# Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος

**Ευαγγελία Βαγενά**
*Δικηγόρος, ΔΝ, DEA et Informatique*

*Η χώρα μας πρόσφατα εκσυγχρόνισε το νομοθετικό πλαίσιο καταπολέμησης του κυβερνοεγκλήματος μέσω της κύρωσης της Σύμβασης για το Κυβερνοέγκλημα και της ενσωμάτωσης των προβλέψεων της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου μέσω τροποποιήσεων του Ποινικού Κώδικα. Η έστω και καθυστερημένη υιοθέτηση αυτών των ρυθμίσεων αναμένεται να διευκολύνει την δίωξη του ηλεκτρονικού εγκλήματος αλλά ήδη έχουν δρομολογηθεί μέσω του δικαίου της ΕΕ εξελίξεις σε άλλους τομείς δικαίου, όπως η προστασία των προσωπικών δεομένων ή η λήψη μέτρων για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, οι οποίες θα υποχρεώσουν σε περαιτέρω αναμόρφωση των ρυθμίσεων που αφορούν άμεσα ή έμμεσα το κυβερνοέγκλημα και την κυνβερνοασφάλεια.*

Πρόσφατα, στις 3.8.2016,τέθηκε σε ισχύ ο νέος νόμος για το κυβερνοέγκλημα στην Ελλάδα Ν 4416/2016 (ΦΕΚ 142/Α΄/3.8.2016) με τίτλο «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».

Ο νόμος, που υιοθετήθηκε μετά από μια μακρόχρονη και περιπετειώδη νομοπαρασκευαστική διαδικασία, συμβάλει στον εκσυγχρονισμό του θεσμικού πλαισίου καταπολέμησης του ηλεκτρονικού εγκλήματος[1] στη χώρα μας επιφέροντας απόλυτα αναγκαίες τροποποιήσεις. Ήδη ωστόσο νέες εξελίξεις σε ευρωπαϊκό επίπεδο θα καταστήσουν αναγκαία την ενσωμάτωση νέων νομοθετικών κειμένων και τη λήψη θεσμικών πρωτοβουλιών για την υλοποίηση ενός θεσμικού πλαισίου που θα προβλέπει εκτός άλλων την ανάπτυξη υπηρεσιακών δομών και μεθόδων ανταπόκρισης στα συμβάντα προσβολής της ασφάλειας των πληροφοριακών συστημάτων από εγκληματικές ενέργειες. Η παρούσα μελέτη αναλύει τόσο τις νέες εθνικές διατάξεις, όσο και τις πρόσφατα υιοθετημένες σε επίπεδο ΕΕ σκιαγραφώντας ταυτόχρονα τους εμπλεκόμενους φορείς στην καταπολέμηση του ηλεκτρονικού εγκλήματος στη χώρα μας. Στόχος είναι η χαρτογράφηση και η κριτική ανάλυση ενός πολύπλοκου και κατακερματισμένου θεσμικού πλαισίου που σύντομα θα πρέπει ανασκευαστεί προκειμένου η χώρα μας να μην είναι ευάλωτη σε δραστηριότητες ηλεκτρονικής εγκληματικότητας με άμεσες συνέπειες τόσο στη λειτουργία του κράτους όσο και στην καθημερινή ζωή των πολιτών.

## I. Μια περιπετειώδης νομοπαρασκευαστική διαδικασία

Η κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο (Σύμβαση της Βουδα-

1. Μια πρώτη εννοιολογική προσέγγιση είχε αποπειραθεί να κάνει ο *Αγγελής Ι.*, τότε Εισαγγελέας Πρωτοδικών, στη μελέτη του «Διαδίκτυο και Ποινικό Δίκαιο-Έγκλημα στον Κυβερνοχώρο», ΠοινΧρ 2000, 675. Γενικά για το ηλεκτρονικό έγκλημα. βλ. *Βλαχόπουλου Κ.*, Ηλεκτρονικό Έγκλημα: Μορφές, Πρόληψη, Αντιμετώπιση, Νομική Βιβλιοθήκη, 2007, *Αργυρόπουλου Α.*, Ηλεκτρονική Εγκληματικότητα, Αντ. Ν. Σάκκουλας, 2001, *Ζαννή Α.*, Το Διαδικτυακό Έγκλημα, Αντ. Ν. Σάκκουλας, 2005, *Ιγγλεζάκη Ι.*, Δίκαιο της Πληροφορικής, Σάκκουλας, 2008, *Αγγελή Ι.*, «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 2001, 1293, *Κιούπη Δ.*, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, Το δίκαιο στην ψηφιακή εποχή, εκδόσεις Νομική Βιβλιοθήκη, 2012, σελ. 150, *Σφακιανάκη Ε.*, Ο Κώδικας του Διαδικτύου, εκδόσεις All about internet, 2016, σελ. 17. Όπως όμως επισημαίνει ο *Jougleux P.*, Ευρωπαϊκό Δίκαιο Διαδικτύου, εκδόσεις Σάκκουλα 2016, σελ. 107-108, η διάκριση σε κυβερνοέγκλημα με τη στενή έννοια και σε κυβερνοέγκλημα με την ευρεία έννοια πρέπει να σχετικοποιηθεί καθώς η αναγκαία προσαρμογή των νομικών καθεστώτων δύναται να οδηγήσει στη θέσπιση ειδικών διατάξεων για το διαδίκτυο, όπως στην περίπτωση της παιδικής πορνογραφίας.

πέστης)[2] γίνεται στη χώρα μας με καθυστέρηση 15 ετών[3], ενώ ως προθεσμία ενσωμάτωσης της Οδηγίας 2013/40/ΕΕ (γνωστής ως «οδηγίας για το κυβερνοέγκλημα»)[4] είχε τεθεί η 4η Σεπτεμβρίου 2016.

Για την κύρωση της Σύμβασης της Βουδαπέστης από τη χώρα μας καταρτίστηκε αρχικώς επιτροπή από το Υπουργείο Δικαιοσύνης στις 19.7.2004. Η επιτροπή παρέδωσε το έργο της τον Σεπτέμβριο του 2006. Αποφασίστηκε, όμως, τότε *ανασύσταση της επιτροπής*, ώστε να της ανατεθεί και η απόφαση πλαίσιο υπ' αριθμόν 2005/222 του Συμβουλίου, για τις επιθέσεις κατά των συστημάτων πληροφορικής. Στις 22.10.2013 με την υπ' αρ. 84280 απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων[5] συστάθηκε εκ νέου νομοπαρασκευαστική επιτροπή με αντικείμενο ***την επικαιροποίηση σχεδίου νόμου*** σύμφωνα με την οποία έπρεπε το έργο της επιτροπής να έχει περατωθεί μέχρι τις 30.6.2016. Παρόλα αυτά, συστάθηκε εκ νέου με την υπ' αρ. 94396/2015 ΥΑ (ΦΕΚ Β΄ 2892/30.12.2015) νέα ειδική νομοπαρασκευαστική επιτροπή με αντικείμενο την ***τελική επεξεργασία*** σχεδίου νόμου για την προσαρμογή στο εσωτερικό δίκαιο των διατάξεων της Σύμβασης του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο, καθώς και του Πρόσθετου Πρωτοκόλλου αυτής σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως, όπως επίσης και την τελική επεξεργασία διατάξεων για την ενσωμάτωση στην εθνική έννομη τάξη της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών. Τελικά, στις 18.3.2016 τέθηκε σε δημόσια διαβούλευση το σχετικό σχέδιο νόμου[6].

## II. Η ανεπάρκεια του προηγούμενου θεσμικού πλαισίου & η έκταση της κυβερνοεγκληματικότητας

Στο εθνικό δίκαιο μέχρι την ψήφιση του επίμαχου νόμου δεν υπήρχαν εξειδικευμένες διατάξεις και τα κυβερνοεγκλήματα τιμωρούνταν κυρίως βάσει των διατάξεων του Ν 1805/1988 με τον χαρακτηριστικό τίτλο «εκσυγχρονισμός του θεσμού του ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων», ο οποίος είχε εισάγει τα άρθρα 370Β, 370Γ, 386Α[7] στον ΠΚ[8] προκειμένου να καλυφθούν εγκλήματα διαπραττόμενα μέσω ηλεκτρονικών υπολογιστών και διεύρυνε την έννοια των εγγράφων ώστε να περιλαμβάνονται σε αυτά και τα ηλεκτρονικά έγγραφα[9] διά της προσθήκης της περίπτωσης γ΄ στο άρθρο 13 ΠΚ. Η έλλειψη εξειδικευμένων διατάξεων είχε επισημανθεί πολλάκις τόσο από νομικούς όσο και από αστυνομικούς εμπλεκόμενους στην εξιχνίαση και δίωξη ηλεκτρονικών εγκλημάτων στην χώρα μας.

Θα μπορούσε ενδεικτικά να αναφερθεί ότι το προηγουμένως ισχύον νομοθετικό πλαίσιο δεν κάλυπτε περιπτώσεις όπως η παρακώλυση λειτουργίας συστήματος υπολογιστή και δεν υπήρχε ξεχωριστή ρύθμιση για την αλλοίωση ή φθορά των δεδομένων[10]. Η τελευταία, όπως γινόταν

2. Βλ. *Αγγελή Ι.*, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 2001, 1218, *Μαρκοπούλου Π.*, Η Σύμβαση για το Κυβερνοέγκλημα, Intellectum, Τεύχος 04, Μάιος 2008, σελ. 43-52.
3. Βλ. ακριβείς ημερομηνίες κύρωσης από τις υπόλοιπες χώρες στη σελίδα http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (διαθέσιμη στις 10.10.2016).
4. Βλ. *Τσόλια Γ.*, Η πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου», Αντιμέτωποι με τις σύγχρονες τεχνολογικές εξελίξεις, Προσωπικά δεδομένα - Ηλεκτρονικό έγκλημα - Ηλεκτρονικό εμπόριο (2ο Πανελλήνιο Συνέδριο), εκδόσεις Νομική Βιβλιοθήκη 2011, σελ. 3, *Νουσκαλη Γ.*, Οικονομική εγκληματικότητα στο διαδίκτυο - Οι νέες προκλήσεις για τον Έλληνα νομοθέτη, Δίκαιο Πληροφορικής, LegalTech&Data Protection (4ο Πανελλήνιο Συνέδριο), εκδόσεις Νομική Βιβλιοθήκη, 2013, σελ. 81.
5. ΦΕΚ 2767/Β΄/30.10.2013.
6. Σημειωτέον ότι μέχρι τις 4.9.2017 θα πρέπει να έχει ολοκληρωθεί η έκθεση αξιολόγησης της Οδηγίας 2013/40 ΕΕ. Στο πλαίσιο της αξιολόγησης μπορεί να κριθούν αναγκαίες περαιτέρω τροποποιήσεις του θεσμικού πλαισίου της οδηγίας.
7. Βλ. ειδικά για το θέμα αυτό ιδίως *Νούσκαλη Γ.*, Απάτη με Ηλεκτρονικό Υπολογιστή (Η/Υ): Το Παρελθόν και το Μέλλον του Άρθρου 386Κ ΠΚ, Ιδίως Υπό το Πρίσμα των Εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκής Ένωσης, ΠοινΔικ 2003, 178-90, *Σάμιου Θ.*, Κάρτες Αυτόματης Συναλλαγής και Ποινικό Δίκαιο: Η De Lege Lata Αξιολόγηση της Αθέμιτης Κτήσης και Χρήσης Καρτών Αυτόματης Συναλλαγής για Ανάληψη Μετρητών από ΑΤΜ, Π. Ν. Σάκκουλας, 2010.
8. Βλ. ενημέρωση των πολιτικών συντακτών και ανταποκριτών ξένου τύπου από τον τότε Υπουργό Επικρατείας στις 27.2.2008, http://www.hri.org/news/greek/kyber/2008/08-02-27.kyber.html (διαθέσιμη στις 10.10.2016).
9. Βλ. ανάλυση τους εκτός άλλων σε *Βασιλάκη Ε.*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 74 επ., *Καϊάφα- Γκπαντι Μ.*, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμ 2007, 1064 επ., *Κιούπη Δ.*, Ποινικό Δίκαιο και Ίντερνετ, 1999, σελ. 131 επ., *του ιδίου*, Αλλοίωση Ηλεκτρονικών Δεδομένων και Αθέμιτη Πρόσβαση σε ηλεκτρονικά Δεδομένα, Υπερ 2000, 960 επ., *Μυλωνόπουλου Χ.*, Ηλεκτρονικοί Υπολογιστές και ποινικό δίκαιο, 1991, σελ. 39 επ., *Κριθάρα Θ.*, Ποινικό Δίκαιο και Διαδίκτυο, Νομική Βιβλιοθήκη, 2009, *Λάζου Γ.*, Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, 2001, *Τσουραμάνη Χ.Ε*, Ψηφιακή Εγκληματικότητα: Η (Αν)ασφαλής Όψη του Διαδικτύου, εκδόσεις Βασ. Ν. Κατσαρού, 2005, *Spinellis D.*, ed. Computer Crimes, Cyber-terrorism, Child Pornography and Financial Crimes: Reports Presented to the Preparatory Colloquy for the Round Table II of the 17th International Congress of Penal Law (Beijing, 2004), Athens, Ant. N. Sakkoulas, 2004. Πρόσφατα επίσης η ελληνική νομοθεσία με την ψήφιση του Ν 4267/2014 εναρμονίσθηκε με την Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της Απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου.
10. Βλ. ιδίως *Κιούπη Δ.*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα – Κενά και αδυναμίες της ποινικής νομοθεσίας, Υπερ 2000, 959 και *ιδίου*, Οι διατάξεις του

δεκτό από μέρος της θεωρίας, μπορούσε σε ορισμένες περιπτώσεις να καλυφθεί από το πραγματικό της διάταξης για τη φθορά της ξένης ιδιοκτησίας. Συγκεκριμένα, βάσει του νόμου, στην προϊσχύουσα μορφή του, η φθορά, αλλοίωση, διαγραφή ή άλλη επέμβαση σε δεδομένα δεν μπορούσε να τιμωρηθεί, γιατί τα δεδομένα δεν αποτελούν «πράγμα» με την έννοια του άρθρου 381 ΠΚ, δηλαδή της φθοράς ξένης ιδιοκτησίας. Τιμωρητέα ήταν μόνο η φθορά στον υλικό φορέα των δεδομένων (π.χ στον η/υ ή στον server). Ενόψει του μέχρι πρόσφατα υφιστάμενου δικαίου η αλλοίωση αυτών καθαυτών των δεδομένων μπορούσε να τιμωρηθεί μόνο αν επρόκειτο: α) για προσωπικά δεδομένα, μέσω του νόμου προστασίας προσωπικών δεδομένων και β) για «έγγραφο» με την έννοια του άρθρου 13 περ. γ΄ ΠΚ, μέσω της υπεξαγωγής εγγράφου (222 ΠΚ). Ομοίως, υπήρχε πρόβλημα υπαγωγής της παρακώλυσης λειτουργίας ενός πληροφοριακού συστήματος στις διατάξεις του ποινικού δικαίου πριν την τροποποίησή τους, ιδίως λόγω της ιδιαιτερότητας ότι δεν προκαλούταν απαραίτητα «μόνιμη» βλάβη σε ένα πληροφοριακό σύστημα και άρα ούτε «φθορά».

Όλα αυτά σε μια εποχή όπου οι επιθέσεις άρνησης εξυπηρέτησης / Denial of Services (DOS) είχαν ήδη εμφανισθεί από το 2000 και είχαν φτάσει στο σημείο να χρησιμοποιούνται για τη διενέργεια πράξεων κυβερνοπολέμου το 2008. Οι επιθέσεις αυτές είναι σχεδιασμένες ώστε να οδηγούν σε κατάρρευση το δίκτυο μιας επιχείρησης ή ενός διαδικτυακού τόπου ηλεκτρονικού εμπορίου με το να το βομβαρδίζουν με έναν τεράστιο όγκο δεδομένων κίνησης, σαν να καλούσαν επανειλημμένα χιλιάδες άνθρωποι τον ίδιο τηλεφωνικό αριθμό με αποτέλεσμα να το κρατούν απασχολημένο[11]. Η πρώτη παρόμοια επίθεση καταγράφηκε στις 7.2.2000 όταν ένας 15χρονος Καναδός χάκερ «ενορχήστρωσε» σειρά από αντίστοιχες επιθέσεις εναντίον αρκετών ιστοσελίδων ηλεκτρονικού εμπορίου, όπως το Amazon.com και το eBay.com[12]. Το 2005 καταδικάσθηκε για πρώτη φορά στις ΗΠΑ[13]ιδιώτης για παράνομες πράξεις μέσω χρήσης botnets[14]. Το 2008 επιθέσεις αυτού του τύπου χρησιμοποιήθηκαν στο πλαίσιο κυβερνοεπιθέσεων[15] που εξαπόλυσε η Ρωσία προς τη Γεωργία με στόχο και επιτευχθέν αποτέλεσμα να μην μπορέσει η Γεωργία να μεταφέρει τη δική της άποψη για τον πόλεμο που ήδη λάμβανε χώρα στον υπόλοιπο κόσμο[16]. Είχαν προηγηθεί αντίστοιχα περιστατικά στην Εσθονία το 2007

Ποινικού Κώδικα για το διαδικτυακό έγκλημα, Το δίκαιο στην ψηφιακή εποχή, εκδόσεις Νομική Βιβλιοθήκη, 2012, σελ. 150.

11. Ένα αποκεντρωμένο σύστημα «επίθεσης άρνησης εξυπηρέτησης» χρησιμοποιεί τις ίδιες μεθόδους με ένα συνηθισμένο σύστημα «επίθεσης άρνησης εξυπηρέτησης» αλλά εξαπολύεται από πολλαπλές πηγές. Κατά κανόνα, ο διενεργών την επίθεση θα χρησιμοποιήσει εργαλεία κατεβασμένα από το διαδίκτυο για να διεισδύσει στους ανυποψίαστους διακομιστές φιλοξενίας. Αφού αποκτήσει την απαραίτητη πρόσβαση στον διακομιστή φιλοξενίας, ο επιτιθέμενος θα εγκαταστήσει ένα λογισμικό που θα παρέχει υπηρεσίες ή «δαίμονες» στο σύστημα φιλοξενίας (εφεξής καλούμενοι πράκτορες). Αυτοί οι πράκτορες θα αναμένουν εωσότου λάβουν εντολή από τον επιτιθέμενό τους. Ο επιτιθέμενος θα τους διατάξει να επιτεθούν ενάντια σε συγκεκριμένο στόχο. Με την έκταση των καλωδιακών modems, των συνδέσεων DSL, και τη διαθεσιμότητα ισχυρών εργαλείων hacking tools- υπάρχουν πολλοί εύκολα προσβάσιμοι διακομιστές φιλοξενίας. Ο κίνδυνος με τις αποκεντρωμένες επιθέσεις DOS είναι ότι ο επιτιθέμενος μπορεί να εξαπολύσει χιλιάδες επιθέσεις DOS ενάντια στον ίδιο στόχο ταυτόχρονα. Ενώ μια μεμονωμένη επίθεση DOS μπορεί να μην κατακλύσει την ιστοσελίδα με υψηλή κίνηση δεδομένων πρόσβασης (bandwidth Internet access), οι χιλιάδες ταυτόχρονες επιθέσεις προερχόμενες από κάθε γωνία του κόσμου θα το κάνουν. Αυτές οι επιθέσεις θα καταστήσουν αδύνατη την πρόσβαση στο διαδίκτυο. Αυτό θα δυσκολέψει τις περισσότερες επιχειρήσεις και θα συνεπάγεται απώλεια παραγωγικότητάς τους. Για τις βασιζόμενες στο διαδίκτυο επιχειρήσεις και τις επιχειρήσεις ηλεκτρονικού εμπορίου αυτό θα συνεπάγεται σημαντική απώλεια χρημάτων από τις πωλήσεις και θα έχει συνέπειες για την εμπιστοσύνη των πελατών. Σε γενικές γραμμές ο σκοπός αυτών των επιθέσεων δεν είναι να διεισδύσουν στο δίκτυο σου, αλλά να σε αποκόψουν από τον έξω κόσμο. Μερικές φορές μπορεί να χρησιμοποιηθούν για σε μικρότερη κλίμακα για να αποκρύψουν προσπάθειες διείσδυσης από τον επιτιθέμενο. Σε αυτές τις περιπτώσεις ο επιτιθέμενος θα εξαπολύσει αρκετές επιθέσεις για να κρατάει απασχολημένη την είσοδο στο σύστημα σου και τα συστήματα ασφαλείας σου. Αυτό δεν είναι πολύ σύνηθες καθώς ο επιτιθέμενος θα πρέπει να χειρίζεται τόσο τις επιθέσεις DOS όσο και τις (ταυτόχρονες) νόμιμες συνδέσεις στο bandwidth. Αυτές οι επιθέσεις επίσης στέλνουν «ειδικά σχεδιασμένα» πακέτα που σαμποτάρουν το εξ αποστάσεως λογισμικό και τις υπηρεσίες που «τρέχουν» σε ένα μηχάνημα. Αυτό το καταφέρνουν με την αποστολή ενός μεγάλου όγκου άχρηστων πακέτων όπως τα «SYN» ή τα «PING». Τα περισσότερα Firewalls και συστήματα ανίχνευσης διείσδυσης (Intrusion Detection Systems) αναγνωρίζουν και αναφέρουν αυτές τις επιθέσεις, βλ. αντίστοιχα για τους ορισμούς και *Σφακιανάκη Ε./Μακρυπούλια Ι.*, Τα κλειδιά του διαδικτύου, εκδόσεις All about internet, 2016, σελ. 26.

12. Βλ. https://www.britannica.com/topic/denial-of-service-attack (διαθέσιμη στις 13.09.2016).

13. Βλ. πλήρες κείμενο καταδικαστικής απόφασης http://euro.ecom.cmu.edu/program/law/08-732/Crime/usVancheta.pdf (διαθέσιμη στις 13.09.2016).

14. Βλ. ορισμό σε *Σφακιανάκη Ε./Μακρυπούλια Ι.*, ό.π., σελ. 21: *«Με τον όρο botnet περιγράφουμε ένα δίκτυο από υπολογιστές, οι οποίοι έχουν παραβιαστεί από κάποιο κακόβουλο χρήστη και δύναται να χρησιμοποιηθούν για κακόβουλες ενέργειες. Η παραβίαση των υπολογιστών γίνεται συνήθως με τη χρήση ειδικά διαμορφωμένου κακόβουλου λογισμικού, το οποίο εγκαθίσταται στους υπολογιστές των θυμάτων εν αγνοία τους συνήθως παρουσιάζοντας τον εαυτό του ως νομότυπο λογισμικό. Οι υπολογιστές αυτοί αφού παραβιαστούν δίνουν τη δυνατότητα απομακρυσμένης διαχείρισής τους στο δράστη για την πραγματοποίηση παράνομων ενεργειών. Τα botnets χρησιμοποιούνται συνήθως για πραγματοποίηση επιθέσεων DDoS (Distributed Denial of Service)»[..]), για την αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, για τη διενέργεια απατών καθώς και για την παραβίαση υπολογιστικών συστημάτων όπου απαιτείται μεγάλη υπολογιστική ισχύ.»*

15. Όπως επισημαίνει η *Mitrou E.*, Attacks against Information Systems: Technical Definitions, σε συλλογικό έργο Iglezakis I. (ed.), The Legal Regulation of Cyber Attacks, Kluwer Law International, 2016, σελ. 12, είναι αξιοσημείωτη η απουσία ορισμού με νομικά δεσμευτικό τρόπο των εννοιών της κυβερνοεπίθεσης και της κυβερνοασφάλειας.

16. Για την ακρίβεια σημειώθηκαν επιθέσεις DDoS προς Γεωργιανά hackerforums (για τον περιορισμό κυβερνο-αντιποίνων, DDoS επιθέσεις προς γεωργιανά Μέσα Μαζικής Ενημέρωσης στην Οσετία (totalmediaBlackout), επιθέσεις προς Γεωργιανές κυβερνητικές ιστοσελίδες (καμία επίσημη ενημέρωση προς τους πολίτες), επιθέσεις προς γεωργιανές επιχειρήσεις (για παράδειγμα το e-banking δεν λειτουργούσε για 10 μέρες).

και ένα άλλο έλαβε χώρα στη Λιθουανία το 2008[17]. Στη χώρα μας μεγάλη δημοσιότητα είχε λάβει η σύλληψη[18] δύο ημεδαπών - δημιουργών του κακόβουλου λογισμικού "Lecpetex" που μόλυνε παγκοσμίως εκατοντάδες χιλιάδες ηλεκτρονικούς υπολογιστές το 2014. Το ηλεκτρονικό έγκλημα έχει τεράστιο οικονομικό κόστος[19] και συχνά πολιτική στόχευση ιδίως με τη μορφή κυβερνοακτιβισμού (hacktivism)[20], δηλ. του ακτιβισμού που τονώνει τη μαχητική προάσπιση πολιτικών, περιβαλλοντικών, κοινωνικών, πολιτιστικών αιτημάτων και αιτημάτων των πολιτών χωρίς να έχει κατ' ανάγκη καθορισμένη ιδεολογία, ιεραρχία ή πρόγραμμα, και ο οποίος χρησιμοποιεί για την ανάπτυξή του τεχνολογικά μέσα που προωθούν τη διάδοση και τη συμμετοχή μέσω διαδικτύου[21].

Όπως ήταν φυσικό η πρώτη χώρα που υιοθέτησε σχετική νομοθεσία ήταν οι ΗΠΑ, οι οποίες ήδη από το 1984 είχαν ψηφίσει τον νόμο για την ηλεκτρονική απάτη, Computer Fraud and Abuse Act of 1984 (CFAA).

Σε διεθνές επίπεδο, το 1990 η Γενική Συνέλευση του ΟΗΕ σε απόφασή της τόνιζε την ανάγκη υιοθέτησης νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα[22] και σε επόμενες την ανάγκη καταπολέμησης της παραποίησης (misuse) των τεχνολογιών πληροφορικής (2000, 2002). Παράλληλα, το 1997 το Συμβούλιο της Ευρώπης ανέλαβε την πρωτοβουλία για τη συγκρότηση μιας ειδικής επιτροπής εμπειρογνωμόνων με σκοπό την υιοθέτηση της κατάλληλης νομοθεσίας και την ενίσχυση της διεθνούς συνεργασίας για την αντιμετώπιση της εγκληματικότητας στον Κυβερνοχώρο («cyber-space»). Αποτέλεσμα αυτής της διεργασίας ήταν η Σύμβαση για το Κυβερνοέγκλημα, την οποία η χώρα μας κύρωσε τον Αύγουστο 2016.

Στο πλαίσιο της Ευρωπαϊκής Ένωσης, οι κυριότερες από τις νομοθετικές δράσεις[23] με στόχο την αντιμετώπιση του κυβερνοεγκλήματος ήταν οι ακόλουθες: α) η Απόφαση-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου, της 28ης Μαΐου 2001, για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούνστα μέσα πληρωμής πλην των μετρητών, β) η Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της Οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του Κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών, γ) η Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[24] και την αντικατάσταση της Απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου και δ) η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

## III. Οι νέες ρυθμίσεις

Η ανάγκη προσαρμογής του θεσμικού πλαισίου υπό αυτές τις συνθήκες ήταν αυταπόδεικτη όχι μόνο λόγω της υποχρέωσης που απορρέει από τη συμμετοχή μας στο Συμβούλιο της Ευρώπης (ΣτΕ) και στην ΕΕ, αλλά πρωτίστως για την κάλυψη των πραγματικών κενών της εθνικής νομοθεσίας στον τομέα του διαδικτυακού εγκλήματος με στόχο την προστασία των πολιτών αλλά και του ίδιου του κράτους από έκνομες συμπεριφορές μέσω του διαδικτύου.

17. Βλ. αναλυτικά μελέτη, EnekenTikk, KadriKaskaandLiisVihul, *International CyberIncidents: Legal Considerations*, CCDCOE Publications, 2010, στην ιστοσελίδα https://ccdcoe.org/publications/books/legalconsiderations.pdf (διαθέσιμη στις 13.09.2016).
18. Βλ. σχετικό δελτίο τύπου αστυνομίας http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=42947&Itemid=1333EN (διαθέσιμη στις 13.9.2016).
19. Μελέτη της υπολογίζει το κόστος του ηλεκτρονικού εγκλήματος σε 400 δισ. δολάρια ετησίως βλ. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (διαθέσιμη στις 13.09.2016).
20. Βλ. διατριβή *Καραγιαννόπουλου Β.*, The Regulation of Hacktivism in Contemporary Society: Problems and Solutions, University of Strathclyde, 2013.
21. Βλ. εννοιολογική προσέγγιση που αναφέρεται στη Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Κυβερνοακτιβισμός και οργανώσεις της κοινωνίας των πολιτών», (γνωμοδότηση πρωτοβουλίας, 2016/C 013/18), δημοσιευμένη στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 15.1.2016.
22. Βλ. απόφαση 14.12.1990, http://www.un.org/documents/ga/res/45/a45r121.htm (διαθέσιμη στις 13.09.2016).
23. Η αιτιολόγηση της λήψης δράσης εκ μέρους της ΕΕ αποτυπώνεται σαφέστατα στην Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο όπου αναφέρεται ότι «*Η ελευθερία και η ευημερία μας εξαρτώνται όλο και περισσότερο από ένα σταθερό και καινοτόμο διαδίκτυο, το οποίο θα συνεχίσει να ανθίζει εάν η ανάπτυξή του προωθείται από την καινοτομία του ιδιωτικού τομέα και από την κοινωνία των πολιτών. Όμως η διαδικτυακή ελευθερία απαιτεί επίσης ασφάλεια και προστασία από έκνομες ενέργειες*», Brussels, 7.2.2013, JOIN final, σελ. 2.
24. Το θέμα της παιδικής πορνογραφίας μέσω του διαδικτύου έχει εκτενώς αναλυθεί στη χώρα μας, βλ. μεταξύ άλλων *Κιούπη Δ.*, *Ιωαννίδου Α.*, επιμ., Η Παιδική Πορνογραφία στο Διαδίκτυο, Νομική Βιβλιοθήκη, 2007, *Νούσκαλη Γ.*, Πορνογραφία Ανηλίκων: Τα Κρίσιμα Ζητήματα του Άρθρου 348Α ΠΚ., ΠοινΔικ 2006, 908-915, *Μπούρμα Γ.*, Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας, ΠοινΔικ 2009, 322 επ., *Καϊάφα- Γκμπάντι Μ.*, Διαδικτυακές προσβολές της ανηλικότητας, Το δίκαιο στην ψηφιακή εποχή, εκδόσεις Νομική Βιβλιοθήκη, 2012, σελ. 117 επ.

### α) Οι υπό υιοθέτηση προβλέψεις

Με τον νέο νόμο κυρώθηκε, όπως προαναφέρθηκε, η Σύμβαση της Βουδαπέστης, ένα κείμενο πρωτοποριακό για την εποχή της ψήφισης του, του οποίου οι προβλέψεις παραμένουν επίκαιρες μετά από 15 χρόνια, ενώ έχει κυρωθεί από όλες τις μεγάλες χώρες και ιδίως αυτές που έχουν τη μεγαλύτερη υποδομή πρόσβασης στο διαδίκτυο και ελέγχουν το μεγαλύτερο τμήμα των διακινούμενων δεδομένων, όπως οι ΗΠΑ, ο Καναδάς, η Ιαπωνία και τα περισσότερα κράτη μέλη της ΕΕ[25].

Καταρχάς, η σύμβαση προβλέπει τα εγκλήματα για οποία πρέπει να προβλεφθεί τιμωρία και, συνεπώς, τα συμβαλλόμενα κράτη θα πρέπει να προβλέψουν σε περίπτωση που δεν καλύπτονται από τις υπάρχουσες διατάξεις *ουσιαστικού ποινικού δικαίου* τους, όπως η παράνομη πρόσβαση σε συστήματα (π.χ. το hacking), η παρεμβολή σε δεδομένα (π.χ. στις επιθέσεις DDos)[26], ή η κατασκευή και εν γένει χρήση προγραμμάτων με σκοπό τη διάπραξη ενός από τα τιμωρητέα εγκλήματα (π.χ. τα προγράμματα Trojans, worms κ.ο.κ).

Στο κείμενο της Σύμβασης περιλαμβάνονται διατάξεις *ποινικού δικονομικού δικαίου* αλλά και *διεθνούς συνεργασίας* με σκοπό τη διευκόλυνση ανίχνευσης και επιβολής κυρώσεων σε περιπτώσεις ηλεκτρονικού εγκλήματος.

Στην πρώτη κατηγορία βρίσκει κανείς διατάξεις σχετικά με: α) τη διαφύλαξη των αποθηκευμένων δεδομένων σε έναν υπολογιστή, β) τη διαφύλαξη και τη γνωστοποίηση των μεταδιδόμενων δεδομένων, γ) την παροχή πληροφοριών, δ) την έρευνα και την κατάσχεση αποθηκευμένων στοιχείων, ε) την πραγματικού χρόνου συλλογή διακινουμένων δεδομένων και στ) την παρακολούθηση – υποκλοπή του περιεχομένου δεδομένων.

Από τις διατάξεις αυτές μέγιστης σημασίας είναι η πρόβλεψη για συμπλήρωση των δικονομικών διατάξεων, που ισχύουν στα Συμβαλλόμενα Μέρη, προκειμένου να βελτιωθεί η δυνατότητα των Δικαστικών και Αστυνομικών Αρχών να διεξάγουν τις *έρευνές τους «σε πραγματικό χρόνο»* («in realtime», «en temps reel»), ώστε να συλλέγουν τα απαραίτητα αποδεικτικά στοιχεία, στα γεωγραφικά όρια της εκάστοτε εθνικής επικράτειας, πριν τα στοιχεία αυτά χαθούν (άρθρο 20 Σύμβασης). Η πρόβλεψη αυτή μπορεί να υλοποιηθεί ιδίως βάσει των προβλέψεων των άρθρων 29 έως 34 της σύμβασης σχετικά με την ταχεία διατήρηση των δεδομένων (άρθρο 29), της αποκάλυψης των δεδομένων (άρθρο 30), των ερευνών και κατασχέσεων αποθηκευμένων δεδομένων (άρθρα 31 και 32) και τα της υποκλοπής δεδομένων κίνησης και περιεχομένου (άρθρα 33 και 34).

Η δυνατότητα διασυνοριακής *πρόσβασης σε δεδομένα χωρίς την τήρηση της διαδικασίας παροχής δικαστικής συνδρομής* προβλέπεται σε δύο μόνο περιπτώσεις (άρθρο 32): α) σε δεδομένα στα οποία έχει πρόσβαση το κοινό («data publicly available», «donnees accessibles au public», «ανοικτά δεδομένα») και β) σε δεδομένα στα οποία το Συμβαλλόμενο Μέρος απέκτησε πρόσβαση ή έλαβε μέσω ενός συστήματος υπολογιστή που βρίσκεται στην Επικράτειά του και για τα οποία έχει λάβει τη νόμιμη και εκούσια συγκατάθεση του προσώπου που έχει το νόμιμο δικαίωμα να τα διαθέσει σε αυτό μέσω του συστήματος υπολογιστή. Στην τελευταία αυτή κατηγορία περιλαμβάνονται διατάξεις σχετικά με: α) την έκδοση καταζητούμενων, β) τις ισχύουσες βάσει της σύμβασης γενικές αρχές σχετικές με την αμοιβαία συνδρομή, γ) τη δυνατότητα αυτεπάγγελτης πληροφόρησης, δ) τη δημοσιοποίηση αποθηκευμένων δεδομένων σε ένα υπολογιστικό σύστημα και ε) τη γνωστοποίηση των δεδομένων κίνησης.

Ενδιαφέρον παρουσιάζει επίσης η πρόβλεψη για την *αυθόρμητη παροχή πληροφοριών* (άρθρο 26) εκ μέρους ενός κράτους μέλους προς ένα άλλο όταν κρίνει ότι στοιχεία που βρίσκει στο πλαίσιο των δικών του ερευνών μπορεί να είναι χρήσιμες για τη διερεύνηση άλλων ποινικών αδικημάτων στο έτερο συμβαλλόμενο μέρος.

Οι συνέπειες του διασυνοριακού χαρακτήρα του διαδικτυακού εγκλήματος επιβάλουν την διακρατική συνεργασία η οποία ενισχύεται μέσα από μια σειρά προβλέψεων και ιδίως την πρόβλεψη για δημιουργίας ενός *δικτύου σημείων διαρκούς επαφής* για τη διευκόλυνση της ταχείας επεξεργασίας των αιτημάτων συνδρομής που προέρχονται από την αλλοδαπή (άρθρο 35).

Ιδιαίτερης σημασίας για τη χώρα μας, λόγω της πολύ μεγάλης αυξημένης ροής μεταναστών, είναι και η κύρωση του Πρόσθετου Πρωτοκόλλου της Σύμβασης για το έγκλημα στον Κυβερνοχώρο αναφορικά με την *ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων υπολογιστών*, όπως υπεγράφη στο Στρασβούργο στις 28.1.2013. Ουσιαστικά με το Πρόσθετο Πρωτόκολλο διευρύνεται το πεδίο εφαρμογής της Σύμβασης για το έγκλημα στον Κυβερνοχώρο, προκειμένου να αντιμετωπισθούν και ξενοφοβικής και ρατσιστικής φύσης πράξεις. Ως ρατσιστικό και ξενοφοβικό υλικό νοείται κάθε γραπτό υλικό, εικόνα ή οποιαδήποτε άλλη εκπροσώπηση των ιδεών ή θεωριών, που υποστηρίζει, προωθεί ή εξωθεί μίσος, διακρίσεις ή βία, κατά οποιουδήποτε ατόμου ή ομάδας ατόμων, με βάση τη φυλή, το χρώμα, την καταγωγή, εθνική ή εθνοτική, τη θρησκεία, καθώς και αν χρησιμοποιείται ως πρόσχημα για οποιονδήποτε από αυτούς τους παράγοντες.

Η υπ' αριθ. 2013/40/ΕΕ Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά

25. Εξίσου μεγάλη σημασία έχουν βεβαίως και οι χώρες που δεν την έχουν κυρώσει όπως η Ρωσία και η Κίνα.

26. Βλ. ανωτέρω ιδίως υποσ. 12 και 16 και μεταξύ άλλων *Politis D., Kozyris P., Iglezakis I.*, eds. Socioecomonic and Legal Implications of Electronic Intrusion, Hershey, Information Science Reference, 2009.

συστημάτων πληροφοριών και την αντικατάσταση της Απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου σε ένα μεγάλο μέρος της επιχείρησε να εναρμονίσει τη νομοθεσία των κρατών μελών σε αντιστοιχία[27] με τις προβλέψεις της Σύμβασης για το Κυβερνοέγκλημα.

Συνεπώς, οι νέες εθνικές ρυθμίσεις ανταποκρίνονται ταυτόχρονα στις απαιτήσεις τόσο της Σύμβασης όσο και της οδηγίας.

## β) Οι ψηφισθείσες τελικές διατάξεις

Οι νέες διατάξεις εισάγουν στο εθνικό νομοθετικό πλαίσιο πρόβλεψη για τα τρία βασικά αδικήματα που αποτελούν τον πυρήνα του κυβερνοεγκλήματος με τη στενή έννοια: α) την παράνομη πρόσβαση σε πληροφοριακό σύστημα, β) την παράνομη παρέμβαση σε πληροφοριακό σύστημα και γ) την παράνομη παρέμβαση σε δεδομένα μαζί με τα αδικήματα της υποκλοπής και της διάδοσης εργαλείων για τον σκοπό της διαδικτυακής πειρατείας[28]. Κοινά βασικά χαρακτηριστικά των νεοεισαχθέντων διατάξεων είναι ότι όλα τα σχετικά αδικήματα εμπίπτουν στην κατηγορία των τελούμενων εκ προθέσεως αδικημάτων και πρέπει να γίνονται «χωρίς δικαίωμα».

Με τον νέο νόμο καταρχήν εισάγονται στο ποινικό μας δίκαιο οι έννοιες του πληροφοριακού συστήματος[29] και των ψηφιακών δεδομένων και ο αναγκαίος ορισμός τους ως περιπτώσεις στο ήδη υπάρχον άρθρο 13 του ΠΚ στο οποίο περιλαμβάνεται αυθεντική ερμηνεία των όρων που χρησιμοποιεί ο ΠΚ προκειμένου να μπορούν να διωχθούν τα εγκλήματα που αφορούν σε παράνομες πράξεις σχετικά με αυτά τα αγαθά και εισάγονται με τις νέες διατάξεις. Στην κατεύθυνση αυτή εισάγεται χάριν ομοιογένειας των χρησιμοποιούμενων όρων ο όρος «*πληροφοριακό σύστημα*» στο άρθρο 348Α ΠΚ σχετικά με την πορνογραφία ανηλίκων[30] όπως και στο άρθρο 348Β ΠΚ. Όπως έχει επισημανθεί, το κρίσιμο στοιχείο του ορισμού του πληροφοριακού συστήματος είναι η δυνατότητα αυτόματης επεξεργασίας ψηφιακών δεδομένων και η περαιτέρω αποσαφήνιση του όρου ψηφιακό δεδομένο[31].

Έπειτα, εισάγεται νέο άρθρο το 292Β ΠΚ με τον τίτλο «***Παρακώλυση λειτουργίας συστήματος πληροφοριών***» το οποίο ενσωματώνει ουσιαστικά τις προβλέψεις του άρθρου 4 της οδηγίας. Ουσιαστικά με αυτό ποινικοποιούνται οι επιθέσεις άρνησης εξυπηρέτησης τύπου DoS, οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS) έναντι πληροφοριακών συστημάτων και οι πράξεις παράνομης πρόσβασης (τύπου hacking/ cracking) οι οποίες προκαλούν προσωρινές επιπλοκές και όχι σοβαρή δυσλειτουργία σε ένα πληροφοριακό σύστημα. Η διάταξη προβλέπει κυρώσεις σε περίπτωση σοβαρής παρεμπόδισης ή διακοπής της λειτουργίας ενός συστήματος. Δεν ορίζεται όμως κάποιο ελάχιστο επίπεδο παρακώλυσης το οποίο θα επιφέρει τις προβλεπόμενες συνέπειες[32]. Αντιθέτως, οι προβλεπόμενες ποινές, στο πλαίσιο της επιβαλλόμενης από την οδηγία τήρησης της αρχής της αναλογικότητας ανάλογα με το είδος και την ένταση της προσβολής που οι πράξεις αυτές επιφέρουν, είναι αυστηρότερες στις περιπτώσεις στις οποίες η αξιόποινη συμπεριφορά: α) προκαλεί ζημία σε *σημαντικό* αριθμό πληροφοριακών συστημάτων μέσω της χρήσης εργαλείων που έχουν σχεδιαστεί κυρίως για τον σκοπό αυτόν, β) τελείται στο πλαίσιο δράσης εγκληματικής οργάνωσης, σε αντιστοιχία με τον ορισμό αυτής στο άρθρο 187 ΠΚ[33], γ) προκαλεί ιδιαίτερα μεγάλη ζημία ή πλήττει πληροφοριακά συστήματα τα οποία αποτελούν μέρος υποδομής που παρέχει ζωτικής σημασίας αγαθά ή υπηρεσίες για την κοινωνία και το κράτος. Ως ζωτικής σημασίας αγαθά νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια[34]. Υπενθυμίζουμε επίσης ότι σύμ-

27. Βλ. αναλυτικά στην αιτιολογική έκθεση νόμου σελ. 5 «*[…] Το άρθρο 3 (το οποίο αντιστοιχεί στο άρθρο 2 της Σύμβασης του Συμβουλίου της Ευρώπης) αναφέρεται στο έγκλημα της παράνομης πρόσβασης σε συστήματα πληροφοριών. Το άρθρο 4 (το οποίο αντιστοιχεί στο άρθρο 5 της Σύμβασης του Συμβουλίου της Ευρώπης) ρυθμίζει τις παράνομες παρεμβολές σε συστήματα. Το άρθρο 5 (το οποίο αντιστοιχεί στο άρθρο 4 της Σύμβασης του Συμβουλίου της Ευρώπης) ποινικοποιεί τις παράνομες παρεμβολές σε δεδομένα. Το άρθρο 6 (το οποίο αντιστοιχεί στο άρθρο 3 της Σύμβασης του Συμβουλίου της Ευρώπης) προσδιορίζει την αξιόποινη πράξη της παράνομης υποκλοπής. Το άρθρο 7 (αντίστοιχο του άρθρου 6 της Σύμβασης του Συμβουλίου της Ευρώπης) αναφέρεται στα εργαλεία που χρησιμοποιούνται για τη διάπραξη των παραπάνω αναφερόμενων εγκλημάτων.[…]*»

28. *Jougleux P.*, ό.π., σελ. 110.

29. Βλ. *Συμεωνίδου - Καστανίδου Ε.*, Επιθέσεις κατά συστημάτων πληροφοριών: οι θέσεις της ΕΕ για την ποινική τους αντιμετώπιση και το ελληνικό ποινικό δίκαιο, Δίκαιο Πληροφορικής, Legal Tech & Data Protection (4ο Πανελλήνιο Συνέδριο), εκδόσεις Νομική Βιβλιοθήκη, 2013, σελ. 59.

30. Το άρθρο αυτό έχει ήδη τροποποιηθεί από τον Έλληνα Νομοθέτη με τον Ν 4267/2014, που εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της Απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου.

31. Βλ. *Mitrou E.*, Attacks against Information Systems: Technical Definitions, ό.π., σελ. 11.

32. Βλ. *Jougleux P./Mitrou L./Synodinou T.*, Criminalization of Attacks against Information Systems, σε συλλογικό έργο *Iglezakis I.* (ed.), The Legal Regulation of Cyber Attacks, Kluwer Law International, 2016, σελ. 34.

33. Έχει επισημανθεί ότι η περίσταση αυτή δύσκολα θα μπορούσε να εφαρμοσθεί στην περίπτωση των επιθέσεων από τους «Ανώνυμους» δοθέντος ότι είναι δύσκολος ο χαρακτηρισμός της δράσης τους στο πλαίσιο μιας «δομημένης» ομάδας και συνήθως ο ιδεολογικός σκοπός των δράσεων τους δεν συνάδει με κάποιο υλικό ή οικονομικό όφελος, βλ. *Jougleux P./Mitrou L./Synodinou T.*, ό.π., σελ. 27.

34. Βλ. και Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008 , σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), ιδίως άρθρο 2: «*ως «υποδομές ζωτικής σημασίας» νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζω-*

φωνα με την οδηγία μπορεί να θεωρηθεί ως επιβαρυντική περίσταση (άρθρο 9 παρ. 5) η τέλεση του συγκεκριμένου εγκλήματος με υφαρπαγή δεδομένων (κλοπή ταυτότητας, identity theft) προσωπικού χαρακτήρα άλλου ατόμου, έτσι ώστε να αποκτηθεί εμπιστοσύνη τρίτων προκαλώντας ζημία στο νόμιμο κάτοχο της ταυτότητας. Η οδηγία επέτρεπε να μην προβλεφθεί η συγκεκριμένη επιβαρυντική περίσταση εφόσον καλύπτεται από άλλο αδίκημα που τιμωρείται βάσει του εθνικού δικαίου. Ο εθνικός νομοθέτης δεν προέβλεψε τη συγκεκριμένη επιβαρυντική περίσταση ενδεχομένως έχοντας στον νου του την δυνατότητα εφαρμογής σε αυτές τις περιπτώσεις του υφιστάμενου άρθρου 386 ΠΚ περί της κοινής απάτης.

Ακολούθως ενσωματώνεται το άρθρο 7 της Οδηγίας με την εισαγωγή του άρθρου **292Γ** ΠΚ το οποίο προβλέπει ποινικές κυρώσεις για τις προπαρασκευαστικές ενέργειες τέλεσης του εγκλήματος 292Β ΠΚ. Προβλέπει συγκεκριμένα κυρώσεις για την με οποιονδήποτε τρόπο διάθεση ή απόκτηση των μέσων τέλεσης των εγκλημάτων του άρθρου 292Β ΠΚ. Σύμφωνα με την αιτιολογική σκέψη 16 της οδηγίας τέτοια εργαλεία μπορούν να περιλαμβάνουν το κακόβουλο λογισμικό -συμπεριλαμβανομένων των εργαλείων που μπορούν να δημιουργούν «botnet»- το οποίο χρησιμοποιείται για τη διάπραξη επιθέσεων στον κυβερνοχώρο. Στο συγκεκριμένο σημείο της οδηγίας εξάλλου αποσαφηνίζεται ότι ως κριτήριο εφαρμογής του αδικήματος απαιτείται να αποδειχθεί μια *ειδική πρόθεση* το εργαλείο να χρησιμοποιηθεί με σκοπό την τέλεση της συγκεκριμένης παράνομης πράξης.

Στη συνέχεια τροποποιείται το άρθρο 370Γ ΠΚ το οποίο αποκτά τον τίτλο **«*Παράνομη πρόσβαση σε πληροφοριακό σύστημα*»** και ενσωματώνει το άρθρο 3 της οδηγίας. Με τη διάταξη αυτή προβλέπεται πλέον στο ποινικό μας δίκαιο ρητά ως ποινικό αδίκημα η παράνομη πρόσβαση σε πληροφοριακό σύστημα με οποιοδήποτε τρόπο και συνεπώς καλύπτονται οι ενέργειες hacking ή/και cracking. Μέχρι σήμερα η διάταξη γινόταν δεκτό ότι κάλυπτε κυρίως την απόκτηση πρόσβασης μέσω pharming, δηλαδή της διαδικασίας μέσω της οποίας ένα ειδικό πρόγραμμα (Trojanhorse ή virus) χρησιμοποιεί κενά ασφαλείας του συστήματος, διεισδύει στον η/υ του θύματος και τον επηρεάζει κατά τέτοιο τρόπο ώστε ο συγκεκριμένος η/υ να επισκέπτεται στο διαδίκτυο πλαστές ιστοσελίδες και αντί να επικοινωνεί για παράδειγμα με την Τράπεζα του το θύμα, να δίνει ακούσια στους δράστες όλες τις πληροφορίες που είναι αναγκαίες για την μεταβίβαση σε αυτούς περιουσιακών του στοιχείων[35]. Στη διάταξη, όπως τροποποιήθηκε, δεν γίνεται διάκριση ανάλογα με το μέγεθος της ζημίας που προκλήθηκε. Οι προϋποθέσεις για την επιβολή κυρώσεων είναι: α) η χωρίς δικαίωμα απόκτηση πρόσβασης σε πληροφοριακό σύστημα ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, β) με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας, γ) που έχει λάβει ο νόμιμος κάτοχός του, ο οποίος υποβάλλει την απαιτούμενη έγκληση. Ο Έλληνας νομοθέτης εξαντλώντας την αυστηρότητά του ποινικοποίησε με αυτόν τον τρόπο και τις περιπτώσεις ήσσονος σημασίας χωρίς αυτό να συνιστά απαίτηση της οδηγίας[36] με αποτέλεσμα για παράδειγμα να τιμωρούνται και οι περιπτώσεις που κάποιος νέος προσπαθώντας να αποκτήσει ικανότητες και εμπειρία, δοκιμάζει τις ικανότητες του και πετυχαίνει να αποκτήσει πρόσβαση σε πληροφοριακό σύστημα. Στις περιπτώσεις αυτές, όπως και στην περίπτωση του χακτιβισμού, συνήθως δεν προκαλούνται μόνιμες βλάβες στη λειτουργία ενός συστήματος ή στο περιεχόμενο μιας ιστοσελίδας. Με την 3η παράγραφο του άρθρου φαίνεται να καλύπτονται οι περιπτώσεις του αποκαλούμενου white hacking ή ethical hacking[37]. Με τον όρο αυτόν καλύπτονται οι δοκιμές διείσδυσης, (ευρύτερα γνωστές στην αγγλική ως *penetration tests*) με τις οποίες κάποιος ειδικός στην πληροφορική, συνήθως μετά από εντολή του κατόχου ενός πληροφοριακού συστήματος, προσπαθεί να αποκτήσει πρόσβαση σε αυτό προκειμένου να ελέγξει το επίπεδο ασφάλειας του. Με βάση τις προβλέψεις της νέας διάταξης, αυτές οι περιπτώσεις αλλά και κάθε απόκτηση πρόσβασης με παραβίαση απαγόρευσης ή μέτρου ασφαλείας θα τιμωρούνται μόνο αν απαγορεύονται

*τικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών·».*

35. Βλ. *Μαργαρίτη Μ.*, Ποινικός Κώδικας, Ερμηνεία – Εφαρμογή, εκδόσεις Δίκαιο & Οικονομία, Π.Ν. Σάκκουλας, 2014, σελ. 1151, *Βασιλάκη*, Τα φαινόμενα «Phishing», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, 860.

36. Βλ. σημείο 11 προοιμίου οδηγίας: *«Η παρούσα οδηγία προβλέπει ποινικές κυρώσεις, τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας. Τα κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές. Η περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης.»* καθώς και τελευταίο εδάφιο άρθρου 3 *«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»*

37. Δεδομένου ότι ο όρος χρησιμοποιείται κυρίως στην «διαδικτυακή αργκό» ο βασικό ορισμός μπορεί να εντοπισθεί στο διαδίκτυο στη σελίδα http://searchsecurity.techtarget.com/definition/white-hat (διαθέσιμη στις 8.10.2016).

ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

Με το νέο άρθρο 370Δ ΠΚ που εισάγεται ενσωματώνεται το άρθρο 6 της οδηγίας σχετικά με την ***παράνομη υποκλοπή επικοινωνιών μέσω πληροφοριακών συστημάτων*** και τιμωρείται πλέον αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων και η χρήση των πληροφοριών με ποινές αντίστοιχες της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών που προβλέπονται στη διάταξη του άρθρου 370Α ΠΚ. Μέχρι σήμερα αντίστοιχες πράξεις με αυτές που αναφέρθηκαν παραπάνω, διώκονταν σύμφωνα με το άρθρο 10 του Ν 3115/2003 για παραβίαση του απορρήτου των επικοινωνιών, τα άρθρα 4 & 15 του Ν 3471/2006, το άρθρο 22 παρ. 4 του Ν 2472/1997 σχετικά με τα δεδομένα προσωπικού χαρακτήρα, τα άρθρα 370Α, 370 Β, 370 Γ, 292 Α και σύμφωνα με το άρθρο 15 του Ν 3471/2006 για υποκλοπή, τροποποίηση, καταστροφή δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών.

Σε συμμόρφωση με τις προβλέψεις του άρθρου 7 της οδηγίας προβλέπεται πλέον και στον ελληνικό νόμο (νέο άρθρο 370Ε ΠΚ[38]) η τιμωρία ως ποινικό αδίκημα της με οποιονδήποτε τρόπο εκ προθέσεως διάθεσης προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα, προκειμένου να διαπραχθούν τα εγκλήματα που αναφέρονται στα άρθρα 370Α μέχρι 370Δ ΠΚ. Και σε αυτήν την κατηγορία θα μπορούσαν να ενταχθούν πράξεις όπως για παράδειγμα η διάδοση κακόβουλου λογισμικού ή ιών, με σκοπό την προσβολή μεγάλου πλήθους υπολογιστών και τη μετέπειτα χρησιμοποίησή τους για την εκδήλωση επιθέσεων (botnets).

Το άρθρο 5 της οδηγίας, που ενσωματώθηκε ως άρθρο **381Α** ΠΚ με τίτλο «Φθορά ηλεκτρονικών δεδομένων», καλύπτει ένα κενό της ελληνικής νομοθεσίας, όπως επισημάνθηκε ήδη ανωτέρω, και πλέον προστατεύονται αυτοτελώς και ρητώς τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής αλλοίωσής τους κ.λπ. Με αυτόν τον τρόπο αποφεύγεται το άτοπο τα ψηφιακά δεδομένα να προστατεύονται μόνο εφόσον και στην έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, φορητή μνήμη κ.λπ.). Όπως ήδη αναφέρθηκε, μέχρι σήμερα αντίστοιχα αδικήματα διώκονταν σύμφωνα με το άρθρο 381 ΠΚ για φθορά ξένης περιουσίας, το άρθρο 22 παρ. 4 του Ν 2472/1997 που αφορά τα δεδομένα προσωπικού χαρακτήρα και το άρθρο 15 του Ν 3471/2006 για υποκλοπή, τροποποίηση και καταστροφή ψηφιακών δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών. Στις παραγράφους 2 και 3 του νέου άρθρου προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της οδηγίας, ενώ στην παράγραφο 4 προβλέπεται ότι το βασικό αδίκημα διώκεται κατόπιν έγκλησης χωρίς να υπάρχει πρόβλεψη για τυχόν ιδιαίτερα ελαφρές περιπτώσεις.

Με το νέο άρθρο **381Β** ΠΚ. η ελληνική νομοθεσία εναρμονίζεται με το άρθρο 7 της οδηγίας, που προβλέπει την ποινική ευθύνη προσώπων για πράξεις αγοράς, πώλησης, προμήθειας, κατοχής κ.λπ. προγραμμάτων ή κωδικών που μπορούν να χρησιμοποιηθούν για την τέλεση διάφορων αξιόποινων πράξεων μεταξύ των οποίων και οι προβλεπόμενες πλέον στο άρθρο 381Α ΠΚ. Συνεπώς με τις νέες διατάξεις θα διώκονται οι επιθέσεις που διαπράττονται με διάδοση ιών και κακόβουλου λογισμικού.

Βάσει του νέου νόμου τροποποιείται το άρθρο **386Α** ΠΚ σχετικά με την απάτη υπολογιστή κατά τα οριζόμενα στο άρθρο 8 της Σύβασης. Το άρθρο αυτό στην προηγούμενη μορφή του παραδοσιακά στη χώρα μας είχε χρησιμοποιηθεί για την επιβολή κυρώσεων στις υποθέσεις υποκλοπής καρτών ανάληψης ή της δημιουργία πλαστών πιστωτικών καρτών / κλώνων με η/υ και χρήση τους με παρέμβαση στα στοιχεία υπολογιστή κατά την εφαρμογή του προγράμματος των ΑΤΜ[39]. Στην προηγούμενη μορφή της η διάταξη είχε επικριθεί για αοριστία γιατί είχε μια ενδεικτική παράθεση τρόπων τέλεσης του προβλεπόμενου αδικήματος η οποία αναιρούταν από την φράση που ακολουθούσε βάσει της οποίας το αδίκημα τιμωρούταν ακόμα και αν τελούταν «*με οποιονδήποτε άλλο τρόπο*[40]». Η νέα τροποποίηση της διάταξης έχει απαλείψει αυτή την αναφορά. Ομοίως, η παλαιότερη διατύπωση είχε διχάσει θεωρία και νομολογία ως προς το αν η κλοπή κάρτας ανάληψης και κωδικού χρήσης της (pin) έπρεπε να τιμωρείται βάσει αυτής της διάταξης ή αν συνιστούσε απλή κλοπή. Σύμφωνα με τη νέα διάταξη περιλαμβάνεται πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου.

38. Παράλληλα μπορεί να εφαρμοσθεί το άρθρο 9 παρ. 6 του Ν 3674/2008 σύμφωνα με το οποίο: «*όποιος παράνομα διαθέτει στο εμπόριο ή διαθέτει προς εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων της παρ. 1 ή διαφημίζει δημόσια και προσφέρει υπηρεσίες για την τέλεση των πράξεων της παρ. 1, τιμωρείται με φυλάκιση 1 έτους και χρηματική ποινή από 10.000 ως 50.000 ευρώ*».

39. Βλ. χαρακτηριστικά ΣυμβΕφΘεσ 28/2010, ΑΠ 131/2013.

40. Βλ. επίμαχη διατύπωση προηγούμενης μορφής άρθρου βάσει της οποίας τιμωρούταν όποιος: «*βλάπτει ξένη περιουσία επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλον τρόπο*». Για άλλους πάντως η αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του η/υ ήταν σε κάθε περίπτωση αναγκαίο στοιχείο για την εφαρμογή της διάταξης βλ. ΑΠ 1152/1999 ΠοινΔ 2000, 141, ΑΠ 1277/1998 ΠοινΧρ ΜΘ΄, 697, *Καράκωστα Ι.*, Δίκαιο και Ίντερνετ 2003, σελ. 236.

Τέλος, θα πρέπει να σημειωθεί ότι σε συμμόρφωση με την πρόβλεψη της οδηγίας (άρθρο 11) εισήχθη στον νέο νόμο (άρθρο 4 Ν 4411/2016) πρόβλεψη για την **ευθύνη των νομικών προσώπων** εφόσον αποδειχθεί ότι κάποια από τις ανωτέρω περιγραφόμενες πράξεις τελέστηκε, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, από φυσικό πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου ή της ένωσης προσώπων και έχει εξουσία εκπροσώπησής τους ή εξουσιοδότηση για τη λήψη αποφάσεων για λογαριασμό τους ή για την άσκηση ελέγχου εντός αυτών. Σε αυτήν την περίπτωση επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων, με ειδικά αιτιολογημένη απόφαση της Αρχής Διασφάλισης του Απόρρητου των Επικοινωνιών, κατά περίπτωση σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις: α) σύσταση για συμμόρφωση με απειλή προστίμου σε περίπτωση παράλειψης συμμόρφωσης, ή β) διοικητικό πρόστιμο από 20.000 έως 1.000.000 ευρώ, ή γ) ανάκληση ή αναστολή της άδειας λειτουργίας τους για χρονικό διάστημα από έναν (1) μήνα έως δύο (2) έτη, ή δ) απαγόρευση άσκησης της επιχειρηματικής τους δραστηριότητας για το ίδιο χρονικό διάστημα, ή ε) αποκλεισμός από δημόσιες παροχές, ενισχύσεις, επιδοτήσεις, αναθέσεις έργων και υπηρεσιών, προμήθειες, διαφημίσεις και διαγωνισμούς του Δημοσίου ή των νομικών προσώπων του δημόσιου τομέα για το ίδιο διάστημα. Η ανάγκη της σχετικής πρόβλεψης οφείλεται στο γεγονός ότι πλέον οι σχετικές ενέργειες με την παράνομη διείσδυση ή παρακώλυση πληροφοριακών συστημάτων στοχεύουν συχνά σε παρεμπόδιση της δραστηριότητας ενός ανταγωνιστή μιας επιχείρησης ενός φορέα ή κάποιου που προωθεί διαφορετικές ιδέες ή θέσεις από ένα άλλο νομικό πρόσωπο. Παρόλα αυτά ρητά εξαιρούνται της ευθύνης για σχετικές ενέργειες το κράτος, οι φορείς δημόσιας εξουσίας και οι διεθνείς οργανισμοί δημοσίου δικαίου. Η εξαίρεση αυτή κατά μια άποψη απηχεί μια πραγματιστική προσέγγιση βάσει της οποίας ήδη από την υπόθεση Snowden[41] κι έπειτα έχει επαληθευθεί ότι τουλάχιστον δύο σχετικές επιθέσεις έχουν ενορχηστρωθεί από κράτη και οι σχετικές διαφορές είναι δύσκολο να λυθούν στα δικαστήρια[42].

Εκτός από τις τροποποιήσεις του ποινικού κώδικα, ο νέος νόμος τροποποιεί τη διάταξη που αποτελεί ακρογωνιαίο λίθο για την αποτελεσματική επιβολή κυρώσεων στο διαδίκτυο στη χώρα μας, η οποία είναι το άρθρο 4 του Ν 2225/1994, όπως ισχύει. Ουσιαστικά η διάταξη αυτή προβλέπει τα εγκλήματα για τα οποία επιτρέπεται η άρση του απορρήτου. Υπενθυμίζουμε ότι η προστασία του απορρήτου των επικοινωνιών καλύπτει και τη διεύθυνση IP την οποία λαμβάνει κάθε σύνδεση ηλεκτρονικού υπολογιστή στο διαδίκτυο και η οποία αποτελεί μια από τις βασικότερες ενδείξεις για την ταυτότητα των υπόπτων τέλεσης διαδικτυακών εγκλημάτων[43]. Με την τελευταία τροποποίηση προβλέπεται δυνατότητα άρσης του απορρήτου για την εξιχνίαση των εγκλημάτων που προβλέπονται στα νέα άρθρα 292Α ΠΚ, 292Β ΠΚ, 292Γ, 370Γ, 370Ε, 381Α και 381Β ΠΚ. Ομοίως, προβλέπεται (προσθήκη τελευταίου εδαφίου στο άρθρο 5 παρ. 11 του Ν 2225/1994) να τιμωρείται όποιος γνωστοποιεί σε τρίτους το γεγονός της άρσης του απορρήτου, καθώς και όποιος παραβιάζει την υποχρέωση εχεμύθειας κατά τη διαδικασία της άρσης του απορρήτου.

Στην ίδια κατεύθυνση, στο άρθρο 7 του νέου νόμου διατυπώνεται από τη χώρα μας η επιφύλαξη ότι θα προβαίνει σε συγκέντρωση δεδομένων κίνησης σε πραγματικό χρόνο (βλ. ανωτέρω σχετικά με άρθρο 20 Σύμβασης) με τις προϋποθέσεις που επιτρέπεται, κατά το ελληνικό δίκαιο, η άρση του απορρήτου των επικοινωνιών. Στη δεύτερη παράγραφο του ίδιου άρθρου δηλώνεται από την Ελλάδα ότι θα ισχύει η αρχή του διττού αξιόποινου και για τα αιτήματα διατήρησης των δεδομένων. Συνεπώς, θα πρέπει η πράξη για την οποία ζητείται η διατήρηση των δεδομένων να θεωρείται αξιόποινη τόσο για τη χώρα προέλευσης του αιτήματος όσο και για τη χώρα μας. Στην αιτιολογική έκθεση του νέου νόμου αποσαφηνίζεται σχετικά με το ίδιο ζήτημα, αυτό της διατήρησης δεδομένων ότι οι διατάξεις των εθνικών μας Ν 3471/2006 και 3917/2011, που εισήχθησαν με μεταγενέστερες της Σύβασης της Βουδαπέστης, σχετικές οδηγίες της Ευρωπαϊκής Ένωσης, δεν συγκρούονται με το άρθρο 16 παρ. 2 (κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών) της Σύβασης στο οποίο ορίζεται το ανώτατο διάστημα χορήγησης των δεδομένων, κατόπιν του αιτήματος των αρμοδίων αρχών για χορήγηση των ήδη διατηρουμένων δεδομένων.

Ένας τομέας που δεν θίγεται καθόλου από τις νέες διατάξεις είναι ενδεχόμενες αναγκαίες τροποποιήσεις στο ποινικό δίκαιο και ιδίως στην ποινική δικονομία σχετικά με τις ιδιαιτερότητες της εξιχνίασης ηλεκτρονικού εγκλήματος και ιδίως της εξέτασης ψηφιακών πειστηρίων[44] τα

41. Βλ. συλλογή σχετικών επίσημων κειμένων σε http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/(διαθέσιμη στις 8.10.2016).

42. Βλ. *Jougleux P./Mitrou L./Synodinou T.*, Criminalization of Attacks against Information Systems, ό.π, σελ. 26.

43. Βλ. ενδεικτικά *Βαγενά Ε.*,Ζητήματα προστασίας και επιβολής των πνευματικών δικαιωμάτων στο περιβάλλον του διαδικτύου, ΝοΒ 2007, 1058.

44. Βλ. ενδεικτικά στην ελληνική αρθρογραφία *Μανιάτη Α.*, Δικαστική των Ηλεκτρονικών Υπολογιστών, ΔiΜΕΕ 4/2011 και *Αγγελόπουλου Δ.*, *Πάσχου Ι.*, Κατάσχεση Ανάλυση ψηφιακών πειστηρίων, ΠοινΔικ 2003, 438, *Τσουραμάνη Χ.Ε.*, *Χαϊνά Ε.*, Η Εγκληματολογία στο Διαδίκτυο, Αντ. Ν. Σάκκουλας, 2007, *Φασούλα, Ε.- Ζ.*, Η Χρήση των Πολυμέσων στη Δικαστική Γραφολογία: Τεχνικά Στοιχεία, Εφαρμογές, Κριτική Αξιολόγηση, Αντ. Ν. Σάκκουλας, 2007, *Chang-Tsun L.*, ed. Handbook of Research on Computational Forensics, Digital Crime, and Investigation. Hershey, PA: Information Science Reference, 2010, *Περπέρη Α.*,Το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος και ο ρόλος των «εγκληματι-

οποία λόγω της φύσης τους είναι πιο δύσκολα ανιχνεύσιμα και πιο ευάλωτα σε αλλοιώσεις από τις συνηθισμένα. Σε άλλες χώρες, όπως η Αγγλία, έχουν εκδοθεί οδηγοί καλής πρακτικής σε ό,τι αφορά τη συλλογή και επεξεργασία των σχετικών πειστηρίων[45] ενώ στην Ευρώπη ο ENISA έχει εκδώσει έναν σχετικό οδηγό[46].

Σημειώνεται τέλος ότι η οδηγία που ενσωματώνεται (άρθρο 13 παρ. 1 Οδηγίας 2013/40) επιβάλει προκειμένου να μπορούν να ανταλλαχθούν πληροφορίες σχετικά με τα αδικήματα που εισήχθησαν με τις νέες διατάξεις, τα κράτη μέλη να εξασφαλίσουν ότι διαθέτουν ένα λειτουργικό εθνικό σημείο επαφής και να κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας (24/7). Τα κράτη μέλη βάσει της οδηγίας θα πρέπει επίσης να εξασφαλίζουν ότι διαθέτουν διαδικασίες ώστε, σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής.

## IV. Συνεργασία φορέων

Στη χώρα μας υπάρχουν πολλοί διαφορετικοί δημόσιοι αλλά και ιδιωτικοί φορείς που ασχολούνται θεσμικά στο πλαίσιο των αρμοδιοτήτων τους με την αντιμετώπιση του κυβερνοεγκλήματος.

Σε αυτούς περιλαμβάνονται από πλευράς Υπουργείου αρμόδιου για την Εθνική Άμυνα η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ) αλλά και το ΓΕΕΘΑ ως αρμόδιο για την έκδοση του Εθνικού Κανονισμού Ασφάλειας[47], σχετικά με τις πολιτικές ασφαλείας και τα ειδικά σχέδια που εφαρμόζονται από τα υπουργεία, τις δημόσιες υπηρεσίες και τα ΝΠΔΔ που κατέχουν διαβαθμισμένο υλικό.

Η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ), σύμφωνα με τον Ν 39/2008 είναι υπεύθυνη για το εθνικό CERT (Computer Emergency and Response Team) και αποτελεί την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων[48]. Ταυτόχρονα, αποτελεί Αρχή Ασφάλειας Πληροφοριών (INFOSEC) και φροντίζει για την ασφάλεια των επικοινωνιών και συστημάτων πληροφοριών σε εθνικό επίπεδο, καθώς και για την πιστοποίηση του διαβαθμισμένου (απόρρητου) υλικού των εθνικών επικοινωνιών[49].

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα, έχει ως αποστολή την πρόληψη, έρευνα και καταστολή των εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Είναι αυτοτελής υπηρεσία που υπάγεται απευθείας στον Αρχηγό της ΕΛΑΣ. Βάσει του νέου νόμου (άρθρο 5) ορίζεται ως το σημείο επαφής για την εκπλήρωση των σκοπών του άρθρου 35 της Σύβασης («Δίκτυο 24/7»)[50].

Στο πλαίσιο του Υπουργείο Εσωτερικών η Διεύθυνση Πολιτικού Σχεδιασμού Έκτακτης Ανάγκης (ΠΣΕΑ) του Υπουργείου Εσωτερικών, καταρτίζει τα σχέδια εξυπηρέτησης των υπηρεσιών της Γενικής Γραμματείας ΔΔ και Ηλεκτρονικής Διακυβέρνησης. Πρόσφατα επίσης[51] το «Κέντρο Μελετών Ασφαλείας (ΚΕΜΕΑ)[52] που υπάγεται στο Υπουργείο Εσωτερικών & Διοικητικής Ανασυγκρότησης, αποτελεί ιδρυτικό μέλος του «Ευρωπαϊκού Οργανισμού Ασφαλείας» στο Βέλγιο[53]. Το ΚΕΜΕΑ σε συνεργασία με το Ίδρυμα Τεχνολογίας & Έρευνας (ΙΤΕ) και το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΑΠΘ), δημιούργησαν το «Ελληνικό Κέντρο για το Κυβερνοέγκλημα» (GCC – GreekCybercrimeCenter) το οποίο αποσκοπεί στην παροχή προγραμμάτων κατάρτισης και εκπαίδευσης, προκειμένου να καταστεί κέντρο αριστείας στον τομέα της έρευνας του εγκλήματος στον κυβερνοχώρο.

Στο πλαίσιο της ΕΕ λειτουργεί εντός της Europol[54] από το 2013 Το Ευρωπαϊκό Κέντρο Διαδικτυακού Εγκλήματος

κών ευκαιριών» στη δημιουργία του, Εγκληματολογία, Τεύχος 1-2/2015, Ιανουάριος-Δεκέμβριος, *Αγγελή Ι.*, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, ΠοινΔικ 8-9, Αύγουστος-Σεπτέμβριος 2005, *Ξένου Μ.*, Η χρήση της χαρτογράφησης της εγκληματικότητας μέσω ηλεκτρονικού υπολογιστή από τις αστυνομικές αρχές, ΠοινΔικ 4/2000, Απρίλιος και *Karyda M.*, *Mitrou L.*, Internet Forensics: Legal and Technical Issues, WDFIA, International, Workshop on Digital Forensics and Incident Analysis, International 2007, 3 (2007), *Simou S.*, Cloud Forensics: Identifying the Major Issues and Challenges, in Advanced Information Systems Engineering, Springer International Publishing 2014, σελ. 271.

45. Βλ. (ACPO) Good Practice Guide for Computer-Based Electronic Evidence διαθέσιμο στην ιστοσελίδα https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf (10.08.2016).
46. ENISA, Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders, 2014 διαθέσιμος στην ιστοσελίδα https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (10.102016).
47. Βλ. ΠΔ 17/1974.
48. Βλ. άρθρο 4 παρ. 8 Ν 3649/2008.
49. Βλ. άρθρο 2 παρ. 4 ΠΔ 325/2003.
50. Αξίζει να σημειωθεί ότι τον Οκτώβριο του 2016 λειτουργεί η διαδικτυακή πύλη του «Ηλεκτρονικού Αστυνομικού Τμήματος» μέσω του οποίου εκτός των άλλων θα μπορούν να υποβάλλονται καταγγελίες και αιτήσεις σχετικά με ηλεκτρονικό έγκλημα, βλ. https://portal.astynomia.gr/ (διαθέσιμη στις 30.10.2016).
51. Βλ. ΠΔ 178/2014.
52. Βλ. ίδρυση και λειτουργία του με Ν 3387/2005, όπως τροποποιήθηκε με άρθρο 4 Ν 3938/2011.
53. Βλ. European Organization for Security – EOS, http://www.eos-eu.com.(διαθέσιμη στις 13.9.2016).
54. Της οποίας επίσης ο Κανονισμός Λειτουργίας τροποποιήθηκε πρόσφατα προκειμένου να μπορεί να ανταπεξέλθει πιο αποτελεσματικά σε επιθέσεις όπως τα τρομοκρατικά χτυπήματα βλ. https://www.europol.europa.eu/content/european-parliament-adopts-new-regulation-europol(διαθέσιμη στις 13.9.2016)και ακριβές νομοθετικό κείμενο ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/794 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 11ης Μαΐου 2016 για

(European Cybercrime Centre -EC3). Το EC3 λειτουργεί ως το κεντρικό σημείο της πάταξης του κυβερνοεγκλήματος στην Ένωση[55]. Υπάρχει επίσης ο ENISA –The European Network and Information Security Agency που εδρεύει στην Ελλάδα και επικεντρώνεται στην ενίσχυση της συνεργασίας για την αντιμετώπιση απειλών και περιστατικών προσβολής της ασφάλειας των πληροφοριών και την ανταλλαγή καλών πρακτικών μεταξύ των κρατών μελών. Σε διεθνές επίπεδο υφίσταται ομάδα εργασίας ΕΕ- ΗΠΑ για την Κυβερνοασφάλεια και το Κυβερνοέγκλημα[56] αλλά και άλλοι διεθνείς οργανισμοί οι οποίοι ασχολούνται με τα σχετικά ζητήματα όπως ο ΟΟΣΑ, η Γενική Συνέλευση των Ηνωμένων Εθνών, η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ/ OSCE), η Παγκόσμια Συνεδρίαση Κορυφής για την Κοινωνία της πληροφορίας (WSIS) και το Φόρουμ για τη Διακυβέρνηση του Διαδικτύου (IGF).

## V. Επικείμενες εξελίξεις

Την ίδια στιγμή που στη χώρα μας μόλις εκσυγχρονίσθηκε το εθνικό νομοθετικό πλαίσιο για το κυβερνοέγκλημα, σε επίπεδο ΕΕ η νομοθεσία πήγε ένα βήμα παραπέρα με την ψήφιση οδηγίας η οποία αποσκοπεί στην αύξηση του επιπέδου κυβερνοασφάλειας σε όλα τα κράτη μέλη της ΕΕ και της συνεργασίας τους για αυτόν το σκοπό. Η νέα Οδηγία 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ευρέως γνωστή από ως Οδηγία NIS από τα αρχικά του αγγλικού όρου Network and Information Systems) στοχεύει στην υιοθέτηση μέτρων από όλα τα κράτη μέτρα για ένα υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε όλη την ΕΕ. Η προθεσμία ενσωμάτωσης της λήγει στις 9.5.2018 και τα μέτρα που προβλέπει θα πρέπει να τεθούν σε εφαρμογή από τις 10.5.2018. Βάσει της οδηγίας θα πρέπει τα κράτη-μέλη βάσει κριτηρίων, να ορίσουν ποιες επιχειρήσεις παρέχουν βασικές ή ζωτικής σημασίας υπηρεσίες στους τομείς της ενέργειας, υγείας, τραπεζών, μεταφορών, ψηφιακών υπηρεσιών και παροχής νερού. Οι επιχειρήσεις αυτές θα πρέπει να τηρούν συγκεκριμένα επίπεδα, προκειμένου να αυξήσουν την ασφάλειά τους στον κυβερνοχώρο. Επιπλέον, θα πρέπει να αναφέρουν περιστατικά ασφαλείας στις εθνικές αρχές τους. Τα ανωτέρω αποφασίστηκαν λόγω «έλλειψης επαρκούς καταγραφής», καθώς τα περιστατικά που γνωστοποιούνται ή για τα οποία ενημερώνονται οι αρχές είναι πολύ λιγότερα από το πλήθος των κυβερνοεγκλημάτων που πραγματοποιούνται. Οι εταιρίες συνήθως που δέχονται επιθέσεις, προτιμούν να μη δώσουν στοιχεία και λεπτομέρειες καθώς θα πλήξουν τη δημόσια εικόνα τους, τη φήμη, την αξιοπιστία και την εμπιστοσύνη των πελατών τους. Στο πλαίσιο της οδηγίας επιβάλλεται ο ορισμός ενός εθνικού ενιαίου κέντρου επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («ενιαίο κέντρο επαφής») και η ίδρυση ενός δικτύουCSIRT, γνωστών επίσης ως «ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams — CERT)[57].

Στο πλαίσιο των επικείμενων εξελίξεων αξίζει να σημειωθεί η πρόταση της Ρωσίας για την έκδοση νέας σύμβασης για το έγκλημα στον κυβερνοχώρο, αφού έχουν περάσει περίπου 15 χρόνια από τη Συνθήκη της Βουδαπέστης το 2001, αλλά και η πρόταση του Νορβηγού δικαστή Stein Schjolber για νέα σύμβαση για το κυβερνοέγκλημα ενώπιον του ΟΗΕ και την ίδρυση διεθνούς δικαστηρίου για τον κυβερνοχώρο (International Court or Tribunal for Cyberspace – ICTC)[58].

Τέλος, σε αντιστάθμισμα όλων των νομοθετικών προβλέψεων για την ενίσχυση της ασφάλειας στον κυβερνοχώρο βρίσκονται οι νομοθετικές προβλέψεις σχετικά με την ενίσχυση της προστασίας του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο ψηφιακό περιβάλλον που επιχειρούνται στο πλαίσιο του αποκαλούμενου «data reform package»[59] ή άλλως της

---

τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ. Στα καθήκοντα της βάσει του Κανονισμού της προβλέπεται ρητά η «ανάπτυξη κέντρων εμπειρογνωσίας στην Ένωση για την καταπολέμηση ορισμένων μορφών εγκλήματος που εμπίπτουν στο πεδίο αρμοδιοτήτων της Ευρωπόλ, συγκεκριμένα ανάπτυξη του Ευρωπαϊκού Κέντρου για τα Εγκλήματα στον Κυβερνοχώρο» (άρθρο 4 παρ. 1 (ιβ)).

55. Υπάρχει επίσης και η Παγκόσμια Συμμαχία κατά της Σεξουαλικής Κακοποίησης Παιδιών στον Κυβερνοχώρο, Global Alliance against Child Sexual Abuse Online Βλ. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm(διαθέσιμη στις 13.09.2016).

56. http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

57. Υπάρχει ήδη σε επίπεδο ΕΕ το CSIRT Network, που προάγει την επιχειρησιακή συνεργασία σε περίπτωση συμβάντων κυβερνοασφάλειας. Λειτουργεί ακόμα στο πλαίσιο της πολιτικής ΕΕ για την κυβερνοασφάλεια από τον Ιούνιο του 2013 μια πλατφόρμα ανταλλαγής τεχνογνωσίας για την ασφάλεια των πληροφοριακών συστημάτων με διαθέσιμα δημόσια έγγραφα στην ακόλουθη διεύθυνση, https://resilience.enisa.europa.eu/nis-platform/shared-documents(διαθέσιμη στις 13.9.2016).

58. Βλ. *Judge Stein Schjolberg*, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group, March 2012διαθέσιμο στη διεύθυνση http://www.cybercrimelaw.net/documents/ICTC.pdf (διαθέσιμη στις 20.8.2016).

59. Βλ. επίσημο αναλυτικό δελτίο τύπου http://europa.eu/rapid/press-release_IP-12-46_el.htm (διαθέσιμη στις 13.9.2016). Οι άλλες σχετικές νομοθετικές δράσεις περιλαμβάνουν τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων / General Data Protection Regulation/ GDPR)

μεταρρύθμισης των κανόνων περί προστασίας δεδομένων από τη ΕΕ. Στο πλαίσιο αυτό εντάσσεται και η ψήφιση της Οδηγίας 2016/680/ΕΕ της 27ης Απριλίου 2016[60] η οποία θα πρέπει να έχει ενσωματωθεί έως τις 6 Μαΐου 2018. Η οδηγία θέτει τους κανόνες της σύννομης, διασυνοριακής ή εγχώριας επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Περιλαμβάνει, εκτός άλλων, δικαίωμα πρόσβασης του ενδιαφερομένου αλλά και αποζημίωσής του σε περίπτωση ζημίας του από τη μη τήρηση των προβλεπόμενων κανόνων. Οι ρυθμίσεις στον τομέα αυτό αποτελούν ένα ανάχωμα στη διαρκώς επεκτεινόμενη τάση του ηλεκτρονικού «πανοπτισμού»[61] στο όνομα της πάταξης της κυβερνοεγκληματικότητας ώστε να μπορούν να εξισορροπηθούν τα δύο συγκρουόμενα δικαιώματα, δηλ. αυτό της ασφάλειας και, από την άλλη, αυτό της ιδιωτικότητας.

## VI. Επίλογος

Παρόλο που τα νέα θεσμικά εργαλεία ήταν απαραίτητα για τη δίωξη του ηλεκτρονικού εγκλήματος, όσοι ασχολούνται με τον τομέα αυτόν συμφωνούν ότι η πρόληψη είναι ο πιο αποφασιστικός παράγοντας για τη μείωση της τέλεσης των εγκλημάτων αυτού του είδους. Όσα χρήματα και αν ξοδέψει κανείς για να προστατευτεί για παράδειγμα από μια διαδικτυακή επίθεση, ο πιο αδύναμος κρίκος παραμένει ο ανθρώπινος παράγοντας καθώς έχει αποδειχθεί ότι μέσω της αποκαλούμενης «*κοινωνικής μηχανικής*»[62] τελικά η εξαπάτηση, η άγνοια ή η ευήθεια κάποιου ανθρώπου σε θέση κλειδί είναι που θα ανοίξει την «κερκόπορτα» για την διάπραξη ενός ηλεκτρονικού εγκλήματος ή/και την επίθεση σε ένα πληροφοριακό σύστημα[63]. Ο νέος νόμος παρέχει τα έννομα μέσα διευκόλυνσης επιβολής κυρώσεων αλλά -όπως πάντα- η πρόληψη είναι προτιμότερη της καταστολής του εγκλήματος[64] και στο πλαίσιο αυτό η δράση φορέων ενημέρωσης και ευαισθητοποίησης για τις δυνατότητες και τις συνέπειες των ηλεκτρονικών ή/και διαδικτυακών εγκλημάτων θα είναι καθοριστική. Η χώρα μας έχει το ανθρώπινο δυναμικό και την τεχνογνωσία να ανταποκρίνεται εγκαίρως στις προκλήσεις αντιμετώπισης του ηλεκτρονικού εγκλήματος αρκεί να υπάρχει η σχετική θεσμική βούληση και ένας κεντρικός συντονισμός όλων των διεσπαρμένων εμπλεκόμενων φορέων, όπως επιβάλλεται πλέον και από τις νομοθετικές και θεσμικές εξελίξεις σε επίπεδο ΕΕ.

και την Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

60. Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.

61. Βλ. ιδίως *Πανούση Ι.*, Επτά αλήθειες, μια πρόταση και ένα υστερόγραφο για τον μεγάλο αδερφό, Το δίκαιο στην ψηφιακή εποχή, εκδόσεις Νομική Βιβλιοθήκη, 2012, σελ. 79 επ.

62. Βλ. ενδεικτικά ανάλυση *Σπυρόπουλου Φ.*, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών, εκδόσεις Αντ. Ν. Σάκκουλα, 2016, σελ. 95.

63. Ο παράγοντας του *ανθρώπινου λάθους* άλλωστε είναι καίριος και στα συμβάντα σχετικά με την ασφάλεια πληροφοριακών συστημάτων, βλ. Annual Incident Reports 2015, ENISA, σελ. 33.

64. Βλ. προς αυτήν την κατεύθυνση και τις προτάσεις που απορρέουν από την πολύχρονη εμπειρία του στη Δίωξη Ηλεκτρονικού εγκλήματος του *Σφακιανάκη Ε.*, Ο Κώδικας του Διαδικτύου, ό.π., σελ. 109.