

ΕΠΙΜΕΛΕΙΑ

*Γεώργιος Αθ. Γέρμανος*

**Η ποινική αντιμετώπιση  
των κυβερνοεπιθέσεων  
κατά τον ελληνικό Ποινικό Κώδικα**  
*[Ν. 4619/2019 (με τις αλλαγές μέχρι και το Ν. 5023/2023)]*



Αθήνα, Απρίλιος 2023

\*\*\*\*\*

Με την ταχεία πρόοδο της τεχνολογίας και την αυξανόμενη εξάρτηση από το Διαδίκτυο και τις ψηφιακές συσκευές, οι κυβερνοεπιθέσεις αποτελούν πρωταρχική απειλή για τα πληροφοριακά συστήματα σε όλο τον κόσμο. Η Ελλάδα δεν αποτελεί εξαίρεση και το νομικό της σύστημα έχει προσαρμοστεί για να αντιμετωπίσει τις νέες προκλήσεις που θέτει το έγκλημα στον κυβερνοχώρο.

Ο Ποινικός Κώδικας της χώρας μας περιέχει μια σειρά άρθρων που αφορούν μορφές επιθέσεων κατά πληροφοριακών συστημάτων (κυβερνοεπιθέσεων). Αυτό το εγχειρίδιο συγκεντρώνει εκείνα τα άρθρα που τιμωρούν τους εμπλεκόμενους σε κυβερνοεπιθέσεις. Στόχος αυτών των διατάξεων δεν είναι μόνο η προστασία της ακεραιότητας και διαθεσιμότητας της ψηφιακής μας υποδομής και η εμπιστευτικότητα των πληροφοριών, αλλά και η αποτροπή πιθανών παραβατών από τη συμμετοχή σε τέτοιες δραστηριότητες.

Με την αύξηση της ευαισθητοποίησης σχετικά με αυτές τις διατάξεις, ελπίζουμε να προωθήσουμε την καλύτερη κατανόηση του νομικού πλαισίου που περιβάλλει το έγκλημα στον κυβερνοχώρο και να ενθαρρύνουμε μεγαλύτερη επαγρύπνηση και υπεύθυνη χρήση των ψηφιακών τεχνολογιών.

\*\*\*\*\*

© Γεώργιος Αθ. Γέρμανος

Αθήνα, Απρίλιος 2023

ISBN 978-618-00-4517-8

## **Άρθρο 13**

### **Έννοια όρων του Κώδικα**

Στον Κώδικα οι ακόλουθοι όροι χρησιμοποιούνται με την εξής σημασία: [...]

στ) **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.

ζ) **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.

η) **Μέσο πληρωμής πλην των μετρητών** είναι άυλος ή υλικός προστατευμένος μηχανισμός, αντικείμενο ή αρχείο ή συνδυασμός τους, εκτός από το νόμιμο νόμισμα, ο οποίος επιτρέπει, μόνος του ή σε συνδυασμό με διαδικασία ή σειρά διαδικασιών, στον κάτοχο ή στον χρήστη του να μεταφέρει χρήματα ή νομισματική αξία, μεταξύ άλλων, μέσω ψηφιακών μέσων συναλλαγής. Ως «προστατευμένος μηχανισμός, αντικείμενο ή αρχείο» νοείται μηχανισμός, αντικείμενο ή αρχείο που προστατεύεται από την απομίμηση ή δόλια χρήση, για παράδειγμα μέσω σχεδιασμού, κωδικοποίησης ή υπογραφής. [...]

\*\*\*\*\*

## **Άρθρο 292Α**

### **Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών**

1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, και με τον τρόπο αυτόν θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή. Αν ο υπαίτιος της πράξης του προηγούμενου εδαφίου είναι ο εργαζόμενος ή συνεργάτης του παρόχου υπηρεσιών τηλεφωνίας, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή. Με την ποινή του προηγούμενου εδαφίου τιμωρείται και ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπός του ο οποίος αθέμιτα θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών.

2. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού, ο οποίος παραβιάζει διάταξη κανονισμού της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ή όρο της Γενικής Άδειας ή του δικαιώματος χρήσης ραδιοσυχνότητας ή του δικαιώματος χρήσης αριθμού, που αναφέρονται στην ασφάλεια των ηλεκτρονικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή.

3. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού ή ο κατά τον νόμο υπεύθυνος για τη διασφάλιση του απορρήτου των επικοινωνιών, που παραλείπει να λάβει τα αναγκαία μέτρα για την αποτροπή πράξης της παρ. 1, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή, εφόσον η πράξη τελέστηκε ή έγινε απόπειρα τέλεσής της, ανεξάρτητα αν θα τιμωρηθεί ο υπαίτιος.

4. Αν ο υπαίτιος των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον, τιμωρείται με φυλάκιση τουλάχιστον τριών (3) ετών και χρηματική ποινή. Εφόσον το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, ο υπαίτιος τιμωρείται με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή. Αν από τις πράξεις των προηγούμενων παραγράφων μπορεί να τεθούν σε κίνδυνο θεμελιώδεις αρχές και θεσμοί του Πολιτεύματος, όπως μνημονεύονται στο άρθρο 134 του Ποινικού Κώδικα ή απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή στην ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.

5. Οποιος αθέμιτα διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει προς εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων της παρ. 1 ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση έως δύο (2) έτη ή χρηματική ποινή.

\*\*\*\*\*

## **Άρθρο 292B**

### **Παρακώλυση λειτουργίας πληροφοριακών συστημάτων**

1. Οποιος 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 και χρηματική ποινή.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή, 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 ζημιές 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 δύο ετών και χρηματική ποινή, αν προκάλεσε σοβαρές ζημιές και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή, 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.

\*\*\*\*\*

## **Άρθρο 292Γ**

Με φυλάκιση έως δύο έτη ή χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292B 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 292 B, 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.

\*\*\*\*\*

## **Άρθρο 292Δ**

### **Προσβολές του απορρήτου των τηλεπικοινωνιών του κοινού**

1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, εάν από την πράξη μπορεί να προκύψει κοινός κίνδυνος για το απόρρητο του περιεχομένου τηλεφωνικών ή ηλεκτρονικών επικοινωνιών ή των στοιχείων της θέσης ή κίνησης αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.

2. Αν ο δράστης της πράξης της προηγούμενης παραγράφου είναι πάροχος υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος της διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή αποβλέπει να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος επιβάλλεται φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή.

\*\*\*\*\*

## **Άρθρο 292Ε**

### **Παρακώλυση των τηλεπικοινωνιών**

1. Όποιος παρεμποδίζει ή διαταράσσει σε μεγάλη έκταση ή για μεγάλο χρονικό διάστημα τη λειτουργία εγκατάστασης παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικών επικοινωνιών και ιδίως του διαδικτύου με αθέμιτη παρέμβαση σε πράγμα ή σε

σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία αυτής, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.

2. Η παράγραφος 2 του προηγούμενου άρθρου εφαρμόζεται και για την πράξη της παραγράφου 1.

3. Αν η πράξη τελέστηκε από αμέλεια, επιβάλλεται χρηματική ποινή ή παροχή κοινωφελούς εργασίας.

\*\*\*\*\*

## **Άρθρο 370Α**

### **Παραβίαση του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας**

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών σταθερής ή κινητής τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή δεδομένα επικοινωνίας (κίνησης και θέσης) τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον, χωρίς τη ρητή συναίνεση του τελευταίου.

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο



της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.

3. Όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή.

5. Αν οι πράξεις των παραγράφων 1 και 3 συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.

\*\*\*\*\*

## **Άρθρο 370B**

### **Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα**

1. Όποιος κατά παράβαση μέτρου προστασίας και χωρίς δικαίωμα αποκτά πρόσβαση σε μέρος ή στο σύνολο συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή. Σε ιδιαίτερα ελαφρές περιπτώσεις η πράξη μένει ατιμώρητη.

2. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του συστήματος πληροφοριών ή των δεδομένων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.
3. Αν η πράξη της παραγράφου 1 αναφέρεται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή.
4. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας, επιβάλλεται φυλάκιση και χρηματική ποινή.
5. Για την ποινική δίωξη των πράξεων των παραγράφων 1 και 4 απαιτείται έγκληση.

\*\*\*\*\*

### **Άρθρο 370Γ**

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.
2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Οι πράξεις που προβλέπονται στο άρθρο αυτό διώκονται με έγκληση.

\*\*\*\*\*

### **Άρθρο 370Δ**

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.

2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του, τιμωρείται με φυλάκιση.

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.

\*\*\*\*\*

### **Άρθρο 370Ε**

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 περιεχόμενό 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.

3. Αν οι πράξεις των παραγράφων 1 και 2 συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου, επιβάλλεται κάθειρξη.

\*\*\*\*\*

## **Άρθρο 370ΣΤ**

### **Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων**

1. Με φυλάκιση τουλάχιστον δύο (2) ετών τιμωρείται όποιος παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, εξάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί λογισμικά ή συσκευές παρακολούθησης, με δυνατότητα υποκλοπής, καταγραφής και κάθε είδους άντλησης περιεχομένου ή και δεδομένων επικοινωνίας (κίνησης και θέσης), με τα οποία μπορούν να τελεσθούν οι πράξεις του άρθρου 370Α.

2. Με φυλάκιση τουλάχιστον δύο (2) ετών τιμωρείται όποιος, χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ, των παραγράφων 2 και 3 του άρθρου 370Δ και του άρθρου 370Ε, παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, εξάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί 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.

\*\*\*\*\*

## **Άρθρο 379**

### **Φθορά ψηφιακών δεδομένων**

1. 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 δύο (2) έτη και χρηματική ποινή. Αν η ζημία που προκλήθηκε είναι ελαφρά, ο υπαίτιος τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.

2. Η πράξη της παρ. 1 τιμωρείται: α) με φυλάκιση έως τρία (3) έτη και χρηματική ποινή, αν επλήγη μεγάλος αριθμός πληροφοριακών συστημάτων και η πράξη τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για τον σκοπό αυτόν, β) με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή, αν προκάλεσε σοβαρές ζημιές και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, ή αν τελέστηκε κατά πληροφοριακών συστημάτων 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. Με φυλάκιση έως δύο (2) έτη και χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη του εγκλήματος της παρ. 1 κατασκευάζει, κατέχει, εισάγει ή διαθέτει: α) συσκευές ή πληροφοριακά συστήματα, πρωτίστως σχεδιασμένα ή ειδικά προσαρμοσμένα για τον σκοπό της διάπραξης του εγκλήματος της παρ. 1 ή 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. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση τις παραπάνω συσκευές ή προγράμματα υπολογιστή ή δεδομένα πριν τα χρησιμοποιήσει για τη διάπραξη του εγκλήματος του προηγούμενου εδαφίου.

\*\*\*\*\*

## **Άρθρο 379Α**

### **Διακεκριμένες περιπτώσεις στο πλαίσιο εγκληματικής οργάνωσης**

Τα πλημμελήματα της παρ. 1 του άρθρου 372 και του πρώτου εδαφίου της παρ. 1 του άρθρου 375 που αφορούν σε υλικά μέσα πληρωμής πλην των μετρητών, καθώς και των παρ. 1 και 2 του άρθρου 379, όταν τελούνται στο πλαίσιο εγκληματικής οργάνωσης, τιμωρούνται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή.

\*\*\*\*\*

## **Άρθρο 386Α**

### **Απάτη με υπολογιστή**

1. Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή:

- α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή,
- β) με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα,

γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας,

δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας, ή

ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.

Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

2. Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή πληροφοριακό σύστημα που προορίζεται για τη διάπραξη του εγκλήματος της παρ. 1 τιμωρείται με φυλάκιση έως δύο (2) έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή πληροφοριακό σύστημα πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 1.

3. Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του Ελληνικού Δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι (20) έτη. ■

[www.thecybercrimebook.gr](http://www.thecybercrimebook.gr)

ISBN 978-618-00-4517-8

