

Ψυχολογία του Διαδικτύου (ΨΧ109)

Διάλεξη 12 – Διαδικτυακή παρανομία
Παρενόχληση, αδικήματα μίσους, κυβερνοπόλεμος, παιδική
πορνογραφία και παιδεραστία



Γιατί το διαδίκτυο μετασχηματίζει την παρανομία

Προσφέρει ανωνυμία ή ψευδωνυμία.

Διευκολύνει την πρόσβαση σε θύματα και πληροφορίες.

Επιτρέπει ταχεία διάδοση επιβλαβούς περιεχομένου.

Μειώνει την αίσθηση άμεσης κοινωνικής ευθύνης.

Θολώνει τα όρια ανάμεσα σε online και offline βλάβη.



Κυβερνοπαρενόχληση: απόπειρα ορισμού

01

Η παρενόχληση αφορά απειλητικές, εκφοβιστικές ή εξευτελιστικές συμπεριφορές.

02

Στο διαδίκτυο μπορεί να λάβει παρόμοιες μορφές με τη διάζωσης παρενόχληση.

03

Μπορεί όμως να αποκτήσει και νέες μορφές, λόγω της τεχνολογίας.

04

Μπορεί να συμβεί:

- μετά από προσωπική σχέση,
- στον χώρο εργασίας,
- μεταξύ επιχειρήσεων,
- σε κοινωνικά δίκτυα ή εικονικούς κόσμους.



Μορφές κυβερνοπαρενόχλησης

Ανεπιθύμητα
σεξουαλικά
σχόλια ή
προσεγγίσεις.

Φυλετική ή
έμφυλη
παρενόχληση.

Απειλητικά ή
προσβλητικά
μηνύματα.

Παραβίαση
λογαριασμών ή
συσκευών.

Αποστολή ιών ή
κακόβουλου
λογισμικού.

Δημόσια
δυσφήμιση και
καταστροφή
υπόληψης.



Σεξουαλική παρενόχληση στο διαδίκτυο

Ο Barak (2005) διακρίνει τρεις βασικούς τύπους:

- παρενόχληση σχετική με το φύλο,
- ανεπιθύμητο σεξουαλικό ενδιαφέρον,
- σεξουαλικό εξαναγκασμό.

Το διαδίκτυο επιτρέπει επίμονη και επαναλαμβανόμενη προσέγγιση.

Η απόσταση και η ανωνυμία μπορεί να κάνουν τον δράστη πιο τολμηρό.

Η βλάβη στο θύμα μπορεί να είναι σοβαρή, ακόμη και χωρίς φυσική επαφή.



Παρενοχλητική παρακολούθηση (cyberstalking)

Το stalking είναι πιο σοβαρή μορφή παρενόχλησης.

Περιλαμβάνει επαναλαμβανόμενη και ανεπιθύμητη εισβολή στη ζωή του θύματος.

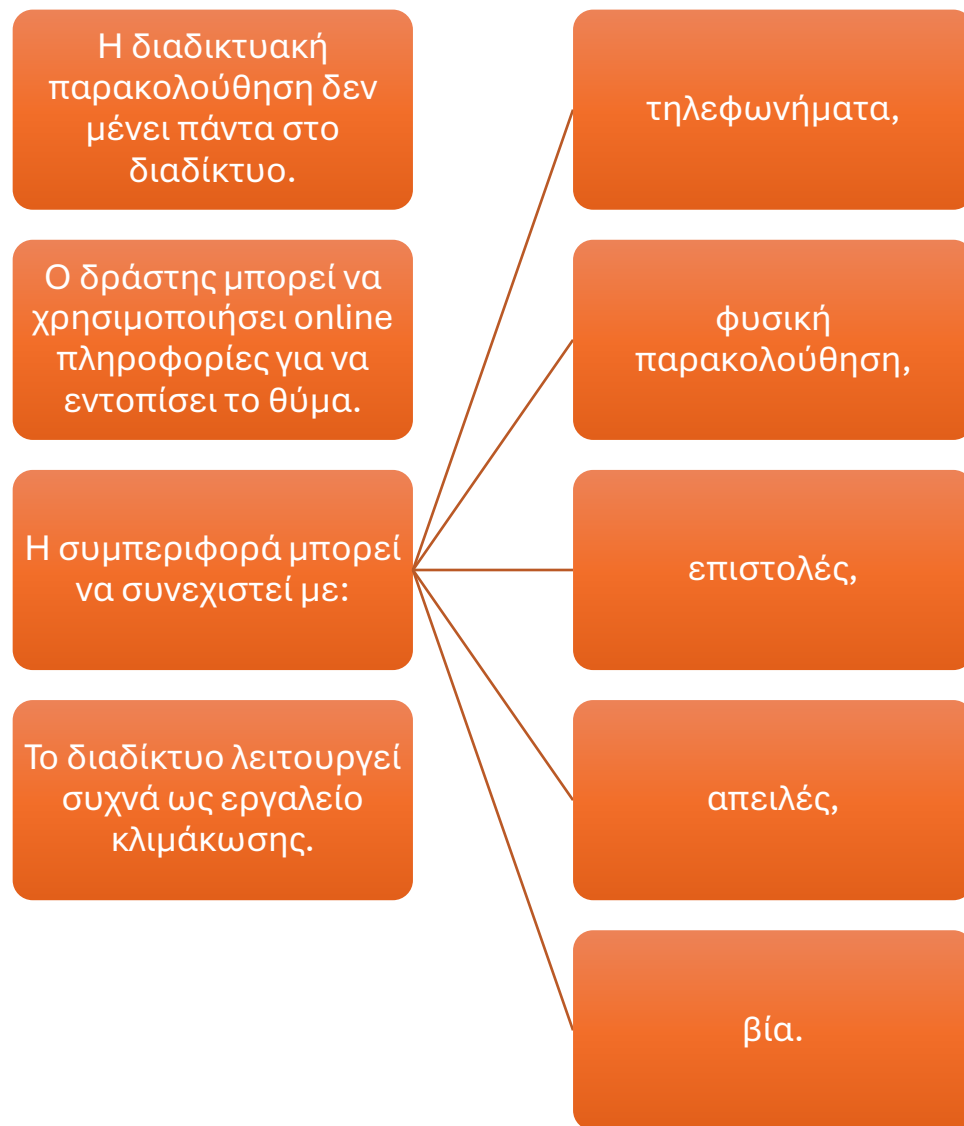
Η κυβερνοπαρακολούθηση χρησιμοποιεί το διαδίκτυο για:

- συλλογή πληροφοριών,
- έλεγχο δραστηριότητας,
- ανεπιθύμητη επικοινωνία,
- απειλές,
- ψευδείς κατηγορίες.

Μπορεί να αφορά άτομα, ομάδες ή οργανισμούς.



Από το cyberstalking στη φυσική απειλή





Νομοθεσία και κυβερνοπαρακολούθηση

Πολλές νομοθεσίες για το stalking αναδιατυπώθηκαν ώστε να καλύπτουν το διαδίκτυο.



Κρίσιμα στοιχεία:

επανάληψη συμπεριφοράς,

πρόκληση φόβου ή ανησυχίας,

ψυχολογική βλάβη,

πρόθεση ή προβλεψιμότητα της βλάβης.



Σε αρκετά πλαίσια χρησιμοποιείται το κριτήριο του «λογικού ατόμου».



Η νομοθεσία προσπαθεί να επιτρέψει παρέμβαση πριν από την κλιμάκωση.



Ψυχολογικές συνέπειες για τα θύματα

Έντονο άγχος και αίσθηση απειλής.

Φόβος νέας επίθεσης ή έκθεσης.

Απώλεια εμπιστοσύνης σε κοινωνικές σχέσεις.

Διατάραξη εργασιακής και κοινωνικής ζωής.

Πιθανή απώλεια σχέσεων με φίλους ή συγγενείς.

Η βλάβη μπορεί να είναι ανάλογη με τη διά ζώσης παρενόχληση.



Αδικήματα μίσους

Τα αδικήματα μίσους έχουν ως κίνητρο αρνητικές στάσεις απέναντι σε κοινωνικές ή πολιτισμικές ομάδες.

Μπορεί να σχετίζονται με:

- φυλή,
- θρησκεία,
- φύλο,
- σεξουαλικό προσανατολισμό,
- εθνικότητα,
- πολιτισμική ταυτότητα.

Ο ορισμός τους είναι δύσκολος.

Υπάρχει συχνή επικάλυψη με κυβερνοπαρενόχληση και κυβερνοπαρακολούθηση.



Το διαδίκτυο ως μέσο μίσους

Το διαδίκτυο
χρησιμοποιείται για:

- απειλές,
- δημόσια στοχοποίηση,
- διάδοση προπαγάνδας,
- στρατολόγηση,
- εκφοβισμό,
- οργάνωση επιθέσεων.

Οι δράστες μπορούν να
βρουν πληροφορίες για τα
θύματα.

Η διαδικτυακή ρητορική
μίσους μπορεί να συνδεθεί
με βλάβη στον φυσικό
κόσμο.

Η έλλειψη σαφούς ορισμού
δυσκολεύει την έρευνα και
τη νομοθεσία.



Κυβερνοπόλεμος

Ο κυβερνοπόλεμος αφορά ενέργειες κρατών ή ομάδων εναντίον δικτύων άλλων κρατών.

Στόχοι μπορεί να είναι:

- στρατιωτικά δίκτυα,
- κρατικές υπηρεσίες,
- κρίσιμες υποδομές,
- οικονομικά συστήματα,
- ευαίσθητα δεδομένα.

Η βλάβη μπορεί να είναι:

- διατάραξη λειτουργίας,
- καταστροφή,
- υποκλοπή,
- οικονομική ζημία.



Ιδιαιτερότητες του κυβερνοπολέμου

Η απόδοση ευθύνης είναι δύσκολη.

Οι επιθέσεις μπορεί να μην έχουν άμεσα ορατές συνέπειες.

Η βλάβη μπορεί να είναι έμμεση ή καθυστερημένη.

Δεν υπάρχουν πάντοτε σαφείς διεθνείς κανόνες.

Η ψυχολογική εμπειρία του δράστη διαφέρει από τη συμβατική σύγκρουση.



Χακτιβισμός

Οι χακτιβιστές χρησιμοποιούν τεχνικές hacking για πολιτικούς ή κοινωνικούς σκοπούς.

Διακρίνονται συχνά σε:

- white hats,
- black hats,
- grey hats.

Οι grey hats κινούνται ανάμεσα στην πολιτική δράση και την παρανομία.

Παραδείγματα δράσης:

- επιθέσεις DDoS (προσπάθειες να καταστεί μη διαθέσιμη μια υπηρεσία),
- διαρροές δεδομένων,
- στοχοποίηση οργανισμών ή ομάδων.



Ψηφιακή επιτήρηση

Οι κυβερνήσεις χρησιμοποιούν επιτήρηση για πρόληψη και εξιχνίαση εγκλημάτων.

Η επιτήρηση μπορεί να βοηθήσει στον εντοπισμό δραστών. Ταυτόχρονα δημιουργεί σοβαρά ζητήματα ιδιωτικότητας.

Βασικό δίλημμα:

- περισσότερη ασφάλεια,
- ή περισσότερη προστασία προσωπικών δεδομένων;

Το ερώτημα είναι ποιος ελέγχει τα δεδομένα και με ποιες εγγυήσεις.



Ψηφιακά δεδομένα και ιδιωτικότητα

Τα ψηφιακά δεδομένα έχουν ιδιαίτερα χαρακτηριστικά:

- μονιμότητα,
- τεράστιο όγκο,
- χαμηλή ορατότητα για τον πολίτη,
- εύκολη προσβασιμότητα,
- δυνατότητα συγκέντρωσης από πολλές πηγές.

Τα Big Data επιτρέπουν εξαγωγή συμπερασμάτων που το ίδιο το άτομο δεν γνωρίζει.

Η απειλή δεν είναι μόνο η συλλογή δεδομένων, αλλά και ο ανασυνδυασμός τους.



Παιδική πορνογραφία και παιδεραστία

- **Γιατί το διαδίκτυο αύξησε το πρόβλημα**
 - Το διαδίκτυο αύξησε την πρόσβαση σε παράνομο υλικό.
 - Διευκόλυνε την προβολή, ανταλλαγή, αγορά και πώληση αρχείων.
 - Δημιούργησε νέες μορφές «παιδοφιλικής εγκληματικότητας στον κυβερνοχώρο».
 - Στις ΗΠΑ καταγράφηκε αύξηση υποθέσεων αποκλειστικά διαδικτυακής παιδικής πορνογραφίας από το 2000 έως το 2009.
 - Το σχετικό υλικό αποτελεί μεγάλο μέρος των υποθέσεων σεξουαλικής εκμετάλλευσης που διώκονται ομοσπονδιακά στις ΗΠΑ.



Ο «κινητήρας των τριών A»

Το διαδίκτυο ενισχύει το φαινόμενο μέσω τριών παραγόντων:

- accessibility / προσβασιμότητα,
- affordability / χαμηλό κόστος,
- anonymity / ανωνυμία.

Το ψηφιακό υλικό αποθηκεύεται και αποκρύπτεται ευκολότερα από το μη ψηφιακό.

Η διακίνηση μπορεί να γίνει γρήγορα και με μικρή προσπάθεια.

Η ανωνυμία μπορεί να δημιουργεί αίσθηση ασφάλειας στους δράστες.



Παιδική πορνογραφία ή υλικό παιδικής κακοποίησης;

Ο όρος «παιδική πορνογραφία» είναι προβληματικός.

Το υλικό δεν είναι απλή πορνογραφία, αλλά αποτύπωση κακοποίησης.

Κάθε εικόνα ή βίντεο μπορεί να συνδέεται με πραγματικό θύμα.

Η επαναδιακίνηση του υλικού μπορεί να συντηρεί την επαναθυματοποίηση.

Για αυτό προτιμάται συχνά ο όρος «εικόνες / υλικό παιδικής κακοποίησης».



Νομικές και εννοιολογικές δυσκολίες

- Οι ορισμοί διαφέρουν ανάμεσα σε χώρες.
- Η ηλικία συναίνεσης δεν ταυτίζεται πάντα με την ηλικία που ορίζει η νομοθεσία για το παράνομο υλικό.
- Οι τεχνολογικές εξελίξεις δυσκολεύουν την εφαρμογή παλαιότερων νόμων.
- Το βασικό ερώτημα είναι τι ακριβώς ποινικοποιείται:
 - η παραγωγή,
 - η κατοχή,
 - η διακίνηση,
 - η θέαση,
 - η πρόθεση χρήσης.



Sexting μεταξύ ανηλίκων

Το sexting δημιουργεί ιδιαίτερες νομικές και ηθικές δυσκολίες.

Μπορεί να αποτελεί έκφραση σεξουαλικής ανάπτυξης των εφήβων.

Μπορεί όμως να οδηγήσει σε εκβιασμό, διαπόμπευση ή διακίνηση χωρίς συναίνεση.

Η νομοθεσία δεν έχει ακόμη αντιμετωπίσει ικανοποιητικά το φαινόμενο.

Κρίσιμο ερώτημα: πρέπει οι ανήλικοι να διώκονται με νόμους περί παιδικής πορνογραφίας;



Ψευδοφωτογραφίες

Οι ψευδοφωτογραφίες είναι ψηφιακά επεξεργασμένες εικόνες.

Μπορεί:

- μια εικόνα ενηλίκου να τροποποιηθεί ώστε να μοιάζει με παιδί,
- μια αθώα εικόνα παιδιού να μετατραπεί σε σεξουαλική εικόνα,
- να δημιουργηθεί υλικό χωρίς άμεση φωτογράφιση πραγματικής κακοποίησης.

Δημιουργούν σοβαρά προβλήματα για τους νομοθέτες.

Θέτουν το ερώτημα αν υπάρχει πραγματικό θύμα και πώς πρέπει να προστατεύεται.



Εικονική παιδική πορνογραφία

Η εικονική παιδική πορνογραφία δεν συνδέεται πάντοτε με πραγματικό παιδί-θύμα.

Στις ΗΠΑ, το Ανώτατο Δικαστήριο έχει διακρίνει την εικονική από την πραγματική παιδική πορνογραφία.

Το σκεπτικό είναι ότι δεν υπάρχει αναγκαστικά άμεση σύνδεση με πραγματική κακοποίηση.

Ωστόσο παραμένει το ερώτημα αν τέτοιο υλικό μπορεί να ενισχύει φαντασιώσεις ή μελλοντικό κίνδυνο.

Πρόκειται για πεδίο έντονης νομικής και ηθικής διαφωνίας.



Ποιοι είναι οι δράστες;

Δεν υπάρχει ένας «τυπικός» δράστης.

Κάποιοι δράστες περιορίζονται στη θέαση ή συλλογή υλικού.

Άλλοι ανταλλάσσουν, αγοράζουν ή πωλούν υλικό.

Άλλοι επιδιώκουν επαφή με παιδιά.

Η διαφοροποίηση είναι σημαντική για την αξιολόγηση κινδύνου και την πρόληψη.



Κατηγοριοποίηση δραστών

Μια βασική διάκριση αφορά:

- δράστες χωρίς γνωστό ιστορικό σεξουαλικής κακοποίησης παιδιών,
- δράστες που έχουν διαπράξει ή επιδιώκουν αδικήματα επαφής.

Η κατοχή ή θέαση υλικού δεν σημαίνει πάντα ίδια επικινδυνότητα.

Όμως μπορεί να συνδέεται με υψηλότερο κίνδυνο σε ορισμένες περιπτώσεις.

Η αξιολόγηση πρέπει να λαμβάνει υπόψη συμπεριφορά, κίνητρα και ιστορικό.



Σχέση θέασης υλικού και αδικημάτων επαφής

Κεντρικό ερώτημα: οδηγεί η θέαση υλικού σε σεξουαλική κακοποίηση παιδιών;

Η σχέση είναι σύνθετη και όχι αυτόματη.

Σε κάποιες μελέτες εντοπίζεται υψηλή επικάλυψη μεταξύ κατοχής υλικού και κακοποίησης.

Άλλες μελέτες βρίσκουν χαμηλότερα ποσοστά επίσημου ιστορικού αδικημάτων επαφής.

Τα αποτελέσματα εξαρτώνται από το δείγμα, τη μέθοδο και το είδος των δεδομένων.



Το επιχείρημα του «ολισθηρού κατήφορου»

Υποστηρίζει ότι η θέαση υλικού μπορεί να οδηγήσει σταδιακά σε σοβαρότερες πράξεις.

Η πιθανή κλιμάκωση μπορεί να αφορά:

- πιο ακραίο υλικό,
- μεγαλύτερη απευαισθητοποίηση,
- αναζήτηση επαφής με παιδιά,
- grooming.

Το επιχείρημα είναι σημαντικό αλλά όχι απόλυτα αποδεδειγμένο.

Απαιτείται προσεκτική εμπειρική έρευνα και όχι απλές γενικεύσεις.



Grooming: βασική έννοια

- Το grooming αφορά τη διαδικτυακή προσέγγιση παιδιού με σκοπό σεξουαλική εκμετάλλευση.
- Συνήθως περιλαμβάνει σταδιακή οικοδόμηση σχέσης.
- Ο δράστης μπορεί να χρησιμοποιήσει:
 - ψεύτικη ταυτότητα,
 - κολακεία,
 - μυστικότητα,
 - συναισθηματική χειραγώγηση,
 - απειλές ή εκβιασμό.
- Το διαδίκτυο διευκολύνει την πρόσβαση σε ανηλίκους χωρίς φυσική παρουσία.



Στάδια και τεχνικές grooming

Εντοπισμός πιθανού θύματος.

Δημιουργία εμπιστοσύνης ή συναισθηματικής εξάρτησης.

Σταδιακή εισαγωγή σεξουαλικού περιεχομένου στη συζήτηση.

Απομόνωση του παιδιού από γονείς ή φίλους.

Πίεση για αποστολή εικόνων ή συνάντηση.

Χρήση ντροπής ή φόβου για διατήρηση σιωπής.



Ο ρόλος των διαδικτυακών κοινοτήτων δραστών

Το διαδίκτυο δεν προσφέρει μόνο πρόσβαση σε υλικό.

Επιτρέπει και επικοινωνία μεταξύ δραστών.

Οι κοινότητες αυτές μπορεί να:

- ανταλλάσσουν υλικό,
- νομιμοποιούν γνωστικά τη συμπεριφορά,
- προσφέρουν τεχνικές απόκρυψης,
- ενισχύουν γνωστικές διαστρεβλώσεις.

Η κοινωνική ενίσχυση μπορεί να μειώνει αναστολές.



Θεωρία κοινωνικής μάθησης

Σύμφωνα με τη θεωρία κοινωνικής μάθησης, οι άνθρωποι μαθαίνουν μέσω παρατήρησης και μίμησης.

Αν μια συμπεριφορά φαίνεται να επιβραβεύεται, αυξάνεται η πιθανότητα μίμησης.

Το διαδίκτυο αυξάνει το εύρος συμπεριφορών που μπορεί κάποιος να δει.

Αυτό περιλαμβάνει και συμπεριφορές σεξουαλικής κακοποίησης παιδιών.

Η θεωρία βοηθά να εξηγηθεί πώς οι διαδικτυακές κοινότητες μπορεί να λειτουργούν ενισχυτικά.



Γνωστικές διαστρεβλώσεις και αυτορρύθμιση

Πολλοί δράστες μπορεί να χρησιμοποιούν γνωστικές διαστρεβλώσεις.

Παραδείγματα:

- υποτίμηση της βλάβης,
- μετατόπιση ευθύνης,
- ψευδής αντίληψη συναίνεσης,
- εξορθολογισμός της συμπεριφοράς.

Οι δυσκολίες αυτορρύθμισης μπορεί να αυξάνουν τον κίνδυνο.

Το διαδίκτυο μπορεί να ενισχύει την παρορμητική ή μυστική συμπεριφορά.

Η παρέμβαση πρέπει να στοχεύει τόσο στη συμπεριφορά όσο και στις πεποιθήσεις.



Πρόληψη και αντιμετώπιση

Απαιτείται συνδυασμός
τεχνολογικών, νομικών και
ψυχολογικών παρεμβάσεων.

Σημαντικά μέτρα:

- ταυτοποίηση θυμάτων,
- αφαίρεση υλικού,
- διεθνής συνεργασία,
- αξιολόγηση κινδύνου δραστών,
- θεραπευτικές παρεμβάσεις,
- εκπαίδευση παιδιών, γονέων
και εκπαιδευτικών.

Η Interpol και διεθνείς
επιχειρήσεις έχουν
χρησιμοποιηθεί για ταυτοποίηση
θυμάτων και δραστών.