[10]

Ανάλογη διάταξη στο ελληνικό δίκαιο δεν υπάρχει. Κατά συνέπεια, προς συμμόρφωση στη Σύμβαση, θα πρέπει να θεσπιστεί μία καινούργια διάταξη, η οποία θα καλύπτει αυτές τις μορφές αξιόποινης συμπεριφοράς, ανάγοντας μάλιστα σε αυτοτελές αγαθό το σύστημα πληροφοριών.

Άρθρο 6: Κακή Χρήση Συσκευών

Το άρθρο 6 της Σύμβασης για το Κυβερνοέγκλημα αξιώνει από τις χώρες να καταστήσουν ποινικά κολάσιμες την παραγωγή, πώληση, κατοχή για χρήση, εισαγωγή ή διάθεση συσκευών, προγραμμάτων Η/Υ ή κωδικών που σχεδιάστηκαν ή προσαρμόστηκαν με σκοπό την τέλεση των αξιόποινων πράξεων που περιγράφονται στα άρθρα 2-5 της Σύμβασης.

Η διάταξη, όπως είναι διατυπωμένη, είναι εξαιρετικά ευρεία, και σε περίπτωση που θα μεταφερθεί έτσι στο ελληνικό δίκαιο θα δημιουργήσει ποικίλα προβλήματα.

Κατ' αρχάς, τιμωρεί προπαρασκευαστικές πράξεις, πολύ πριν το στάδιο ακόμη και της απόπειρας, ανοίγοντας υπερβολικά την ψαλίδα του αξιοποίνου.

Έπειτα, δίνει έμφαση στο υποκειμενικό στοιχείο, δηλαδή στο σκοπό τέλεσης άλλης αξιόποινης πράξης, χωρίς να εξετάζει την επικινδυνότητα αυτών καθαυτών των συσκευών και κωδικών για τα έννομα αγαθά. Πρόκειται για τιμώρηση αντικειμένων καθημερινής χρήσης, η δυνατότητα όμως και μόνο να χρησιμοποιηθούν για την τέλεση

αξιόποινης πράξης σε συνδυασμό με τον σκοπό, που ως υποκειμενικό στοιχείο είναι εξαιρετικά δύσκολο να αποδειχθεί, δεν αρκεί για την ποινικοποίησή τους, ούτε ακόμη σε διάταξη θεμελίωσης ή συντήρησης πηγής κινδύνου.[11] Κι αυτό διότι ακόμη κι αυτές οι διατάξεις απαιτούν να υπάρχει έστω σε αφηρημένο επίπεδο μια ανοιχτή, λειτουργούσα και προσβάσιμη στα έννομα αγαθά πηγή κινδύνου.[12] Οι συσκευές κι οι κωδικοί όπως περιγράφονται στο άρθρο 6, όμως, αντικειμενικά δεν θέτουν κίνδυνο. Αποτέλεσμα είναι να καταλήγει ουσιαστικά σε τιμώρηση του φρονήματος, κάτι που αντίκειται στο Σύνταγμα (άρ.7 Σ).[13]

Τέλος, ενώ σκοπός του άρθρου 6 της Σύμβασης είναι η προστασία των συστημάτων, καταλήγει σε αντίθετα αποτελέσματα, διότι φαίνεται να αγνοεί το γεγονός ότι πολλές από τις συσκευές και τους κωδικούς που αναφέρονται χρησιμοποιούνται για τη θωράκιση των συστημάτων έναντι σε επιθέσεις. Πρόκειται για τα λεγόμενα "hacking tools" που αποτελούν απαραίτητα εργαλεία για την προστασία των Η/Υ και τα οποία, αν το άρθρο 6 μεταφερθεί έτσι όπως αναγράφεται στη Σύμβαση, δεν θα μπορούν πλέον να χρησιμοποιηθούν.[14]

Ενόψει των ανωτέρω, ο Έλληνας νομοθέτης θα έπρεπε ίσως να διατηρήσει την επιφύλαξη του άρθρου 6 ως προς τις συσκευές και τα προγράμματα και να μεταφέρει τη διάταξη μόνον ως προς το σκέλος των κωδικών (που είναι υποχρεωτικό για τις χώρες που υπέγραψαν) προσέχοντας όμως στη διατύπωση της νέας διάταξης ώστε οι κωδικοί να είναι καθαυτοί επικίνδυνοι για τα έννομα αγαθά για να μην φτάσουμε σε ανεπίτρεπτη τιμώρηση του φρονήματος.

ΙΙ. Εγκλήματα που σχετίζονται με Η/Υ

Άρθρο 7: Πλαστογραφία με Ηλεκτρονικό Υπολογιστή

Η διάταξη αυτή της Σύμβασης καλεί τις χώρες να ποινικοποιήσουν την πλαστοποίηση δεδομένων, που έγινε με σκοπό να χρησιμοποιηθούν αυτά ως αυθεντικά, ακόμη κι αν τα δεδομένα δεν είναι άμεσα προσβάσιμα ή αναγνώσιμα.

Ως προς αυτό το άρθρο θα πρέπει να αναφερθεί ότι υπό το ισχύον δίκαιο η πλαστοποίηση δεδομένων δεν τιμωρείται, εκτός αν τα δεδομένα συγκεντρώνουν τα στοιχεία του «εγγράφου» του άρ. 13 περ.γ ΠΚ. Τότε πληρού-

ται η αντικειμενική υπόσταση του άρ. 216 ΠΚ, δηλαδή της κοινής πλαστογραφίας.[15]

Έτσι, όμως, πολλές περιπτώσεις πλαστοποίησης δεδομένων δεν καλύπτονται. Για παράδειγμα, στην περίπτωση του «ψαρέματος» (phishing)[16] ο δράστης δημιουργεί ένα πλαστό ηλεκτρονικό μήνυμα που παραπλανεί το θύμα για να επισκεφτεί μια επίσης πλαστή ιστοσελίδα όπου το θύμα δίνει προσωπικά του δεδομένα, όπως κωδικούς πρόσβασης και λεπτομέρειες πιστωτικών καρτών, που αργότερα θα χρησιμοποιηθούν από το δράστη για παράνομους σκοπούς. Εδώ, ενώ η απάτη θα μπορούσε να τιμωρηθεί με το άρ. 386 ΠΚ,[17] η πλαστογραφία τόσο του ηλεκτρονικού μηνύματος όσο και της ιστοσελίδας μένει ατιμώρητη εάν τα δεδομένα δεν αποτελούν έγγραφο.[18] Με τη συμμόρφωση στο άρθρο 7 της Σύμβασης τα κενά αυτά θα καλυφθούν.

Άρθρο 8: Απάτη με Ηλεκτρονικό Υπολογιστή

Η απάτη με Η/Υ τυποποιείται ήδη υπό το ισχύον ελληνικό δίκαιο στο άρθρο 386Α ΠΚ. Το ερώτημα, λοιπόν, που τίθεται είναι κατά πόσον εν όψει της υποχρέωσης συμμόρφωσης της Ελλάδας προς το άρ. 8 της Σύμβασης, το άρ. 386Α ΠΚ ανταποκρίνεται στην υποχρέωση αυτή, ή θα πρέπει να καταργηθεί και να θεσπιστεί μία νέα διάταξη, ή θα πρέπει απλώς να τροποποιηθεί.

Προτού επιχειρηθεί να δοθεί μια απάντηση σ' αυτό το ερώτημα, θα ήταν χρήσιμο να γίνει αναφορά στο πρόβλημα που ανέκυψε σχετικά με το άρ. 386Α ΠΚ και έχει διχάσει θεωρία και νομολογία. Πρόκειται για την περίπτωση της κλοπής της κάρτας ΑΤΜ και της ανάληψης χρημάτων χωρίς δικαίωμα με την εισαγωγή ορθών δεδομένων στο σύστημα. Σ' αυτήν την περίπτωση διεκδικούν εφαρμογή οι διατάξεις της κλοπής (372 ΠΚ), της υπεξαίρεσης (375 ΠΚ) και της απάτης με Η/Υ (386Α ΠΚ).[19] Σημείο διαφωνίας αποτελεί το κατά πόσον η χωρίς δικαίωμα εισαγωγή ορθών στοιχείων στο σύστημα μπορεί να θεωρηθεί ως επηρεασμός στοιχείων υπολογιστή «με οποιονδήποτε άλλον τρόπο».

Σύμφωνα με το άρθρο 8 της Σύμβασης η περίπτωση αυτή υπάγεται στη νομοτυπική μορφή της απάτης με Η/Υ. Για να είναι λοιπόν συμβατό με τη Σύμβαση το άρ. 386Α ΠΚ, θα αρκούσε να προστεθεί σ' αυτό η φράση «με τη χρησιμοποίηση ορθών δεδομένων». Συνεπώς, η τροποποίηση του άρ. 386Α ΠΚ θα επίλυε τη διαφωνία που ταλανίζει θε-

Στην περίπτωση του «ψαρέματος» ο δράστης δημιουργεί ένα πλαστό ηλεκτρονικό μήνυμα που παραπλανεί το θύμα για να επισκεφτεί μια επίσης πλαστή ιστοσελίδα όπου το θύμα δίνει προσωπικά του δεδομένα

ωρία και νομολογία και θα κάλυπτε την υποχρέωση συμμόρφωσης της Ελλάδας στο άρ. 8 της Σύμβασης.[20]

Η αλματώδης πρόοδος που σημειώνει η τεχνολογία κατά τις τελευταίες δεκαετίες είναι μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει το Ποινικό Δίκαιο σήμερα

Συμπέρασμα

Εν κατακλείδι, η αλματώδης πρόοδος που σημειώνει η τεχνολογία κατά τις τελευταίες δεκαετίες είναι μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει το Δίκαιο γενικότερα και το Ποινικό Δίκαιο ειδικότερα. Παρόλο που τα προβλήματα που αναφύονται αναζητούν επιτακτικά λύσεις, ο νομικός κόσμος πρέπει να προχωρήσει με σταθερά και προσεχτικά βήματα, χωρίς βεβιασμένες κινήσεις, ώστε να διασφαλίσει την ορθή απονομή της δικαιοσύνης και την αποτελεσματική προστασία των πολιτών με παράλληλο σεβασμό στα δικαιώματα του ανθρώπου.

Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα με τη μεταφορά της στην ελληνική έννομη τάξη, θα καλύψει πολλά κενά της κείμενης νομοθεσίας. Ο Έλληνας νομοθέτης, όμως, οφείλει να την επεξεργαστεί με κριτική ματιά και να την προσαρμόσει στις ανάγκες και τα δεδομένα της ελληνικής κοινωνίας και του ελληνικού νομικού πολιτισμού, προσέχοντας ιδίως τη διατύπωση των νέων διατάξεων, ώστε να ανταποκρίνονται στο σκοπό τους και να είναι σύμφωνες με το Σύνταγμα.

Σημειώσεις Τέλους

1. Για την ορολογία που χρησιμοποιείται βλ.: Καϊάφα-Γκμπάντι Μ., Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, Αρμεν 2007, σ. 1061 επ. και Κιούπη Δ., Ηλεκτρονικά Οικονομικά Εγκλήματα, σε Κουράκη Ν., «Τα Οικονομικά Εγκλήματα ΙΙ Ειδικό Μέρος», Εκδ. Αντ. Ν. Σάκκουλα , σ. 405 επ.

2. βλ. και Αγγέλη Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), ΠοινΔικ 2001, σ. 1218 επ.

3. Για τις χώρες που υπέγραψαν τη Σύμβαση, βλ. και http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, τελευταία επίσκεψη στις 7/3/2008.

4. Θα μπορούσε να υποστηριχθεί ότι πέρα από το απόρρητο η διάταξη προστατεύει και το έννομο αγαθό της περιουσίας, ειδικά όταν ο νόμιμος κάτοχος του συστήματος είναι κάποιο νομικό πρόσωπο. Κι αυτό διότι η πρόσβαση σε σύστημα κάποιας εταιρίας θα της κοστίσει χρόνο και χρήμα, επειδή θα πρέπει να γίνει έλεγχος για να εντοπιστεί το σημείο πρόσβασης, να διορθωθεί η ατέλεια του προστατευτικού τείχους, πιθανόν να αλλάξει το πρόγραμμα προστασίας, ενώ παράλληλα θα γίνεται έλεγχος των αρχείων και φακέλων για να διαπιστωθεί αν λείπει ή έχει αλλοιωθεί κάτι, μια σειρά ενεργειών που απαιτεί αυξημένες δαπά-

νες. Βλ. και Carr I. and Williams S. K., Draft Cybercrime Convention, Criminalization and the Council of Europe (Draft) Convention on Cybercrime, Computer Law & Security Report 2002, 84 επ.

5. Διατυπώνονται πάντως επιφυλάξεις ως προς το αν η μικρή ποινή του άρ. 370Γ§2 μπορεί να επιτύχει τον αντεγκληματικό στόχο της διάταξης, βλ. Κιούπη Δ., Ποινικό Δίκαιο και Internet, Εκδ. Αντ. Ν. Σάκκουλα 1999, σ. 127 επ.

6. Εφαρμογή θα μπορούσε να διεκδικήσει και το άρθρο 370 ΠΚ, τηρουμένων των προϋποθέσεων που θέτει και εφόσον τα δεδομένα πληρούν τα στοιχεία του εγγράφου του άρ. 13γ ΠΚ, καθώς και το άρθρο 10 του ν. 3115/2003 σχετικά με την προστασία του απορρήτου των επικοινωνιών, μια επικουρική διάταξη που τιμωρεί την με οποιοδήποτε τρόπο παραβίαση του απορρήτου των επικοινωνιών.

7. Βλ. Carr I. and Williams S. K., ό.π., σ. 84 επ.

8. Βλ. Μανωλεδάκη Ι.-Μπιτζιλέκη Ν., Εγκλήματα κατά της Ιδιοκτησίας, Εκδ. Σάκκουλα 2004, 12η έκδ., σ. 269, Κιούπη Δ., ό.π., σ. 140 επ. και Μυλωνόπουλου Χ., Ποινικό Δίκαιο-Ειδικό Μέρος, Β΄Έκδ., εκδ Π. Ν. Σάκκουλα, Αθήνα 2006, σ.11επ. και σ. 343, ο οποίος όμως δέχεται περαιτέρω ότι η μόλυνση με ιούς συνεπάγεται μείωση της κατά προορισμό χρησιμότητας του υλικού φορέα κι άρα στοιχειοθετείται φθορά ξένης ιδιοκτησίας, ό.π. σ. 348.

9. Για τις τρεις λειτουργίες του εγγράφου βλ. Μυλωνόπουλου Χ., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Εκδ. Αντ. Ν. Σάκκουλα, 1991, σ. 42 επ. και Τζαννέτη Α., Το Πλαστό Έγγραφο, Εκδ. Π. Ν. Σάκκουλα, σ.9 επ.

10. Το spamming, δηλαδή η αποστολή ηλεκτρονικών μηνυμάτων διαφημιστικού περιεχομένου (ανεπιθύμητη ή απρόκλητη αλληλογραφία), δεν εμπίπτει σ' αυτή τη διάταξη, εκτός από την περίπτωση που θα αποδειχθεί ότι υπήρχε πρόθεση να παρεμποδιστεί η λειτουργία του συστήματος. Βλ. και Carr I. and Williams S. K., ό.π. , σ. 85 επ.

11. Άλλως καλούμενη και διάταξη αφηρημένης διακινδύνευσης.

12. Για την προβληματική των εγκλημάτων διακινδύνευσης βλ. Καϊάφα-Γκμπάντι Μ., Κοινώς Επικίνδυνα Εγκλήματα, Γ΄ έκδ., Εκδ. Σάκκουλα 2005, σ. 40 επ.

13. Βλ. Καϊάφα-Γκμπάντι Μ., Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, Αρμεν 2007, σ. 1086 επ.

14. Βλ. Carr I. and Williams S. K., ό.π. , σ. 85. Έχει προταθεί μάλιστα ως λύση στο πρόβλημα που αναφύεται, η σύνταξη μητρώου και η χορήγηση αδειών για τη χρήση "hacking tools", κατ' αναλογία μ' ό,τι γίνεται για τη χρήση όπλων, εκφράζονται ωστόσο βάσιμες αμφιβολίες ως προς το κατά πόσο κάτι τέτοιο θα ήταν αποτελεσματικό και οικονομικά συμφέρον για το Κράτος. Άλλωστε, θα μπορούσε ίσως να προστεθεί ότι τα "hacking tools" δεν παρουσιάζουν την ίδια επικινδυνότητα με τα όπλα, άρα δεν χρειάζεται να αντιμετωπίζονται με τα ίδια μέτρα.

15. Βλ. και παραπάνω, σημ. 8.

16. Αναλυτικότερα για το «phishing» βλ. Βλαχόπουλου Κ., Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη 2007, σ. 58 επ.

17. Κοινή απάτη κι όχι απάτη με Η/Υ (386Α ΠΚ) διότι υπάρχει πλάνη προσώπου κι όχι επηρεασμός στοιχείων μηχανής. Το στοιχείο που θα πρέπει να σημειωθεί είναι ότι στο phishing η περιουσιακή βλάβη

δεν είναι άμεση, διότι το θύμα δίνει κάποια προσωπικά δεδομένα κι όχι χρήματα, άρα δεν είναι βέβαιο ότι θα πληρούται σε κάθε περίπτωση η αντικειμενική υπόσταση του 386 ΠΚ.
18. Αν πληρούν τους όρους του 13γ ΠΚ στοιχειοθετείται πλαστογραφία του 216 ΠΚ.
19. Για τις διάφορες απόψεις που έχουν υποστηριχθεί βλ., μεταξύ άλλων, Μανωλαδάκη Ι.-Μπιτζιλέκη Ν., ό.π, σ. 40 επ., υπέρ της εφαρμογής της υπεξαίρεσης, Μυλωνόπουλου Χ., ό.π., σ. 65 επ. και Νούσκαλη Γ., Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 189 επ., υπέρ της εφαρμογής της απάτης με Η/Υ, και Παπαδαμάκη Α., Τα περιουσιακά εγκλήματα, Εκδ. Σάκκουλα 2000, σ. 190 επ., υπέρ της εφαρμογής της κλοπής.
20. Υποστηρίζεται κι η άποψη ότι το άρθρο 386Α ΠΚ καλύπτει ήδη τις υποχρεώσεις της χώρας προς τη Σύμβαση, βλ. Νούσκαλη Γ., ό.π., διότι περιλαμβάνει την χρησιμοποίηση ορθών δεδομένων, αυτό όμως δεν γίνεται δεκτό από το σύνολο της νομολογίας και της θεωρίας, επομένως η διατήρηση του άρθρου όπως είναι σήμερα διατυπωμένο δεν λύνει το πρόβλημα της διαφωνίας και δεν εξυπηρετεί την ασφάλεια δικαίου.

Βιβλιογραφία

- *Βλαχόπουλου Κ., Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη 2007.*
- *Καϊάφα-Γκμπάντι Μ., Κοινώς Επικίνδυνα Εγκλήματα, Γ΄ έκδ., Εκδ. Σάκκουλα 2005.*
- *Κιούπη Δ., Ποινικό Δίκαιο και Internet, Εκδ. Αντ. Ν. Σάκκουλα 1999.*
- *Μανωλεδάκη Ι.-Μπιτζιλέκη Ν., Εγκλήματα κατά της Ιδιοκτησίας, Εκδ. Σάκκουλα 2004, 12η έκδ.*
- *Μυλωνόπουλου Χ., Ποινικό Δίκαιο-Ειδικό Μέρος, Β΄Έκδ., εκδ Π. Ν. Σάκκουλα, Αθήνα 2006.*
- *Μυλωνόπουλου Χ., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Εκδ. Αντ. Ν. Σάκκουλα, 1991.*
- *Παπαδαμάκη Α., Τα περιουσιακά εγκλήματα, Εκδ. Σάκκουλα 2000.*
- *Τζαννέτη Α., Το Πλαστό Έγγραφο, Εκδ. Π. Ν. Σάκκουλα.*

Αρθρογραφία

- *Carr I. and Williams S. K., Draft Cybercrime Convention, Criminalization and the Council of Europe (Draft) Convention on Cybercrime, Computer Law & Security Report 2002, σ. 83 επ.*
- *Αγγέλη Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cybercrime), ΠοινΔικ 2001, σ. 1218 επ.*
- *Καϊάφα-Γκμπάντι Μ., Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής, Αρμεν 2007, σ. 1058 επ.*
- *Κιούπη Δ., Ηλεκτρονικά Οικονομικά Εγκλήματα, σε Κουράκη Ν., «Τα Οικονομικά Εγκλήματα ΙΙ Ειδικό Μέρος», Εκδ. Αντ. Ν. Σάκκουλα*
- *Νούσκαλη Γ., Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 178 επ.*