Broker's Time

ΤΟ ΤΡΙΜΗΝΙΑΙΟ ΔΕΛΤΙΟ ΤΟΥ ΣΕΜΑ, ΧΡΟΝΟΣ 15ος, 2ο ΤΡΙΜΗΝΟ 2017

49

ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΚΑΙ ΤΙΜΩΡΙΑ Ή ΠΡΟΣΤΑΣΙΑ;

ΠΩΣ ΤΙΜΩΡΕΙΤΑΙ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

ΣΤΙΣ 3 ΑΥΓΟΥΣΤΟΥ 2016, ΤΕΘΗΚΕ ΣΕ ΙΣΧΥ Ο ΝΕΟΣ ΝΟΜΟΣ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΥΠ' ΑΡ. 4416/2016, Ο ΟΠΟΙΟΣ ΚΥΡΩΣΕ ΤΗ ΣΥΜΒΑΣΗ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΗΣ ΕΥΡΩΠΗΣ (ΣΥΜΒΑΣΗ ΤΗΣ ΒΟΥΔΑΠΕΣΤΗΣ) ΚΑΙ ΤΟ ΠΡΟΣΘΕΤΟ ΠΡΩΤΟΚΟΛΛΟ ΑΥΤΗΣ, ΕΝΣΩΜΑΤΩΣΕ ΣΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΔΗΓΙΑ 2013/40/ΕΕ ΚΑΙ ΑΝΤΙΚΑΤΕΣΤΗΣΕ ΤΗΝ ΑΠΟΦΑΣΗ-ΠΛΑΙΣΙΟ 2005/22/ΔΕΥ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (ΕΦΕΞΗΣ Ο «ΝΟΜΟΣ»).

της ΚΑΛΛΙΟΠΗΣ ΠΑΠΑΝΤΩΝΙΟΥ*

Μέχρι την ψήφιση του Νόμου, τα κυβερνοεγκλήματα στην Ελλάδα τιμωρούνταν βάσει των άρθρων 370Β, 370Γ και 386 Α του Ποινικού Κώδικα (εφεξής ο «ΠΚ»), που ρύθμιζαν την τιμωρία των εγκλημάτων που διαπράττονταν μέσω των ηλεκτρονικών υπολογιστών. Όμως το νομοθετικό αυτό καθεστώς παρουσίαζε σημαντικά κενά, επειδή δεν κάλυπτε την παρακώλυση λειτουργίας συστήματος υπολογιστή και δεν ρύθμιζε ξεχωριστά την αλλοίωση ή τη φθορά των ηλεκτρονικών δεδομένων, λόγω αθέμιτων προσβάσεων. Σε ορισμένες περιπτώσεις, μέρος της θεωρίας δεχόταν ότι για την αλλοίωση ή φθορά των ηλεκτρονικών δεδομένων μπορούσαν κατ' αναλογία να εφαρμοστούν οι διατάξεις για τη φθορά ξένης ιδιοκτησίας του άρθρου 381 ΠΚ. Όμως, βάσει αυτού του άρθρου, μπορούσε να τιμωρηθεί μόνο η φθορά στον υλικό τομέα των δεδομένων, δηλαδή η φθορά του υπολογιστή ή του server και όχι η καθεαυτή φθορά των δεδομένων, επειδή τα ηλεκτρονικά δεδομένα δεν αποτελούν πράγμα. Η καθεαυτή φθορά/αλλοίωση των ηλεκτρονικών δεδομένων μπορούσε να τιμωρηθεί μόνο εάν τα δεδομένα αυτά ήταν προσωπικά δεδομένα και μπορούσαν έτσι να εφαρμοστούν οι διατάξεις της νομοθεσίας περί προσωπικών δεδομένων ή βάσει των διατάξεων του άρθρου 13 περ. γ ΠΚ περί ηλεκτρονικού εγγράφου σε συνδυασμό με το άρθρο 222ΠΚ περί υπεξαγωγής εγγράφου.

Με τις νέες διατάξεις του Νόμου εισάγονται πλέον τα κάτωθι τρία βασικά αδικήματα: α) η παράνομη πρόσβαση σε πληροφοριακό σύστημα, β) η παράνομη παρέμβαση σε πληροφοριακό σύστημα και γ) η παράνομη παρέμβαση σε πληροφορικά δεδομένα συμπεριλαμβανομένης της υποκλοπής και διάδοσης εργαλείων για τον σκοπό της διαδικτυακής πειρατείας. Με το άρθρο δε 13 του ΠΚ εισάγονται πλέον και ερμηνεύονται οι όροι «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα».

Επιπλέον, εισάγονται στον ΠΚ τα κάτωθι νέα άρθρα και τροποποιούνται ισχιστάμενα άρθρα αυτού ως εξής:

- Άρθρο 292 Β, με το οποίο ποινικοποιούνται οι επιθέσεις άρνησης εξυπηρέτησης τύπου DoS, οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS) έναντι πληροφοριακών συστημάτων και οι πράξεις παράνομης πρόσβασης (hacking/cracking) και προβλέπονται κατά περίπτωση ποινικές κυρώσεις.
- Άρθρο 292 Γ, το οποίο προβλέπει ποινικές κυρώσεις για τις προπαρασκευαστικές ενέργειες τέλεσης του αδικήματος του άρθρου 292 Β (π.χ. διάθεση κακόβουλου λογισμικού και εργαλείων που μπορούν να δημιουργούν "botnet", το οποίο χρησιμοποιείται για τη διάπραξη επιθέσεων στον κυβερνοχώρο).
- Τροποποιείται το άρθρο 370 Γ, με το οποίο πλέον προβλέπεται ρητά ως ποινικό αδίκημα η παράνομη πρόσβαση σε πληροφοριακό σύστημα με οποιονδήποτε τρόπο, και συνεπώς καλύπτονται οι ενέργειες hacking και cracking.
- Άρθρο 370 Δ, με το οποίο τιμωρείται πλέον αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφορι-

ακών συστημάτων.
-Άρθρο 370 Ε, με το οποίο τιμωρείται πλέον ως ποινικό αδίκημα η με οποιονδήποτε τρόπο εκ προθέσεως διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων με τα οποία είναι δυνατή η πρόσβαση σε πληροφοριακό σύστημα, προκειμένου να διαπραχθούν τα αδικήματα που αναφέρονται στα άρθρα 370Α-370 Δ του ΠΚ.

Άρθρο 381 Α, το οποίο προστατεύει πλέον αυτοτελώς τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής, αλλοίωσης κ.λπ.
- Άρθρο 381 Β, με το οποίο προβλέπεται ποινική δίωξη των επιθέσεων που διαπράττονται με διάδοση κακόβουλου λογισμικού ή ιών.
- Τροποποιείται το άρθρο 386 Α σχετικά με την απάτη με υπολογιστή, όπου πλέον περιλαμβάνεται και η χρήση ορθών δεδομένων που γίνεται χωρίς δικαίωμα (π.χ. παράνομη απόκτηση ονόματος και κωδικού χρήστη).

Επιπλέον, σύμφωνα με το άρθρο 4 του Νόμου, προβλέπεται ειδική ποινική ευθύνη νομικών προσώπων, εφόσον αποδειχθεί ότι κάποιες από τις προαναφερόμενες ποινικά κολάσιμες πράξεις τελέστηκαν προς όφελος ή για λογαριασμό του νομικού προσώπου. Επιπροσθέτως, θα πρέπει να αναφέρουμε ότι, σύμφωνα με το ανωτέρω άρθρο, προβλέπεται και η δυνατότητα της άρσης του απορρήτου, προκειμένου να εξιχνιαστούν τα αδικήματα των άρθρων 292 Α-Γ ΠΚ, 370Γ ΠΚ, 370 Ε ΠΚ και 381 Α-Β ΠΚ.
Ο ανωτέρω Νόμος αποτελεί θεσμικό εργαλείο για τη δίωξη του ηλεκτρονικού εγκλήματος, όμως αποφασιστικό παράγοντα για την καταπολέμηση του αποτελεί η πρόληψη, η οποία είναι προτιμότερη της καταστολής και η οποία μπορεί να επιτευχθεί μόνο με συνεχή ενημέρωση και ευαισθητοποίηση των πολιτών.
Στο σημείο αυτό θα πρέπει να αναφερθεί ότι, ενώ η Ελλάδα κύρωσε τη Σύμβαση της Βουδαπέστης για την αντιμετώπιση του κυβερνοεγκλήματος με καθυστέρηση 15 ετών, η ευρωπαϊκή νομοθεσία εκσυγχρονίζεται με αλματώδη ρυθμό, τον οποίο θα πρέπει να ακολουθήσει η Ελλάδα εάν θέλει να έχει αισθητά αποτελέσματα στον τομέα αυτό. Ήδη, έχει εκδοθεί η νέα Ευρωπαϊκή Οδηγία 2016/1148 (η αποκαλούμενη ως Οδηγία NIS), η οποία στοχεύει στην υιοθέτηση μέτρων από όλα τα κράτη για ένα υψηλό κοινό επίπεδο ασφαλείας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση, με προθεσμία ενσωμάτωσης την 9-5-2018 και εφαρμογής των μέτρων την 10-5-2018. Σύμφωνα με την Οδηγία αυτή, θα πρέπει τα κράτη-μέλη, βάσει κριτηρίων, να ορίσουν ποιες υπηρεσίες παρέχουν ζωτικής σημασίας υπηρεσίες στους τομείς της ενέργειας, υγείας, τραπεζών, μεταφορών, παροχής νερού και ψηφιακών υπηρεσιών, έτσι ώστε αυτές να αυξήσουν τα μέτρα ασφαλείας στον κυβερνοχώρο και να αναφέρουν περιστατικά παραβίασης ασφαλείας στις εθνικές τους.

Επιπλέον, θα πρέπει να γίνει ειδική μνεία και στις νομοθετικές προβλέψεις οι οποίες ενισχύουν την προστασία του ατόμου από αθέμιτη επεξεργασία προσωπικών δεδομένων και λειτουργούν ως αντιστάθμισμα όλων των ανωτέρω προβλέψεων για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Ειδικότερα, από τις 25 Μαΐου 2018 θα εφαρμοστεί σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης ο υπ' αρ. 679/2016 Γενικός Ευρωπαϊκός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR), ο οποίος θα έχει άμεση ισχύ από την ως άνω ημερομηνία εφαρμογής του. Ο ανωτέρω Κανονισμός αντικαθιστά την Ευρωπαϊκή Οδηγία 95/46/ΕΚ και τον νόμο 2472/1997, ο οποίος ενσωμάτωσε την ανωτέρω οδηγία. Ο ανωτέρω Κανονισμός προβλέπει, μεταξύ άλλων, αυστηρότερες διατάξεις αναφορικά με την επιβολή πρόστιμων (μπορεί να επιβληθεί πρόστιμο που μπορεί να ανέλθει σε 20 εκατ. ευρώ ή στο 4% του συνολικού ετήσιου κύκλου εργασιών), έχει ευρεία εφαρμογή, εφαρμόζεται δηλαδή τόσο στους υπευθύνους επεξεργασίας όσο και στους εκτελούντες την επεξεργασία, οι υπεύθυνοι επεξεργασίας σε ορισμένες περιπτώσεις πρέπει να κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων αν η φύση των δεδομένων που χάθηκαν το απαιτεί. Επιπλέον, προβλέπεται ότι για τις εταιρείες και τις δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων που ενέχουν κινδύνους θα πρέπει να έχουν ορίσει υπεύθυνο προστασίας δεδομένων (DPO).

Στο πλαίσιο αυτό, εντάσσεται και η ψήφιση της Ευρωπαϊκής Οδηγίας 2016/680/27-4-2016, η οποία θα πρέπει να έχει ενσωματωθεί στα κράτη-μέλη έως και τις 6 Μαΐου 2018. Αυτή η οδηγία προβλέπει ειδικούς κανόνες για τη νόμιμη διασυνοριακή ή εγχώρια επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και της ελεύθερης κυκλοφορίας των δεδομένων αυτών. ●

*Senior Associate, Μπαχάς, Γραμματίδης και Συνεταίροι - Δικηγορική Εταιρεία