Το Ποινικό Δίκαιο της πληροφορικής στην Ελλάδα μετά τον ν. 4411/2016

Κριτική Επισκόπηση

Δρ. Φώτης Σπυρόπουλος

Καθηγητής Ποινικού Δικαίου Πυροσβεστικής Ακαδημίας

Διδάσκων ΑΕΙΤΤ Πειραιά

Δικηγόρος (ΜΔΕ) – οικονομολόγος

Δ. Ν. ποινικών επιστημών τμήματος Νομικής Πανεπιστημίου Αθηνών

Μέλος Δ.Σ. «Κέντρου Μελέτης του Εγκλήματος (ΚΕ.Μ.Ε.)»

Αθήνα, Μάρτιος 2018

Πληροφοριακά Συστήματα (Ι)

- **Πληροφοριακό Σύστημα**: συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών (ά. 13 παρ. η ΠΚ και 2§a της Οδηγίας 2013/40ΕΕ του Ευρωπαϊκού Κοινοβουλίου).
- **Ασφάλεια Πληροφοριακών Συστημάτων**: ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος (ΠΣ), αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή (ά. 3 ν. 3979/2011).
- **Ασφάλεια Τεχνολογίας Πληροφορικής και Επικοινωνιών - ΤΠΕ**: η ασφάλεια της τεχνολογικής υποδομής των ΠΣ, συμπεριλαμβανομένων και των επικοινωνιακών (υπο) συστημάτων του (ά. 3 ν. 3979/2011).
- **Ασφάλεια Πληροφοριών - δεδομένων**: η ασφάλεια των πληροφοριών και δεδομένων που διακινούνται, υποβάλλονται σε επεξεργασία και αποθηκεύονται στα στοιχεία του ΠΣ (ά. 3 ν. 3979/2011).

Πληροφοριακά Συστήματα (ΙΙ)

Η ασφάλεια των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να καλύπτει:

Εμπιστευτικότητα των δεδομένων (η ιδιότητα να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος).

Ακεραιότητα των δεδομένων (η ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα).

Διαθεσιμότητα των πόρων ενός πληροφοριακού συστήματος (η ιδιότητα τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος).

Πληροφοριακά Συστήματα (ΙΙΙ)

- Η διάδοση της χρήσης των ηλεκτρονικών υπολογιστών, η ταχύτατη εξέλιξη του διαδικτύου [πριν από μερικά έτη οι λειτουργίες του συμμετοχικού διαδικτύου (web 2.0), πρόσφατα το «διαδίκτυο των πραγμάτων» (“internet of things” κ.ο.κ.] και η έκρηξη της νέας ψηφιακής οικονομίας, η πλήρης εξάρτηση από τα ψηφιακά συστήματα επέφεραν ραγδαία αύξηση της λεγόμενης ψηφιακής εγκληματικότητας (digital criminality).

- Οι επιθέσεις κατά συστημάτων πληροφοριών στρέφονται κατά των θεμελιωδών υποδομών ζωτικής σημασίας (ΥΖΣ).

- Οδηγία 2008/114/ΕΚ της 08/12/08 «σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την αξιολόγηση της ανάγκης βελτίωσής της προστασίας τους» ως ΥΠΟΔΟΜΕΣ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ νοούνται «τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών».

Ο ν.4411/2016

- …κύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης (Βουδαπέστη, 2001), για το έγκλημα στον Κυβερνοχώρο
- …μετέφερε στο Ελληνικό Δίκαιο την Οδηγία 2013/40ΕΕ του Ευρωπαϊκού Κοινοβουλίου, για τις επιθέσεις κατά των συστημάτων πληροφοριών.

- Προσετέθησαν οι περιπτώσεις **η** και **θ** στο άρθρο **13** του Ποινικού Κώδικα,
- προσετέθησαν οι διατάξεις των άρθρων: **292 Β, 292 Γ , 370 Δ, 370 Ε, 381 Α και 381 Β** του Ποινικού Κώδικα,
- αντικαταστάθηκαν οι διατάξεις των άρθρων: **παρ.2 και 5 του αρ. 348 Α, 348 Β, 370 Γ και 386 Α** του Ποινικού Κώδικα.

Ο ν.4411/2016| Προστιθέντα Άρθρα

Στο άρθρο 13 Π.Κ. προστίθεται οι περιπτώσεις η) και θ) (έννοια όρων πληροφοριακού συστήματος και ψηφιακών δεδομένων:

η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.

Ο ν.4411/2016| Προστιθέντα Άρθρα

Άρθρο 292 Β:

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

Ο ν.4411/2016| Προστιθέντα Άρθρα

Άρθρο 292 Γ:	**Άρθρο 370 Δ:**
Με φυλάκιση μέχρι 2 ετών τιμωρείται όποιος **χωρίς δικαίωμα** και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292 Β **παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β**, β) **συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση** στο σύνολο ή μέρος ενός πληροφοριακού συστήματος.	**1.**Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη **δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές** από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενο τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. **2.**Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1. Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146.

Ο ν.4411/2016| Προστιθέντα Άρθρα

Άρθρο 370 Ε:	**Άρθρο 381 Α:**
Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370 Β, 370 Γ παράγραφοι 2 και 3 και 370 Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: **α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370 Β, 370 Γ και 370 Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση** στο σύνολο ή μέρος ενός πληροφοριακού συστήματος.	Φθορά ηλεκτρονικών δεδομένων: Όποιος **χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών**, **καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά**, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

Ο ν.4411/2016| Προστιθέντα Άρθρα

Άρθρο 381 Β:

Με φυλάκιση μέχρι δύο (2) ετών, τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα του άρθρου 381Α παράγραφοι 1, 2 και 3 παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος.

Ο ν.4411/2016| Τροποποιηθέντα Άρθρα

Άρθρο 348 Α παρ. 2 και 5 (ως ίσχυε):	**Άρθρο 348 Α παρ. 2 και 5 (σήμερα):**
2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ. 5. Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους.	2.Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, **μέσω πληροφοριακών συστημάτων**, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ. 5.Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας **μέσω πληροφοριακών συστημάτων**, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους.

Ο ν.4411/2016| Τροποποιηθέντα Άρθρα

Άρθρο 348 Β (ως ίσχυε):	**Άρθρο 348 Β (σήμερα):**
Προσέλκυση παιδιών για γενετήσιους λόγους: Όποιος με πρόθεση, μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει αυτόν ή τρίτον, με σκοπό τη διάπραξη σε βάρος του των αδικημάτων των άρθρων 339 παρ.1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μια τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρών.	Προσέλκυση παιδιών για γενετήσιους λόγους: Όποιος με πρόθεση, **μέσω πληροφοριακών συστημάτων**, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παρ.1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μια τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.

Ο ν.4411/2016 | Τροποποιηθέντα Άρθρα

Άρθρο 370 Γ (ως ίσχυε):	**Άρθρο 370 Γ (σήμερα):**
1.Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ. 2.Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29) ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. 3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. 4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.	**Παράνομη πρόσβαση σε πληροφοριακό σύστημα:** 1.Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί **προγράμματα υπολογιστών**, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ. 2.Όποιος **χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται σε συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση**. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. 3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του **πληροφοριακού συστήματος** ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. 4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.

Ο ν.4411/2016 | Τροποποιηθέντα Άρθρα

Άρθρο 386 Α (ως ίσχυε):	Άρθρο 386 Α (σήμερα):
Απάτη με υπολογιστή: Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, 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 άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και να τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα άτομα.	**Απάτη με υπολογιστή:** Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της 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, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα

Ο ν. 4411/2016 | Κριτική Επισκόπηση (Ι)

Στην σύγχρονη πρακτική του ν.4411/2016, εγείρονται τα εξής ζητήματα:

Ο ορισμός των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων (άρθρο 13 περ. η και θ Π.Κ), δημιουργεί κενό προστασίας των ψηφιακών δεδομένων αυτοτελώς.

Εκτός πεδίου προστασίας βρίσκονται τα ψηφιακά δεδομένα που αποθηκεύονται σε εξωτερικούς φορείς.

Δεν καθιερώνεται ως ποινικό αδίκημα η κλοπή ταυτότητας κατά πληροφοριακών συστημάτων (identity theft).

Για την τέλεση των εγκλημάτων αυτών δεν χρησιμοποιούνται μόνο απλοί «συμβατικοί» ηλεκτρονικοί υπολογιστές αλλά και άλλες συσκευές (π.χ.αποκωδικοποιητές, playstation, x-box).

Ο Νόμος 4411/2016 | Κριτική Επισκόπηση (ΙΙ)

Άρθρο 13 παρ. η και θ ΠΚ:

συμπερίληψη των ψηφιακών δεδομένων στην έννοια του πληροφοριακού συστήματος ► σύγχυση

η παρεμβολή στο σύστημα μπορεί να ταυτίζεται με την παρεμβολή στα δεδομένα, μόνο όταν η παρεμπόδιση ή η διακοπή της λειτουργίας του συστήματος αφορά και τα δεδομένα αυτά.

τα ψηφιακά δεδομένα προστατεύονται μόνο όταν εννοιολογικά εντάσσονται στην έννοια του πληροφοριακού συστήματος.

ψηφιακά δεδομένα σε φορείς αποθήκευσης που δεν έχουν τα γνωρίσματα του πληροφοριακού συστήματος ► εκτός πεδίου προστασίας,

Το κενό αυτό προστασίας γίνεται καλύτερα αντιληπτό στην περίπτωση που ο δικαιούχος πρόσβασης στα ψηφιακά δεδομένα είναι άλλος από τον δικαιούχο πρόσβασης στο πληροφοριακό σύστημα.

Ο Νόμος 4411/2016 | Κριτική Επισκόπηση (ΙΙΙ)

- ά. 292 Β ΠΚ: Ανάγονται σε ποινικό αδίκημα οι επιθέσεις κατά συστημάτων πληροφοριών, αποκεντρωμένες ή μη [DoS & DDoS], και επομένως και σχετικές πράξεις κυβερνοακτιβισμού [hacktivism], που τελούνται για πολιτικούς/συμβολικούς λόγους, εφόσον προσβάλλουν ουσιωδώς τη λειτουργία συστημάτων πληροφοριών.

- Μολονότι κάτι τέτοιο προβλέπεται στην Οδηγία (άρθρο 9 § 5 της Οδηγίας), ο σχετικός νόμος, που ενσωματώνει την Οδηγία, δεν ανάγει ούτε σε αυτό το άρθρο, αλλά ούτε και στο άρθρο 381Α ΠΚ, την κλοπή ταυτότητας [identity theft] σε ποινικό αδίκημα κατά της λειτουργίας συστημάτων πληροφοριών, δηλαδή την υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων, και, ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας.

- Εισάγεται στις παραγράφους 2 και 5 του άρθρου 348 Α ΠΚ, καθώς και στο άρθρο 348 Β ΠΚ ο όρος πληροφοριακό σύστημα, προκειμένου **«να αποφευχθεί η ορολογική ανομοιογένεια στις διάφορες διατάξεις του Ποινικού Κώδικα»** (αιτιολογική έκθεση ν.4411/2016, σελ. 6). Ωστόσο, στην παρ.1 του άρθρου 370 Γ ΠΚ και παρά την τροποποίηση αυτού, παραμένει ο όρος **«προγράμματα υπολογιστών»,** με αποτέλεσμα να δημιουργείται αυτή ακριβώς η ανομοιογένεια που θέλησε να αποφύγει ο νομοθέτης.

Ο Νόμος 4411/2016 | Κριτική Επισκόπηση (IV)

Σκόπιμο είναι να τονιστεί ότι για την τέλεση των εγκλημάτων αυτών δεν χρησιμοποιούνται μόνο απλοί «συμβατικοί» ηλεκτρονικοί υπολογιστές αλλά στην κατηγορία αυτή εμπίπτουν και άλλες συσκευές οι οποίες συνδέονται με το διαδίκτυο.

ά.381 Α ΠΚ: επιχειρείται η κάλυψη προϋπάρχοντος κενού της ελληνικής νομοθεσίας, ώστε να προστατεύονται πλέον αυτοτελώς τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής, αλλοίωσής τους κλπ. Ωστόσο, από την διατύπωση του νόμου εσφαλμένα προκύπτει ότι τα ψηφιακά δεδομένα προστατεύονται μόνο όταν εννοιολογικά εντάσσονται στην έννοια του πληροφοριακού συστήματος ► κενό προστασίας επί των ψηφιακών δεδομένων που αποθηκεύονται σε εξωτερικούς φορείς.

Ο Νόμος 4411/2016 | Κριτική Επισκόπηση (V)

Άρθρο 370 Γ παρ. 2 ΠΚ:

- Απαραίτητη προϋπόθεση καθίσταται πλέον η παραβίαση απαγορεύσεων ή μέτρων ασφαλείας.

- Με τις διατάξεις του άρθρου 370 Γ καθίσταται ποινικό αδίκημα η χωρίς δικαίωμα πρόσβαση σε συστήματα πληροφοριών χωρίς άδεια ανεξάρτητα από το είδος του σκοπού του δράστη και ανεξάρτητα από την επέλευση ή μη ζημίας. Έτσι, ποινικοποιούνται και περιπτώσεις ήσσονος σημασίας κατά συστημάτων πληροφοριών, μολονότι κάτι τέτοιο δεν συνιστούσε υποχρέωση κατά την Οδηγία.
- Η απόφαση αυτή του νομοθέτη διακινδυνεύει την πρόοδο της επιστημονικής έρευνας για θέματα ασφάλειας πληροφοριών, επιδεινώνει την εγχώρια ασφάλεια των συστημάτων πληροφοριών και ποινικοποιεί ανεπίτρεπτα πράξεις κυβερνοακτιβισμού [hacktivism], που τελούνται για πολιτικούς/συμβολικούς λόγους δίχως να διακινδυνεύουν τη λειτουργία των συστημάτων πληροφοριών.

Ο Νόμος 4411/2016│Έλλειψη συστημικής προσέγγισης (Ι)

Ο ν. 4411/2016 δεν λαμβάνει συστημικά υπόψιν του λοιπές υπάρχουσες διατάξεις σχετικές με το ηλεκτρονικό έγκλημα και το κυβερνοέγκλημα.

Έλλειψη συστημικής προσέγγισης του νομοθέτη στην αντιμετώπιση του κυβερνοεγκλήματος.

α. 211 ΠΚ: «*Προπαρασκευαστικές πράξεις. Όποιος με σκοπό να διαπράξει κάποιο τα εγκλήματα των άρθρων 207 και 209 κατασκευάζει, αποδέχεται, προμηθεύεται ή κατέχει εργαλεία, αντικείμενα, ηλεκτρονικά προγράμματα ή δεδομένα ή άλλα μέσα χρήσιμα γι' αυτόν το σκοπό, καθώς και χαρακτηριστικά ασφαλείας, όπως ολογράμματα, υδατογραφήματα ή λοιπά συστατικά στοιχεία του νομίσματος, τα οποία χρησιμεύουν για την προστασία από την παραχάραξη, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή. (ά 49 ν. 4443/2016)*

α. 191 ΠΚ: *«Με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή καταδικάζεται όποιος διασπείρει με οποιονδήποτε τρόπο ψευδείς ειδήσεις ή φήμες ικανές να επιφέρουν ανησυχίες ή φόβο στους πολίτες ή να ταράξουν τη δημόσια πίστη ή να κλονίσουν την εμπιστοσύνη του κοινού στο εθνικό νόμισμα ή στις ένοπλες δυνάμεις της χώρας ή να επιφέρουν διαταραχή στις διεθνείς σχέσεις της χώρας».*

α. 5 παρ. 3 ΠΚ: *«Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους».*

Ο Νόμος 4411/2016│Έλλειψη συστημικής προσέγγισης (ΙΙ)

- ά.211 ΠΚ: τροποποιήθηκε μεταγενέστερα με το άρθρο 49 του ν. 4443/2016

  ο όρος «προγράμματα ηλεκτρονικών υπολογιστών», αντικαταστάθηκε με τον όρο «ηλεκτρονικά προγράμματα ή δεδομένα» ► **ανομοιογένεια μεταξύ συναφών διατάξεων και την ελλιπή προσέγγιση του ν. 4411/2016**.

- ά. 191 ΠΚ: δεν ανανεώθηκε με τον ν.4411/2016, ενώ η διασπορά ψευδών ειδήσεων μέσω πληροφοριακών συστημάτων και δη μέσων κοινωνικής δικτύωσης (τα επονομαζόμενα hoaxes) είναι φαινόμενο της εποχής.

- ά. 5 παρ. 3 ΠΚ: η διάταξη κρίνεται ως τουλάχιστον άτεχνη καθώς, σύμφωνα με τη γραμματική της ερμηνεία, φαίνεται η ελληνική επικράτεια ως τόπος τέλεσης όλων ανεξαιρέτως των πράξεων που τελούνται μέσω διαδικτύου ανά την υφήλιο αφού στην Ελλάδα παρέχεται πρόσβαση στο διαδίκτυο.

  Η διάταξη αυτή διευρύνει υπερβολικά την ποινική δικαιοδοσία, σε τέτοιο βαθμό μάλιστα κατά τον οποίο η ελληνική δικαιοσύνη δύναται να καταστεί αντικείμενο forum shopping.

  Ο ν. 4411/2016 ωστόσο δεν φρόντισε να επιλυθεί το εν λόγω ζήτημα.

Ο Νόμος 4411/2016│Έλλειψη συστημικής προσέγγισης (ΙΙΙ)

- Ο ορισμός του συστήματος πληροφοριών που εισάγεται στις παρ. η και θ του άρθρου 13 ΠΚ, μεταφέρει αυτούσιο τον ορισμό της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών.

  Ύπαρξη ήδη δοθέντων ορισμών για την ασφάλεια των συστημάτων πληροφοριών κ.λπ. (βλ. ά. 3 ν. 3979/2011) – **συστημική ακολουθία;**

- Ζητήματα συρροής και εφαρμογής της ορθής διάταξης προκύπτουν μεταξύ των διατάξεων του άρθρου 370Δ και των άρθρων 292Α, 370Α, 370Β και 370Γ ΠΚ, του άρθρου 15 του ν. 3471/2006 για πράξεις αφαίρεσης, αλλοίωσης, καταστροφή δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών, των άρθρων 22 § 4 Ν 2472/1997 και 4 και 15 ν. 3471/2006 αναφορικά με δεδομένα προσωπικού χαρακτήρα, του άρθρου 10 του ν. 3115/2003 για την παραβίαση του απορρήτου των επικοινωνιών.

Συμπερασματικά…

- Ο ν. 4411/2016 μεταφέρει σχεδόν αυτούσια τα κείμενα της Σύμβασης του Συμβουλίου και της Ευρωπαϊκής Οδηγίας, αγνοώντας τυχόν ελλείψεις, αμφισημίες και ερμηνευτικά κενά.

- Η ανομοιογένεια που προκύπτει μεταξύ των διατάξεων του ν. 4411/2016 και των λοιπών προϋπαρχόντων διατάξεων για το κυβερνοέγκλημα, καταδεικνύει έλλειψη συστημικής προσέγγισης του νομοθέτη και οι αμφισημίες εντείνουν την σκέψη ότι οι διατάξεις του ν. 4411/2016 εφαρμόστηκαν απλά για να εφαρμοστεί η Ευρωπαϊκή Οδηγία και όχι για να αντιμετωπιστεί στην ουσία το κυβερνοέγκλημα.

- Ο χώρος των συστημάτων πληροφοριών αναπτύσσεται και εξελίσσεται συνεχώς, ωστόσο ο ν.4411/2016 μετέφερε το κείμενο της Σύμβασης του Συμβουλίου της Ευρώπης δεκαπέντε χρόνια μετά την υπογραφή της (Βουδαπέστη, 2001) και ενώ τα δεδομένα στον κυβερνοχώρο έχουν αλλάξει άρδην.

«Σας ευχαριστώ για την προσοχή σας!»

"Thank you for your attention!"

Δρ. Φώτης Σπυρόπουλος, Καθηγητής Ποινικού Δικαίου Πυροσβεστικής Ακαδημίας, Διδάσκων ΑΕΙΤΤ Πειραιά, Δικηγόρος (ΜΔΕ) – οικονομολόγος, Δ. Ν. ποινικών επιστημών τμήματος Νομικής Πανεπιστημίου Αθηνών

Dr. Fotios Spyropoulos, Professor of Criminal Law (Greek Fire Academy), PostDoc Professor at Piraeus University of Applied Sciences (Greece), Lawyer (master) – financial advisor, Doctorate degree on penal studies, Faculty of Law, University of Athens (Greece)

81, Alexandras av., Athens (Greee), P.C.: 11473

Tel.: (+30)2110135653 – (+30)2110135654

e-mail: fspyropoulos@gmail.com, fs@fspyropoulos.gr

Spyropoulos
Law Offices
Legal and Financial Services & Consultancy