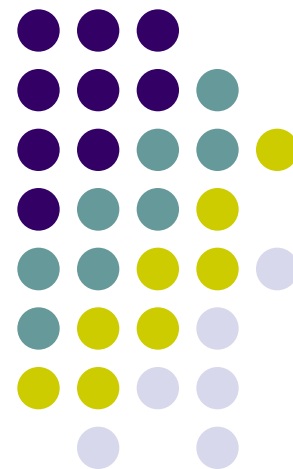


Το δικαίωμα στην ιδιωτικότητα κατά την εξέλιξη του διαδικτύου

*Απο τον ιστό της πληροφορίας στον ιστό
της σημασίας της πληροφορίας*

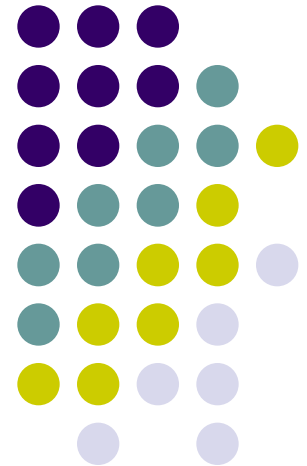
Μαρία Γιαννακάκη

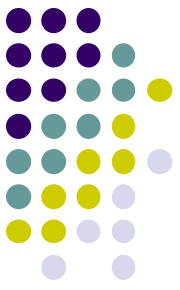
Δικηγόρος, D.E.A., υπ.Δρ. ΕΚΠΑ



Διάγραμμα παρουσίασης

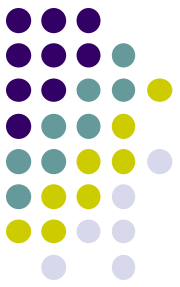
- Η εξέλιξη του διαδικτύου: Web 1.0 – Web 2.0 – Web 3.0
- Τα χαρακτηριστικά της έκρηξης του Μεγάλου όγκου Δεδομένων ('Big Data')
- Οι προκλήσεις για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων
- Οι ρυθμίσεις της Οδηγίας 95/46/ΕΚ
- Οι Προτάσεις υπό το Σχέδιο Κανονισμού
- Νέα προσέγγιση των δεδομένων βάσει της χρήσης τους και της αξίας της πληροφορίας





Η εξέλιξη του διαδικτύου {I}

Web 1.0	Web 2.0	Web 3.0
1996	2006	2016
Το Διαδίκτυο	Το Συμμετοχικό /Κοινωνικό Διαδίκτυο	Το Σημασιολογικό Διαδίκτυο/ the web of data
Διαδίκτυο απλής ανάγνωσης (Read only Web)	Ανοικτό Διαδίκτυο γραφής και ανάγνωσης (Read and write Web)	Ανοικτό Διαδίκτυο γραφής, ανάγνωσης και εκτέλεσης (Read – Write – Execute Web)
Tim Berners Lee	Tim O' Reilly	Sir Tim Berners Lee
45 χιλιάδες χρήστες (1996)	1 δισεκατομμύριο χρήστες (2006)	Τρισεκατομμύρια χρήστες
Προσωπικές ιστοσελίδες	Ιστολόγια	Παγίωση δυναμικού περιεχομένου
Σύνδεση πληροφοριών	Σύνδεση ανθρώπων	Σύνδεση γνώσης
HTML, portals	XML, RSS	Συμπεριφορά χρήστη (me-onomy)



Η εξέλιξη του διαδικτύου {II}

Web 1.0	Web 2.0	Web 3.0
Κατάλογοι/ Συστηματική κατάταξη (taxonomy)	Κατηγοριοποίηση περιεχομένου από χρήστες με τη χρήση ετικετών Tagging (folksonomy)	Κατανόηση συμπεριφοράς χρηστών (user behavior)
Netscape	Google	iGoogle, NetVibes
Αριθμός προβολών ιστοσελίδας	Κόστος ανά κλικ (cost per click)	Πιστότητα χρηστών User engagement
Διαφήμιση: Στατικές ενημερωτικές πύλες οι οποίες παρουσιάζουν διαφήμιση (προβολή και αναζήτηση)	Τοποθέτηση δυναμικής και στοχευμένης διαφήμισης με τη χρήση προηγμένων τεχνολογιών με τη χρήση ευρυζωνικών συνδέσεων, διαδραστικών και οπτικοακουστικών στοιχείων)	Εξατομικευμένη διαφήμιση βασιζόμενη στις προτιμήσεις των χρηστών, στη συμμετοχή του σε κοινότητες και άλλων χαρακτηριστικών

WEB 1.0



Ο Παγκόσμιος Ιστός ξεκίνησε ως μια τεράστια βάση δεδομένων, στην οποία φαινομενικά εύκολα θα μπορούσε κάποιος να πλοηγηθεί χρησιμοποιώντας τη δυνατότητα των υπερσυνδέσμων και εντοπιστών πόρων (URL).

Αποτελούσε πηγή πληροφόρησης, η οποία ήταν επαρκής σε εποχές που η αναζήτηση της πληροφορίας χαρακτηριζόταν από τη **γραμμικότητα** και τη **μονοδιάστατη κατηγοριοποίηση της γνώσης** σε αυστηρά καθορισμένα επιστημονικά πεδία.

Τα χαρακτηριστικά αυτά αποτέλεσαν και το μεγαλύτερο 'πρόβλημα' του Παγκόσμιου Ιστού στην εποχή του Web 1.0. για το λόγο ότι οι εφαρμογές του Web 1.0 δεν διακρίνονταν από τις ικανότητες:

- κατανόησης του νοήματος των λέξεων / των κειμένων / των λέξεων που βρίσκονται δίπλα και πέρα από τις λέξεις των κειμένων,
- διαχωρισμού των πραγματικά σημαντικών λέξεων από αυτές που τυχαία εμφανίζονται στο κείμενο των εγγράφων.
- παραγωγής χρήσιμων κειμένων για τις καθημερινές πρακτικές ανάγκες κάτι το οποίο εξελίσσεται στην εποχή του Web 3.0

WEB 2.0



Το Web 2.0 επιτρέπει στους χρήστες να χρησιμοποιήσουν το **διαδίκτυο ως διαδικτυακή πλατφόρμα επικοινωνίας “Web as a Platform”** προκειμένου να δημιουργήσουν και να διαδώσουν το δικό τους περιεχόμενο - **User Generated Content (“UGC”)**.

Αποτελεί το **συμμετοχικό διαδίκτυο το οποίο επιτρέπει στους χρήστες να δημιουργήσουν περιεχόμενο** (σε αντίθεση με το Web 1.0 στο οποίο οι χρήστες είναι απλά και μόνο ‘καταναλωτές’ περιεχομένου)

Κοινωνικά Δίκτυα: ψηφιακές κοινότητες που μέσω της δημιουργίας ενός προφίλ επιτρέπουν στους ανθρώπους να συναντώνται, να επικοινωνούν, να παραμένουν σε επαφή, να μοιράζονται φωτογραφίες και εικόνες με άλλα μέλη της κοινότητας.

ENISA – “Online as soon as it happens”

Υπηρεσίες Κοινωνικής Δικτύωσης: διαδικτυακές πλατφόρμες επικοινωνίας, οι οποίες επιτρέπουν στα άτομα να προσχωρούν σε ή να δημιουργούν δίκτυα χρηστών με παρόμοιες ιδέες

Data Protection Working Party a. 29

Η διάκριση μεταξύ Web 1.0 και Web 2.0 έχει διάσταση:

- **Τεχνολογική** (τεχνολογικές εφαρμογές που επιτρέπουν τη διαδραστική σχέση των χρηστών)
- **Δομική:** (σκοπός και δομή του ιστοχώρου)
- **Κοινωνιολογική:** (έννοια των φίλων και των ομάδων)

Μήτρου – “Ιδιωτικότητα στο Web 2.0”

WEB 3.0 {I}



Ο Σημασιολογικός Ιστός (Semantic Web) είναι ένα **πλέγμα διασυνδεδεμένων δεδομένων**. Αποτελεί τη νέα γενιά του Διαδικτύου, όπου η πληροφορία αποκτά **δομή και σημασιολογία**, ώστε να υποστηριχθεί η αποδοτική αναζήτηση, επεξεργασία και ενοποίηση δεδομένων, δίνοντας νόημα (σημασιολογία) στο περιεχόμενο των εγγράφων του Παγκόσμιου Ιστού, κατά τρόπο κατανοητό από τους υπολογιστές (Semantic Web) (Hendler, 2004).

Εν συντομία τα χαρακτηριστικά του είναι:

- η **απόδοση σημασίας** στα δεδομένα
- η δημιουργία **υπερσυνδέσμων με σημασιολογικό χαρακτήρα**
- η δυνατότητα **εννοιολογικής συσχέτισης των δεδομένων**
- η δημιουργία **μηχανικά αναγνωρίσιμης, κατανοήσιμης και επεξεργάσιμης πληροφορίας**

Χαρακτηριστική περίπτωση του Σημασιολογικού Ιστού είναι η **σημασιολογική αναζήτηση βάσει της οποίας οι μηχανές αναζήτησης καταλαβαίνουν τη σημασία των δεδομένων ώστε να μπορούν να εντοπίζουν ποιες πληροφορίες χρειάζεται ο χρήστης και να τις παρέχουν πριν καν τις ζητήσει**.

WEB 3.0 {II}



*«Web 3.0 σημαίνει αδιάλειπτη, οποτεδήποτε και οπουδήποτε, επιχειρηματική δραστηριότητα, ψυχαγωγία και κοινωνική δικτύωση **με ταχύτητα, αξιόπιστα και ασφαλή δίκτυα**. Σημαίνει το τέλος μεταξύ κινητών και σταθερών γραμμών. Σηματοδοτεί άλμα δεκαπλασιασμού της κλίμακας του ψηφιακού σύμπαντος που θα έχει συντελεστεί το έτος 2015.»*

Viviane Redding

*«το Web 3.0 θα απαρτίζεται από **εφαρμογές που θα λειτουργούν όλες μαζί** και θα διατίθενται μέσα από κοινωνικά δίκτυα, ηλεκτρονικό ταχυδρομείο κλπ. Οι εφαρμογές θα είναι **εξαιρετικά γρήγορες** και θα μπορούν να τρέξουν **σε οποιοδήποτε υπολογιστή** και να **τροποποιηθούν από οποιονδήποτε χρήστη**.»*

Eric Schmidt – Διευθύνων Σύμβουλος της Google

WEB 3.0 {III}



Το Web 3.0 αναφέρεται σε ένα σύνολο τεχνολογιών και μεθόδων μέσω των οποίων οι υπολογιστές είναι σε θέση να αντιλαμβάνονται τη **σημασία της πληροφορίας**, να διαχειρίζονται και να προσεγγίζουν τις έννοιες των λέξεων **πλησιέστερα στην ανθρώπινη νοημοσύνη** και να τις **αποδίδουν με όρους τους οποίους μπορούν να ερμηνεύσουν και να ανταλλάξουν οι υπολογιστές**.

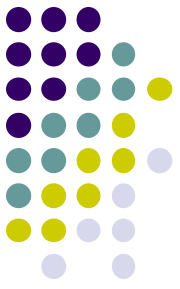
Διακρίνουμε μεταξύ:

- **Δεδομένων:** πρωτογενών –μη επεξεργασμένων πληροφοριών (raw data) στις οποίες δίδεται ή μπορεί να δοθεί μια σημασία και
- **Πληροφορίας:** δηλαδή του στοιχείου της γνώσης που μετουσιώνει και δίνει αξία στα δεδομένα. Η σημασία δίδεται σε ένα σύνολο δεδομένων βάσει κανόνων που έχουν τεθεί εκ των προτέρων.

ΠΛΗΡΟΦΟΡΙΑ = ΔΕΔΟΜΕΝΑ + ΕΠΕΞΗΓΗΣΗ

Η έννοια της πληροφορίας παραπέμπει αυτόματα στην «**πληροφοριακή της αξία**» και **σχετίζεται με τη χρησιμότητα της**, ενώ στην **έννοια των δεδομένων** προσδίδεται **μια ουδετερότητα** όσον αφορά στο σκοπό.

{Μήτρου – “Ιδιωτικότητα στο Web 2.0” }



Εξόρυξη δεδομένων - Data mining

Η απόδοση σημασίας στα δεδομένα του διαδικτύου (σημασιολογικές φόρμες) απελευθερώνει πλήθος δυνατοτήτων για τη **διαχείριση της γνώσης** και για μια πιο **ευφυή εκμετάλλευση** τους.

Με τον τρόπο αυτό παρέχεται η δυνατότητα:

- **επίλυσης προβλημάτων** που θεωρούνται χρονοβόρα, βοηθώντας στη γρήγορη εύρεση πληροφοριών
- **αξιολόγησης μιας πληροφορίας και σωστής διαχείρισής της**, ώστε να παραχθεί γνώση, και
- **η μετατροπή της πληροφορίας σε μεταγνώση.**

Η απόδοση σημασίας στα δεδομένα του διαδικτύου και η εξαγωγή πληροφοριών από αυτά πραγματοποιείται μέσω του data mining, της τεχνικής εξόρυξης χρήσιμων πληροφοριών από τα δεδομένα χρησιμοποιώντας τεχνικές **οργάνωσης, ταξινόμησης, φιλτραρίσματος και μοντελοποίησης.**

Η τεχνική της εξόρυξης δεδομένων (data mining), αποτελεί την **ανακάλυψη γνώσης από τη συσχέτιση (correlation) μεγάλου όγκου δεδομένων** με τη χρήση αλγόριθμων ομαδοποίησης ή κατηγοριοποίησης και των αρχών της στατιστικής, της τεχνικής νοημοσύνης της μηχανικής μάθησης. Μέσω της διαδικασίας αυτής εξευρίσκονται ή εξάγονται **με έμμεσο τρόπο νέες μη προφανείς και δυνητικά χρήσιμες πληροφορίες και πρότυπα** και πιθανολογούνται συμπεράσματα.

Big Data {I}



Η τεχνική της εξόρυξης δεδομένων χρησιμοποιείται κυρίως για την επεξεργασία Μεγάλου όγκου Δεδομένων –

Ως Μεγάλα Δεδομένα - Big Data ορίζονται:

«σύνολα δεδομένων των οποίων το μέγεθος υπερβαίνει την ικανότητα τυπικών λογισμικών βάσεων δεδομένων να συλλάβουν, να αποθηκεύσουν, να διαχειριστούν και να αναλύσουν»

{McKinsey Global Institute (MGI)}

«εκτενής ανάλυση των γιγαντιαίων ψηφιακών αρχείων που κατέχουν εταιρείες, κυβερνήσεις και άλλοι μεγάλοι οργανισμοί που χρησιμοποιούν αλγόριθμους με σκοπό την καλύτερη κατανόηση και την αξιοποίηση των δεδομένων προκειμένου να καταλήξουν σε καλύτερες και πιο ενημερωμένες αποφάσεις»

{Ομάδα Εργασίας α.29 της Οδηγίας 95/46/EK}

Big Data {II}



Τα χαρακτηριστικά των Μεγάλων Δεδομένων (Big Data) είναι :

- **Όγκος - Volume:** η δυνατότητα συλλογής και επεξεργασίας μεγάλου όγκου δεδομένων τα οποία καθίστανται διαχειρίσιμα με τη χρήση εξελιγμένων μεθόδων διαχείρισης (data analytics) και τη χρήση υπολογιστών με μεγάλη υπολογιστική δύναμη και ακολούθως η ικανότητα εταιρειών και κυβερνήσεων να αποκτούν πρόσβαση σε τεράστιες ποσότητες δεδομένων– δομημένων ή μη – ως επί το πλείστον μη δομημένων δεδομένων-raw data.
- **Ταχύτητα-Velocity:** η ταχύτητα στην επεξεργασία με τη χρήση εξελιγμένων προγραμμάτων για την ανάλυση των δεδομένων, τον εντοπισμό των σχέσεων μεταξύ των δεδομένων και την εξαγωγή πληροφοριών από τα δεδομένα μέσω συσχετίσεων και συμπερασμάτων.
- **Διαφορετικές πηγές προέλευσης – Variety:** κινητά δίκτυα επικοινωνιών, tablets, κάμερες, κοινωνικά δίκτυα, εταιρείες εμπορίας πληροφοριών (data brokers)



Χαρακτηριστικό παράδειγμα της μετάβασης **από τον ιστό της πληροφορίας στο σημασιολογικό ιστό και την Εποχή της Έκρηξης των Δεδομένων**, αποτελεί η τροποποίηση της Πολιτικής Ιδιωτικότητας της Google (Μάρτιος 2012).

Η εταιρεία συγχώνευσε τις 60 περίπου πολιτικές της σε 1 με την οποία **επιτρέπεται πλέον - ως προεπιλογή - η συλλογή και συσχέτιση δεδομένων από διαφορετικές υπηρεσίες της** (από την επιγραμμική – online δραστηριότητα των χρηστών μέσω της μηχανής αναζήτησης, του Google Earth, μέσω των συστημάτων Android, YouTube, Gmail και το Google+ social network κλπ)

Η **συλλογή τεράστιου όγκου δεδομένων από διαφορετικές πηγές** επιτρέπει την **κατάρτιση ενός λεπτομερούς προφίλ** των χρηστών των υπηρεσιών της Google, κυρίως για την προβολή **στοχευμένης διαφήμισης**.



Η τροποποίηση αυτή προκάλεσε την αντίδραση των Ευρωπαϊκών Αρχών Προστασίας και της Ομάδας Εργασίας του ά. 29 της Οδηγίας για τους κινδύνους που ενείχε η τροποποίηση αυτή για την ιδιωτικότητα των χρηστών. Συγκεκριμένα:

- ο χρήστης **δεν έχει τη δυνατότητα να αρνηθεί** τη συλλογή και συσχέτιση δεδομένων **για κάποιες από τις υπηρεσίες**
- δεν τηρείται η **αρχή της προστασίας της ιδιωτικότητας εξ ορισμού (privacy by default)**,
- δεν τηρούνται **οι αρχές της ποιότητας και ελαχιστοποίησης των δεδομένων, καθώς και η αρχή της αναλογικότητας**

Το Μάρτιο 2013, εκπρόσωποι της Google Inc συναντήθηκαν με εκπροσώπους των αρχών προστασίας της Γαλλίας, Γερμανίας, Ιταλίας, Ολλανδίας, Ισπανίας και Ηνωμένου Βασιλείου.

Μέχρι σήμερα η Google δεν έχει προβεί σε αλλαγές της Πολιτικής Ιδιωτικότητας της.



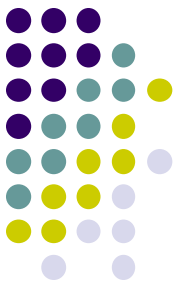
Προκλήσεις για την ιδιωτικότητα {I}

Ήδη από το 1960 με την αύξηση της χρήσης των υπολογιστών υπήρχαν ανησυχίες για την ιδιωτικότητα, οι οποίες αυξήθηκαν κατά την εξέλιξη του παγκόσμιου ιστού στην εποχή του Web 1.0 και του Web 2.0.

Ωστόσο η συλλογή του όγκου των πληροφοριών από διαφορετικές πηγές και η εξαγωγή συμπερασμάτων για ένα πρόσωπο στο πλαίσιο του Web 3.0 και των Μεγάλων Δεδομένων αποτελεί μια από τις μεγαλύτερες προκλήσεις για την ιδιωτικότητα.

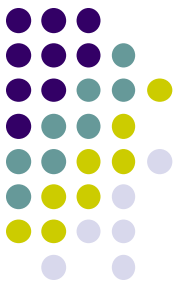
- **Συνάθροιση δεδομένων “Aggregation”**: Η ιδιωτικότητα διαταράσσεται από την συλλογή:
 - Μεγάλου όγκου Δεδομένων, η οποία επιτρέπει την παρακολούθηση σε μαζική κλίμακα μέσω της συνάθροισης πληροφοριών που αφορούν ένα πρόσωπο
 - δεδομένων από πολλές διαφορετικές πηγές
 - με δυνατότητες πολύπλοκης ανάλυσης των δεδομένων που συγκεντρώνονται και
 - συνδυασμό των δεδομένων με νέους απρόβλεπτους τρόπους και την αποκάλυψη πληροφοριών για ένα πρόσωπο οι οποίες δεν ήταν άμεσα γνωστές

Προκλήσεις στην ιδιωτικότητα {II}



- **Πολλαπλότητα σκοπών επεξεργασίας:** οι κίνδυνοι για την ιδιωτικότητα πολλαπλασιάζονται όταν πολλαπλά αρχεία από διαφορετικές πηγές συνδυάζονται μεταξύ τους και προορίζονται να χρησιμοποιηθούν για σκοπούς άμεσης προώθησης προϊόντων και υπηρεσιών (Direct marketing), συμπεριφορικής διαφήμισης (behavioural advertising), εμπορίας πληροφοριών (Data brokering), διαφήμισης βάσει της τοποθεσίας του χρήστη (location based advertising) και έρευνας αγοράς, η οποία βασίζεται σε εντοπισμό των χρηστών βάσει της θέσης τους (tracking-based digital market research).
- **Ύπαρξη δευτερογενών σκοπών (secondary use):** για τους οποίους το ΥΔ ενδέχεται να μην έχει δώσει τη συγκατάθεση του
- **Χρήση δεδομένων χωρίς συμφραζόμενα (context):** δηλαδή τα δεδομένα απομακρύνονται από τα συμφραζόμενα στο πλαίσιο των οποίων χρησιμοποιήθηκαν και χρησιμοποιούνται ανεξάρτητα από αυτά με κίνδυνο τροποποίησης της σημασίας τους
- **Μη έγκυρη συγκατάθεση των χρηστών:** οι οποίοι ενδέχεται να συγκατατίθενται στη χρήση των δεδομένων τους για τους σκοπούς εξόρυξης δεδομένων ή Big Data analytics παρότι δεν γνωρίζουν τον τρόπο και τα κριτήρια εξαγωγής των επαγωγικών συμπερασμάτων και κατά συνέπεια τη σκοπούμενη χρήση τους. Ελλοχεύει δε ο κίνδυνος να υπαχθούν σε αποφάσεις οι οποίες βασίζονται σε μια αυτοματοποιημένη διαδικασία εξαγωγής συμπερασμάτων επί της οποίας δεν έχουν κανένα έλεγχο.
- **Αδυναμία ενημέρωσης από την πλευρά των εταιρειών:** οι οποίες δεν γνωρίζουν και δεν μπορούν να γνωρίζουν εκ των προτέρων τι ενδέχεται να προκύψει από τις πληροφορίες αυτές.

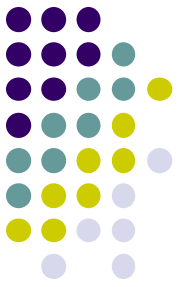
Η προστασία δεδομένων υπό την ισχύουσα νομοθεσία {I}



Η ισχύουσα Οδηγία 95/46/EK περιλαμβάνει τις **βασικές αρχές προστασίας δεδομένων**. Οι αρχές αυτές έχουν τεχνολογικά ουδέτερο χαρακτήρα και σε μια πρώτη προσέγγιση φαίνεται να καλύπτουν τις επιφυλάξεις που εγείρουν τα Μεγάλα Δεδομένα. Οι βασικές αρχές συνοψίζονται στα εξής:

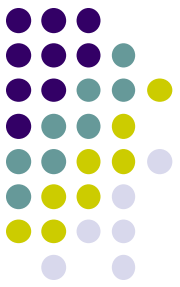
- **Ενημέρωση του υποκειμένου:** τα ΥΔ θα πρέπει να ενημερώνονται για την επεξεργασία των προσωπικών τους δεδομένων, για την ταυτότητα του ΥΕ, το σκοπό επεξεργασίας και θα πρέπει να τους επιτρέπεται να ασκούν κάποιο έλεγχο στα δεδομένα που συλλέγονται (δικαίωμα πρόσβασης, αντίρρησης, διαγραφής)
- **Συναίνεση υποκειμένου και αρχή του σκοπού:** η συλλογή των προσωπικών δεδομένων θα πρέπει να βασίζεται σε μια νόμιμη βάση επεξεργασίας (συναίνεση του υποκειμένου ή συγκεκριμένη διάταξη νόμου) και η χρήση τους θα πρέπει να γίνεται για σαφής και καθορισμένους σκοπούς. Η αρχή του σκοπού συνοδεύει τα δεδομένα κατά τη διαδικασία συλλογής, συνδυασμού, ανάλυσης και χρήσης. Αν υπάρχουν περισσότεροι σκοποί επεξεργασίας τότε το υποκείμενο των δεδομένων θα πρέπει να παρέχει ξεχωριστή συγκατάθεση για καθένα από αυτούς.
- **Απαγόρευση περαιτέρω χρήσης:** οι προσωπικές πληροφορίες δεν μπορούν να συλλέγονται για σκοπούς διαφορετικούς από αυτούς για τους οποίους το υποκείμενο των δεδομένων έδωσε τη συγκατάθεση του.

Η προστασία δεδομένων υπό την ισχύουσα νομοθεσία {II}



- **Αρχή της ακρίβειας:** τα προσωπικά δεδομένα που τηρούνται θα πρέπει να είναι ακριβή, ορθά και επικαιροποιημένα.
- **Διατήρηση δεδομένων:** όσο είναι απαραίτητο με βάση το σκοπό συλλογής τους, οι δε ΥΕ θα πρέπει να φροντίζουν για τη διαγραφή τους εφόσον δεν είναι πλέον απαραίτητα.
- **Επιπρόσθετος έλεγχος στη συλλογή συγκεκριμένων κατηγοριών δεδομένων:** συγκεκριμένες κατηγορίες δεδομένων π.χ. τα αρχεία cookies, χρήση δεδομένων θέσης και κίνησης
- **Επιπρόσθετος έλεγχος στη χρήση συγκεκριμένων δεδομένων:** π.χ. Robinson's lists, Opt-Out Registries
- **Αυτοματοποιημένη λήψη αποφάσεων**

Η προστασία δεδομένων υπό τον Προτεινόμενο Σχέδιο Κανονισμού {II}



Το σχέδιο Κανονισμού διατηρεί τις βασικές αρχές της Οδηγίας και επιπλέον εισάγει τις ακόλουθες καινοτομίες:

- **Κατάρτιση προφίλ**
- **Ανωνυμοποίηση δεδομένων**
- **Ενημέρωση & Συγκατάθεση ΥΔ**
- **Κατάργηση Γενικής Υποχρέωση Γνωστοποίησης - Τεκμηρίωση - Αρχή λογοδοσίας:** υποχρέωση απόδειξης της συμμόρφωσης μεταξύ άλλων και μέσω της θέσπισης εσωτερικών πολιτικών και μηχανισμών διασφάλισης της συμμόρφωσης
- **Μελέτη επιπτώσεων στην ιδιωτικότητα – Privacy Impact Assessment**
- **Μηχανισμός Συνεκτικότητας:** συνεργασία του ΕΣΠΔ (νύν Ο.Ε. ά. 29) με τις αρχές ελέγχου μεταξύ άλλων και για δραστηριότητες οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε ΥΔ σε περισσότερα κράτη μέλη ή με την παρακολούθηση της συμπεριφοράς τους
- **Ορισμός Υπευθύνου Προστασίας Δεδομένων – Data Protection Officer:** εάν η επεξεργασία αφορά πάνω από 500 άτομα το χρόνο ή αν οι βασικές δραστηριότητες του ΥΕ σχετίζονται με την κατάρτιση προφίλ
- **Υποχρεώσεις ΥΕ ήδη από το σχεδιασμό και εξ ορισμού**

Κατάρτιση προφίλ {I}



ΟΔΗΓΙΑ 95/46/ΕΚ

Αυτοματοποιημένες ατομικές αποφάσεις: δικαίωμα του ΥΔ να μη συμμορφωθεί με απόφαση που παράγει νομικά αποτελέσματα έναντι αυτού ή **το θίγει σημαντικά** εφόσον η εν λόγω απόφαση **βασίζεται αποκλειστικώς σε αυτοματοποιημένη επεξεργασία** που αξιολογεί ορισμένες πτυχές της προσωπικότητάς του, όπως η απόδοσή του στην εργασία, η φερεγγυότητά, η αξιοπιστία, η διαγωγή του κ.λπ.

ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ

Κατάρτιση προφίλ: ορίζεται κάθε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων **τα οποία στοχεύουν στην αξιολόγηση συγκεκριμένων προσωπικών πτυχών που σχετίζονται με ένα ΥΔ**, ή στην ανάλυση της αποδοτικότητας του στην εργασία, της οικονομικής του κατάστασης, της θέσης, της υγείας, των προσωπικών προτιμήσεων, της αξιοπιστίας ή της συμπεριφοράς του.

Μέτρα τα οποία βασίζονται στην κατάρτιση προφίλ και **παράγουν νομικά αποτελέσματα** σχετικά με το ΥΔ ή **θίγουν σημαντικά το ΥΔ** δεν θα πρέπει να βασίζονται αποκλειστικά στην αυτοματοποιημένη επεξεργασία

* Δεν αποφεύγεται η αόριστη έννοια 'θίγουν σημαντικά'.

** Ο όρος κατ' ουσία επιβάλλει την ανθρώπινη παρέμβαση προκειμένου να κριθούν οι παράγοντες οι οποίοι οδήγησαν στην αυτοματοποιημένη απόφαση.

Κατάρτιση προφίλ {III}



ΟΔΗΓΙΑ 95/46/ΕΚ

Κατ' εξαίρεση ένα πρόσωπο μπορεί να υποχρεωθεί να συμμορφωθεί με τις ανωτέρω αποφάσεις, εάν η εν λόγω απόφαση:

- έχει ληφθεί στο **πλαίσιο της σύναψης ή της εκτέλεσης σύμβασης**, εφόσον το αίτημα σύναψης ή εκτέλεσης της σύμβασης του προσώπου στο οποίο αναφέρονται τα δεδομένα έχει ικανοποιηθεί ή **πρόσφορα μέτρα**, στα οποία περιλαμβάνεται η δυνατότητα να προβάλει την άποψή του, **κατοχυρώνουν το έννομο συμφέρον του** ή
- επιτρέπεται **από νομοθετική διάταξη** που καθορίζει τα μέτρα τα οποία κατοχυρώνουν το έννομο συμφέρον του προσώπου στο οποίο αναφέρονται τα δεδομένα.

ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ

Η επεξεργασία δπχ για τους σκοπούς της κατάρτισης προφίλ, ακόμη και σε σχέση με την προσφορά ηλεκτρονικών υπηρεσιών πληροφόρησης και επικοινωνιών, είναι νόμιμη εάν:

- **είναι απαραίτητη για τη σύναψη ή την εκτέλεση σύμβασης**, εφόσον το αίτημα για τη σύναψη ή την εκτέλεση της το οποίο υποβλήθηκε από το ΥΔ έγινε δεκτό ή εάν παρασχέθηκαν κατάλληλα μέτρα για τη διασφάλιση των έννομων συμφερόντων του συγκεκριμένου προσώπου (π.χ. δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης) ή
- **επιτρέπεται ρητώς από το δίκαιο της Ένωσης ή το δίκαιο ΚΜ**
{κυρίως στο πλαίσιο των συναλλαγών του δημοσίου}
- **βασίζεται στη ΣΥΝΑΙΝΕΣΗ του υποκειμένου**
{κυρίως μέσω συμβάσεων με ιδιωτικές εταιρείες}

Κατάρτιση προφίλ {IV}



ΟΔΗΓΙΑ 95/46/ΕΚ

ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ

Προκειμένου η συναίνεση να είναι έγκυρη θα πρέπει το ΥΔ να ενημερώνεται με σαφή και κατανοητό τρόπο:

- **Για το γεγονός ότι καταρτίζεται προφίλ**, για την ύπαρξη μέτρων τα οποία βασίζονται στην κατάρτιση προφίλ και για τους τρόπους να αντιταχθούν στην κατάρτιση προφίλ
- **Για τη λογική στην οποία βασίζεται η αυτοματοποιημένη επεξεργασία**

Η υποχρέωση ενημέρωσης του ΥΔ για την κατάρτιση προφίλ είναι ιδιαίτερα σημαντική για την άσκηση του δικαιώματος αντίρρησης. Παρόλα αυτά είναι ιδιαίτερα δύσκολο για το μέσο χρήστη να αντιληφθεί το περιεχόμενο της ενημέρωσης μιας απλής πολιτικής προστασίας δεδομένων – πόσο μάλλον τη λογική μιας διαδικασίας κατάρτισης προφίλ.

Προτείνεται η λύση των **Πολυεπίπεδων Ανακοινώσεων**.

Κατάρτιση προφίλ {IV}



ΟΔΗΓΙΑ 95/46/ΕΚ

ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ

Απαγορεύεται :

- Η κατάρτιση προφίλ που έχει ως **αποτέλεσμα την διάκριση ατόμων** στη βάση της φυλετικής ή εθνικής καταγωγής, πολιτικών ή θρησκευτικών πεποιθήσεων, συμμετοχής σε σωματεία ή ενώσεις, σεξουαλικό προσανατολισμό ή φύλο ή καταλήγει σε μέτρα με αντίστοιχο περιεχόμενο
- Η χρήση τεχνικών κατάρτισης προφίλ για την **ταυτοποίηση παιδιών**

Εκτίμηση επιπτώσεων ιδιωτικότητας

Privacy Impact Assessment



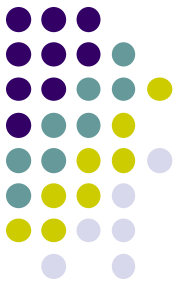
Ο ΥΕ ή ο ΕΕ για λογαριασμό του ΥΕ υποχρεούται να διενεργήσει **ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ** των προβλεπόμενων πράξεων επεξεργασίας αν οι πράξεις επεξεργασίας ενέχουν συγκεκριμένους κινδύνους για τα δικαιώματα και τις ελευθερίες των ΥΔ λόγω της φύσης, της έκτασης ή των σκοπών τους.

Οι ακόλουθες πράξεις επεξεργασίας τεκμαίρεται ότι ενέχουν συγκεκριμένους κινδύνους:

- **κατάρτιση προφίλ**, βάσει του οποίου λαμβάνονται μέτρα τα οποία παράγουν έννομες συνέπειες που αφορούν ή επηρεάζουν σημαντικά το φυσικό πρόσωπο.
- εάν τα δπχ καθίστανται προσπελάσιμα σε πολυάριθμα άτομα, ή **εάν μεγάλες ποσότητες δπχ τυγχάνουν επεξεργασίας ή συνδυάζονται με άλλα δεδομένα**

Εκτίμηση επιπτώσεων θα πρέπει να διενεργείται σε περίπτωση κατάρτισης προφίλ από το οποίο παράγονται έννομες συνέπειες και σε κάθε άλλη περίπτωση επεξεργασίας Μεγάλου όγκου Δεδομένων .

Διαβούλευση με την Αρχή Ελέγχου



Ο ΥΕ υποχρεούται να λαμβάνει ΓΝΩΜΗ της αρχής ελέγχου όταν:

- η εκτίμηση επιπτώσεων υποδεικνύει ότι **οι πράξεις επεξεργασίας ενδέχεται**, λόγω της φύσης, της έκτασης ή του σκοπού τους, να **ενέχουν υψηλό βαθμό συγκεκριμένων κινδύνων** ή
 - η επεξεργασία περιλαμβάνεται στο σχετικό **κατάλογο πράξεων επεξεργασίας που θα δημοσιοποιήσει το ΕΣΠΔ** για τις οποίες η προηγούμενη διαβούλευση θεωρείται απαραίτητη
- * Η επεξεργασία στο πλαίσιο των Μεγάλων Δεδομένων ενδέχεται να εμπίπτει και στις δύο κατηγορίες.

Ανωνυμοποίηση δεδομένων – Επαναταυτοποίηση υποκειμένων



Το Σχέδιο Κανονισμού θέτει εκτός πεδίου εφαρμογής και ενθαρρύνει τη χρήση **ΑΝΩΝΥΜΩΝ ΔΕΔΟΜΕΝΩΝ** ήτοι **δεδομένων που δεν μπορούν να σχετισθούν άμεσα ή έμμεσα, μεμονωμένα ή σε συνδυασμό με συναφή δεδομένα με ένα πρόσωπο** {Αιτ. Εκθ. Αρ. 23}.

Κατά συνέπεια, αρκετά από τα τηρούμενα ανώνυμα δεδομένα θα μπορούσε να θεωρηθεί ότι δεν εγκυμονούν κινδύνους για την ιδιωτικότητα.

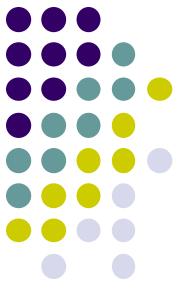
Ωστόσο στην εποχή των Μεγάλων Δεδομένων οι τεχνικές ανωνυμοποίησης δεν είναι πάντα αποτελεσματικές δεδομένων των γρήγορων υπολογιστικών συστημάτων και των βελτιωμένων τεχνικών ανάλυσης δεδομένων (analytic techniques).

Τα τελευταία χρόνια έχουν έρθει στο φώς της δημοσιότητας πολλές περιπτώσεις **επαναταυτοποίησης (de-identification) προσώπων με διαδοχικές παραπομπές (cross-referencing) σε ανωνυμοποιημένα σύνολα δεδομένων με σχετικά αρχεία τα οποία περιέχουν Μοναδικά Αναγνωριστικά Ταυτότητας.**

Τέτοιες τεχνικές εξασθενίζουν την αποτελεσματικότητα της ανωνυμοποίησης, ως τεχνικής για την προστασία των δεδομένων και θέτουν υπό αμφισβήτηση τη θεμελιώδη διάκριση μεταξύ προσωπικών δεδομένων και δεδομένων τα οποία δεν θεωρούνται προσωπικά.

Γνωμοδότηση 3/2013

Αρχή του σκοπού {I}



Ιδιαίτερα χρήσιμες κατευθύνσεις παρέχονται από την Ομάδα Εργασίας του άρθρου 29 της Οδηγίας, η οποία διακρίνει δύο περιπτώσεις επεξεργασίας Μεγάλου όγκου Δεδομένων:

Α' ΠΕΡΙΠΤΩΣΗ:

- η επεξεργασία των ΜΔ στοχεύει στον **ΕΝΤΟΠΙΣΜΟ ΤΩΝ ΣΥΣΧΕΤΙΣΜΩΝ** μεταξύ πληροφοριών
- οι συσχετισμένες πληροφορίες **δεν χρησιμοποιούνται για τη λήψη αποφάσεων**
- τα δεδομένα **ανωνυμοποιούνται**

ΔΕΝ ΑΠΑΙΤΕΙΤΑΙ ΣΥΓΚΑΤΑΘΕΣΗ

Β' ΠΕΡΙΠΤΩΣΗ:

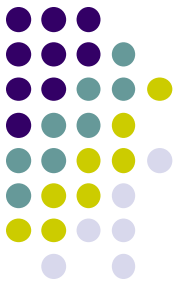
- η επεξεργασία των ΜΔ **στοχεύει στα ΠΡΟΣΩΠΑ στα οποία αναφέρονται τα δεδομένα**
- χρησιμοποιούνται για την ανάλυση ή την πρόβλεψη των προσωπικών προτιμήσεων, της συμπεριφοράς και της στάσης μεμονωμένων καταναλωτών, οι οποίες θα καταλήξουν στην λήψη αποφάσεων ή μέτρων που θα ληφθούν σε σχέση με τους συγκεκριμένους καταναλωτές

ΑΠΑΙΤΕΙΤΑΙ ΣΥΓΚΑΤΑΘΕΣΗ

Επίσης οι ΥΕ θα πρέπει να παρέχουν στα ΥΔ **εύκολη πρόσβαση στο προφίλ τους και να ενημερώνουν για τα κριτήρια** βάσει των οποίων καταρτίστηκαν.

Γνωμοδότηση 3/2013

Αρχή του σκοπού {II}



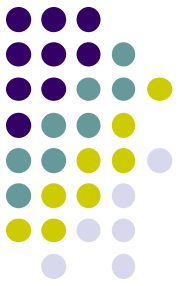
Στη δεύτερη περίπτωση εντάσσεται η κατάρτιση προφίλ για σκοπούς άμεσου μάρκετινγκ, συμπεριφορικής διαφήμισης, «μεσιτείας πληροφοριών», παροχής στοχευμένων διαφημίσεων προς χρήστες βάσει της γεωγραφικής τους θέσης, (location-based advertising), έρευνα αγοράς βάσει του εντοπισμού των χρηστών (“tracking-based digital market research”).

Κατά κανόνα, τα δεδομένα στις περιπτώσεις αυτές τυγχάνουν επεξεργασίας για **δευτερογενείς σκοπούς (secondary use)**, οι οποίοι διαφοροποιούνται σε σχέση με τον αρχικό σκοπό για τον οποίο συλλέχθηκαν.

Η Ομάδα Εργασίας του άρθρου 29 στη Γνωμοδότηση της προσδιόρισε ότι προκειμένου η συγκατάθεση να αποτελέσει έγκυρη βάση επεξεργασίας για την κατάρτιση προφίλ ο σκοπός συλλογής θα πρέπει να είναι:

- **«συγκεκριμένος»** (να έχει καθοριστεί με ακρίβεια και να είναι πλήρως προσδιορισμένος εκ των προτέρων πριν το χρόνο συλλογής των δεδομένων)
- **«ρητός»** (να προκύπτει με σαφήνεια, να επεξηγείται ή να εκφράζεται με αδιαμφισβήτητο τρόπο)
- **«νόμιμος»** (εάν πέρα από το **βασικό σκοπό** τα πδ τυγχάνουν επεξεργασίας και για **δευτερογενείς σκοπούς**, οι σκοποί αυτοί **θα πρέπει να είναι συμβατοί με το βασικό σκοπό ή να επιβάλλονται από το νόμο.**

Περιεχόμενο ενημέρωσης υποκειμένου

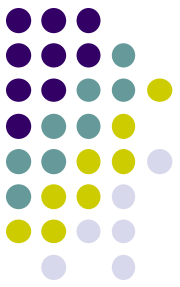


Σύμφωνα με την ΟΕ του α. 29 η ενημερωμένη συγκατάθεση θα πρέπει οι ΥΕ να παρέχει στα ΥΔ:

- **δικαίωμα πρόσβασης στο προφίλ** που τηρούν για εκείνα
- ενημέρωση για την **υποκείμενη λογική της λήψης αποφάσεων** (τον αλγόριθμο) που οδήγησε στην ανάπτυξη του προφίλ και
- ενημέρωση **για τις πηγές των πληροφοριών** από τις οποίες προέκυψαν επαγωγικά τα συμπεράσματα

Περαιτέρω οι βασικές πληροφορίες πρέπει να παρουσιάζονται με τρόπο φιλικό προς το χρήστη (π.χ. **Πολυεπίπεδες Ανακοινώσεις**) για και οι επεξηγήσεις να είναι προσβάσιμες μέσω υπερκείμενου συνδέσμου.

Η αξία των προσωπικών δεδομένων: από τη συλλογή στη χρήση



Ο Ευρωπαϊκός Οργανισμός Ασφάλειας Πληροφοριών χαρακτηρίζει τα προσωπικά δεδομένα ως το «**νέο πετρέλαιο**» (“*new oil*”)

{ENISA, 2011b, pp. 26ff; WEF, 2011/ 2012}

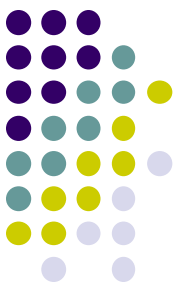
Οι δυνατότητες που παρέχει η Έκρηξη των Δεδομένων δημιουργεί **ΝΕΕΣ ΠΡΟΟΠΤΙΚΕΣ**

Η τεχνολογία των Big Data χρησιμοποιείται ήδη από πολλές **κυβερνήσεις** οι οποίες χρησιμοποιούν νέες τεχνολογίες για την συγκέντρωση και συνδυασμό δεδομένων κοινωνικής ασφάλισης, φορολογικών αρχείων, τραπεζικών λογαριασμών και στοιχείων πιστοληπτικής ικανότητας για να πατάξουν φοροδιαφυγή, δωροδοκία και ξέπλυμα χρήματος. Επίσης χαρακτηριστική είναι η περίπτωση του **Google Flu Trends**, η χρήση των Μεγάλων Δεδομένων για την διερεύνηση των τάσεων της γρίπης ανά τον κόσμο.

Επίσης πολλές **εταιρείες** χρησιμοποιούν τα Μεγάλα Δεδομένα για τη δημιουργία **μοντέλων πρόβλεψης και προγνωστικής ανάλυσης και επιχειρηματικής ευφυΐας**, προκειμένου να ληφθούν υπόψη για την ασφαλέστερη λήψη αποφάσεων και την κατάρτιση **προτύπων αγοραστικής συμπεριφοράς**, αποτελεσματικότερο μάρκετινγκ και αύξηση εσόδων.

Κατά συνέπεια παρά τους κινδύνους που ελλοχεύουν για την ιδιωτικότητα απαιτείται μια **ΝΕΑ ΠΡΟΣΕΓΓΙΣΗ** των δεδομένων, η οποία να είναι ευέλικτη ώστε **να συνδυάζει την καινοτομία με την προστασία των προσωπικών δεδομένων** και να παγιωθούν νέοι τρόποι που θα παρέχουν στο ΥΔ τη δυνατότητα να συμμετέχει ενεργά **στη διαχείριση των δεδομένων** και να κάνει ξεκάθαρες επιλογές **ως προς τη χρήση τους**.

Ξεκλειδώνοντας την αξία των προσωπικών δεδομένων: από τη συλλογή στη χρήση



World Economic Forum

Παραδοσιακή προσέγγιση	Νέα Προσέγγιση
Τα δεδομένα συλλέγονταν άμεσα από το υποκείμενο εν γνώσει του	Τα περισσότερα δεδομένα προκύπτουν από την επικοινωνία μηχανής προς μηχανή – τα υποκείμενα είναι δύσκολο να ενημερωθούν για τη συλλογή
Ο ορισμός των προσωπικών δεδομένων ήταν προκαθορισμένος και δυαδικός	Ο ορισμός των προσωπικών δεδομένων προκύπτει από τα συμφραζόμενα (contextual) και εξαρτάται από κοινωνικούς κανόνες
Τα δεδομένα συλλέγονταν για συγκεκριμένους σκοπούς	Η οικονομική αξία και η καινοτομία απορρέει από το συνδυασμό των δεδομένων και τις δευτερογενείς χρήσεις

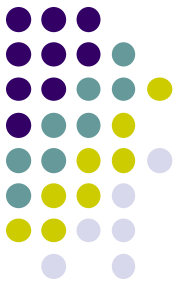
Ξεκλειδώνοντας την αξία των προσωπικών δεδομένων: από τη συλλογή στη χρήση



World Economic Forum

Παραδοσιακή προσέγγιση	Νέα Προσέγγιση
Ο χρήστης είναι το υποκείμενο των δεδομένων	Ο χρήστης μπορεί να είναι το υποκείμενα των δεδομένων, ο υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία
Το υποκείμενο των δεδομένων παρέχει τη συγκατάθεση του αλλά δεν ασχολείται πραγματικά – στην ουσία του	Το υποκείμενο των δεδομένων συμμετέχει και κατανοεί πώς χρησιμοποιούνται τα δεδομένα και πώς δημιουργείται η αξία τους
Οι πολιτικές επικεντρώνονται στην ελαχιστοποίηση των κινδύνων για το υποκείμενο των δεδομένων	Οι πολιτικές εστιάζουν στην εξισορρόπηση της προστασίας της ιδιωτικότητας με την καινοτομία και την οικονομική εξέλιξη

Η ιδιωτικότητα κατά την εξέλιξη του παγκόσμιου ιστού



Ευχαριστώ για την προσοχή σας!

Μαρία Γιαννακάκη
Δικηγόρος, D.E.A., υπ.Δρ. ΕΚΠΑ