

Με τον Νόμο 4411/2016 (ΦΕΚ 142–Α΄/3-8-2016), ο οποίος τιτλοφορείται: «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 και 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 – πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου, αναφορικά με ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».

Η κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλό της προβλέπεται στο πρώτο άρθρο του Νόμου.

Με το Πρόσθετο Πρωτόκολλο της Σύμβασης διευρύνθηκε το πεδίο εφαρμογής της, για να αντιμετωπιστούν ενιαία τα ζητήματα ρατσισμού και ξενοφοβίας που εκδηλώνονται μέσω του Διαδικτύου.

Με τον ίδιο Νόμο ενσωματώνονται και διατάξεις που αφορούν επιθέσεις κατά συστημάτων πληροφοριών, με σκοπό τη διευκόλυνση της πρόληψης των αδικημάτων και τη βελτίωση της συνεργασίας μεταξύ δικαστικών και λοιπών αρχών των κρατών μελών.

Παρόλο που η κύρωση της Σύμβασης και η ενσωμάτωσή της στο εσωτερικό δίκαιο της Χώρας μας, έγινε με μεγάλη καθυστέρηση, ρυθμίζει σειρά κακόβουλων πράξεων που σήμερα ευνοούνται από τη ραγδαία εξέλιξη της τεχνολογίας της πληροφορικής και των Η/Υ και την υιοθέτησή τους από εγκληματίες για τη διάπραξη τέτοιων εγκλημάτων.

Αλλαγές στο Ουσιαστικό Ποινικό Δίκαιο

Το δεύτερο άρθρο του Νόμου 4411/2016, περιλαμβάνει διατάξεις του Ουσιαστικού Ποινικού Δικαίου, που θεσπίστηκαν εξ αρχής ή τροποποιήθηκαν για να εναρμονιστεί η ελληνική νομοθεσία με τη Σύμβαση και ειδικότερα:

Στο άρθρο 13 του Ποινικού Κώδικα (Π.Κ.), εισήχθησαν δύο νέοι ορισμοί και συγκεκριμένα στα εδάφια η΄ και θ΄ εισάγονται οι έννοιες του Πληροφοριακού Συστήματος και των Ψηφιακών Δεδομένων. Οι ορισμοί αυτοί περιλαμβάνονται στο

σύνολο του κειμένου της Σύμβασης και στην Οδηγία και είναι απαραίτητοι τόσο για την ερμηνεία των νέων διατάξεων που είτε εισάγονται στο Ποινικό μας Δίκαιο, όσο και αυτών που τροποποιούνται με το Νόμο 4411/2016. Σύμφωνα με τη νέα νομική ορολογία, α) Πληροφοριακό Σύστημα, νοείται οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, από τις οποίες μία ή περισσότερες εκτελούν αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, επεξεργάζονται ή διαβιβάζονται από τη συσκευή με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών και β) Ψηφιακά Δεδομένα νοούνται γεγονότα και πληροφορίες που μπορούν να επεξεργαστούν από πληροφοριακό σύστημα ή πρόγραμμα που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.

Για την αποτελεσματικότερη προστασία και την ποινική αντιμετώπιση ζητημάτων που αφορούν την δόλια παρακώληση λειτουργίας Πληροφοριακών Συστημάτων, προστέθηκε στον Ποινικό Κώδικα το άρθρο 292B.

Με το άρθρο αυτό η ελληνική νομοθεσία εναρμονίζεται με τις διατάξεις που περιέχονται στα άρθρα 5 της Σύμβασης και 4 της Οδηγίας, επιδιώκοντας την προσαρμογή της ποινικής προστασίας με την αντίστοιχη ποινική πρόβλεψη για επιθέσεις που εκδηλώνονται κατά συστημάτων τηλεφωνικών επικοινωνιών (άρθρο 292Α Π.Κ.), με γνώμονα την τήρηση της αρχής της αναλογικότητας ως προς το είδος και την ένταση της. Δηλαδή προβλέπονται αυστηρότερες ποινές όταν η κακόβουλη πράξη προκαλεί σημαντική ζημιά σε πληροφοριακά συστήματα με τη χρήση ειδικών για το σκοπό αυτό εργαλείων ή τελείται οργανωμένα από εγκληματική οργάνωση, όπως αυτή ορίζεται στο άρθρο 187 Π.Κ. ή προκαλεί ιδιαίτερα μεγάλη ζημιά ή πλήττει πληροφοριακά συστήματα υποδομής που παρέχουν σημαντικές, ζωτικές υπηρεσίες για την κοινωνία και το Κράτος. Η διάταξη αυτή περιλαμβάνει, προστατεύει και τιμωρεί, αναλογικά (ειδικά και αυστηρότερα), τις επιθέσεις κατά κρατικών πληροφοριακών συστημάτων και κρίσιμων υποδομών της Χώρας που χρησιμοποιούνται ευρύτερα από την κοινωνία και το Κράτος.

Για την εναρμόνιση της ελληνικής νομοθεσίας με το άρθρο 7 της Οδηγίας, προστέθηκε στον Ποινικό Κώδικα το άρθρο 292Γ, με το οποίο νομοθετήθηκε για πρώτη φορά στη Χώρα μας το αξιόποιο προπαρασκευαστικών πράξεων για τη διάπραξη των σχετικών με το άρθρο 292B αδικημάτων, ανεξαρτήτως αν αυτά τελικά διαπράχθηκαν. Δηλαδή ποινικοποιούνται αυτοτελώς προπαρασκευαστικές ενέργειες

και συμπεριφορές που στοχεύουν στην τέλεση των εγκλημάτων που περιλαμβάνονται στο άρθρο 292B, όπως η παραγωγή, η πώληση, η εισαγωγή, η κατοχή ή με οποιονδήποτε τρόπο διευκόλυνση αυτών με τη διανομή προγραμμάτων υπολογιστών ή συσκευών. Για τη διασφάλιση και την αποφυγή ποινικοποίησης της επιστημονικής έρευνας, προβλέπεται η τιμωρία της παραγωγής και διάθεσης των σχετικών εργαλείων, υπό την απαραίτητη προϋπόθεση να υπάρχει πρόθεση χρήσης τους για τη διάπραξη σχετικού εγκλήματος.

Για την περεταίρω προστασία των ανηλίκων τροποποιήθηκαν οι διατάξεις περί πορνογραφίας ανηλίκων και ειδικότερα το άρθρο 348Α του Ποινικού Κώδικα, το οποίο σημειωτέων είχε ήδη τροποποιηθεί στη Χώρα μας με το Νόμο 4267/2014, εναρμονίζοντας την ελληνική νομοθεσία με την Οδηγία 2011/93/ΕΕ. Με τη νέα τροποποίηση εισάγεται στις παραγράφους 2 και 5 ο όρος του Πληροφοριακού Συστήματος, όπως ορίζεται στο άρθρο 13 Π.Κ., για να επιτευχθεί ορολογική ομοιογένεια στις διατάξεις του Ποινικού Κώδικα. Επίσης ποινικοποιείται περεταίρω η διαδικτυακή διακίνηση αθέμιτου περιεχομένου, αποσκοπώντας στην προστασία των ανηλίκων από την σεξουαλική κακοποίηση, την σεξουαλική εκμετάλλευση και την προστασία της πνευματικής και της ηθικής τους ανάπτυξης, την προστασία των χρηστών ηθών και της ανθρώπινης αξιοπρέπειας. Οι πράξεις που τιμωρούνται αφορούν τη διακίνηση, τη διάδοση, την προμήθεια του υλικού πορνογραφίας ανηλίκων και τη δημοσίευσή του, μέσω του διαδικτύου.

Για την επίτευξη ορολογικής ομοιογένειας στις διατάξεις του Ποινικού Κώδικα και της απαιτούμενης εννοιολογικής προσέγγισης από τους νομικούς, τροποποιήθηκε και το άρθρο 348B του Ποινικού Κώδικα, «Προσέλκυση παιδιών για γενετήσιους λόγους», το οποίο συμπληρώθηκε με τον όρο «Πληροφοριακά Συστήματα».

Επίσης τροποποιήθηκε η δεύτερη παράγραφος του άρθρου 370Γ Π.Κ. «Παράνομη πρόσβαση σε πληροφοριακό σύστημα». Η αναδιατυπωμένη διάταξη προβλέπει και τιμωρεί την χωρίς δικαίωμα πρόσβαση σε Πληροφοριακό Σύστημα ή τμήμα αυτού. Ο όρος «πρόσβαση» περιλαμβάνει τη «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή σε μέρος αυτού, (όπως π.χ. σε επιμέρους αρχεία και φακέλους). Δεν περιλαμβάνει όμως τη χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων. Για τη θεμελίωση της υποκειμενικής υπόστασης απαιτείται πρόθεση, όπως αυτή προσδιορίζεται σύμφωνα με το

εσωτερικό δίκαιο κάθε Κράτους Μέλους. Οι περισσότερες νομοθεσίες των Κρατών Μελών του Συμβουλίου της Ευρώπης, περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή. Με τη διάταξη αυτή ουσιαστικά ποινικοποιείται το γνωστό κατά στη γλώσσα των δραστών «computer hacking». Ο δικαιολογητικός λόγος ποινικοποίησης της παράνομης πρόσβασης συνίσταται στο γεγονός ότι ο κάθε κάτοχος ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσης του υπολογιστή ή του συστήματος υπολογιστή, καθώς επίσης και να ορίζει εξατομικευμένα τα δικαιώματα πρόσβασης και διαχείρισης των δεδομένων που περιλαμβάνει και τιμωρεί, σε βαθμό Πλημμελήματος, κάθε υπαίτια παράβαση των απαγορεύσεων ή των μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχός τους. Εφόσον ο χρήστης έχει την ιδιότητα του υπαλλήλου σε σχέση με τον κάτοχο, η πράξεις αυτές τιμωρούνται μόνο εφόσον προβλέπονται ρητά από εσωτερικό κανονισμό ή μέτρα ασφαλείας που έχει λάβει αρμόδιος για το σκοπό αυτό υπάλληλος ή ο κάτοχος του υπολογιστή ή του συστήματος υπολογιστών.

Προστέθηκε νέα διάταξη και συγκεκριμένα το άρθρο 370Δ Π.Κ., με το οποίο ποινικοποιείται και τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών με τη χρήση τεχνικών μέσων και πληροφοριακών συστημάτων, καθώς και η χρήση από τον ίδιο ή η διαβίβαση των πληροφοριών αυτών σε τρίτα πρόσωπα, με ποινές αντίστοιχες της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών που προβλέπονται στη διάταξη του άρθρου 370Α Π.Κ. (κάθειρξη μέχρι δέκα χρόνια). Σε περίπτωση που οι πράξεις αυτές έχουν ως αποτέλεσμα την παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους σε καιρό πολέμου, τιμωρούνται σε βαθμό κακουργήματος, με τις προβλεπόμενες στο άρθρο 146 Π.Κ. ποινές «Παραβίαση Μυστικών της Πολιτείας». Με τη διάταξη αυτή ποινικοποιείται περεταίρω η ακρόαση και ο έλεγχος του περιεχομένου των επικοινωνιών και παροχή του περιεχομένου των δεδομένων είτε άμεσα, με πρόσβαση και χρήση των συστημάτων πληροφοριών, είτε έμμεσα με τη χρήση ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα. Σχετικά ποινικά αδικήματα προβλέπονται στα άρθρα 292Α, 370Α, 370Β και 370Γ ΠΚ, στο άρθρο 15 του Ν. 3471/2006 για πράξεις αφαίρεσης, αλλοίωσης, καταστροφή δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών, στα άρθρα 22 § 4 Ν 2472/1997 και 4 και 15 Ν 3471/2006 αναφορικά

με δεδομένα προσωπικού χαρακτήρα, στο άρθρο 10 του Ν. 3115/2003 για την παραβίαση του απορρήτου των επικοινωνιών.

Προστέθηκε νέα διάταξη και συγκεκριμένα το άρθρο 370Ε Π.Κ., με το οποίο ποινικοποιείται και τιμωρείται αυτοτελώς η εισαγωγή, η διανομή, η κατοχή, ο σχεδιασμός και η με οποιοδήποτε τρόπο διάθεση μηχανογραφικών εφαρμογών και προγραμμάτων λογισμικού, συσκευών ή τεχνικών μέσων, με τα οποία ευνοείται και καθίσταται δυνατή η δόλια πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος, με σκοπό τη διάπραξη εγκλημάτων που περιλαμβάνονται στις διατάξεις των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ του Π.Κ..

Επίσης, προστέθηκε στον Ποινικό Κώδικα το άρθρο 381Α Π.Κ., για την εναρμόνιση της ελληνικής νομοθεσίας με το άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Περιλαμβάνει διατάξεις που εξειδικεύουν το αντικείμενο της φθοράς των Ψηφιακών Δεδομένων ενός Συστήματος Πληροφοριών και ποινικοποιούν ειδικά την με δόλο και χωρίς δικαίωμα «Φθορά Ηλεκτρονικών Δεδομένων». Με την προσθήκη του άρθρου αυτού καλύπτεται και συμπληρώνεται η ελληνική νομοθεσία, ως προς την αυτοτελή προστασία των Ψηφιακών Δεδομένων, από πράξεις καταστροφής, απόκρυψης ή ανέφικτης χρήσης τους, διαγραφής ή αλλοίωσής τους.

Έτσι, τα Ψηφιακά Δεδομένα προστατεύονται αυτοτελώς και όχι αυτοματοποιημένα με βάση το βαθμό και την έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, εξωτερική φορητή μνήμη κ.λπ.). Στις παραγράφους 2 και 3 του εν λόγω άρθρου προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της Οδηγίας και ειδικότερα προβλέπονται και τιμωρούνται βαρύτερα οι επιθέσεις που έγιναν με τη χρήση ειδικού για το σκοπό αυτό εργαλείου ή στρέφονται κατά μεγάλου αριθμού Πληροφοριακών Συστημάτων ή προκαλούν ζημιές ευρείας έντασης και έκτασης ή τελέστηκαν κατά Πληροφοριακών Συστημάτων που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες, όπως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια ή τελέστηκαν από δομημένη και με διαρκή δράση ομάδα τριών ή περισσότερων προσώπων, που επιδιώκουν την τέλεση τέτοιων εγκλημάτων μαζικά. Τα παραπάνω δίδονται σε βαθμό Πλημμελήματος γενόμενης μνείας ότι τα αναφερόμενα στην πρώτη παράγραφο δίδονται εφόσον υποβληθεί έγκληση κατά κανόνα του παθόντος, ενώ τα αναφερόμενα στις παραγράφους δύο και τρία αυτεπαγγέλτως. Με τη διάταξη αυτή ποινικοποιούνται οι επιθέσεις κατά

πληροφοριακών συστημάτων με ιομορφικό λογισμικό, πράξεις που πριν την ψήφιση του Νόμου αντιμετωπίζονταν ποινικά ως φθορά ξένης ιδιοκτησίας, άρθρο 381 Π.Κ..

Προστέθηκε το άρθρο 381B Π.Κ., για την ενσωμάτωση στην ελληνική νομοθεσία των διατάξεων του άρθρου 7 της Οδηγίας. Στο νέο άρθρο περιλαμβάνονται διατάξεις που ποινικοποιούν την ευθύνη των προσώπων που δρουν με σκοπό την τέλεση αξιόποινων πράξεων, κυρίως αυτών που προβλέπονται στο άρθρο 381Α Π.Κ. και αφορούν την αγορά, την πώληση, την προμήθεια, την κατοχή και διακίνησης συσκευών και προγραμμάτων υπολογιστών και των συνθηματικών ή κωδικών εισόδου, προκειμένου αυτά να χρησιμοποιηθούν με δόλο για την επίτευξη παράνομης πρόσβασης σε μέρος ή στο σύνολο ενός Πληροφοριακού Συστήματος.

Τροποποιήθηκε το άρθρο 386Α Π.Κ. (Απάτη με Υπολογιστή), κατά τα οριζόμενα στο άρθρο 8 της Σύμβασης. Η τροποποιημένη διάταξη διαφοροποιεί την κλασική – συμβατική Απάτη από την Απάτη με Υπολογιστή, η οποία πλέον ποινικοποιεί την χωρίς δικαίωμα χρήση ψηφιακών δεδομένων και στοιχείων άλλου προσώπου, όπως π.χ. η δόλια χρήση από το δράστη του παράνομα αποκτηθέντος ονόματος διαδικτυακού χρήστη και του κωδικού χρήσης υπηρεσιών διαδικτύου του δικαιούχου. Το νέο στοιχείο που εισάγεται στην Απάτη με Υπολογιστή και τη διαχωρίζει από την απλή είναι ότι ο δράστης για να προσπορίσει στον εαυτό του ή άλλον παράνομο περιουσιακό όφελος, επηρεάζει το αποτέλεσμα μιας διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με τη χωρίς δικαίωμα χρήση δεδομένων, είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα. Η περιουσιακή βλάβη υφίσταται ακόμα και στην περίπτωση που τα πρόσωπα που την υπέστησαν είναι άδηλα ή στρέφονται κατά μεγάλου ή αορίστου αριθμού ατόμων, ενώ για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα. Ως προς τις ποινές η πράξη αντιμετωπίζεται και τιμωρείται σύμφωνα με τα προβλεπόμενα στο Άρθρο 386 Π.Κ..

ΑΡΣΗ ΑΠΟΡΡΗΤΟΥ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΚΥΒΕΝΡΕΟΓΚΛΗΜΑΤΩΝ

Με το τρίτο άρθρο του Ν. 4411/2016 επέρχονται τροποποιήσεις στο Ν. 2225/1994 και ειδικότερα, επικαιροποιείται και συμπληρώνεται η παρ. 1 του άρθρου

4 του Νόμου αυτού, που αναφέρεται στις περιπτώσεις για τις οποίες συντρέχει λόγος άρσης του απορρήτου και συγκεκριμένα προστίθενται στον κατάλογο των σχετικών εγκλημάτων τα νέα άρθρα του Π.Κ. που εισήχθησαν με το νέο Νόμο, καθώς τα εγκλήματα αυτά και η διερεύνησή της, εξαιτίας της φύσης του διαδικτύου αλλά και του τρόπου τέλεσής τους, είναι εξαιρετικά δυσχερές να εξιχνιασθούν χωρίς την άρση του απορρήτου της επικοινωνίας. Επίσης, λόγω συνάφειας με τα νεοεισαχθέντα εγκλήματα, προστέθηκαν στον κατάλογο του άρθρου 4 του Ν. 2225/1994, τα αδικήματα των άρθρων 370Α Π.Κ., 292Α Π.Κ., 11 του Ν. 3917/ 2011, 15 του Ν. 3471/2006 και 10 του Ν. 3115/2003. Η υφιστάμενη νομοθεσία για τη διατήρηση δεδομένων και συγκεκριμένα οι διατάξεις των Νόμων 3471/2006 και 3917/2011, που εισήχθησαν με μεταγενέστερες της παρούσας Σύμβασης, Οδηγίες της Ευρωπαϊκής Ένωσης, δεν συγκρούονται με το άρθρο 16 παρ. 2 αυτής, (κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών), καθώς με το τελευταίο ορίζεται το ανώτατο διάστημα χορήγησης των δεδομένων, κατόπιν αιτήματος των αρμόδιων αρχών για τη χορήγηση των ήδη διατηρούμενων δεδομένων. Επίσης, προστίθεται εδάφιο στο άρθρο 5 παρ. 11 του Ν. 2225/1994 με το οποίο 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 που προβλέπεται από το άρθρο 8 του Π.Δ. 47/2005 (Α' 64).

Με το τέταρτο άρθρο του ίδιου Νόμου, ρυθμίζεται το ζήτημα των διοικητικών κυρώσεων κατά νομικών προσώπων σύμφωνα με τις διατάξεις του άρθρου 12 της Σύμβασης και του άρθρου 10 της Οδηγίας. Συγκεκριμένα ποινικοποιείται η ευθύνη για αξιόποινες πράξεις που αναφέρονται στα άρθρα 292Β, 370Γ, 370Δ, 370Ε, 381Α και 386Α του Ποινικού Κώδικα, οι οποίες τελέστηκαν 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. Οι διοικητικές κυρώσεις επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων με ειδικά αιτιολογημένη απόφαση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, κατά περίπτωση, σωρευτικά ή διαζευκτικά. Η υιοθέτηση του συστήματος διοικητικών κυρώσεων ακολουθεί το πρότυπο αντίστοιχων ρυθμίσεων εναρμόνισης της ελληνικής νομοθεσίας με τις λοιπές οδηγίες.

Με το πέμπτο άρθρο του Ν. 4411/2016 και σε σχέση με τις προβλεπόμενες από τη Σύμβαση διατάξεις, ορίζεται το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων ως αρμόδια αρχή περί των διαδικασιών έκδοσης και παροχής αμοιβαίας δικαστικής συνδρομής, για τη συλλογή σε πραγματικό χρόνο δεδομένων κίνησης συγκεκριμένων επικοινωνιών εντός της Ελληνικής επικράτειας και σύμφωνα με το ισχύον εσωτερικό μας δίκαιο.

ΚΥΒΕΝΠΡΟΕΓΚΛΗΜΑ ΚΑΙ Δίκτυο 24/7

Με το έκτο άρθρο του Νόμου και προς εκπλήρωση των σκοπών του άρθρου 35 της Σύμβασης («Δίκτυο 24/7»), η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) της Ελληνικής Αστυνομίας, ορίζεται ως σημείο επαφής που λειτουργεί σε 24ωρη βάση, επτά ημέρες την εβδομάδα, παρέχοντας άμεση συνδρομή σε περιπτώσεις έρευνας και δίωξης αδικημάτων σχετικών με υπολογιστικά συστήματα και δεδομένα, υπό την εποπτεία Εισαγγελέα Εφετών. Στο πλαίσιο αυτό, η ΔΙ.Δ.Η.Ε. ως αρμόδιο σημείο επαφής παρέχει τεχνικές συμβουλές, προβαίνει σε ενέργειες διατήρησης ψηφιακών δεδομένων σε κατεπείγουσες περιπτώσεις σύμφωνα με τα άρθρα 29 και 30 της Σύμβασης, τη συλλογή των αποδεικτικών στοιχείων, την παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων, επικοινωνώντας για το σκοπό αυτό με οποιοδήποτε σημείο επαφής άλλου Συμβαλλόμενου Μέρους.

Στο έβδομο άρθρο του Νόμου διατυπώνεται από την Ελλάδα η επιφύλαξη ότι θα προβαίνει σε συγκέντρωση δεδομένων κίνησης σε πραγματικό χρόνο με τις προϋποθέσεις που επιτρέπεται η άρση του απορρήτου των επικοινωνιών, κατά το ελληνικό δίκαιο, ενώ στη δεύτερη παράγραφο του ίδιου άρθρου δηλώνεται από την Ελλάδα η διατήρηση του δικαιώματος άρνησης ικανοποίησης αιτήματος δικαστικής συνδρομής, αναγνωρίζοντας την ισχύ της αρχής του διπλού αξιόποινου και για τα αιτήματα διατήρησης των δεδομένων.

Παρότι η ενσωμάτωση της Σύμβασης της Βουδαπέστης στο ελληνικό εσωτερικό δίκαιο καθυστέρησε αρκετά, με το Ν. 4411/2016, παρέχονται σημαντικά δικονομικά μέσα για την ποινική αντιμετώπιση των εγκλημάτων στον Κυβερνοχώρο και παράλληλα θεσπίζεται ένα περισσότερο αναγκαίο και ικανό θεσμικό πλαίσιο αντιμετώπισης της διακίνησης υλικού ξενοφοβικής και ρατσιστικής φύσης μέσω του διαδικτύου.

Η κατ' αρχήν αναγνώριση της ανάγκης θέσπισης νέων κανόνων δικαίου για το έγκλημα στον Κυβερνοχώρο και οι αλλαγές που έγιναν με το Νόμο αυτό στο εσωτερικό δίκαιο της Χώρας μας, αναδεικνύουν το γεγονός και δείχνουν ξεκάθαρα ότι το πεδίο τέλεσης εγκλημάτων για αδικήματα που δεν «απαιτούν» την αυτοπρόσωπη παρουσία του δράστη και του θύματος έχει μετατοπιστεί από τον φυσικό – επίγειο χώρο στον εικονικό διαδικτυακό χώρο, όπου η τέλεση εγκλημάτων δύναται να τελεστεί απομακρυσμένα και κεκαλυμμένα με τη χρήση ενός υπολογιστή και την πληκτρολόγηση μερικών εντολών, ενώ η εύρεση των ηλεκτρονικών ιχνών του εγκληματία αναγνωρίστηκε πως είναι μια ιδιαίτερα δύσκολη και χρονοβόρα διαδικασία που απαιτεί εξειδικευμένες γνώσεις και στενή διεθνή συνεργασία μεταξύ των διωκτικών αρχών.

Ο Νόμος 4411/2016 περιλαμβάνει διατάξεις που κινούνται προς τη σωστή κατεύθυνση για την αντιμετώπιση του Κυβερνοεγκλήματος. Η ελληνική νομοθεσία έπρεπε να προσαρμοστεί στις νέες τεχνολογικές εξελίξεις και να διαφυλάξει τα έννομα αγαθά των πολιτών της, σε μια εποχή που το έγκλημα παρουσιάζει βελτιωμένα ποιοτικά και τεχνολογικά χαρακτηριστικά, τεχνολογικούς τρόπους και πολλαπλούς τόπους τέλεσης. Όμως, ο βραχύς βίος του νέου Νόμου δεν μας επιτρέπει να εξάγουμε σαφή και ασφαλή συμπεράσματα ως προς την επάρκεια και την αποτελεσματικότητά του. Κατά την πρακτική εφαρμογή των νέων διατάξεων για το έγκλημα στον Κυβερνοχώρο το προσεχές διάστημα, θα αναδειχθεί το γεγονός εάν οι αλλαγές αυτές επαρκούν για την «αστυνόμευση» του Κυβερνοχώρου και την αποτελεσματική διερεύνηση και τιμωρία των διαδικτυακών εγκλημάτων ή αν θα χρειαστούν νέες νομοθετικές παρεμβάσεις.