Ευαγγελία Βαγενά, Δικηγόρος, ΔΝ DEA Droit et Informatique

ΔΙΚΑΙΟ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Διαδικτυακή παρουσία- ιστοσελίδες- Domain name

DNS

Domain Name System (DNS): Αντιστοιχία διεύθυνσης με μοναδικό όνομα

- xxx.xxx.xxx.xxx
- (32 bit - IP address) πχ. 132.43.20.34

με χρήση ειδικής βάσης δεδομένων σε ειδικό server

- 13 παγκόσμιοι root servers (7 στις ΗΠΑ)

http://www.bro.org.gr

- hypertext transfer protocol
- Top Level Domain (TLD): .gr – country code top level domain/ ccTLD
- Second Level Domain: .org –generic top level domain/ gTLD
- Third level domain name: bro

Διεθνές επίπεδο

Εώς το 1997

IANA: Internet Assigned Numbers Authority/ ΗΠΑ

ΑΡΧΙΚΑ: 7 g(eneric) TLD: .mil .gov .int .edu .net .com .org

Από το 1998

ICANN: Internet Corporation for Assigned Names and Numbers - www.icann.org = διεθνής μη κερδοσκοπικός οργανισμός

- aero, arpa, asia, biz, cat, coop, info, jobs, museum, mobi, name, pro, tel, travel
- Χορηγοί (sponsored gTLD)

*UDRP= Uniform Domain-Name Dispute-Resolution Policy

Διαπιστευμένοι φορείς από τον ICANN, όπως WIPO Arbitration and Mediation Center

Εθνικό επίπεδο

ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων)

www.eett.gr (αρ. 12 παρ. κδ΄ Ν. 4070/2012):

«...πόροι του Ελληνικού Κράτους, που εκχωρούνται κατά χρήση στην ΕΕΤΤ ...»

Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr ή .ελ (Απόφαση 843/2/01-03-2018) της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων

Τροποποίηση του Κανονισμού Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr ή .ελ (Απόφαση 852/5/21-05-2018) της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων

Απόφαση ΕΕΤΤ 750/2/19.02.2015- Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr και άλλες διατάξεις

- Από τις 24 Ιανουαρίου 2016 το Μητρώο Ονομάτων Internet .gr παρέχει την **Υπηρεσία Αυξημένης Ασφάλειας** (ΥΑΑ): Με την ενεργοποίηση της υπηρεσίας για ένα όνομα χώρου δεν επιτρέπονται μεταβολές στα στοιχεία του (και στα στοιχεία τυχόν ενεργοποιημένων δεσμευμένων μορφών του) ή άλλες πράξεις επί του ονόματος χώρου (π.χ. αλλαγές στοιχείων δικαιούχου, διαγραφή του ονόματος, μεταβολές ή/και διαγραφές θυγατρικών εξυπηρετητών του, αλλαγές εγγραφών DS της τεχνολογίας DNSSEC). Αλλαγές σε ένα όνομα χώρου με ενεργή Υπηρεσία Αυξημένης Ασφάλειας επιτρέπονται μόνο εφόσον ζητηθεί από τον δικαιούχο του ονόματος χώρου και για συγκεκριμένο χρονικό διάστημα, το οποίο ο ίδιος θα ορίσει. Για την επαλήθευση σχετικού αιτήματος του δικαιούχου, το Μητρώο αποστέλλει ξεχωριστά στον δικαιούχο και τον καταχωρητή του ονόματος χώρου από έναν κωδικό. Η επαλήθευση του αιτήματος επιτυγχάνεται με την διαβίβαση και των δύο αυτών κωδικών από τον καταχωρητή στο Μητρώο.

Άρθρο 7: γεωγραφικοί όροι (ΟΤΑ), δημόσια τάξη & χρηστά ήθη, κρατικά και θρησκευτικά σύμβολα κλπ.

Εθνικό επίπεδο

Κοινόχρηστα Ονόματα Χώρου με κατάληξη .gr

- .com.gr : Για όσους ασκούν εμπορική δραστηριότητα (εταιρίες ή ατομικές επιχειρήσεις)
- .edu.gr : Για εκπαιδευτικούς οργανισμούς
- .net.gr : Για παρόχους Υπηρεσιών Διαδικτύου (I.S.P.'s) και παρόχους δικτύων
- .org.gr : Για μη κυβερνητικούς Οργανισμούς
- .gov.gr : Για κυβερνητικούς Οργανισμούς

First come, first served

Αρχή της χρονικής προτεραιότητας

Το δικαίωμα αποκτάται με την εκχώρηση, ανατρέχει όμως στον χρόνο υποβολής της αίτησης εκχώρησης στο μητρώο της ΕΕΤΤ

Απόρριψη: Αν συντρέχει κάποιος λόγος απόρριψης π.χ.

- Γεωγραφικό όνομα
- Όνομα που αντίκειται στη δημόσια τάξη / χρηστά ήθη
- Αίτηση έγινε με προφανή κακοπιστία

Νομικός χαρακτηρισμός

Διακριτικά γνωρίσματα: ενδείξεις που ***εξατομικεύουν και διακρίνουν*** στις συναλλαγές το πρόσωπο που ασκεί εμπορική δραστηριότητα και τα μέσα που χρησιμοποιεί, δηλ. την επιχείρηση και τα εμπορεύματα ή προϊόντα που αυτή θέτει σε κυκλοφορία ή παράγει

Ν.146/14 περί αθεμίτου ανταγωνισμού (αστικές & ποινικές κυρώσεις)

Domain name ως διακριτικό γνώρισμα

Η εκχώρηση ενός ονόματος χώρου δεν συνεπάγεται αυτοδίκαια την απόκτηση δικαιώματος διακριτικού γνωρίσματος επιχείρησης, αλλά πρέπει να συντρέχουν **οι προϋποθέσεις απόκτησής του**, σύμφωνα με τις ισχύουσες διατάξεις (π.χ. διακριτική δύναμη, χρησιμοποίηση στις συναλλαγές κ.λ.π.)

Σε περίπτωση σύγκρουσης, υπερισχύει εκείνο από τα γνωρίσματα, το οποίο ***καθιερώθηκε πρώτο στις συναλλαγές***

Σύγκρουση Ονόματος Χώρου με Δικαίωμα Τρίτου;

- Προστασία δικαιούχου προηγούμενων δικαιωμάτων επί του σημείου που συνθέτει το όνομα χώρου
  - Δικαστήρια → Προσωρινή απενεργοποίηση ή οριστική διαγραφή ονόματος χώρου
  - ΕΕΤΤ → Διαγραφή, κατόπιν ακροάσεως, εάν συντρέχει περίπτωση:

    -αίτησης εκχώρησης αντίθετης στην καλή πίστη

    -χρήσης η οποία είναι κακόπιστη ή αντίθετη στην καλή πίστη

Ενδεικτικές περιπτώσεις κακοπιστίας:

- Καταχώρηση με σκοπό την πώληση/ εκμίσθωση / μεταβίβαση σε κάτοχο δικαιωμάτων επί του ονόματος (π.χ. σήμα, διακριτικός τίτλος, επωνυμία)
- Καταχώρηση με σκοπό την παρεμπόδιση των εργασιών ανταγωνιστή
- Καταχώρηση με σκοπό την χωρίς έννομο δικαίωμα εκμετάλλευση της φήμης/ αναγνωρισιμότητας ενός ονόματος επί του οποίου έχει θεσπισθεί ή αναγνωρισθεί προηγούμενο δικαίωμα τρίτου (π.χ. σήμα, διακριτικός τίτλος κλπ)

Δικαίωμα επί DN

Αποκλειστικό δικαίωμα **χρήσης**

Ο,τι **περιεχόμενο** θέλει στην ιστοσελίδα του ΕΚΤΟΣ ΑΝ .com, edu, gov κλπ (βλ. παράρτημα Γ, κανονισμού ΕΕΤΤ)

Ελεύθερη **μεταβίβαση** με προηγούμενη απόφαση ΕΕΤΤ (αίτηση μεταβίβασης)

Διάρκεια ισχύος: 2 χρόνια από την υποβολή της αίτησης εκχώρησης

- 3 εργάσιμες ημέρες πριν τη λήξη: Ανανέωση με αίτηση στον Καταχωρητή
- 15 ημέρες μετά τη λήξη: Αποκλειστικό δικαίωμα υποβολής αίτησης εκχώρησης από τον προηγούμενο Φορέα του Ονόματος Χώρου

Δεσμεύονται για τον Φορέα:

- Ονόματα χώρου που φέρουν σημεία στίξης σε διαφορετικά σημεία από αυτά της πεζής μορφής που δηλώνει ο Καταχωρούμενος στην αίτησή του π.χ. *μάτινα.gr / ματινά.gr*
- Ομόγραφα Ονόματα δηλαδή Ονόματα Χώρου που ομοιάζουν οπτικά με την εκχωρηθέν Όνομα Χώρου π.χ. *MATINA.GR (με ελληνικούς χαρακτήρες) MATINA.GR (με λατινικούς χαρακτήρες)*

Οι δεσμευμένες μορφές ενεργοποιούνται κατόπιν αιτήσεως του Καταχωρούμενου χωρίς να απαιτείται Απόφαση της ΕΕΤΤ

Λόγοι διαγραφής

Μη ακριβής αίτηση εκχώρησης, εκτός εάν εκχώρηση μέχρι 30.12.2002

Έλλειψη διακριτικού χαρακτήρα, εκτός εάν εκχώρηση μέχρι 30.12.2002

Συνδρομή κάποιου λόγου απόρριψης, σύμφωνα με α. 8 του Κανονισμού, εκτός εάν εκχώρηση μέχρι 30.12.2002

Μη κοινοποίηση μεταβολής στοιχείων εκχώρησης (π.χ. διεύθυνση Φορέα) εντός 7 ημερών

Αίτηση αντίθετη στην καλή πίστη, εκτός εάν εκχώρηση μέχρι 30.12.2002

Χρήση αντίθετη στην καλή πίστη ή κακόπιστη

Λύση νομικού προσώπου

Θάνατος φυσικού προσώπου, εάν οι εκτελεστές της διαθήκης ή οι νόμιμοι κληρονόμοι δεν ζητήσουν εντός 6 μηνών από την ημερομηνία θανάτου τη μεταβολή ονοματεπωνύμου του Φορέα του Ονόματος Χώρου

Αμετάκλητη απόφαση δημόσιας αρχής ή δικαστηρίου/ απόφαση διαιτητικού οργάνου

Σε περίπτωση παύσης λειτουργίας του Καταχωρητή, εάν δεν ορισθεί νέος Καταχωρητής εντός 90 ημερών από τη σχετική δημοσίευση της παύσης από την ΕΕΤΤ

Το μεταβλητό πεδίο ταυτίζεται με ονομασία δημοτικού διαμερίσματος ή ιστορική επωνυμία Ο.Τ.Α.

Cybersquatting Κυβερνοσφετερισμός

Ελληνικές υποθέσεις:

Amazone.gr (ΜΠρ Σύρου 637/1999)

Google.gr

Rolex.gr

Ταύτιση με προγενέστερα κατοχυρωμένο σήμα τρίτου= σύγχυση στο κοινό

Βλ. Όμως υπόθεση zara.gr

Typosquatting

πρόβλεψη συνηθέστερων λαθών πληκτρολόγησης πολύ γνωστών, ήδη εκχωρημένων διαδικτυακών τόπων

Υποθέσεις:

- Nasdasq.com (αντί Nasdaq)
- Wallsreetjournal.com (αντί Wallsrteetjournal)
- Dosney.com (αντί disney)
- Playstaion.com (αντί playstation)

Ειδικά θέματα adwords

Adwords: σύνδεση λέξεων- πιθανών αναζητήσεων με διαφημιζόμενους

Αν περιλαμβάνουν ονόματα/domain names ανταγωνιστικών επιχειρήσεων; Προσβολή σήματος; Παράνομη χρήση;

Συνήθως νόμιμη πρακτική μηχανών αναζήτησης βλ. όμως αποφάσεις ΔΕΚ 2010

Κρίσιμο στοιχείο: σύγχυση κοινού

Ειδικά θέματα metatags

Πεδίο με λέξεις που εισάγει κανείς οι οποίες χαρακτηρίζουν το περιεχόμενο της ιστοσελίδας/ κωδικοί στη γλώσσα προγραμματισμού οι οποίοι χρησιμοποιούνται από τις μηχανές αναζήτησης για την ταξινόμηση των αποτελεσμάτων ανά θέμα

Λέξεις μαγνήτες ή διακριτικά γνωρίσματα που δεν έχουν σχέση με το περιεχόμενο αλλά προσελκύουν χρήστες (*spamdexing*= spam indexing βλ. και *word stuffing*=αόρατες λέξεις που αναγνωρίζονται από τις μηχανές αναζήτησης)

Υπάρχει προσβολή διακριτικού γνωρίσματος;

Δημιουργείται κίνδυνος σύγχυσης;

Είναι παράνομη πράξη κατά το δίκαιο του αθεμίτου ανταγωνισμού;

Διίστανται οι απόψεις-η πλειοψηφία το δέχεται

Σχετικές δικαστικές αποφάσεις (γερμανικές)

Περισσότερα για domain names:

https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DomainNames/ListOfNews.html

https://grweb.ics.forth.gr/public/faqs

E commerce
Ηλεκτρονικό Εμπόριο

Συναλλαγές μεταξύ:

Business to business/ B2B

Business to consumer/ B2C

Business to administration

User to user

Ηλεκτρονικές συμβάσεις

Οι συμβάσεις που καταρτίζονται με ηλεκτρονικά μέσα ≠ όχι συμβάσεις που συνάπτονται με ατομικά μέσα επικοινωνίας (email κλπ)

Νομοθετικό πλαίσιο

Οδηγία για το ηλεκτρονικό εμπόριο (e commerce directive)- ΠΔ 131/2003

Νομοθεσία για την προστασία του καταναλωτή

E -commerce directive

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των ***υπηρεσιών της κοινωνίας της πληροφορίας****, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)

*= κάθε υπηρεσία που συνήθως παρέχεται εξ αποστάσεως έναντι αμοιβής, μέσω εξοπλισμών ηλεκτρονικής επεξεργασίας συμπεριλαμβανομένης της ψηφιακής συμπίεσης) και αποθήκευσης δεδομένων και κατόπιν ατομικού αιτήματος του αποδέκτη της υπηρεσίας

Οδηγία 2000/31 – ΠΔ 131/03

- Ελεύθερη διακίνηση, υπηρεσιών της Κοινωνίας της Πληροφορίας, μεταξύ των κρατών μελών.
- Αρχή του «κράτους προέλευσης »= για την νόμιμη δραστηριότητα του*

ΠΡΟΟΙΜΙΟ 19 (& νομολογία ΔΕΚ): Ο τόπος εγκατάστασης εταιρείας που παρέχει υπηρεσίες μέσω διεύθυνσης (site) Internet, δεν βρίσκεται εκεί που είναι η τεχνολογία που υποστηρίζει την εν λόγω διεύθυνση ούτε εκεί που παρέχεται πρόσβαση στην εν λόγω διεύθυνση, αλλά εκεί που ασκεί την οικονομική της δραστηριότητα.

*οι συμβάσεις με τους χρήστες- πελάτες διέπονται από το δίκαιο της χώρας διαμονής τους

ΕΞΑΙΡΕΣΕΙΣ :(αρ. 9)

α) επί ακινήτου περιουσίας εκτός από τα δικαιώματα μίσθωσης,

β) εκ του νόμου προσφυγή σε δικαστήρια, δημόσιες αρχές ή επαγγέλματα που ασκούν δημόσια εξουσία (π.χ συμβολαιογράφοι),

γ) στις συμβάσεις εγγυοδοσίας και

δ) στις συμβάσεις οι οποίες εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο.

Οδηγία 2000/31 – ΠΔ 131/03

Αρχή της ***ελεύθερης κυκλοφορίας των υπηρεσιών*** της κοινωνίας της πληροφορίας

- Π.χ αγγλική διαδικτυακή επιχείρηση που πωλεί συσκευές και στη Ελλάδα δεν υποχρεούται να εγγραφεί σε ελληνικό επιμελητήριο στην Ελλάδα εφόσον τηρεί τις προϋποθέσεις νόμιμης άσκησης δραστηριότητας με το αγγλικό δίκαιο και δεν οφείλει να τηρεί τους κανόνες της σύννομης διαφήμισης με βάση το ελληνικό δίκαιο. Τα προϊόντα της όμως οφείλουν να τηρούν και τις προδιαγραφές της ελληνικής νομοθεσίας για την ασφάλεια τους
- Εξαιρέσεις για λόγους πρόληψης/ δίωξης εγκλημάτων, δημόσιας υγείας και ασφάλειας, προστασία καταναλωτή

Αρχή της ***μη αναγκαίας προηγούμενης άδειας***

Νόμος 2251/1994 (όπως ισχύει) προστασία του καταναλωτή

Εφαρμόζονται παράλληλα οι διατάξεις του

Γίνεται δεκτό ότι καλύπτει και το ηλεκτρονικό εμπόριο στο πλαίσιο των συμβάσεων από απόσταση

Σύμβαση από απόσταση= *«κάθε σύμβαση που αφορά αγαθό ή υπηρεσία, η οποία συνάπτεται μεταξύ ενός προμηθευτή και ενός καταναλωτή, χωρίς την ταυτόχρονη φυσική παρουσία τους, στο πλαίσιο ενός συστήματος προμήθειας αγαθών ή παροχής υπηρεσιών από απόσταση, που οργανώνεται από τον προμηθευτή, ο οποίος χρησιμοποιεί, αποκλειστικά, ένα ή περισσότερα μέσα τεχνικής επικοινωνίας από απόσταση μέχρι και τη σύναψη της σύμβασης. Μέσα τεχνικής επικοινωνίας από απόσταση, με την έννοια του άρθρου αυτού, είναι ιδίως τα έντυπα χωρίς παραλήπτη, τα έντυπα με παραλήπτη, οι τυποποιημένες επιστολές, τα διαφημιστικά έντυπα με στέλεχος παραγγελίας, οι κατάλογοι, το τηλέφωνο με ή χωρίς ανθρώπινη παρέμβαση, το ραδιόφωνο, το εικονοτηλέφωνο, το βιντεοτέξτ (μικροϋπολογιστής και τηλεοπτική οθόνη)»* με πληκτρολόγιο ή οθόνη αμφίδρομης επικοινωνίας, το ηλεκτρονικό ταχυδρομείο, η τηλεομοιοτυπία και η τηλεόραση.

Δηλ. καλύπτει εκτός από e commerce και telemarketing, cold calling, κ.ο.κ

Υποχρεώσεις προμηθευτή - Υποχρέωση ενημέρωσης Ι

Γενικές πληροφορίες:

(α) επωνυμία

(β) διεύθυνση

(γ) στοιχεία επικοινωνίας

(δ) τον αριθμό εγγραφής του σε μητρώο (αν προβλέπεται)

(ε) στοιχεία διοικητικής έγκρισης που τυχόν έχει λάβει για τη διάθεση των προϊόντων ή των υπηρεσιών του εφόσον προβλέπεται σχετική διαδικασία

(ζ) αριθμό του ΦΠΑ

Υποχρεώσεις προμηθευτή - Υποχρέωση ενημέρωσης ΙΙ

Ειδικές πληροφορίες (βάσει α. 4 ν.2251/1994) :

1. τα ουσιώδη χαρακτηριστικά του αγαθού ή της υπηρεσίας,
2. την τιμή, την ποσότητα και τις δαπάνες μεταφοράς, καθώς και το φόρο προστιθέμενης αξίας, εφόσον δεν περιλαμβάνεται στην τιμή,
3. τον τρόπο πληρωμής, παράδοσης και εκτέλεσης,
4. τη διάρκεια ισχύος της προσφοράς ή της τιμής,
5. το δικαίωμα υπαναχώρησης και
6. την ελάχιστη διάρκεια ισχύος της σύμβασης στην περίπτωση συμβάσεων για την προμήθεια αγαθών ή υπηρεσιών που επιτελείται διαρκώς ή περιοδικώς.

Επιπλέον, θα πρέπει να αναφέρονται (βάσει ΠΔ 131/2003):

α) τα διάφορα τεχνικά στάδια έως τη σύναψη της σύμβασης,

(β) εάν ο φορέας παροχής υπηρεσιών θα αρχειοθετήσει ή όχι τη σύμβαση μετά τη σύναψη της καθώς και εάν προβλέπεται δυνατότητα πρόσβασης σε αυτήν,

(γ) τα τεχνικά μέσα που θα επιτρέπουν τον εντοπισμό και τη διόρθωση σφαλμάτων ηλεκτρονικού χειρισμού πριν από την ανάθεση της παραγγελίας,

(δ) οι γλώσσες στις οποίες μπορεί να συναφθεί η σύμβαση,

(ε) οι σχετικοί κώδικες δεοντολογίας στους οποίους υπόκειται, καθώς και τα στοιχεία που επιτρέπουν την πρόσβαση στους εν λόγω κώδικες με ηλεκτρονικά μέσα.

Υποχρεώσεις προμηθευτή Υποχρέωση εγγραφής σε ΓΕΜΗ

*Αρχικά: «Κάθε προμηθευτής, ο οποίος προτίθεται να συνάπτει συμβάσεις από απόσταση, υποχρεούται πριν από την έναρξη της δραστηριότητάς του αυτής να ζητήσει την καταχώρισή του στο **ειδικό μητρώο που τηρείται στο Υπουργείο Ανάπτυξης**. Κανένας προμηθευτής δεν μπορεί να προτείνει τη σύναψη των ανωτέρω συμβάσεων, εάν εντός τριών (3) μηνών από τη δημοσίευση του παρόντος δεν εγγραφεί στο μητρώο αυτό*

Βάσει άρθρο 14 παρ. 4 Ν.4242/2014: ««Κάθε προμηθευτής, ο οποίος προτίθεται να συνάπτει με τους καταναλωτές συμβάσεις από απόσταση αγαθών και υπηρεσιών, υποχρεούται να ζητήσει την καταχώρισή του στο Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.) σύμφωνα με το άρθρο 1 του ν. 3419/2005 - Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.) και Εκσυγχρονισμός της Επιμελητηριακής Νομοθεσίας.»

Σύναψη σύμβασης- Νομικές απαιτήσεις

Κατά την παραγγελία:

- ο φορέας παροχής υπηρεσιών οφείλει να αποστείλει **αποδεικτικό παραλαβής της παραγγελίας** του αποδέκτη χωρίς περιττή καθυστέρηση και με ηλεκτρονικά μέσα,
- -η παραγγελία και το αποδεικτικό παραλαβής θεωρείται ότι έχουν παραληφθεί όταν τα μέρη στα οποία απευθύνονται έχουν **πρόσβαση σ' αυτά**,
- -ο φορέας παροχής οφείλει να θέτει στη διάθεση του αποδέκτη της υπηρεσίας κατάλληλα, αποτελεσματικά και προσιτά μέσα που θα επιτρέψουν να επισημάνει και να διορθώσει τα **λάθη** του κατά τον ηλεκτρονικό χειρισμό πριν από την ανάθεση της παραγγελίας.

ΓΕΝΙΚΟΙ ΟΡΟΙ ΣΥΝΑΛΛΑΓΩΝ (ΓΟΣ)

Όροι που έχουν διατυπωθεί εκ των προτέρων για μελλοντικές συμβάσεις (γενικοί όροι των συναλλαγών), δεν δεσμεύουν τον καταναλωτή, εάν κατά την κατάρτιση της σύμβασης τους αγνοούσε ανυπαιτίως, όπως, ιδίως, όταν ο προμηθευτής δεν του υπέδειξε την ύπαρξή τους ή του στέρησε τη δυνατότητα να λάβει πραγματική γνώση του περιεχομένου τους

Δικαίωμα υπαναχώρησης

Σε κάθε σύμβαση από απόσταση ο καταναλωτής έχει το δικαίωμα να υπαναχωρήσει αναιτιολογήτως εντός δεκατεσσάρων (14) ημερολογιακών ημερών, αν δεν συμφωνήθηκε μεγαλύτερη προθεσμία, επιστρέφοντας το αγαθό στην αρχική του κατάσταση, χωρίς να επιβαρύνεται με οποιαδήποτε δαπάνη, εκτός από τα έξοδα επιστροφής.

*ο προμηθευτής υποχρεούται να επιστρέψει τα ποσά που του κατέβαλε ο καταναλωτής εντός τριάντα (30) ημερολογιακών ημερών.**

**δεν ισχύει για τις διαδικτυακές παρεχόμενες υπηρεσίες ταξιδιωτικών γραφείων*

Πληρωμή στις συναλλαγές μέσω διαδικτύου

Συνήθως

Πιστωτική κάρτα

Ηλεκτρονικό χρήμα

Ηλεκτρονικό χρήμα

Λειτουργικό υποκατάστατο πραγματικού χρήματος

«*οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη*»

- προ-πληρωμένες κάρτες πολλαπλών χρήσεων (e-purse),
- Προ-πληρωμένα προϊόντα λογισμικού, που είναι εγκατεστημένα στη μνήμη η/υ συνδεδεμένου με το Διαδίκτυο (network money)
- Ψηφιακά / Ηλεκτρονικά Μετρητά (Digital Cash / e-Cash)

- Ιδρύματα Ηλεκτρονικού Χρήματος εποπτεία από Τράπεζα της Ελλάδος, ν. 4021/2011
- Ανακοίνωση της Ευρωπαϊκής Αρχής Τραπεζών (EBA) με τίτλο: «Προειδοποίηση προς τους καταναλωτές για τα εικονικά νομίσματα» : http://www.skai.gr/files/1/%CE%B13/eba_2013_01030000_el_tra_eg.pdf

Spamming*

(ανεπιθύμητη ηλεκτρονική επικοινωνία/ unsolicited email)

Εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με ηλεκτρονικό ταχυδρομείο και εφόσον δεν απαγορεύεται, πρέπει να αναγνωρίζεται σαφώς και επακριβώς ευθύς ως περιέλθει σ' αυτόν.

Δύο συστήματα:

Opt-in (ρητή συγκατάθεση),

Opt-out (ρητή αντίθεση)

Ελληνική νομοθεσία: Opt-in (αρ.9 παρ.10 & αρ.4 παρ.6 ν. 2251/1994)

Μητρώο θετικής επιλογής, opt in register (οδ. 2002/58)= η αποστολή emails για απευθείας εμπορική προώθηση, επιτρέπεται μόνο στην περίπτωση συνδρομητών που έχουν δώσει εκ των προτέρων τη συγκατάθεση τους

ΟΜΩΣ αν τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που *αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων* ή υπηρεσιών ή άλλης συναλλαγής, *μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του* προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο *η δυνατότητα να αντιτάσσεται,* με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση (α.11 παρ. 3 ν.3471/2006).

**SPAM=Spiced Pork And Meat, σκετς Monty Pythons ☺ βλ. http://en.wikipedia.org/wiki/Spam_(Monty_Python)*

Διαφήμιση στο διαδίκτυο

Δεν επιτρέπεται (είτε online, είτε offline):

- Παραπλανητική και αθέμιτη διαφήμιση
  - Όταν γίνεται με σκοπό ανταγωνισμού και αντίκειται στα χρηστά ήθη-τιμωρείται βάσει του αρ. 1., ν. 146/1914
  - Απαγορεύεται εις δημοσία γενομένας γνωστοποιήσεις ή ανακοινώσεις προοριζομένας δι ευρύν κύκλον προσώπων, πάσα ανακριβής δήλωσις περί σχέσεων αναφερομένων εις τας κατά το άρθρον 1 συναλλαγάς, ιδία δε περί της ποιότητος, της αρχικής προελεύσεως, του τρόπου της κατασκευής ή της τιμολογήσεως εμπορευμάτων ή βιομηχανικών εργασιών, περί του τρόπου ή της πηγής της προμηθείας, της κατοχής βραβείων ή άλλων τιμητικών διακρίσεων, περί της αιτίας ή του σκοπού της πωλήσεως ή περί του ποσού των προς διάθεσιν εμπορευμάτων, ικανή να παραγάγη την εντύπωσιν ιδιαιτέρας, ευνοϊκής προσφορά
- Αθέμιτες εμπορικές πρακτικές = παραπλανητικές ή επιθετικές,
  - α. 9 α- 9θ ν.2251/1994 (βλ. σημειώσεις διαφάνειας)

Συγκριτική διαφήμιση: επιτρέπεται (α. 9 παρ. 2 ν.2251/1994, βλ. σημειώσεις διαφάνειας)

Εξωδικαστική επίλυση διαφορών

Ίδρυση και Οργάνωση Ειδικών Οργανισμών σε Εθνικό Επίπεδο, για τη διαμεσολάβηση μεταξύ προμηθευτών και καταναλωτών.

- Φιλική επίλυση διαφορών τους χωρίς προσφυγή στα δικαστήρια
- Αρ. 17. 2000/31/ΕΚ

Ελλάδα

- **Συνήγορος του Καταναλωτή**: Αποτελεί ανεξάρτητη αρχή με στόχο την εξωδικαστική και φιλική διευθέτηση διαφορών μεταξύ προμηθευτών και καταναλωτών, http://www.synigoroskatanaloti.gr/
- **Ευρωπαϊκό Κέντρο Καταναλωτή**: παρέχει πληροφορίες και συμβουλές σε καταναλωτές που πραγματοποιούν αγορές αγαθών και υπηρεσιών στην Ευρωπαϊκή Ένωση. Υπηρετεί την ανάγκη της εξωδικαστικής επίλυσης διαφορών που προκύπτουν σε διασυνοριακές συναλλαγές μεταξύ καταναλωτών και προμηθευτών που βρίσκονται σε διαφορετικές χώρες της Ευρωπαϊκής Ένωσης καθώς και της Ισλανδίας και Νορβηγίας http://www.synigoroskatanaloti.gr/index_ecc.html
  - **Μεσολαβητής Τραπεζικών - Επενδυτικών Υπηρεσιών (Μ.Τ.Ε.Υ.)**, http://www.hobis.gr/

Βλ. και **ηλεκτρονική επίλυση διαφορών (ΗΕΔ),** Online Dispute Resolution http://europa.eu/rapid/press-release_MEMO-13-193_el.htm

Κανονισμός 2019/1150 (Platforms to Business Regulation -P2B)

για *«την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης»*

“on promoting fairness and transparency for business users of online intermediation services”

Online gambling
Τυχερά παιχνίδια στο διαδίκτυο

ν. 4002/2011- ανεστάλη ωστόσο η ισχύς των διατάξεων σχετικά με τον διαδικτυακό τζόγο ως τα μέσα του 2013

Επιτροπής Εποπτείας και Ελέγχου Παιγνίων (ΕΕΕΠ)- www.gamingcommission.gov.gr

Η διεξαγωγή κι εκμετάλλευση παιγνίων μέσω Διαδικτύου προϋποθέτει την προηγούμενη έκδοση διοικητικής άδειας από την ΕΕΕΠ- **Black list** με όσους ιστότοπους δεν έχουν άδεια ΕΕΕΠ, υποχρέωση ISPs να μπλοκάρουν την πρόσβαση (βλ. 65/8/24.7.2013 απόφασή ΕΕΕΠ)

Η συμμετοχή σε τυχερά παίγνια επιτρέπεται μόνο σε φυσικά πρόσωπα που έχουν συμπληρώσει το **21ο έτος ηλικίας** (βλ. ατομική κάρτα παίκτη)

Ε.Ε.Ε.Π. αριθμ. απόφ. 51/3/26.4.2013 -Τροποποίηση και κωδικοποίηση της υπ' αριθμ. 23/3/23−10−2012 (Β΄ 2952) απόφασης της Ε.Ε.Ε.Π με τίτλο: «*Ρυθμίσεις θεμάτων, τα οποία διέπονται από τον Κανονισμό Διεξαγωγής και Ελέγχου Παιγνίων ως προς την επιβολή διοικητικών κυρώσεων, οι οποίες επιβάλλονται στην περίπτωση παροχής υπηρεσιών τυχερών παιγνίων που διεξάγονται μέσω του διαδικτύου χωρίς την προβλεπόμενη άδεια*»* Βλ. Link στις σημειώσεις

Χρήσιμες διευθύνσεις

https://ec.europa.eu/digital-single-market/en/boosting-e-commerce-eu

https://ec.europa.eu/digital-single-market/en/boosting-e-commerce-eu

http://www.efpolis.gr/el/diasfalisi-oikonomikon-symefronton-katanaloton/ilektroniko-emporio.html

http://www.greekecommerce.gr/

Οδηγία για το ηλεκτρονικό εμπόριο

Ενδιάμεσοι στην κοινωνία της πληροφορίας, μεσάζοντες (intermediaries)=

ιδίως

φορείς παροχής πρόσβασης, access provider

φορείς παροχής φιλοξενίας, web hosts

Θυροφύλακες, gatekeepers

Ευθύνη Παρόχων

Για το περιεχόμενο

Οδηγία για το ηλεκτρονικό εμπόριο

Καθεστώς ασυλίας= για να μην αποθαρρυνθούν οι ενδιάμεσοι από την διακίνηση των πληροφοριών και συνεπώς την ανάπτυξη του ηλεκτρονικού εμπορίου

Το «ανεύθυνο» των ενδιαμέσων

- Απλή μετάδοση
  Άρθρο 12 Οδηγίας – 11 ΠΔ 131/03

- Αποθήκευση σε κρυφή μνήμη
  Άρθρο 13 Οδηγίας – 12 ΠΔ 131/03

- Φιλοξενία
  Άρθρο 14 Οδηγίας – 13 ΠΔ 131/03

- Απουσία γενικής υποχρέωσης ελέγχου
  Άρθρο 15 Οδηγίας - 14 ΠΔ 131/03

- Υπερσύνδεσμοι /Μηχανισμοί έρευνας
  Άρθρο 21 παρ. 2 Οδηγίας

Απλή μετάδοση (e commerce directive)

[…] δεν υφίσταται ευθύνη του φορέα παροχής υπηρεσιών όσον αφορά τις μεταδιδόμενες πληροφορίες, υπό τους όρους ότι ο φορέας παροχής υπηρεσιών:

α) δεν αποτελεί ***την αφετηρία της μετάδοσης*** των πληροφοριών,

β) δεν επιλέγει τον ***αποδέκτη της μετάδοσης*** και

γ) ***δεν επιλέγει και δεν τροποποιεί*** τις μεταδιδόμενες πληροφορίες.

[…] Το παρόν άρθρο δεν θίγει τη δυνατότητα να επιβληθεί δικαστικά ή διοικητικά στον φορέα παροχής υπηρεσιών η παύση ή η πρόληψη της παράβασης.

Ζητήματα απλής μετάδοσης

Αφετηρία της μετάδοσης

- Τεχνική mirroring?αναμεταδίδει τότε ή από αυτόν εκκινούν οι πληροφορίες;

Επιλογή αποδέκτη μετάδοσης

- Προγράμματα αθροιστές; π.χ. RSS feed ποιος επιλέγει τότε ο χρήστης αποδέκτης ή ο υπολογιστής αποστολέας των πληροφοριών;

Επιλογή & τροποποίηση πληροφοριών

- Βλ. ελληνική υπόθεση: κάτοχος BBS , bulletin Board System έχει ενεργητικό όχι παθητικό ρόλο αφού επιλέγει και διακινεί έναντι αμοιβής τις πληροφορίες (ΑΠ 2087/2003- παιδική πορνογραφία)

Αυτόματη, ενδιάμεση και προσωρινή αποθήκευση πληροφοριών

- Αν υπάρχει καταστρατήγηση ή τυχόν συνεργασία με χρήστη για διάπραξη παράνομων πράξεων, δεν θα υπάρχει ασυλία

Αποθήκευση σε κρυφή μνήμη - Caching

1[…] δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας, όσον αφορά την ***αυτόματη, ενδιάμεση και προσωρινή αποθήκευση*** των πληροφοριών, η οποία γίνεται με αποκλειστικό ***σκοπό να καταστεί αποτελεσματικότερη η μεταγενέστερη μετάδοση των πληροφοριών*** προς άλλους αποδέκτες της υπηρεσίας, κατ' αίτηση τους, υπό τους όρους ότι ο φορέας παροχής υπηρεσιών:

(α) ***δεν τροποποιεί*** τις πληροφορίες,

(β) τηρεί ***τους όρους πρόσβασης*** στις πληροφορίες [σ.σ.: οι δικαιούμενοι υπό τους όρους της νομοθεσίας για την προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών],

(γ) τηρεί τους κανόνες που αφορούν την ***ενημέρωση των πληροφοριών***, οι οποίοι καθορίζονται κατά ευρέως αναγνωρισμένο τρόπο και χρησιμοποιούνται από τον κλάδο [σ.σ. ενημέρωση των δεδομένων από τον υπεύθυνο της επεξεργασίας, βλ. δίκαιο προστασίας προσωπικών δεδομένων +ειδικά πρωτότυπα πρωτοκόλλου http για πρόσφατες τροποποιήσεις όπως έλεγχος ημερομηνίας επικεφαλίδας δεδομένων, νεκρό γράμμα δεν υπάρχουν επίσημοι κανόνες],

(δ) δεν παρεμποδίζει τη ***νόμιμη χρήση της τεχνολογίας***, η οποία αναγνωρίζεται και χρησιμοποιείται ευρέως από τον κλάδο, προκειμένου να αποκτήσει ***δεδομένα σχετικά με τη χρησιμοποίηση*** των πληροφοριών [σ.σ.: στατιστικά δεδομένα χρήσης], και

(ε) ενεργεί άμεσα προκειμένου να ***αποσύρει τις πληροφορίες*** που αποθήκευσε ή να ***καταστήσει την πρόσβαση σε αυτές αδύνατη***, μόλις αντιληφθεί ότι οι πληροφορίες ***έχουν αποσυρθεί*** από το σημείο του δικτύου στο οποίο βρίσκονταν αρχικά ή η πρόσβαση στις πληροφορίες κατέστη αδύνατη ή ***μια δικαστική ή διοικητική αρχή διέταξε την απόσυρση*** των πληροφοριών ή απαγόρευσε την πρόσβαση σε αυτές.

Φιλοξενία (e commerce directive)

1. Σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας συνισταμένης στην *αποθήκευση πληροφοριών* παρεχομένων από ένα αποδέκτη υπηρεσίας, δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας για τις πληροφορίες *που αποθηκεύονται μετά από αίτηση αποδέκτη της υπηρεσίας*, υπό τους όρους ότι:

(α) ο φορέας παροχής της υπηρεσίας ***δεν γνωρίζει πραγματικά*** ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία και ότι, σε ό,τι αφορά αξιώσεις αποζημιώσεως, δεν γνωρίζει τα γεγονότα ή τις περιστάσεις από τις οποίες προκύπτει η παράνομη δραστηριότητα ή πληροφορία, ή

(β) ο φορέας παροχής της υπηρεσίας, μόλις αντιληφθεί τα προαναφερθέντα, ***αποσύρει ταχέως τις πληροφορίες*** ή καθιστά την πρόσβαση σε αυτές αδύνατη.

2. Η παράγραφος 1 δεν εφαρμόζεται όταν ο αποδέκτης της υπηρεσίας ενεργεί υπό την εξουσία ή υπό τον έλεγχο του φορέα παροχής της υπηρεσίας *[σ.σ. προστηθέντες, βοηθοί εκπλήρωσης για παράδειγμα*]

Ζητήματα φιλοξενίας

Πραγματική γνώση=???

- Με βάση τις κοινές διατάξεις δικαίου για δόλο ή αμέλεια
- Βλ. κυμαινόμενη νομολογία για τον απαιτούμενο βαθμό γνώσης (ιδίως αλλοδαπή)
- UK:The Electronic Commerce (EC Directive) Regulations 2002
  - Ειδική διάταξη με οδηγίες προς τα δικαστήρια για το τι συνιστά «πραγματική γνώση»
  - Ειδοποίηση από θιγόμενο χρήστη με: α) τα πλήρη στοιχεία και της δ/νση του αποστολέα, β) λεπτομέρειες για την ιστοσελίδα με το επίμαχο περιεχόμενο, γ) λεπτομέρειες για τον χαρακτηρισμό του περιεχομένου ως παράνομου

«Καθιστά αδύνατη την πρόσβαση»

≠ αρχή της ελευθερίας της έκφρασης,

αποτροπή προληπτικής λογοκρισίας

Διαδικασίες γνωστοποίησης & απόσυρσης περιεχομένου

Η οδηγία παροτρύνει τα κράτη μέλη να υιοθετήσουν τέτοιες διαδικασίες

USA: DMCA, Digital Millenium Copyright Act

- «safe harbour» διατάξεις
- δικαιούχος ενημερώνει (notice) υπεύθυνο ιστοσελίδας και αυτός είτε σταματάει πλήρως την παροχή πρόσβασης στην επίμαχη σελίδα, είτε την απομακρύνει πλήρως από το διακομιστή του. Αφού το πράξει, ενημερώνει τον ιδιοκτήτη της. Ο ιδιοκτήτης έχει τότε το δικαίωμα, εάν θεωρεί ότι εσφαλμένα διακόπηκε η πρόσβαση στην ιστοσελίδα του να του το δηλώσει εγγράφως (counter notice). Ο web host ενημερώνει τον δικαιούχο και αν αυτός δεν ακολουθήσει τη δικαστική οδό εναντίων του ιδιοκτήτη της ιστοσελίδας εντός 14 ημερών, τότε ο πάροχος απαιτείται να επαναφέρει το απομακρυσμένο από τη θέση του υλικό (put back procedure).

Φιλανδία (για πνευματική ιδιοκτησία)

UK: οδηγίες ΥπΕξ ια υποβολή Ειδοποιήσεων από αρμόδιες αρχές προς παρόχους φιλοξενίας για περιεχόμενο αντικείμενο στην βρετανική αντιτρομοκρατική νομοθεσία

Απουσία γενικής υποχρέωσης ελέγχου

1. *Οι φορείς παροχής υπηρεσιών* ***δεν έχουν****, […]* ***γενική υποχρέωση ελέγχου*** *των πληροφοριών που μεταδίδουν ή αποθηκεύουν ούτε γενική υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες.*

2. Χωρίς να παραβιάζονται οι διατάξεις περί προστασίας του απορρήτου και των προσωπικών δεδομένων, οι φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας ***είναι υποχρεωμένοι να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές*** *για τυχόν υπόνοιες περί χορηγουμένων παράνομων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους, και να ανακοινώνουν στις αρμόδιες αρχές κατ' αίτηση τους πληροφορίες που διευκολύνουν την εντόπιση αποδεκτών των υπηρεσιών τους με τους οποίους έχουν συμφωνίες αποθήκευσης.*

Βλ. εξαίρεση Σουηδίας για bulletin boards, ηλεκτρονικού χώρους ανάρτησης όπου υπάρχει υποχρέωση ελέγχου

Εξαίρεση Γαλλίας για σύστημα ειδοποίησης για εγκλήματα κατά της ανθρωπότητας, πρόκληση ρατσιστικού μίσους, παιδική πορνογραφία κλπ

ΕΝΝΟΜΗ ΠΡΟΣΤΑΣΙΑ

(α.17 ΠΔ 131/2003)

Εφόσον πιθανολογείται προσβολή δικαιωμάτων προερχομένων από τις υπηρεσίες της κοινωνίας της πληροφορίας, το Μονομελές Πρωτοδικείο διατάσσει ως ***ασφαλιστικό μέτρο*** οποιοδήποτε πρόσφορο μέτρο, ιδίως τη συντηρητική κατάσχεση των αντικειμένων που κατέχονται από τον καθ' ου ή από τρίτον και αποτελούν μέσο τέλεσης ή προϊόν ή απόδειξη της προσβολής.

ΠΡΟΣΦΑΤΗ ΝΟΜΟΛΟΓΙΑ

Υπόθεση Promusicae C-275/06: «..*επιτρέπεται αλλά δεν επιβάλλεται να ζητήσουν προσωπικά δεδομένα*…»

C-236 -238 /08 Google France v Louis Vuitton

C-324/09 L'Oréal v eBay

C-70/2010 Scarlet v SABAM & C-360/2010 SABAM

C C v Netlog (Tiscali , Βέλγιο, τεχνολογικά μέτρα)

Lycos (Ολλανδικό ακυρωτικό),

Totalise plc v Motley Fool (Μεγ. Βρετανία)

Heise Zeitschriften (OLG Dusseldorf)

Γνωμοδοτήσεις Γ. Σανιδά (7/09) , Ι. Τέντε (9/09), Αθ. Κατσιρώδη (5/11)

Συνεργασία παρόχων με διωκτικές αρχές

Οφείλει ο πάροχος να αίρει το απόρρητο των επικοινωνιών και να παραδίδει στις διωκτικές αρχές ή σε τρίτους στοιχεία των συνδρομητών του;

- Α. 4 Ν.2225/1994 με λίστα εγκλημάτων για τα οποία επιτρέπεται η άρση του απορρήτου (ιδιαιτέρως σοβαρά εγκλήματα)
- Αντίθετες γνωμοδοτήσεις Εισαγγελέων Αρείου Πάγου δημιούργησαν σύγχυση στους παρόχους- θεωρούσαν ότι μπορούσε να διευρυνθεί κατ' εντολή τους
- Αντίθετη (στις γνωμοδοτήσεις των Εισαγγελέων) γνώμη της ΑΔΑΕ
- Τελικά επιβεβαίωση σε α. 1 Ν 3917/2011 : *«1. Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών υποχρεούνται να διατηρούν τα δεδομένα του άρθρου 5 που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, όπως αυτά ορίζονται στο άρθρο 4 του ν. 2225/1994 (ΦΕΚ 121 Α')*.»

Υποχρέωση παρόχων να διατηρούν ορισμένα δεδομένα επικοινωνίας χρηστών τους (data retention directive)

Linking

Δεν υπάρχει ρητή νομοθετική πρόβλεψη στο ελληνικό δίκαιο

Ιδιαίτερα προβληματικές περιπτώσεις:

- Deep inking: παράκαμψη homepage, δεν μετράται η επισκεψιμότητα, συνέπειες για διαφημιστική λειτουργία
- Framing: πλαίσιο στο οποίο εμφανίζεται ιστοσελίδα τρίτων χωρίς να διακρίνεται η προέλευση
- Νομολογία αλλοδαπή με προσφυγή στο δικαίωμα του κατασκευαστή βάσης δεδομένων *

Αυστρία, Ισπανία, Πορτογαλία: πλήρης απαλλαγή ευθύνης

Η ελληνική νομολογία ποικίλλει:

- ΤρΠλημΚιλκίς (greekmovies): linking προς σελίδες με έργα δεν προσβάλει δικαίωμα πνευματικής ιδιοκτησίας εφόσον δεν παρακάμπτει τεχνολογικά μέτρα
- ΜΠρΑθ 4042/2010: ιστοσελίδα ραδιοφωνικού σταθμού με σύνδεσμο προς ιστοσελίδα άλλου με μουσικά έργα προσβάλει το δικαίωμα πνευματικής ιδιοκτησίας επί των έργων αυτών

Search engines

Δεν υπάρχει ρητή νομοθετική πρόβλεψη

Η (αλλοδαπή) νομολογία ποικίλλει:

- Γαλλία: υπόθεση UEJF, Licra κατά Yahoo → χρήση φίλτρων στους μηχανισμούς έρευνας
- Βέλγιο: Copiepress κατά Google → google news, google cache παραβίαζαν δικαιώματα πνευματικής ιδιοκτησίας λόγω αναπαραγωγής εφημερίδων, άρθρων και φωτογραφιών

Πληροφορίες & ιστολόγια (blogs)

Ευθύνη με βάση τις ρυθμίσεις για τη «φιλοξενία»

Ελευθερία της έκφρασης ή λογοκρισία

- Ad hoc στάθμιση - Αρχή της αναλογικότητας
- Πρέπει ο διαχειριστής να ελέγχει το περιεχόμενο;

Blogs & νομοθεσία περί τύπου

- ΜΠρΡοδόπης 44/2008 & ΕφΘράκης 91/2012 (ναι)
- ΠΠρΠειρ 27/2009, 4980/2009 (όχι)
- ΠΠρΘεσ 25552/2010 &16790/09 (όχι)

Social networks

Ιδίως ζητήματα προστασίας προσωπικών δεδομένων

Για να είναι δωρεάν πρέπει να καλύπτουν τα έξοδα τους από διαφημίσεις

Ιδιαίτερα ζητήματα προστασίας ανηλίκων (π.χ cyberbulling)

Δικαίωμα στην «ψηφιακή λήθη»;

≠δικαίωμα στην πληροφόρηση

≠δικαίωμα στην ελευθερία της έκφρασης

ΕΞΕΛΙΞΕΙΣ…

Η Επιτροπή για τη Γνωστοποίηση Διαδικτυακής Προσβολής Δικαιωμάτων Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων (ΕΔΠΠΙ) συστήθηκε με τον ν. 4481/2017 και στόχο έχει να διευκολύνει την εξωδικαστική αντιμετώπιση περιπτώσεων διαδικτυακής προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας ή/και συγγενικών δικαιωμάτων.

fake news I

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 596/2014 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 16ης Απριλίου 2014 για την κατάχρηση της αγοράς (κανονισμός για την κατάχρηση της αγοράς) και την κατάργηση της οδηγίας 2003/6/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των οδηγιών της Επιτροπής 2003/124/ΕΚ, 2003/125/ΕΚ και 2004/72/ΕΚ

Π.χ *) δίδει, ή είναι πιθανόν να δώσει* **ψευδείς ή παραπλανητικές ενδείξεις***σχετικά με την προσφορά, τη ζήτηση ή την τιμή ενός χρηματοπιστωτικού μέσου ή ενός σχετικού συμβολαίου άμεσης παράδοσης επί εμπορεύματος ή ενός εκπλειστηριαζόμενου προϊόντος βασιζομένου επί δικαιωμάτων εκπομπής·γ)***διάδοση πληροφοριών διά των μέσων μαζικής ενημέρωσης, συμπεριλαμβανομένου του διαδικτύου, ή με οποιοδήποτε άλλο μέσο, η οποία δίδει, ή είναι πιθανόν να δώσει ψευδείς ή παραπλανητικές ενδείξεις***σχετικά με την προσφορά, τη ζήτηση ή την τιμή ενός χρηματοπιστωτικού μέσου ή ενός συνδεδεμένου με αυτά συμβολαίου άμεσης παράδοσης επί εμπορεύματος ή ενός εκπλειστηριαζόμενου προϊόντος βασιζομένου επί δικαιωμάτων εκπομπής ή διαμορφώνει, ή είναι πιθανόν να διαμορφώσει, την τιμή ενός ή περισσότερων χρηματοπιστωτικών μέσων ή ενός συνδεομένου με αυτά συμβολαίου άμεσης παράδοσης επί εμπορεύματος σε μη κανονικό ή τεχνητό επίπεδο,* **συμπεριλαμβανομένης της διάδοσης φημών,εφόσον το πρόσωπο που τις διέδωσε γνώριζε, ή όφειλε να γνωρίζει, ότι οι πληροφορίες ήταν ψευδείς ή παραπλανητικές***·*

*Α. 23 οι αρμόδιες αρχές έχουν την εξουσία.. ιγ)***να λαμβάνουν όλα τα αναγκαία μέτρα για την ορθή ενημέρωση του κοινού, συμπεριλαμβανομένης της διόρθωσης ψευδών ή παραπλανητικών πληροφοριών που δημοσιοποιήθηκαν, μεταξύ άλλων απαιτώντας από οποιονδήποτε εκδότη ή άλλο πρόσωπο που δημοσίευσε ή διέδωσε ψευδείς ή παραπλανητικές πληροφορίες τη δημοσίευση διορθωτικής δήλωσης.**

Fake news II

Διαταραχή της Πληροφορίας: Προς ένα διεπιστημονικό πλαίσιο για την έρευνα και τη χάραξη πολιτικής», Έκθεση δημοσιευμένη από το Συμβούλιο της Ευρώπης, 27 Σεπτεμβρίου 2017

Μια πολυδιάστατη προσέγγιση της παραπληροφόρησης», Έκθεση της ανεξάρτητης ομάδας υψηλού επιπέδου (High level expert group) για τις ψευδείς ειδήσεις και την διαδικτυακή παραπληροφόρηση για λογαριασμό της Ευρωπαϊκής Επιτροπής, Μάρτιος 2018

«Αντιμετώπιση της παραπληροφόρησης στο διαδίκτυο: μια Ευρωπαϊκή Προσέγγιση», ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ, Βρυξέλλες, 26.4.2018

EU Code of Practice on Disinformation

- ανεξάρτητο δίκτυο επαληθευτών γεγονότων (factcheckers),

Κοινή Διακήρυξη για τα “fakenews", την παραπληροφόρηση και την προπαγάνδα, [Γενεύη / Βιέννη, 3 Μαρτίου 2017

ψευδείς πληροφορίες- παραπληροφόρηση

Ψηφιακή οικονομία: η πολιτική εκτίμηση που οδηγεί στην νομική ρύθμιση

Challenges for the sector in the EU

Two billion people are currently connected to the internet and by 2016, this number will exceed 3 billion – **almost half of the world's population**.

Businesses that fail to get digitally connected will become excluded from the global market.

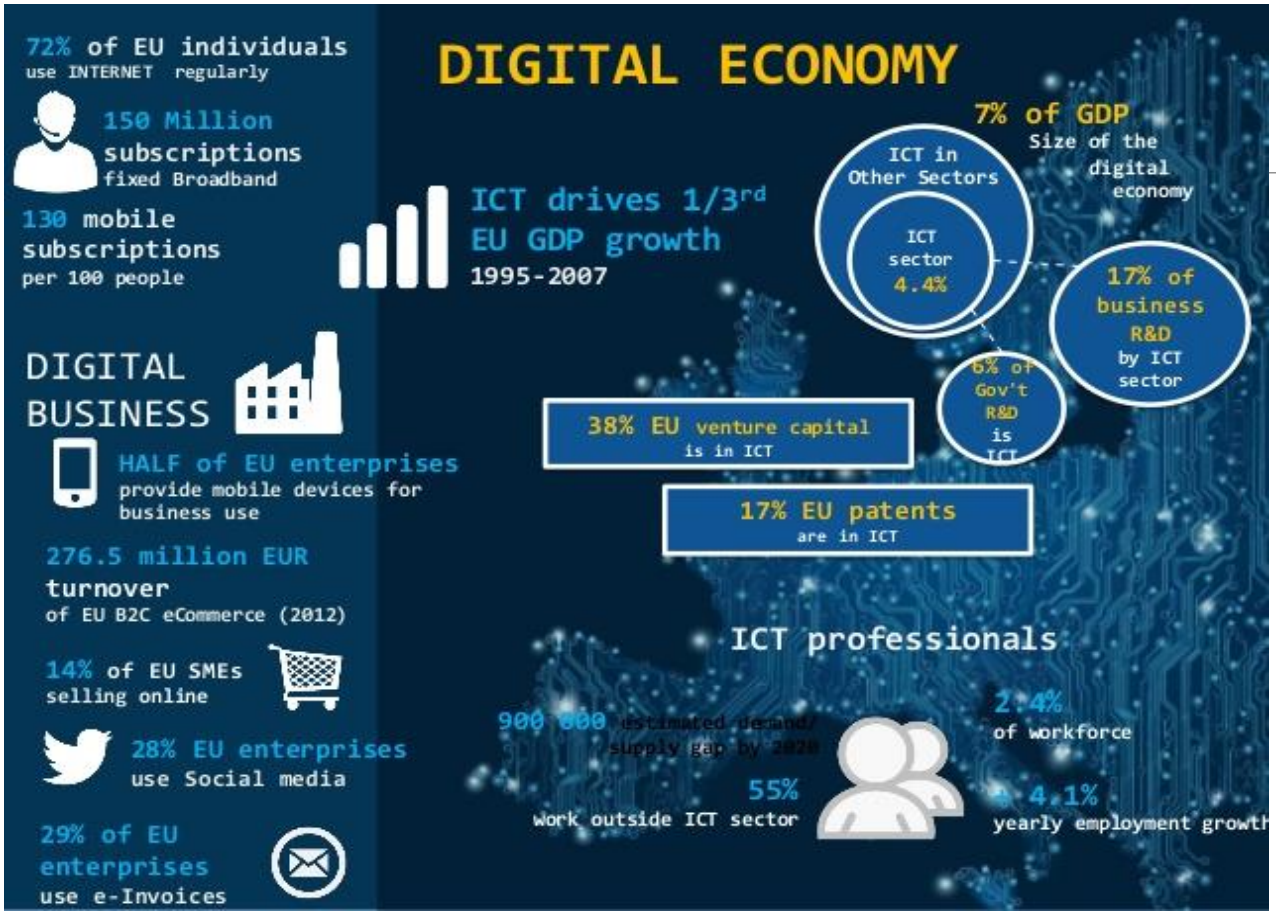
The huge potential of the digital economy is underexploited in Europe, with 41% of enterprises being non-digital, and only two percent taking full advantage of digital opportunities.

New digital opportunities create new business opportunities. Now that **youth unemployment** has risen to over 20% in the EU (and to over 55% in Spain and **Greece**), the growth prospects offered by the digital economy in Europe are promising.

Other regions of the world are already ahead of the game. The digital economy now contributes up to **eight percent of the GDP of the G-20** major economies, powering growth and creating jobs.

Over the last five years, the development of mobile applications alone has created nearly **500 000 new jobs in the US**, implying strong employment growth prospects. That type of growth is not seen across the EU. It is estimated **that 1.5 million additional jobs could be created in the EU** digital economy if it mirrors the performance of the US or Sweden.

Source: https://ec.europa.eu/growth/sectors/digital-economy/importance_en



(Source: http://www.slideshare.net/INCA_NextGen/john-doyle-digital-agenda-for-europe)

Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης

Ψηφιακή ενιαία αγορά είναι εκείνη στην οποία διασφαλίζεται η ελεύθερη κυκλοφορία των εμπορευμάτων, των προσώπων, των υπηρεσιών και των κεφαλαίων και **στην οποία τα άτομα και οι επιχειρήσεις μπορούν**, ανεξαρτήτως της εθνικότητάς τους ή του τόπου κατοικίας τους, **να έχουν αδιάλειπτη πρόσβαση και να ασκούν διαδικτυακές δραστηριότητες σε συνθήκες θεμιτού ανταγωνισμού και με υψηλό επίπεδο προστασίας των καταναλωτών και των δεδομένων προσωπικού χαρακτήρα**.[..]

Η Στρατηγική για την ψηφιακή ενιαία αγορά θα οικοδομηθεί σε τρεις πυλώνες:

- Βελτίωση της πρόσβασης για τους καταναλωτές και τις επιχειρήσεις στα διαδικτυακά αγαθά και υπηρεσίες σε όλη την Ευρώπη — για το σκοπό αυτό απαιτείται να καταργηθούν σύντομα οι βασικές διαφορές μεταξύ του εντός και του εκτός διαδικτύου περιβάλλοντος, ώστε να εξαλειφθούν τα εμπόδια στις διασυνοριακές διαδικτυακές δραστηριότητες.
- Δημιουργία των κατάλληλων συνθηκών για την ανάπτυξη των ψηφιακών δικτύων και υπηρεσιών — **για το σκοπό αυτό απαιτούνται υποδομές και υπηρεσίες περιεχομένου υψηλής ταχύτητας, ασφαλείς και αξιόπιστες, οι οποίες να υποστηρίζονται από κατάλληλο σύνολο κανονιστικών όρων που να ευνοεί την καινοτομία, τις επενδύσεις**, τον θεμιτό ανταγωνισμό και να προσφέρει ισότιμους όρους ανταγωνισμού.
- Μεγιστοποίηση του δυναμικού ανάπτυξης της ευρωπαϊκής ψηφιακής οικονομίας — για το σκοπό αυτό απαιτούνται επενδύσεις σε υποδομές και τεχνολογίες ΤΠΕ, όπως η νεφοϋπολογιστική και τα μαζικά δεδομένα, και στην έρευνα και καινοτομία με στόχο την τόνωση της βιομηχανικής ανταγωνιστικότητας καθώς και τη βελτίωση των δημόσιων υπηρεσιών και των δεξιοτήτων και την αποφυγή των αποκλεισμών.

[Ανακοίνωση Ευρωπαϊκής Επιτροπής, 6.05.2016, COM(2015) 192 final]

Ψηφιακή οικονομία: η δημιουργία των κατάλληλων συνθηκών

«Ενίσχυση της εμπιστοσύνης και της **ασφάλειας** όσον αφορά τις ψηφιακές υπηρεσίες και τον χειρισμό των **δεδομένων προσωπικού χαρακτήρα**»

Ψηφιακή οικονομία: η δημιουργία των κατάλληλων συνθηκών (συνέχεια)

Μόνο το 22 % των Ευρωπαίων έχουν πλήρη εμπιστοσύνη στις εταιρείες όπως οι μηχανές αναζήτησης, οι ιστότοποι κοινωνικής δικτύωσης και οι υπηρεσίες ηλεκτρονικού ταχυδρομείου.

Το 72 % των χρηστών του διαδικτύου ανησυχούν ότι όταν είναι συνδεδεμένοι τους ζητούνται υπερβολικά πολλά δεδομένα προσωπικού χαρακτήρα.

Τι είναι *έγκλημα;*

"πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο"

(α.14 ΠΚ)

«η πράξη εκείνη που θίγει τις αξίες της κοινωνική ζωής στις γενικότερης αποδοχής πλευρές της, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά απόλυτα αναγκαία» [Μαγκάκης]

n.c.n.p.s.l

«nullum crimen nulla poena sine lege»

α. 7 § 1 εδ. ά του Συντάγματος

«Έγκλημα δεν υπάρχει ούτε ποινή επιβάλλεται χωρίς νόμο που να ισχύει πριν από την τέλεση της πράξης και να ορίζει τα στοιχεία της»

Κυβερνοέγκλημα

Ορισμός

Θεσμικό πλαίσιο

Διεθνές / ΕΕ

Ελλάδα

Ψηφιακή εγκληματολογία

Ορισμός κυβερνοεγκλήματος

«κυβερνοεγκληματικότητα» («cybercriminality»), δηλαδή η διάπραξη ποινικών αδικημάτων μέσω του Διαδικτύου […]

Βλ. Αιτιολογική έκθεση ν. 4411/2016

Ορισμός κυβερνοεγκλήματος (συνέχεια)

Ηλεκτρονικό έγκλημα ή έγκλημα με υπολογιστή (computer crime): αφορά φυσική παρέμβαση σε έναν μη συνδεδεμένο υπολογιστή ή υπολογιστές συνδεδεμένους σε τοπικά δίκτυα

«Μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της»

[Forester and Morrison]

Διαδικτυακό έγκλημα (cyber crime): προϋποθέτει την διασύνδεση των υπολογιστικών συστημάτων στο Διαδίκτυο και την τέλεση της πράξης μέσω διαδικτυακής διακίνησης των δεδομένων

Σύγχρονη τάση: «**εγκλήματα πληροφορικής**»

Διακρίσεις*

Α) Εγκλήματα που διαπράττονται **τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο**

π.χ η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελεστεί σε «περιβάλλον internet» τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

Β) Εγκλήματα που διαπράττονται **μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών** (χωρίς την χρήση του διαδικτύου)

Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παράγρ. 1 του Π.Κ., π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή cd-Rom σε ηλεκτρονικό υπολογιστή.

Γ) «**Γνήσια εγκλήματα κυβερνοχώρου**» (cyber crimes)

ποινικοποίηση συμπεριφοράς που έχει αποκλειστικά σχέση με τον κυβερνοχώρο.

Μια τέτοια αξιόποινη συμπεριφορά θα μπορούσε να είναι π.χ η μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου.

*Διάκριση Ι. Αγγελή

ΔΙΑΚΡΙΣΗ ΜΕ ΒΑΣΗ ΤΟΝ ΡΟΛΟ ΤΟΥ Η/Υ

Ο υπολογιστής ως στόχος.

εγκλήματα που αφορούν τη δολιοφθορά των ηλεκτρονικών υπολογιστών ή των δικτύων υπολογιστών, τη δολιοφθορά των λειτουργικών συστημάτων και των προγραμμάτων, την κλοπή των πληροφοριών, τεχνο-βανδαλισμός και τεχνο-παραβίαση

Ο υπολογιστής ως συμβολή του εγκλήματος.

Για παράδειγμα η διαδικτυακή άπατη, απάτες πιστωτικών καρτών, απάτες που περιλαμβάνουν τις ηλεκτρονικές μεταφορές χρημάτων, απάτες τηλεπικοινωνιών και απάτες σχετικά με το ηλεκτρονικό εμπόριο και την ηλεκτρονική ανταλλαγή δεδομένων.

Ο υπολογιστής ως «συνεργός/πλατφόρμα» σε άλλα εγκλήματα.

π.χ. διάδοση ναρκωτικών, ξέπλυμα χρήματος, παράνομες τραπεζικές συναλλαγές, παιδική πορνογραφία, BBSs που υποστηρίζουν την παράνομη δραστηριότητα, τζόγος Διαδικτύου.

Εγκλήματα σχετικά με την εξάπλωση των υπολογιστών

πειρατεία λογισμικού, προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας επί προγραμμάτων υπολογιστών, «πλαστός» εξοπλισμός υπολογιστών αγοράς και προγράμματα.

ΔΙΑΚΡΙΣΗ
ΜΕ ΒΑΣΗ ΠΡΟΣΤΑΤΕΥΟΜΕΝΟ ΕΝΝΟΜΟ ΑΓΑΘΟ

Προσβολές της **ιδιωτικότητας**

- καθαρές προσβολές της ιδιωτικότητας συναντώνται σε περιοχές που ισχύουν και τα παραδοσιακά επαγγελματικά απόρρητα : ιατρικό, δικηγορικό, τραπεζικό. Επίσης τα cookies συνιστούν παράνομη δραστηριότητα.

Αδικήματα κατά της **περιουσίας**

- computer hacking: ο όρος αυτός δηλώνει παραδοσιακά την προσβολή πληροφορικών συστημάτων που δεν γίνεται με σκοπό την manipulation , το σαμποτάζ ή την κατασκοπεία αλλά χάριν της ευχαρίστησης της προσβολής των τεχνικών συστημάτων ασφαλείας.
- Ηλεκτρονική κατασκοπεία: την παράνομη αυτή δραστηριότητα διευκολύνει ιδιαίτερα η σύγκλιση των τεχνολογιών πληροφορικής και τηλεπικοινωνιών.
- Πειρατεία προϊόντων πνευματικής ιδιοκτησίας:
- Σαμποτάζ και εκβίαση : όχι φυσικές ζημιές αλλά ζημιές που χαρακτηρίζονται ως ζημιές στο σύστημα με προγράμματα που καταστρέφουν δεδομένα. Βλ. viruses, worm programs , διάδοση ελαττωματικού λογισμικού
- Ηλεκτρονική απάτη: οι συνήθεις μορφές ψηφιακής απάτης αφορούν την διαχείριση παραστατικών κλπ. που αφορούν την πληρωμή λογαριασμών, μισθών, την κίνηση λογαριασμών τραπεζών κλπ.

Παράνομο και αθέμιτο/επιβλαβές **περιεχόμενο**:

π.χ. παιδική πορνογραφία, διάδοση μισαλλόδοξου λόγου στα διεθνή δίκτυα. Προβλήματα δίωξης, έλλειψη αρμοδιότητας και δικαιοδοσίας, ανωνυμία, τεχνική κάλυψη που εξασφαλίζουν συστήματα όπως οι anonymous remailers (βλ. γαλλική υπόθεση YAHOO).

Διάκριση βάσει σύμβασης για το Κυβερνοέγκλημα Σύμβαση 185 Συμβουλίου της Ευρώπης, Βουδαπέστη 23.11.2001

- Εγκλήματα κατά της **Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των Δεδομένων και Συστημάτων**
- Εγκλήματα που σχετίζονται με **Η/Υ**
- Εγκλήματα που σχετίζονται με το **Περιεχόμενο** των Δεδομένων
- Εγκλήματα κατά της **Πνευματικής Ιδιοκτησίας** και των Συγγενών Δικαιωμάτων
- Ψηφιακή εγκληματολογία

Συνοπτικό περιεχόμενο Σύμβασης Βουδαπέστης

διατάξεις ***ουσιαστικού ποινικού δικαίου***

- τη διαφύλαξη των αποθηκευμένων δεδομένων σε έναν υπολογιστή
- τη διαφύλαξη και γνωστοποίηση των μεταδιδόμενων δεδομένων
- την παροχή πληροφοριών
- την έρευνας και την κατάσχεση αποθηκευμένων στοιχείων
- με την πραγματικού χρόνου συλλογή διακινουμένων δεδομένων
- την παρακολούθηση – υποκλοπή του περιεχομένου δεδομένων

διατάξεις ***ποινικού δικονομικού δικαίου*** αλλά και ***διεθνούς συνεργασίας***

- δυνατότητα των Δικαστικών και Αστυνομικών Αρχών να διεξάγουν τις *έρευνές τους «σε πραγματικό χρόνο»* ("in real time")
  - ταχεία διατήρηση των δεδομένων (α.29), αποκάλυψη των δεδομένων (α. 30), των ερευνών και κατασχέσεων αποθηκευμένων δεδομένων

Σε τί αφορά το Πρόσθετο Πρωτόκολλο της Σύμβασης της Βουδαπέστης;

Διευρύνεται το πεδίο εφαρμογής της Σύμβασης για το έγκλημα στον Κυβερνοχώρο, προκειμένου να αντιμετωπισθούν και **ξενοφοβικής και ρατσιστικής φύσης πράξεις**

= 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 ή εθνική ή εθνοτική καταγωγή, τη θρησκεία*

ΣΥΜΒΑΣΗ ΓΙΑ ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ
ΣΥΜΒΑΣΗ 185 ΣΥΜΒΟΥΛΙΟΥ ΕΥΡΩΠΗΣ, ΒΟΥΔΑΠΕΣΤΗ 23.11.2001

- ✓Πλήρες κείμενο: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

- ✓Η Ελλάδα την έχει υπογράψει και την κύρωσε με νόμο το 2016

Συνηθέστερα εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο

Άρθρο 333. Απειλή

1. Όποιος προκαλεί σε άλλον τρόμο ή ανησυχία απειλώντας τον με βία ή άλλη παράνομη πράξη ή παράλειψη τιμωρείται με φυλάκιση μέχρι ενός έτους ή με χρηματική ποινή. 2. Για την ποινική δίωξη απαιτείται έγκληση.

Άρθρο 361. Εξύβριση

1. Όποιος, εκτός από τις περιπτώσεις της δυσφήμησης (άρθρα 362 και 363), προσβάλλει την τιμή άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλο τρόπο, τιμωρείται με φυλάκιση μέχρι ενός έτους ή με χρηματική ποινή. Η χρηματική ποινή μπορεί να επιβληθεί και μαζί με την ποινή της φυλάκισης. 2. Όταν η προσβολή της τιμής δεν είναι ιδιαίτερα βαριά αν ληφθούν υπόψη οι περιστάσεις και το πρόσωπο του ατόμου που προσβλήθηκε, ο υπαίτιος τιμωρείται με κράτηση ή με πρόστιμο.

Άρθρο 362. Δυσφήμηση

Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση μέχρι δύο ετών ή με χρηματική ποινή. Η χρηματική ποινή μπορεί να επιβληθεί και μαζί με την ποινή της φυλάκισης.

Άρθρο 363. Συκοφαντική δυσφήμηση

Αν στην περίπτωση του άρθρου 362, το γεγονός είναι ψευδές και ο υπαίτιος γνώριζε ότι αυτό είναι ψευδές τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών· μαζί με τη φυλάκιση μπορεί να επιβληθεί και χρηματική ποινή. Μπορεί επίσης να επιβληθεί και στέρηση των πολιτικών δικαιωμάτων κατά το άρθρο 63.

Συνηθέστερα εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο

Άρθρο 381. Φθορά ξένης ιδιοκτησίας

1.Όποιος με πρόθεση καταστρέφει ή βλάπτει ξένο (ολικά ή εν μέρει) πράγμα ή με άλλον τρόπο καθιστά ανέφικτη τη χρήση του τιμωρείται με φυλάκιση μέχρι δύο ετών.

2. Αν η φθορά έχει αντικείμενο πράγμα ευτελούς αξίας ή η ζημία που προξενήθηκε από τη φθορά είναι ελαφρά, ο υπαίτιος τιμωρείται με κράτηση έως έξι (6) μήνες ή με πρόστιμο έως τρεις χιλιάδες (3.000) ευρώ.*(*

Άρθρο 382. Διακεκριμένες περιπτώσεις φθοράς

1. Με φυλάκιση τουλάχιστον τριών μηνών τιμωρείται η φθορά ξένης ιδιοκτησίας της πρώτης παραγράφου του άρθρου 381, αν έγινε χωρίς πρόκληση από τον παθόντα.

2. Με την ποινή της προηγούμενης παραγράφου τιμωρείται ο δράστης, αν το αντικείμενο της πράξης που προβλέπεται στην πρώτη παράγραφο του άρθρου 381: α) είναι πράγμα που χρησιμεύει για κοινό όφελος· β) είναι ιδιαίτερα μεγάλης αξίας· γ) η φθορά έγινε με φωτιά ή με κάποιο από τα μέσα που προβλέπει το άρθρο 270.

3. Αν στην πράξη της πρώτης παραγράφου συμμετείχαν δύο ή περισσότεροι ή συντρέχει και μία από τις περιπτώσεις της δεύτερης παραγράφου, επιβάλλεται φυλάκιση τουλάχιστον έξι μηνών.

Εθνική νομοθεσία μέχρι τις 3.8.2016

- Απουσία κύρωσης σύμβασης Βουδαπέστης
- Κάλυψη ηλεκτρονικού & διαδικτυακού εγκλήματος μέσα από διατάξεις Π.Κ:
  - Άρθρο 386Α ΠΚ Απάτη με υπολογιστή
  - Άρθρο 370 Β ΠΚ (Παραβίαση απορρήτων)
  - Άρθρο 370Γ ΠΚ (Αντιγραφή προγράμματος η/υ, παράνομη πρόσβαση)
  - Άρθρο 337 ΠΚ Προσβολή της γενετήσιας αξιοπρέπειας
  - Άρθρο 348Α ΠΚ Πορνογραφία ανηλίκων
  - Άρθρο 348Β ΠΚ Προσέλκυση παιδιών για γενετήσιους λόγους

Ενδεικτικά κενά της Ελληνικής νομοθεσίας

- Δεν καλύπτονταν η παρακώλυση λειτουργίας συστήματος υπολογιστή
- Δεν υπήρχε ξεχωριστή ρύθμιση για την αλλοίωση ή φθορά των δεδομένων («φθορά ξένης ιδιοκτησίας»; μόνο αν υπήρχε φθορά στον υλικό φορέα των δεδομένων)
- Η αλλοίωση των δεδομένων μπορούσε να τιμωρηθεί μόνο:
  - αν επρόκειτο για προσωπικά δεδομένα, μέσω του νόμου προστασίας προσωπικών δεδομένων
  - αν επρόκειτο για «έγγραφο» με την έννοια του άρθρου 13περ.γ ΠΚ, μέσω της υπεξαγωγής εγγράφου (222 ΠΚ)

Ν. 4411/2016
(νόμος για το κυβερνοέγκλημα)

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

Ν. 4411/2016 (νόμος για το κυβερνοέγκλημα)

Κύρωσε Σύμβαση Βουδαπέστης

Κύρωση Πρόσθετου Πρωτόκολλο της Σύμβασης για το έγκλημα στον Κυβερνοχώρο σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών

Τροποποίηση – εκσυγχρονισμός διατάξεων ΠΚ

Διεύρυνση περιπτώσεων άρσης απορρήτου

Άρθρο 337 ΠΚ Προσβολή της γενετήσιας αξιοπρέπειας

1. Όποιος με ασελγείς χειρονομίες ή προτάσεις που αφορούν ασελγείς πράξεις προσβάλλει βάναυσα την αξιοπρέπεια άλλου στο πεδίο της γενετήσιας ζωής του τιμωρείται με φυλάκιση μέχρι ενός έτους ή χρηματική ποινή.

2. Με φυλάκιση τριών μηνών μέχρι δύο ετών τιμωρείται η πράξη της προηγούμενης παραγράφου, αν ο παθών είναι νεότερος από 12 ετών.

3. Ενήλικος, ο οποίος **μέσω διαδικτύου** ή άλλου μέσου επικοινωνίας, αποκτά επαφή με *πρόσωπο που δεν συμπλήρωσε τα δεκαπέντε* έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.

4. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο *που εμφανίζεται ως ανήλικο* κάτω των δεκαπέντε ετών και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπειά του στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση με το εμφανιζόμενο ως ανήλικο πρόσωπο, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.

5. Όποιος τελεί την πράξη της παραγράφου 1 του άρθρου αυτού, εκμεταλλευόμενος την εργασιακή θέση του παθόντος ή τη θέση προσώπου που έχει ενταχθεί σε διαδικασία αναζήτησης θέσης εργασίας διώκεται κατ□έγκληση και τιμωρείται με φυλάκιση από έξι (6) μήνες μέχρι τρία (3) έτη και με χρηματική ποινή τουλάχιστον χιλίων (1.000) ευρώ.

Άρθρο 348Α ΠΚ Πορνογραφία ανηλίκων Η ρύθμιση

1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

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 ***διά συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου,*** τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ: α) αν τελέσθηκαν κατ επάγγελμα ή κατά συνήθεια β) αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος. Αν η πράξη της περίπτωσης β΄ είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ, αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

Άρθρο 348Α ΠΚ
Πορνογραφία ανηλίκων -επισημάνσεις

Αφορά και ανηλίκους που έχουν συμπληρώσει το 15 έτος της ηλικίας τους (ηλικία σεξουαλικής συναίνεσης)

Τιμωρείται και το εικονικό παιδο- πορνογραφικό υλικό (morphing- απόδοση ανύπαρκτων προσώπων)

Άρθρο 348Β ΠΚ. Προσέλκυση παιδιών για γενετήσιους λόγους

«Όποιος με πρόθεση, **μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας**, προτείνει σε ενήλικο να συναντήσει ανήλικο, που δεν συμπλήρωσε τα δεκαπέντε έτη, με σκοπό τη διάπραξη σε βάρος του των αδικημάτων των παραγράφων 1 και 2 του άρθρου 339 και 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν στη διάπραξη των αδικημάτων αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.»

- Grooming
- Ψηφιακές καραμέλες

Ν. 4411/2016 - Εκσυγχρονισμός διατάξεων ΠΚ

292Β ΠΚ με τον τίτλο- «Παρακώλυση λειτουργίας συστήματος πληροφοριών» [νέο]

370Γ ΠΚ «Παράνομη πρόσβαση σε πληροφοριακό σύστημα» [Τροποποίηση]

370Δ Π.Κ. (παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων)

- 370 Ε ΠΚ (διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων για παράνομη πρόσβαση σε πληροφοριακό σύστημα) [νέο]

381 Α ΠΚ «Φθορά ηλεκτρονικών δεδομένων» [νέο]

- 381Β Π.Κ (διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων για φθορά δεδομένων)

386Α Π.Κ. (απάτη με ηλεκτρονικό υπολογιστή) [τροποποίηση]

[Πληροφοριακά συστήματα και ψηφιακά δεδομένα]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
1.Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η' και θ' ως εξής:
«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».

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων- ν. 4411/2016

2.Μετά το άρθρο 292Α του Ποινικού Κώδικα προστίθεται άρθρο 292Β ως εξής:
« Άρθρο 292Β
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.Γ ια την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

[Προπαρασκευαστικές ενέργειες για παρακώλυση λειτουργίας πληροφοριακών συστημάτων]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
3.Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται άρθρο 292Γ ως εξής:
« Άρθρο 292Γ
Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β 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».
4.Οι παράγραφοι 2 και 5 του άρθρου 348Α του Ποινικού Κώδικα αντικαθίστανται ως εξής:
«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».

Προσέλκυση παιδιών για γενετήσιους λόγους- ν.4411/2016

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
5.Το άρθρο 348Β του Ποινικού Κώδικα αντικαθίσταται ως εξής:
«Άρθρο 348Β
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 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ».

[Παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
7.Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:
«Άρθρο 370Δ
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 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

[Παρεμβολές σε δεδομένα - Παράνομη Υποκλοπή Ψηφιακών Δεδομένων]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
8.Μετά το άρθρο 370Δ του Ποινικού Κώδικα προστίθεται άρθρο 370Ε ως εξής:
«Άρθρο 370Ε
Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ 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 370Β, 370Γ και 370Δ, 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».

Παράνομη Παρεμβολή σε Ψηφιακά Δεδομένα -Φθορά ηλεκτρονικών δεδομένων

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
9.Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται άρθρο 381Α ως εξής:
«Άρθρο 381Α
Φθορά ηλεκτρονικών 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 τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.
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 ζημία 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, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.
4.Γ ια την ποινική δίωξη της πράξης της παραγράφου 1απαιτείται έγκληση».

Άρθρο 386Α- Απάτη με υπολογιστή

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο
11.Το άρθρο 386Α του Ποινικού Κώδικα αντικαθίσταται ως εξής:
«Άρθρο 386Α
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».

[Άρση του απορρήτου]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο τρίτο

Τροποποιήσεις του Ν. 2225/1994

1.Η παρ. 1 του άρθρου 4 του Ν. 2225/1994 αντικαθίσταται ως εξής:

«1. Η άρση του απορρήτου είναι επιτρεπτή για τη διακρίβωση των κακουργημάτων που προβλέπονται από: α) τα άρθρα 134, 135 παράγραφοι 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2,150, 151, 157 παρ. 1, 159, 159Α, 168 παρ. 1, 187 παράγραφοι 1, 2, 187Α παράγραφοι 1 και 4, 207, 208 παρ. 1, 235 παρ. 2, 236 παρ. 2, 237 παράγραφοι 2 και 3β', 264 περιπτώσεις β' και γ', **270, 272, 275 περίπτωση β', 291 παρ. 1 περιπτώσεις β' και γ', 292Α παρ. 4 εδάφιο β' και παρ. 5, 299, 322, 323Α παράγραφοι 1, 2, 4, 5 και 6, 324 παράγραφοι 2 και 3, 336 σε βάρος ανηλίκου, 338 παρ. 1 σε βάρος ανηλίκου, 339 παράγραφοι 1 περιπτώσεις α' και β', 342 παράγραφοι 1 και 2, 348Α παρ. 4, 348Γ παρ. 1 περιπτώσεις α' και β', 349 παρ. 1 και 2, 351 παράγραφοι 1, 2, 4 και 5, 351Α παράγραφοι 1 περιπτώσεις α' και β' και 3, 370Α, 370Δ, 374, 380, 385 παρ. 1 περιπτώσεις α' και β' του Ποινικού Κώδικα,**
β) τα άρθρα 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 28,29, 30, 46, 47, 59, 140 και 144 του Στρατιωτικού Ποινικού Κώδικα,
γ) το άρθρο 15 παρ. 1 του Ν. 2168/1993,
δ) τα άρθρα 20, 22 και 23 του Ν. 4139/2013,
ε) το άρθρο 157 παρ. 1γ του Ν. 2960/2001,
στ) το άρθρο 3 περίπτωση ιε' του Ν. 3691/2008, σε συνδυασμό με το άρθρο δεύτερο του Ν. 2656/1998,
ζ) το άρθρο 3 παρ. 2 του Ν. 2803/2000,
η) το άρθρο 45 παρ. 1 περιπτώσεις α', β' και γ' του Ν. 3691/2008,
θ) το άρθρο 28 του Ν. 1650/1986.

Επίσης, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα, καθώς επίσης και για τα εγκλήματα των παραγράφων 1, 2, 3, 4 εδάφιο α' και 6 του άρθρου 292Α, του άρθρου 292Β, του άρθρου 292Γ, των παραγράφων 1 περίπτωση γ' και 4 του άρθρου 339, της παρ. 3 του άρθρου 342, του άρθρου 348, των παραγράφων 1, 2 και 5 του άρθρου 348Α, του άρθρου 348Β, της παρ. 1 περιπτώσεις γ' και δ' του άρθρου 348Γ και της παρ. 1 περίπτωση γ' του άρθρου 351Α, των άρθρων 370Γ και 370Ε, του άρθρου 381Α, του άρθρου 381Β και του άρθρου 386Α του Ποινικού Κώδικα.

Επιπλέον, η άρση του απορρήτου είναι επιτρεπτή για τη διακρίβωση των εγκλημάτων που προβλέπονται από το άρθρο 11 του Ν. 3917/2011, το άρθρο 15 του Ν. 3471/2006 και το άρθρο 10 του Ν. 3115/2003».

2.Στο τέλος της παρ. 11 του άρθρου 5 του Ν. 2225/1994 προστίθεται εδάφιο ως εξής:

«Με την ίδια ποινή τιμωρείται αν ανακοινώνει σε τρίτους ή γνωστοποιεί οπωσδήποτε το γεγονός της άρσης του απορρήτου, καθώς και αν παραβιάσει την υποχρέωση εχεμύθειάς του κατά τη διαδικασία άρσης του απορρήτου που προβλέπεται από το άρθρο 8 του π.δ. 47/2005 (Α' 64)».

[Ευθύνη νομικών προσώπων]

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο τέταρτο
Ευθύνη νομικών προσώπων
(Άρθρο 11 της Οδηγίας)
1.Αν κάποια από τις πράξεις των άρθρων 292Β, 370Γ, 370Δ, 370Ε, 381Α και 386Α του Ποινικού Κώδικα τελέστηκε, **προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωση 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, 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 μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,
β) διοικητικό πρόστιμο από 20.000 έως 1.000.000 ευρώ,
γ) ανάκληση ή αναστολή της άδειας λειτουργίας τους για χρονικό διάστημα από ένα (1) μήνα έως δύο (2) έτη ή απαγόρευση άσκησης της επιχειρηματικής τους δραστηριότητας για το ίδιο χρονικό διάστημα,
δ) 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.
Σε περίπτωση υποτροπής οι κυρώσεις των περιπτώσεων γ' και δ' μπορεί να έχουν οριστικό χαρακτήρα και εφόσον πρόκειται περί σωματείων ή ενώσεων προσώπων, η υποτροπ μπορεί να έχει ως συνέπεια τη διάλυσή τους, σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις.
2.Όταν η **έλλειψη εποπτείας ή ελέγχου από φυσικό πρόσωπο** που αναφέρεται στην παράγραφο 1, κατέστησε δυνατή την τέλεση από πρόσωπο που τελεί υπό την εξουσία του κάποιας από τις αξιόποινες πράξεις που αναφέρονται στην ίδια ως άνω παράγραφο, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, επιβάλλονται στο νομικό πρόσωπο, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις:
α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,
β) διοικητικό πρόστιμο από 10.000 έως 1.000.000 ευρώ,
γ) οι προβλεπόμενες στις περιπτώσεις γ' και δ' της προηγούμενης παραγράφου κυρώσεις για χρονικό διάστημα από δέκα (10) ημέρες έως έξι (6) μήνες.
3.Για τη σωρευτική ή διαζευκτική επιβολή των κυρώσεων που προβλέπονται στις προηγούμενες παραγράφους και για την επιμέτρηση των κυρώσεων αυτών λαμβάνονται υπόψη ιδίως η βαρύτητα της παράβασης, ο βαθμός της υπαιτιότητας, η οικονομική επιφάνεια του νομικού προσώπου ή της ένωσης προσώπων και η τυχόν υποτροπή τους.
4.Η εφαρμογή των διατάξεων των προηγούμενων παραγράφων είναι **ανεξάρτητη από την αστική, πειθαρχική ή ποινική ευθύνη των αναφερόμενων σε αυτές φυσικών προσώπων**. Καμιά κύρωση δεν επιβάλλεται χωρίς προηγούμενη κλήτευση των νόμιμων εκπροσώπων του νομικού προσώπου ή της ένωσης προσώπων προς παροχή εξηγήσεων Η κλήση κοινοποιείται τουλάχιστον δέκα (10) ημέρες πριν από την ημέρα της ακρόασης. Κατά τα λοιπά, εφαρμόζονται οι διατάξεις των παραγράφων 1 και 2 του άρθρου 6 του Κώδικα Διοικητικής Διαδικασίας. Σε περίπτωση άσκησης ποινικής δίωξης για κάποια από τις προβλεπόμενες στην παράγραφο 1 αξιόποινες πράξεις που τελέστηκε από πρόσωπ αναφερόμενο στις παραγράφους 1 και 2 και προκειμένου να εφαρμοστεί η προβλεπόμενη στο άρθρο αυτό διαδικασία επιβολής διοικητικών κυρώσεων, οι εισαγγελικές αρχές ενημερώνουν αμέσως τον Υπουργό Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και αποστέλλουν σε αυτόν αντίγραφα της δικογραφίας.
5.Σε περίπτωση αμετάκλητης απαλλαγής του παραπεφθέντος οι κατά τα ανωτέρω αποφάσεις επιβολής διοικητικών κυρώσεων ανακαλούνται.
6.Οι διατάξεις των προηγουμένων παραγράφων δεν εφαρμόζονται στο κράτος, στους φορείς δημόσιας εξουσίας και στους διεθνείς οργανισμούς δημοσίου δικαίου, χωρίς αυτό να επηρεάζει την εφαρμογή των ισχυουσών κάθε φορά διατάξεων περί αστικής, πειθαρχικής ή ποινικής ευθύνης.

ΠΟΙΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΣΕ ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Νόμος 4624/2019 "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις".:

1. Όποιος, χωρίς δικαίωμα: α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών· β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.

2. Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση α΄ της παραγράφου 1 ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών, τιμωρείται με φυλάκιση, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.

3. Εάν η πράξη της παραγράφου 2 αφορά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα του άρθρου 9 παράγραφος 1 του ΓΚΠΔ ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή τα σχετικά με αυτά μέτρα ασφαλείας του άρθρου 10 του ΓΚΠΔ, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.

4. Με κάθειρξη μέχρι δέκα (10) ετών τιμωρείται ο υπαίτιος των πράξεων των προηγούμενων παραγράφων, εάν είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον ή να βλάψει άλλον και το συνολικό όφελος ή η συνολική ζημία υπερβαίνει το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ.

5. Εάν από τις πράξεις των παραγράφων 1 έως και 3 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή έως τριακόσιες χιλιάδες (300.000) ευρώ.

ΠΟΙΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΝΟΜΟΘΕΣΙΑΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Α. 66 Ν. 2121/1993 όπως ισχύει

- Προσβολή περιουσιακών & ηθικών εξουσιών δημιουργού και δικαιούχων συγγενικών δικαιωμάτων= φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 -15.000 ευρώ
- Διανομή ή κατοχή με σκοπό διανομής συστήματα ή μέσα που έχουν ως μοναδικό σκοπό να διευκολύνουν τη χωρίς άδεια αφαίρεση ή εξουδετέρωση τεχνικού συστήματος που προστατεύει ένα πρόγραμμα ηλεκτρονικού υπολογιστή= φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 - 15.000 ευρώ
- Αν το όφελος που επιδιώχθηκε ή η ζημία που απειλήθηκε είναι ιδιαίτερα μεγάλα= φυλάκιση τουλάχιστο δύο ετών και χρηματική ποινή έξι χιλιάδων (6.000) έως τριάντα χιλιάδων (30.000) ευρώ.
- Αν ο υπαίτιος τελεί τις παραπάνω πράξεις κατ'' επάγγελμα ή σε εμπορική κλίμακα ή αν οι περιστάσεις κάτω από τις οποίες έγινε η πράξη μαρτυρούν ότι ο υπαίτιος είναι ιδιαίτερα επικίνδυνος για την προστασία της πνευματικής ιδιοκτησίας ή των συγγενικών δικαιωμάτων= κάθειρξη μέχρι 10 ετών και χρηματική ποινή δεκαπέντε χιλιάδων (15.000) έως εξήντα χιλιάδων (60.000) ευρώ, καθώς και αφαίρεση της άδειας λειτουργίας της επιχείρησης στα πλαίσια της οποίας εκτελέσθηκε η πράξη.

**Θεωρείται ότι η πράξη έχει τελεσθεί κατ'' επάγγελμα και όταν ο δράστης έχει καταδικασθεί για παρόμοια αδικήματα με αμετάκλητη απόφαση σε ποινή στερητική της ελευθερίας.*

Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (EU CYBER CRIME DIRECTIVE)

τροποποίηση και επέκταση των διατάξεων της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, της 24ης Φεβρουαρίου 2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών

ανάγκη καταπολέμησης του **οργανωμένου εγκλήματος** και της **τρομοκρατίας** και ιδίως των επιθέσεων κατά των συστημάτων πληροφοριών να που εμφανίζονται ως συνεχώς αυξανόμενη απειλή

«Η παρούσα οδηγία σκοπεύει, μεταξύ άλλων, στην εισαγωγή ποινικών κυρώσεων για τη δημιουργία των «**botnet**», ήτοι πράξη της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο»

Στόχοι οδηγίας

- προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον **ορισμό των ποινικών αδικημάτων** και των **σχετικών κυρώσεων**, και
- η **βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών**, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη και των ευρωπαϊκών οργάνων

EU CYBER CRIME DIRECTIVE- ΤΑ ΕΓΚΛΗΜΑΤΑ

Άρθρο 3 **Παράνομη πρόσβαση σε συστήματα πληροφοριών**

[…] 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.

Άρθρο 4 **Παράνομη παρεμβολή σε σύστημα**

[…] η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

EU CYBER CRIME DIRECTIVE- ΤΑ ΕΓΚΛΗΜΑΤΑ

Άρθρο 5 **Παράνομη παρεμβολή σε δεδομένα**

[..] η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Άρθρο 6 **Παράνομη υποκλοπή**

[..] η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

EU CYBER CRIME DIRECTIVE- ΕΠΙΣΗΜΑΝΣΕΙΣ

«τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις»

δεν θα αποδίδεται ποινική ευθύνη, σε περίπτωση που δεν υπάρχει εγκληματική πρόθεση, όπως όταν το πρόσωπο δεν γνωρίζει ότι απαγορεύεται η πρόσβαση ή στην περίπτωση εξουσιοδοτημένης δοκιμής ή προστασίας συστημάτων πληροφοριών, όπως όταν μια εταιρεία ή ένας πωλητής αναθέτει σε ένα πρόσωπο να ελέγξει την ισχύ του συστήματος ασφαλείας του.

Και τα νομικά πρόσωπα θα πρέπει να μπορούν να φέρουν ποινική ευθύνη με βάση την οδηγία

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΑΡΕΝΟΧΛΗΣΕΙΣ

Cyberbulling: ανήλικος προς ανήλικο

- http://issuu.com/de_jure/docs/de_jure_vol._9
- http://stopcyberbullying.org/index2.html

Cyberstalking "Cyberstalking is the use of the Internet, email or other electronic communications to stalk, and generally refers to a pattern of *threatening or malicious* behaviors. Cyberstalking may be considered the most dangerous of the three types of Internet harassment, based on a posing ***credible threat*** of harm. Sanctions range from misdemeanors to felonies".

Cyberharassment: "Cyberharassment differs from cyberstalking in that it may generally be defined as ***not involving a credible threat***. Cyberharassment usually pertains to threatening or harassing email messages, instant messages, or to blog entries or websites dedicated solely to tormenting an individual. Some states approach cyberharrassment by including language addressing electronic communications in general harassment statutes, while others have created stand-alone cyberharassment statutes."

- http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx

Α. 333 ΠΚ (απειλή)

, «[…] τιμωρείται και όποιος, χωρίς απειλή βίας ή άλλης παράνομης πράξης ή παράλειψης, προκαλεί σε άλλον τρόμο ή ανησυχία, με την επίμονη καταδίωξη ή παρακολούθησή του, όπως ιδίως με την επιδίωξη διαρκούς επαφής μέσω ***τηλεπικοινωνιακού ή ηλεκτρονικού μέσου*** *ή με επανειλημμένες επισκέψεις στο οικογενειακό, κοινωνικό ή εργασιακό περιβάλλον αυτού, παρά την εκπεφρασμένη αντίθετη βούλησή του.».*

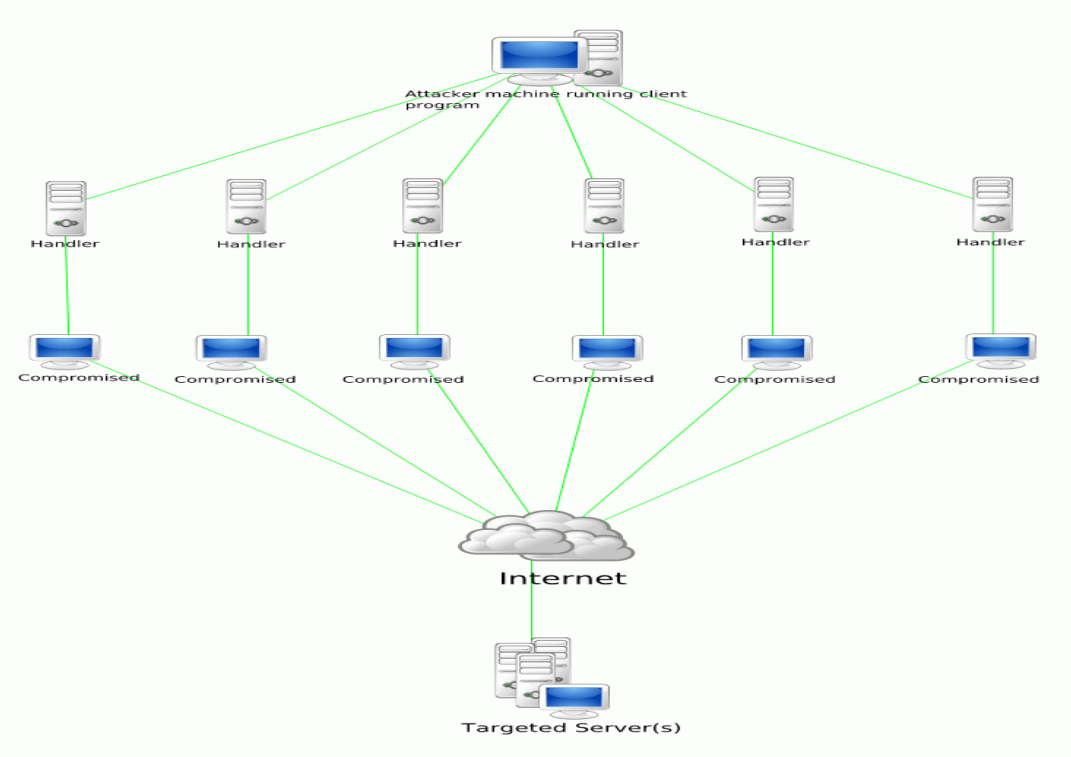
αιτιολογική έκθεση ν. 4531/2018, βλ. τον όρο «stalking»= Με την τέταρτη παράγραφο και σύμφωνα με το άρθρο 34 της Σύμβασης ποινικοποιείται το λεγόμενο Stalking, δηλαδή μία επίμονη συμπεριφορά καταδίωξης ή παρακολούθησης, με την οποία η επέμβαση στην ιδιωτική σφαίρα του θύματος είναι ιδιαιτέρως επαχθής. Ως εκ τούτου, στην παράγραφο 1 του άρθρου 333 ΠΚ προστίθεται δεύτερο εδάφιο. Το νέο αδίκημα που τυποποιείται, σε αντίθεση με αυτό της απειλής, δεν τελείται με απειλή βίας ή άλλης παράνομης πράξης ή παράλειψης, αλλά με την επίμονη καταδίωξη ή παρακολούθηση του θύματος, η οποία πραγματοποιείται είτε με την επιδίωξη διαρκούς επαφής μέσω τηλεπικοινωνιακού ή ηλεκτρονικού μέσου (π.χ. αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, τηλέφωνα κλπ.), είτε με διαρκείς επισκέψεις στο περιβάλλον του θύματος, παρά την εκπεφρασμένη αντίθετη βούλησή του, προκαλώντας στο θύμα τρόμο ή ανησυχία.

Επιθέσεις άρνησης εξυπηρέτησης / Denial of Services (DOS)

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 τον κρατούν απασχολημένο. 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.

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 επιτιθέμενο τους. Ο επιτιθέμενος θα τους διατάξει να επιτεθούν ενάντια σε συγκεκριμένο στόχο. Με την έκταση των καλωδιακών modems, των συνδέσεων DSL, και την 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 παραγωγικότητας 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.

DDoS


Attacker machine running client program
Handler
Handler
Handler
Handler
Handler
Handler
Compromised
Compromised
Compromised
Compromised
Compromised
Compromised
Internet
Targeted Server(s)

Επιθέσεις άρνησης εξυπηρέτησης / Denial of Services (DOS)

Μεγαλύτερες υποθέσεις:

- Εσθονία 2007
- Γεωργία 2008

- Βλ. αναλυτικά μελέτη, Eneken Tikk, Kadri Kaska and Liis Vihul , *International Cyber Incidents: Legal Considerations,* CCD COE Publications, 2010
- https://www.ccdcoe.org/231.html

* NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

Hacktivism

Α) επιχειρεί να γιατρέψει το Internet από κάθε κακό κώδικα και ελαττωματικό πρόγραμμα.

Β) χρησιμοποιεί του δικτύου ως όργανο για κοινωνική δικαιοσύνη, διαμέσου διαφόρων δραστηριοτήτων διαμαρτυρίας ή ως μέσο για δημοσιότητα

Defacement of a website

Phising

«Social Engineering »=υφαρπαγή εμπιστευτικών πληροφοριών μετά από εξαπάτηση των υποκειμένων των εμπιστευτικών πληροφοριών.

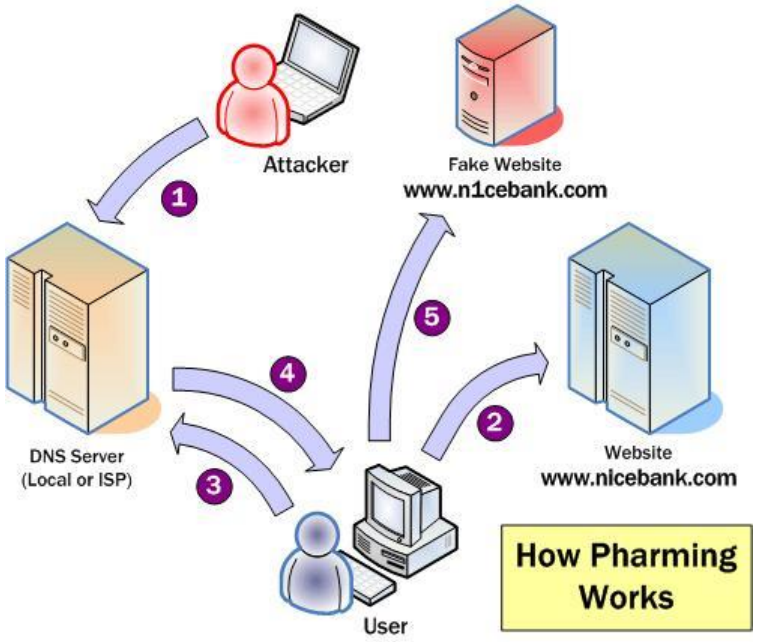
http://www.antiphishing.org/ : "*the global industry, law enforcement, and government coalition focused on unifying the global response to cyber crime through development of data resources, data standards and model response systems and protocols for private and public sectors*."

«Νηγιαριανές» επιστολές

386 ΠΚ περί απάτης

Pharming

παραβίαση απορρήτου κατά το άρθρο 370Γ § 2 ΠΚ



http://www.ecybercrime.com/2011/05/pharming.html

Π.χ: http://www.networkworld.com/news/2008/012208-drive-by-pharming.html

Cyber warfare

Stuxnet

[…] *in June 2009, someone had silently unleashed a sophisticated and destructive digital worm that had been slithering its way through computers in Iran with just one aim — to sabotage the country's uranium enrichment program and prevent President Mahmoud Ahmadinejad from building a nuclear weapon. But it would be nearly a year before the inspectors would learn of this. The answer would come only after dozens of computer security researchers around the world would spend months deconstructing what would come to be known as the most complex malware ever written — a piece of software that would ultimately make history as the world's first real cyberweapon*

http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/8/

Βλ. παρουσίαση Γεωργίου Κυριακόπουλου σε http://www.ethemis.gr/5o-panellinio-sinedrio/parousiasis/

The **International Journal of Cyber Warfare and Terrorism (IJCWT),** http://www.igi-global.com/journal/international-journal-cyber-warfare-terrorism/1167

2019


ΝΕΕΣ ΥΠΟΘΕΣΕΙΣ ΠΟΥ ΧΕΙΡΙΣΤΗΚΕ Η ΔΙ.Δ.Η.Ε. ΚΑΤΑ ΤΟ ΕΤΟΣ 2018
Νομοθεσία περί πνευματικής ιδιοκτησίας 19
Συνδρομή σε ημεδαπές αρχές 478
Διάφορα άλλα 73
Απάτη / Παράνομη νομιμοποίηση εσόδων 1448
Αιτήματα πολιτών 807
Εκδηλώσε πρόθεσης αυτοκτονίας 368
Φορολογικές παραβάσεις 1
Νομοθεσία περί προστασίας ζώων 202
Πορνογραφία ανηλίκων & εγκλήματα κατά της γενετήσιας ελευθερίας 282
Παράνομη πρόσβαση σε υπολογιστικά συστήματα / Υποκλοπή δεδομένων (phishing) / Παραβίαση απορρήτου επικοινωνιών κι άλλα σχετικά αδικήματα 279
Νομοθεσία περί τυχερών παιγνίων 34
Νομοθεσία περί Προσωπικών Δεδομένων / Απειλή 866

2019

Αδίκημα	Συλληφθέντες
Διεξαγωγή τυχερών παιγνίων	5
Νομοθεσία περί πνευματικής ιδιοκτησίας	2
Απάτη/Απάτη με υπολογιστή	11
Πορνογραφία ανηλίκων	17
Νομοθεσία περί προσωπικών δεδομένων	6
Λοιποί ειδικοί ποινικοί νόμοι	1

ΕΥΡΩΠΑΙΚΟΙ ΦΟΡΕΙΣ

- Eurojust
- Europol
  - Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος (EC3)
- Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA)

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

http://www.youtube.com/watch?feature=player_embedded&v=R6swtAUKzws#t=118

Κυβερνοασφάλεια

Βλ. δελτίο τύπου **Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security,** Release Date: October 7, 2016:

> «The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. [..]»

ENISA REPORT: Article 13a of the Framework Directive (2009/140/EC) :

Malicious actions are not focused on causing disruptions: the total number of incidents caused by malicious actions dropped to 2.5% from higher previous values (9.6% in 2014). This may indicate that the malicious actions are not necessarily aiming at causing unavailability of services.

Malicious actions started causing long lasting incidents: Incidents caused by malicious actions (e.g. DDoS), although we didn't have too many of them, had most impact in terms of duration, on average almost two days per incident.

Κυβερνοασφάλεια

Οδηγία NIS

Η υφιστάμενη εθνική ρύθμιση και οι εμπλεκόμενοι φορείς

Οδηγία NIS
(*Network and Information Systems)

Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό **κοινό επίπεδο ασφάλειας συστημάτων δικτύου** και πληροφοριών σε ολόκληρη την Ένωση για την **ασφάλεια δικτύων και πληροφοριών** (ΑΔΠ)

Ασφάλεια συστημάτων δικτύου και πληροφοριών

η ικανότητα συστημάτων δικτύου και πληροφοριών **να ανθίστανται**, σε δεδομένο βαθμό αξιοπιστίας, **σε ενέργειες που πλήττουν τη διαθεσιμότητα**, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών

Οδηγία NIS

Υποχρεώσεις κρατών μελών

- Εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών
- Εθνικές ομάδες παρέμβασης -national CSIRTs (Computer Security Incident Response Teams)
- Δίκτυο ομάδων παρέμβασης- network of the national CSIRTs
- Εθνικό σημείο επαφής
- «Ομάδα Συνεργασίας»/ Cooperation Group: κράτη μέλη, Επιτροπή, ENISA για την υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας καθώς και της ανταλλαγής πληροφοριών, και την καλλιέργεια πνεύματος αξιοπιστίας και εμπιστοσύνης
- Κυρώσεις - επιβολή

Υποχρεώσεις άλλων εμπλεκομένων

- Φορείς εκμετάλλευσης βασικών υπηρεσιών/ Operators of Essential Services (OES)
  - σε τομείς ζωτικής σημασίας όπως η ενέργεια, οι μεταφορές, η υγεία και οι χρηματοπιστωτικές υπηρεσίες
- Πάροχοι ψηφιακών υπηρεσιών/ Digital Service Providers
  - διαδικτυακές αγορές, τις μηχανές αναζήτησης και τις υπηρεσίες νεφοϋπολογιστικής

Πότε;

- Έως 9 Μαΐου **2018** τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με τη νέα οδηγία
- Από 10 Μαΐου **2018** τα μέτρα αυτά θα τεθούν σε εφαρμογή

Υποχρεώσεις φορέων εκμετάλλευσης βασικών υπηρεσιών/ Operators of Essential Services (OES)

κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων

κατάλληλα μέτρα αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων

κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια αρχή ή στην CSIRT συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών

Κριτήρια για «Σοβαρότητα»

- ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας
- η διάρκεια του συμβάντος
- το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν

Υποχρεώσεις παρόχων ψηφιακών υπηρεσιών/ Digital Service Providers (DSPs)

προσδιορίζουν και λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων

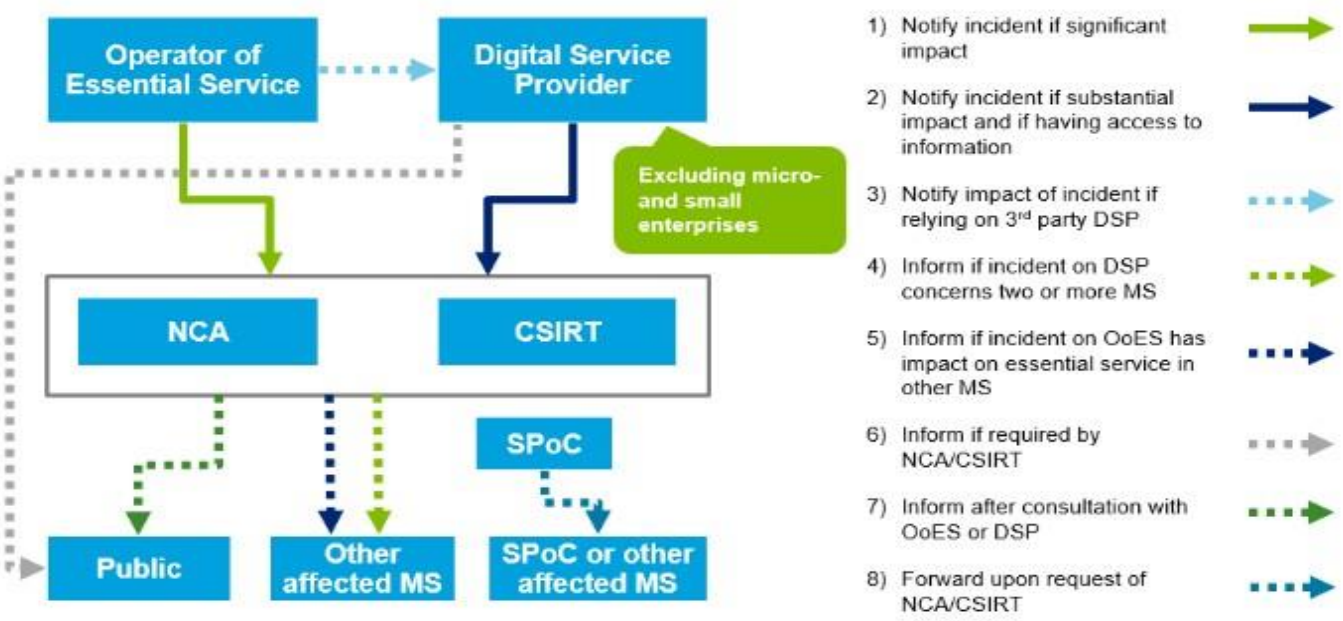
λαμβάνουν μέτρα για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια

κοινοποιούν στην αρμόδια αρχή ή την CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει **σημαντικό** αντίκτυπο

Κριτήρια:

- ο **αριθμός των χρηστών** που επηρεάζονται από το συμβάν, ιδίως των χρηστών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών
- η **διάρκεια** του συμβάντος
- το **γεωγραφικό εύρος** της περιοχής που επηρεάζεται από το συμβάν
- η **έκταση της διατάραξης** της λειτουργίας της υπηρεσίας
- η **έκταση του αντίκτυπου** στις οικονομικές και κοινωνικές δραστηριότητες

Σχηματοποιημένος τρόπος αντίδρασης OES & DSPs



Source: http://www2.deloitte.com/be/en/pages/risk/articles/nis-directive.html

National Competent Authorities (NCAs), **Single Point of Contact (SPoC)**

Εθνικοί παράγοντες

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, σχετικά με τις πολιτικές ασφαλείας και τα ειδικά σχέδια που εφαρμόζονται από τα υπουργεία, τις δημόσιες υπηρεσίες και τα Ν.Π.Δ.Δ. που κατέχουν διαβαθμισμένο υλικό.

Η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ), σύμφωνα με το ν. 39/2008 είναι υπεύθυνη για το εθνικό CERT (Computer Emergency and Response Team) και αποτελεί την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων. 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.

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 για το κυβερνοέγκλημα (α.5) ορίζεται ως το σημείο επαφής για την εκπλήρωση των σκοπών του άρθρου 35 της Σύμβασης («Δίκτυο 24/7»).

Στο πλαίσιο του Υπουργείου Εσωτερικών η Διεύθυνση Πολιτικού Σχεδιασμού Έκτακτης Ανάγκης (ΠΣΕΑ), καταρτίζει τα σχέδια εξυπηρέτησης των υπηρεσιών της Γενικής Γραμματείας ΔΔ και Ηλεκτρονικής Διακυβέρνησης.

Υπάρχει επίσης το “Κέντρο Μελετών Ασφαλείας(ΚΕΜΕΑ) που υπάγεται στο Υπουργείο Εσωτερικών & Διοικητικής Ανασυγκρότησης και αποτελεί ιδρυτικό μέλος του “Ευρωπαϊκού Οργανισμού Ασφαλείας” στο Βέλγιο.

Διεύθυνσης Κυβερνοασφάλειας Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης

Εθνική Στρατηγική Κυβερνοασφάλειας

Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, Νίκου Παππά, εγκρίθηκε στις 7/3/2018 η Εθνική Στρατηγική Κυβερνοασφάλειας.

Με την Εθνική Στρατηγική Κυβερνοασφάλειας αναπτύσσεται ο κεντρικός σχεδιασμός της Ελληνικής Πολιτείας για την ασφάλεια στον κυβερνοχώρο. Η σημασία της είναι κρίσιμη με δεδομένη την ολοένα αυξανόμενη χρήση του Διαδικτύου και των Τεχνολογιών Πληροφορικής και Επικοινωνιών σε κάθε πτυχή των δραστηριοτήτων του δημόσιου και του ιδιωτικού τομέα. Στόχος είναι η δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών και στην τόνωσης της οικονομικής ανάπτυξης της χώρας μας.

Την συνολική ευθύνη για την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας φέρει η Εθνική Αρχή Κυβερνοασφάλειας, που συστάθηκε και λειτουργεί στη Γενική Γραμματεία Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης. Η Αρχή αυτή, ως φορέας υψηλού πολιτικού-κυβερνητικού επιπέδου με εξειδικευμένα στελέχη, παρακολουθεί και υλοποιεί τις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Είναι επίσης αρμόδια για τον συντονισμό μεταξύ των φορέων που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Στις προτεραιότητες της Εθνικής Αρχής Κυβερνοασφάλειας εντάσσεται η συνεργασία με τους αρμόδιους φορείς για την ενσωμάτωση της Οδηγίας (ΕΕ) 2016/1148 «Σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση» (NIS Directive) στο ελληνικό δίκαιο

Εθνική στρατηγική

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGR.pdf/

Νόμος 4577/2018 για την ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις

Εθνική Αρχή Κυβερνοασφάλειας

Σύμφωνα με τον Νόμο, ως Εθνική Αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, εφεξής «Αρμόδια Αρχή» ή «Εθνική Αρχή Κυβερνοασφάλειας», ορίζεται η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης.

Η Εθνική Αρχή Κυβερνοασφάλειας, μεταξύ άλλων:

α) παρακολουθεί την εφαρμογή του Νόμου,

β) ορίζεται ως το εθνικό ενιαίο κέντρο επαφής, εφεξής «Ενιαίο Κέντρο Επαφής», για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ασκώντας καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών, καθώς και με τις Αρμόδιες Αρχές άλλων κρατών-μελών στο πλαίσιο των μηχανισμών συνεργασίας,

γ) συνεργάζεται με την αρμόδια CSIRT, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος νόμου, ε) διαβουλεύεται και συνεργάζεται με τις Αρμόδιες Εθνικές Αρχές επιβολής του νόμου, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), καθώς και τις λοιπές αρμόδιες ρυθμιστικές ή εποπτικές αρχές και τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τα θέματα που άπτονται της εφαρμογής του Νόμου,

δ) συνεργάζεται με τις Αρμόδιες Αρχές των λοιπών κρατών-μελών.

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- Ι

έκδοση των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών, της διαδικασίας παροχής πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές,

η μεθοδολογία προσδιορισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) καθώς και η μεθοδολογία αξιολόγησης και ελέγχου, σύμφωνα με τις προβλέψεις της Οδηγίας 2016/1148/ΕΕ, του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 και του ν. 4577/2018, ο οποίος κατ' εφαρμογή της ως άνω Οδηγίας θεσπίζει μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων αυτών

στον κατάλογο βασικών υπηρεσιών εντάσσονται οι τομείς της ενέργειας (Ηλεκτρική, Πετρέλαιο, Αέριο), των μεταφορών (αεροπορικών, πλωτών, οδικών και σιδηροδρομικών), των τραπεζών, των χρηματοπιστωτικών αγορών, της υγείας, του νερού και των ψηφιακών υποδομών

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- **Ενιαία Πολιτική Ασφάλειας**

η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) ορίζει τις απαιτήσεις της.

κάθε Οργανισμός πρέπει να έχει Πολιτική Ασφαλείας των συστημάτων δικτύου και πληροφοριών του η οποία καλύπτει τουλάχιστον όσα ορίζει η Ενιαία Πολιτική Ασφάλειας.

Η Πολιτική Ασφάλειας:

- ορίζει τους στόχους ασφάλειας
- περιγράφει τη διακυβέρνηση
- παραπέμπει σε άλλες συμπληρωματικές πολιτικές, σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών του Οργανισμού.

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- **Επιλογή μέτρων ασφάλειας**

- Αποτελεσματικά, ώστε να αυξάνουν το επίπεδο ετοιμότητας του Οργανισμού έναντι τωρινών και μελλοντικών απειλών ασφάλειας.
- Αποδοτικά, ώστε να επιλέγονται αυτά τα οποία θα έχουν το μεγαλύτερο αντίκτυπο στην ενίσχυση της ασφάλειας ενός Οργανισμού, σε σχέση με τις απαιτήσεις κτήσης και διατήρησής τους.
- Κατάλληλα, ώστε να είναι συμβατά και να διευκολύνουν τη παροχή των βασικών υπηρεσιών του Οργανισμού.
- Αναλογικά, ώστε να επιλέγονται συναρτήσει του εκάστοτε επιπέδου επικινδυνότητας.
- Συγκεκριμένα, ώστε να διασφαλίζεται ότι τα μέτρα θα εφαρμόζονται στην πράξη και θα ενισχύουν ενεργά το επίπεδο ασφάλειας.
- Αξιόπιστα, ώστε να παρέχουν δείκτες και αποδείξεις για την αποτελεσματική και αποδοτική εφαρμογή τους.
- Περιεκτικά, ώστε η εφαρμογή τους να καλύπτει όσες περισσότερες βασικές απαιτήσεις ασφάλειας είναι δυνατό.
- Κατά προτίμηση βάσει διεθνώς αποδεκτών προτύπων, προδιαγραφών και οδηγών.

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- **Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων**

Κάθε Οργανισμός οφείλει να ορίσει συγκεκριμένο εργαζόμενο του ως Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων του ο οποίος :

- Αποτελεί το σημείο επαφής με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT.
- Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας και με το αρμόδιο CSIRT.
- Συντονίζει και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις που απορρέουν από τον ν. 4577/2018 (Α΄ 199), από την παρούσα υπουργική απόφαση και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών.
- Εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας, την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων καθώς, και τη σύνταξη της αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοσφάλειας.
- Παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοσφάλειας, και της παρέχει όλα τα κατάλληλα μέσα για να διευκολύνει το έργο της.
- Ο ρόλος του στην οργανωτική δομή του Οργανισμού προτείνεται να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Κάθε Οργανισμός κοινοποιεί στην Εθνική Αρχή Κυβερνοασφάλειας τα στοιχεία επικοινωνίας του εκάστοτε Υπευθύνου που έχει οριστεί και το αργότερο εντός 2 μηνών από την έκδοση της παρούσας υπουργικής απόφασης

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- **Κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών**

---

1. Σοβαρή διατάραξη, θεωρείται οποιοδήποτε συμβάν με επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών, σε συνδυασμό με τους παράγοντες της περίπτωσης 2 του άρθρου 5 του ν. 4577/2018 (Α΄ 199) και ειδικότερα όταν πληροί τουλάχιστον μία από τις ακόλουθες συνθήκες:

α) Κάθε συμβάν κατά το οποίο η συνέχεια της υπηρεσίας που παρέχεται από τον φορέα επηρεάζεται για πάνω από 100.000 χρηστοώρες. Ως συνέχεια της υπηρεσίας ορίζεται η δυνατότητα παροχής της υπηρεσίας σε αποδεκτά επίπεδα εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας.

β) Κάθε συμβάν που επηρεάζει πληθυσμό τουλάχιστον 50.000 χρηστών.

γ) Απειλή σε ανθρώπινη ζωή. Σε περίπτωση απώλειας ανθρώπινης ζωής το συμβάν κρίνεται αυτομάτως κοινοποιήσιμο.

δ) Το συμβάν έχει προκαλέσει υλικές ζημιές στον ίδιο τον φορέα ή σε άλλους φορείς που υπερβαίνουν το 1.000.000 ευρώ.

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Ενσωμάτωση NIS)- **Ενημέρωση του Κοινού**

1. Κατόπιν διαβούλευσης με τον Οργανισμό, και όταν αυτό κρίνεται απαραίτητο για την καλύτερη διαχείριση του συμβάντος, η ΕΑΚ μεριμνά για την ενημέρωση του κοινού που απολαμβάνει την υπηρεσία που επηρεάστηκε από το συμβάν σχετικά με την ύπαρξή του, την αντιμετώπισή του και την πιθανή διατάραξη της ομαλής λειτουργίας την οποία υπέστησαν.

2. Η ενημέρωση του κοινού δεν ενδείκνυται όταν:

α) αφορά ευαίσθητες ή διαβαθμισμένες πληροφορίες

β) επηρεάζει δυσανάλογα τα έννομα συμφέροντα του Οργανισμού.

Σε περίπτωση που η ΕΑΚ κρίνει ότι δεν συντρέχουν οι λόγοι (α) και (β) μπορεί να ενημερώσει το κοινό κρίνοντας κατά περίπτωση και αναλογικά.

Υπουργική Απόφαση 1027/8.10.2019 του Υπουργού Επικρατείας, για θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Ενσωμάτωση NIS)- **Κυρώσεις**

1. Λαμβάνοντας υπόψη τις διατάξεις του άρθρου 15 του ν. 4577/2018 (Α΄ 199), ο Υπουργός Ψηφιακής Διακυβέρνησης, μετά από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, επιβάλλει σε φυσικά ή νομικά πρόσωπα, διαζευκτικά ή σωρευτικά, τη λήψη συγκεκριμένων διορθωτικών μέτρων εντός τακτού χρονικού διαστήματος, καθώς και διοικητικές κυρώσεις για τις διαπιστούμενες παραβάσεις στις οποίες αυτά υποπίπτουν είτε μία ή περισσότερες από τις εξής κυρώσεις:

α) Σύσταση προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που, κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι δεν τηρούνται τα απαιτούμενα από το νόμο μέτρα ασφαλείας.

β) Επίπληξη προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι παρά την πρότερη σύσταση της αρχής δεν συμμορφώθηκαν με τις υποδείξεις της ΕΑΚ. γ) Στην περίπτωση μη συμμόρφωσης του Οργανισμού με την διαδικασία σύστασης η επίπληξης, επιβάλλεται διοικητικό πρόστιμο στον Οργανισμό σύμφωνα με τις διατάξεις του άρθρου 15 του ν. 4577/2018 (Α΄ 199).

2. Κατά την επιμέτρηση της κύρωσης λαμβάνονται υπόψη τα κριτήρια της αποτελεσματικότητας, της αναλογικότητας και του αποτρεπτικού χαρακτήρα της κύρωσης.

Το νέο θεσμικό πλαίσιο "data reform package"

Κανονισμός (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**).

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.

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.

Διαδικασία αναθεώρησης Οδηγίας **e- privacy** - (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

Ο νέος Κανονισμός

Αντικαθιστά τη βασική Οδηγία 95/46/ΕΚ

Έχει τεθεί σε ισχύ από τις 4.5.2016, θα τεθεί σε εφαρμογή από τις **25 Μαΐου 2018**

Έως τότε οι εταιρείες θα πρέπει να εξασφαλίσουν ότι ανταποκρίνονται στις επιβαλλόμενες **νέες υποχρεώσεις**

Θα βοηθηθούν από οδηγίες, γνωμοδοτήσεις, κατευθυντήριες γραμμές αρμόδιων αρχών

Βασικές ρυθμίσεις νέου Κανονισμού

Ανανεωμένοι & νέοι ορισμοί, π.χ.:
- Κατάρτιση προφίλ
- Ψευδωνυμοποίηση
- Γενετικά δεδομένα, βιομετρικά δεδομένα

Ευαίσθητα: +**γενετικά, βιομετρικά**

Ειδικές προϋποθέσεις για συγκατάθεση **παιδιού**

Επαναδιατύπωση αρχών επεξεργασίας

Νέα δικαιώματα «υποκειμένων»
- Διαγραφής- **δικαίωμα λήθης** (Βλ. υπόθεση Costeja)
- Φορητότητας δεδομένων
- Εναντίωσης στην κατάρτιση προφίλ ή σε απόφαση βάσει αυτού
- Πληροφόρησης για παραβίαση

Τροποποίηση υποχρεώσεων υπεύθυνων επεξεργασίας
- Κατάργηση υποχρέωσης γνωστοποίησης αρχείου
- Privacy by design & privacy by default
- Διατήρηση αρχείων επεξεργασίας
- Γνωστοποίηση εντός 72 ωρών παραβιάσεων
- Impact assessment

Νέος θεσμός **Data Protection Officer (DPO)**- υπεύθυνος προστασίας δεδομένων

Νέες ρυθμίσεις για εποπτεύουσες αρχές

Κυρώσεις για υπεύθυνους ή εκτελούντες την επεξεργασία

GDPR- TOMs

1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,

β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,

δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

3. Η τήρηση εγκεκριμένου κώδικα δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της παραγράφου 1 του παρόντος άρθρου.

4. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Γιατί να τα τηρήσω όλα αυτά;

«Παραβάσεις …επισύρουν, … **διοικητικά πρόστιμα έως**

20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, **έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο»

Ασφαλιστική κάλυψη για κινδύνους από κυβερνοέγκλημα ή διαρροή προσωπικών δεδομένων;

Ελληνικές Υποθέσεις

Στο πλαίσιο της διεθνούς επιχείρησης «Pangea X» ολοκληρώθηκε η έρευνα και σχηματίσθηκε δικογραφία σε βάρος διαχειριστών (16) ιστοσελίδων, που προωθούσαν και πωλούσαν μέσω διαδικτύου πλήθος παράνομων φαρμακευτικών προϊόντων και σκευασμάτων, σε παγκόσμιο επίπεδο

Συμμετοχή σε διεθνή επιχείρηση, υπό το συντονισμό της Europol , για την προστασία της πνευματικής ιδιοκτησίας και των συνδρομητικών υπηρεσιών στο διαδίκτυο

Συμμετοχή, από 18 έως 22 Ιουνίου 2018, σε διεθνούς κλίμακας αστυνομική επιχείρηση για την καταπολέμηση των απατών στον τομέα των αερομεταφορών. Συνελήφθησαν (13) άτομα και σχηματίστηκε δικογραφία σε βάρος (25) ατόμων

Συμμετοχή σε διεθνή αστυνομική επιχείρηση για την καταπολέμηση των απατών στον τομέα του ηλεκτρονικού εμπορίου (e-commerce) υπό το συντονισμό και την υποστήριξη της Europol

Από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος σχηματίσθηκε δικογραφία σε βάρος (2) ημεδαπών, οι οποίοι εξαπατούσαν συστηματικά πολίτες μέσω διαδικτύου. Εξιχνιάστηκαν συνολικά τριάντα μία (31) υποθέσεις

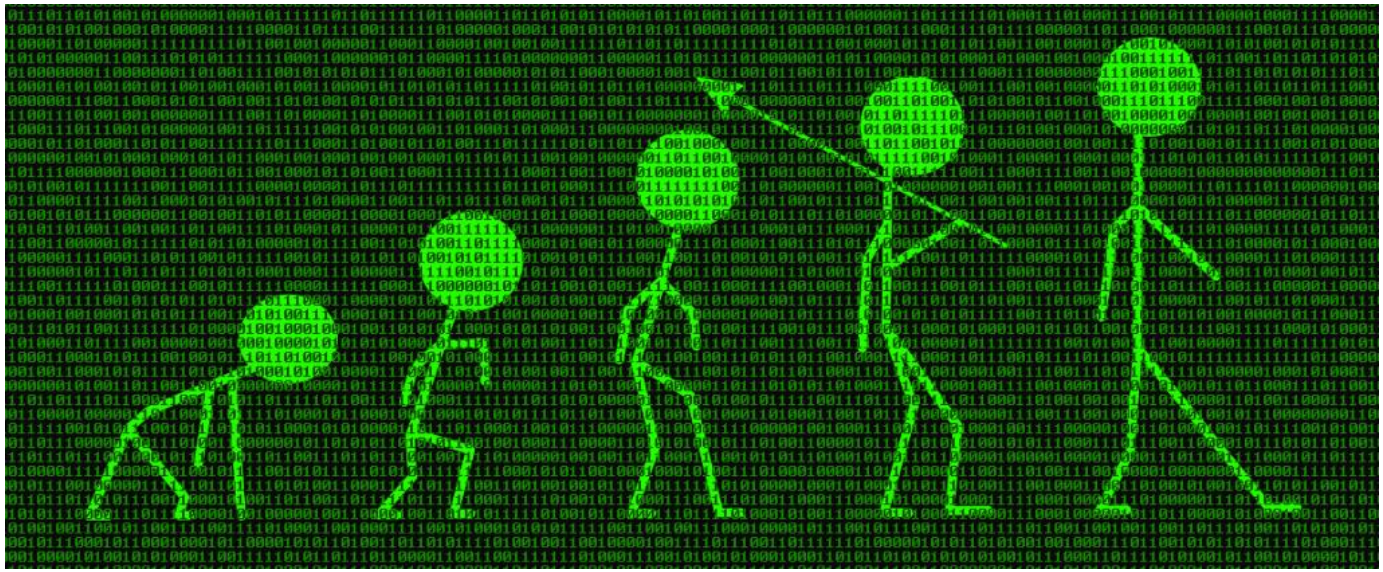
Στο πλαίσιο ελέγχων για τον παράνομο στοιχηματισμό, λόγω της διεξαγωγής του Παγκόσμιου Κυπέλλου Ποδοσφαίρου 2018, σχηματίστηκε δικογραφία για (2) ιστότοπους, που παρείχαν υπηρεσίες τυχερών παιγνίων μέσω διαδικτύου, χωρίς νόμιμη άδεια

Συμμετοχή, από 9 έως 16 Οκτωβρίου 2018, στην 11η διεθνή επιχείρηση με την κωδική ονομασία «Pangea XI», που πραγματοποιήθηκε υπό το συντονισμό της Interpol, για την καταπολέμηση της παράνομης διακίνησης και πώλησης φαρμάκων και ιατροτεχνολογικών προϊόντων μέσω διαδικτύου

Σχηματίσθηκε δικογραφία τακτικής διαδικασίας, σε βάρος τριών ατόμων για απάτη και νοθεία τροφίμων που λάμβαναν χώρα μέσω ιστοσελίδων και με τη χρήση απατηλής διαφήμισης
http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=86396&Itemid=2273&lang=


MR. ROBOT

Εν κατακλείδι



ΕΞΕΛΙΞΕΙΣ...

https://ec.europa.eu/digital-single-market/en/e-commerce-directive

Liability of Intermediaries

The Directive exempts intermediaries from liability for the content they manage if they fulfil certain conditions:

service providers hosting content, once they are aware of the illegal nature of the hosted content, they need to remove it or disable access to it expeditiously.

to be covered by the liability exemption they have to play a neutral, merely technical and passive role towards the hosted content.

Member States cannot impose to intermediaries any general obligation to monitor the content they manage.

The Commission, in its Staff Working Document on online services, including e-commerce, in the Single Market (2012), reported on the functioning of the Directive and identified that the liability regime outlined in it needed some clarification. It also announced a horizontal initiative on notice and action procedures.

A public consultation on The future of electronic commerce already took place in 2010, and a public consultation on notice-and-action procedures followed on 2012. Both will equally feed the present work on the DSM Strategy.