



9<sup>ο</sup> Πανελλήνιο Συνέδριο Ε.Ε.Ν. Ε-θέμις

# “SMART HOME”

ή

ο νέος, έξυπνος μεγάλος αδελφός

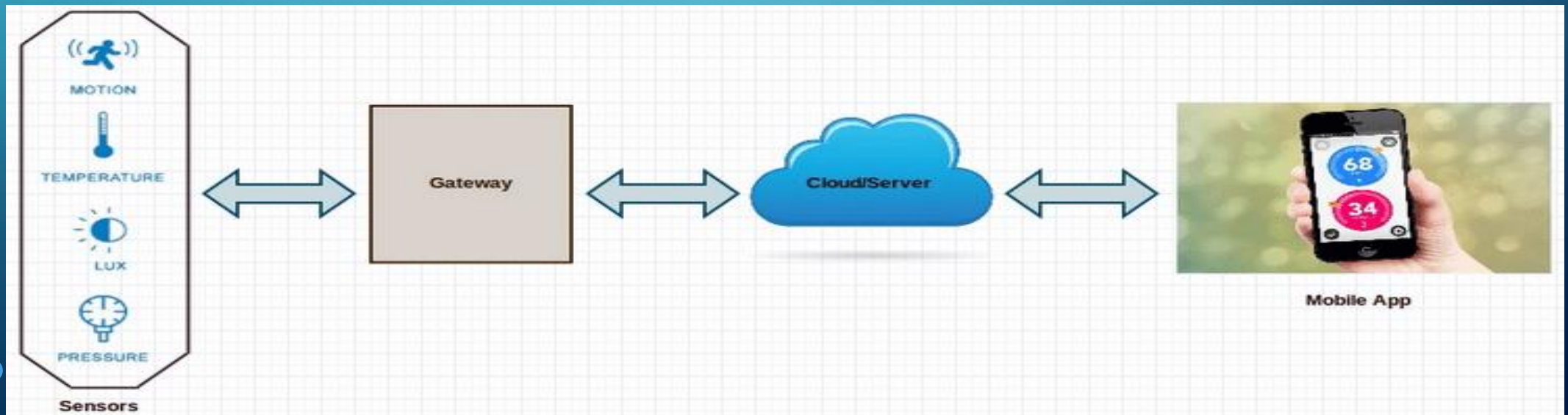
Δημήτριος Ι. Γκύζης, LL.M.

Αντισταγγελέας Εφετών

# Το “διαδίκτυο των πραγμάτων” ή Internet of things (IoT).

Η σύνδεση διάφορων μικρών και μεγάλων συσκευών με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης (tablets, τηλέφωνα, ηχεία, wearables, κάμερες, αισθητήρες κ.α.), τόσο μεταξύ τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά ψηφιακά δεδομένα (data) με στόχο να προσφέρουν αυτοματοποιημένες και εξατομικευμένες υπηρεσίες.

## Η αρχιτεκτονική του IoT.



## «Έξυπνο» σπίτι. Τομέας του ΙοΤ.

- Αισθητήρες ανιχνεύουν τις δραστηριότητες των παρευρισκόμενων στον οικιακό ή εργασιακό χώρο ώστε να ρυθμίζουν την θερμοκρασία με σκοπό την εξοικονόμηση ενέργειας
- «Έξυπνα» ψυγεία ελέγχουν την κατανάλωση και τη διαθεσιμότητα των προϊόντων μέσα από την τοποθέτηση μικροσκοπικών ετικετών και ενημερώνουν τους χρήστες για την έλλειψη τους ή κάνουν αυτόματα παραγγελία στο σούπερ μάρκετ.
- «Έξυπνο» σύστημα ασφάλειας ελέγχει κάμερες εσωτερικών και εξωτερικών χώρων, τον συναγερμό, τις κλειδαριές και τα παράθυρα με την συσκευή του smartphone.



# Χιονοστιβάδα Δεδομένων

Σε ένα «έξυπνο» σπίτι παράγεται τεράστιος αριθμός δεδομένων με την συχνή χρήση των «έξυπνων» οικιακών συσκευών. Τα δεδομένα αυτά πρέπει να αποθηκεύονται και να αναλύονται για τη λήψη πληροφοριών σχετικά με ορισμένες παραμέτρους. Όταν συνδέονται όλες οι συσκευές, ο αριθμός των δεδομένων που συλλέγονται θα αυξηθεί πολλές φορές. Η συλλογή, η ανάλυση και η αποθήκευση όλων αυτών των δεδομένων είναι ένα δύσκολο έργο κάτι που χρειάζεται καλύτερη υποδομή για τη διαχείριση της χιονοστιβάδας δεδομένων που δημιουργούνται (“SWOT Analysis of the Internet of Things”, Saloni Bansal, 2015).

# Έννομα Αγαθά Σε Κίνδυνο.

Δεδομένα.
<b>Κυβερνοέγκλημα</b>

Περιεχόμενο δεδομένων.	
Δεδομένα Προσωπικού Χαρακτήρα	Δεδομένα Επικοινωνίας
<b>Παράνομη Επεξεργασία ΔΠΧ</b>	<b>Παραβίαση απορρήτου</b>

# Επιθέσεις Κατά Πληροφοριακών Συστημάτων/ Attacks Against Information Systems Νομικό Πλαίσιο/Legal Framework

- Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο («Σύμβαση Βουδαπέστης», 23.ΧΙ.2001).
- Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.
- Κύρωση/ενσωμάτωση με Ν. 4411/2016.
- Νέα άρθρ. 13 στοιχ. γ' εδ. β', η', θ', 292B, 292Γ, 370Γ, 370Δ, 370Ε, 381Α, 381Β Π.Κ.
- CoE Convention on Cybercrime (Budapest, 23.XI.2001).
- Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems.
- Ratification L. 4411/2016.
- New articles 13.h, i, 292B, 292C, 370C, 370D, 370E, 381A, 381B P.C.

# Βασικές Έννοιες/Definitions

## Άρθρο 13 ΠΚ

- γ) ... . **Έγγραφο** είναι **και** κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.
- 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.

## Directive 2013/40/EU

For the purposes of this **Directive**, the following definitions shall apply:

- (a) '**information system**' means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;
- (b) '**computer data**' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function; (Article 2)

## Budapest Convention

For the purposes of this **Convention**:

- a "**computer system**" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "**computer data**" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; (Article 1)

## Έννομα Αγαθά/Legitimate Interests

- Διαθεσιμότητα Π.Σ.
  - Παρακώλυση λειτουργίας Π.Σ.
- Ακεραιότητα Π.Σ.
  - Φθορά Ψ.Δ.
- **Εμπιστευτικότητα Π.Σ.**
  - Παράνομη πρόσβαση σε Π.Σ.
  - Υποκλοπή Ψηφιακών Δεδομένων (Ψ.Δ.)
- Availability of I.S.
  - Illegal system interference
- Integrity of I.S. and C.D.
  - Illegal data interference
- **Confidentiality of I.S.**
  - Illegal access to I.S.
  - Illegal interception of computer data (C.D.)



# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## I. Παράνομη πρόσβαση σε Π.Σ./Illegal access to I.S.

### Παράνομη πρόσβαση σε Π.Σ.

- ά. 13 η', θ', 370Γ παρ. 2-4 ΠΚ
- ά. 3 Οδηγίας 2013/40/ΕΕ
- ά. 2 Σύμβασης Βουδαπέστης

### Προπαρασκευαστικές πράξεις

- ά. 370Ε ΠΚ
- ά. 7 Οδηγίας 2013/40/ΕΕ
- ά. 6 Σύμβασης Βουδαπέστης

### Illegal access to I.S

- Art. 13.h, i, 370C par. 2-4 P.C.
- Art. 3 Directive 2013/40/EU
- Art. 2 Budapest Convention

### Misuse of devices

- Art. 370E P.C.
- Art. 7 Directive 2013/40/EU
- Art. 6 Budapest Convention

# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## I. Παράνομη πρόσβαση σε Π.Σ./Illegal access to I.S.

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

**Διακεκριμένη μορφή** : Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το ά. 148 ΠΚ (κατασκοπεία).

(ά. 370Γ ΠΚ)

The intentional access without right, to the whole or to any part of an information system, where committed by infringing a security measure (Art. 3 Directive 2013/40/EU)

The intentional access to the whole or any part of a computer system, without right (Art. 2 Budapest Convention)

## Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

### Ι. Παράνομη πρόσβαση σε Π.Σ./Illegal access to I.S.

#### Α. Πράξεις παράνομης πρόσβασης σε πληροφοριακό σύστημα

1. **Παράνομη πρόσβαση σε πληροφοριακό σύστημα** (βασικό έγκλημα).
2. **Παράνομη πρόσβαση σε πληροφοριακό σύστημα**, που αφορά στις διεθνείς σχέσεις ή την ασφάλεια του κράτους (διακεκριμένη μορφή).
3. **Παράνομη πρόσβαση σε πληροφοριακό σύστημα**, που αφορά στις διεθνείς σχέσεις ή την ασφάλεια του κράτους **με σκοπό κατασκοπείας** (διακεκριμένη μορφή).
4. **Παράνομη πρόσβαση σε πληροφοριακό σύστημα**, που αφορά στις διεθνείς σχέσεις ή την ασφάλεια του κράτους **με σκοπό κατασκοπείας σε καιρό πολέμου** (διακεκριμένη μορφή).

# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## I. Παράνομη πρόσβαση σε Π.Σ./Illegal access to I.S.

## B. [Προπαρασκευαστικές πράξεις]/Misuse of devices

Όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των ά. ... 370Γ παρ. 2 και 3 ... παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί:

α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των ά. ... 370Γ ...,

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.

(ά. 370Ε ΠΚ)

Tools used for committing offences : the intentional production, sale, procurement for use, import, distribution or otherwise making available, of (a) a computer programme, (b) a computer password, access code, or similar data, without right and with the intention that it be used to commit the offences referred to in Art 3 to 6 (Art. 7 Directive 2013/40/EU)

Misuse of devices : a. the production, sale, procurement for use, import, distribution or otherwise making available of : i. device, including a computer program, ii. computer password, access code, or similar data, b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5 (Art. 6 Budapest Convention)

Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

**I. Παράνομη πρόσβαση σε Π.Σ./Illegal access to I.S.**

**A. Προπαρασκευαστικές πράξεις παράνομης πρόσβασης σε πληροφοριακό σύστημα.**

- 1. Διακίνηση** συσκευών ή προγραμμάτων υπολογιστή με σκοπό την παράνομη πρόσβαση σε πληροφοριακό σύστημα.
- 2. Διακίνηση** συνθηματικών κλπ. με σκοπό την παράνομη πρόσβαση σε πληροφοριακό σύστημα.

# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## II. Υποκλοπή Ψ.Δ./Illegal Interception Of C.D.

### Υποκλοπή/Χρήση Ψ.Δ.

- ά. 13 η', θ', 370Δ ΠΚ
  - ά. 6 Οδηγίας 2013/40/ΕΕ
  - ά. 3 Σύμβασης Βουδαπέστης
- ### Προπαρασκευαστικές πράξεις
- ά. 370Ε ΠΚ
  - ά. 7 Οδηγίας 2013/40/ΕΕ
  - ά. 6 Σύμβασης Βουδαπέστης

### Illegal interception

- Art. 13.h, i, 370D P.C.
  - Art. 6 Directive 2013/40/EU
  - Art. 3 Budapest Convention
- ### Misuse of devices
- Art. 370E P.C.
  - Art. 7 Directive 2013/40/EU
  - Art. 6 Budapest Convention

## Εμπιστευτικότητα Π.Σ./Confidentiality of I.S. II. Υποκλοπή Ψ.Δ./Illegal Interception Of C.D.

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.

Όποιος κάνει **χρήση** της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους ανωτέρω τρόπους.

Διακεκριμένη μορφή : Αν οι πράξεις συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το ά. 146 ΠΚ (παραβίαση μυστικών της Πολιτείας).

The intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right (Art. 6 Directive 2013/40/EU)

The intentional interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data (Art. 3 Budapest Convention)

# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## II. Υποκλοπή Ψ.Δ./Illegal Interception Of C.D.

### A. Πράξεις υποκλοπής ψηφιακών δεδομένων

1. Υποκλοπή **ψηφιακών δεδομένων** (βασικό έγκλημα).
2. Υποκλοπή **απόρρητων ψηφιακών δεδομένων** (διακεκριμένη μορφή).
3. Υποκλοπή **απόρρητων ψηφιακών δεδομένων σε καιρό πολέμου** (διακεκριμένη μορφή).

άρθρ. 370Δ παρ. 1 ΠΚ.

1. Χρήση **ψηφιακών δεδομένων**, που έχουν υποκλαπεί (βασικό έγκλημα).
2. Χρήση **απόρρητων ψηφιακών δεδομένων**, που έχουν υποκλαπεί (διακεκριμένη μορφή).
3. Χρήση **απόρρητων ψηφιακών δεδομένων**, που έχουν υποκλαπεί, **σε καιρό πολέμου** (διακεκριμένη μορφή).

άρθρ. 370Δ παρ. 2 ΠΚ.



# Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

## II. Υποκλοπή Ψ.Δ./Illegal Interception Of C.D.

### B. [Προπαρασκευαστικές πράξεις]/Misuse of devices

Όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των ά. ... 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 ά. ... 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.

Tools used for committing offences : the intentional production, sale, procurement for use, import, distribution or otherwise making available, of (a) a computer programme, (b) a computer password, access code, or similar data, without right and with the intention that it be used to commit the offences referred to in Art 3 to 6 (Art. 7 Directive 2013/40/EU)

Misuse of devices : a. the production, sale, procurement for use, import, distribution or otherwise making available of : i. device, including a computer program, ii. computer password, access code, or similar data, b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5 (Art. 6 Budapest Convention)

Εμπιστευτικότητα Π.Σ./Confidentiality of I.S.

II. Υποκλοπή Ψ.Δ./Illegal Interception Of C.D.

B. Προπαρασκευαστικές πράξεις υποκλοπής ψηφιακών δεδομένων.

**1. Διακίνηση** συσκευών ή προγραμμάτων υπολογιστή με σκοπό την υποκλοπή ψηφιακών δεδομένων.

**2. Διακίνηση** συνθηματικών κλπ με σκοπό την υποκλοπή ψηφιακών δεδομένων.