ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Κοκολάκη Εμμανουέλας (Α.Μ.: ΜΔΙ2326)

Η ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ CSAR (CHILD SEXUAL ABUSE REGULATION) ΚΑΙ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

THE PROPOSAL FOR THE CHILD SEXUAL ABUSE REGULATION AND FUNDAMENTAL RIGHTS

Επιβλέπουσα

Καθηγήτρια Λίλιαν Μήτρου

Πειραιάς, Νοέμβριος 2025

Στα γενναία παιδιά-επιζώντες

Περιεχόμενα

Συντομογραφίες

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Δεδομένων

Βλ.: Βλέπε

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

ΔΕΕ: Δικαστήριο της Ευρωπαϊκής Ένωσης

ΕΕ: Ευρωπαϊκή Ένωση

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου

ΕΕΠΔ: Ευρωπαίος Επόπτης Προστασίας Δεδομένων

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

ΕΣΠΔ: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

ο.π.: όπως παραπάνω

Παρ.: παράγραφος

Σ.: Σύνταγμα

Σελ. : Σελίδα

ΣΛΕΕ: Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης

CSAR: Child Sexual Abuse Regulation (Proposal)

Europol (Ευρωπόλ): Οργανισμός της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της επιβολής του Νόμου

e-Privacy Directive: Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Περίληψη

Η σεξουαλική κακοποίηση παιδιών αποτελεί ένα διαρκώς αυξανόμενο πρόβλημα παγκοσμίως, με υλικό σεξουαλικής κακοποίησης ανηλίκων να διακινείται και να αποθηκεύεται μέσω διαδικτυακών υπηρεσιών. Η διευρυμένη χρήση των ψηφιακών πλατφορμών από τους νέους, σε συνδυασμό με τις δυνατότητες της σύγχρονης ψηφιακής εποχής η οποία διευκολύνει την επικοινωνία μέσω κοινωνικών δικτύων και εφαρμογών ανταλλαγής μηνυμάτων, έχει οδηγήσει επίσης σε σημαντική αύξηση περιστατικών άγρας παιδιών, με σκοπό την σεξουαλική κακοποίηση.

Μέχρι σήμερα, η ανίχνευση και αναφορά στις αρχές των ανωτέρω εγκλημάτων από τους παρόχους υπηρεσιών της Κοινωνίας της Πληροφορίας στην ΕΕ γινόταν κυρίως σε εθελοντική βάση. Ως εκ τούτου, τα μέτρα και οι διαδικασίες που εφαρμόζονταν από πλευράς παρόχων παρουσίαζαν σημαντική ανομοιογένεια, με αποτέλεσμα η άνιση εφαρμογή μεταξύ κρατών μελών να διαμορφώνει ένα κατακερματισμένο τοπίο και ουσιαστικά κενά στην προστασία των παιδιών από τη σεξουαλική κακοποίηση. Ως απάντηση στις υφιστάμενες ανεπάρκειες των σχετικών μέτρων που έχουν καθιερωθεί προτείνεται η θέσπιση του Κανονισμού CSAR, με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο. Οι βασικές ρυθμίσεις που εισάγει ο Κανονισμός περιλαμβάνουν τον υποχρεωτικό εντοπισμό, αναφορά και αφαίρεση υλικού παιδικής διαδικτυακής σεξουαλικής κακοποίησης και άγρας από τους παρόχους σε περίπτωση έκδοσης σχετικής εντολής εντοπισμού, αφαίρεσης ή αποκλεισμού, και την δημιουργία του Κέντρου της ΕΕ κατά της σεξουαλικής κακοποίησης, η δράση του οποίου θα στοχεύει στην ανταλλαγή εμπειρογνωσίας και στον συντονισμό των εμπλεκόμενων φορέων που ασχολούνται με την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, ιδίως στο διαδίκτυο.

Η Πρόταση ωστόσο, έχει προκαλέσει έντονο προβληματισμό, καθώς η εφαρμογή της συνεπάγεται κινδύνους για θεμελιώδη δικαιώματα. Οι κυριότερες ανησυχίες επικεντρώνονται στις επιπτώσεις στην προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας των χρηστών από την εφαρμογή εντολών υποχρεωτικού εντοπισμού, στην εμπιστευτικότητα των επικοινωνιών η οποία ενδέχεται να επηρεαστεί από μέτρα όπως η σάρωση από την πλευρά του πελάτη σε περίπτωση υπονόμευσης της κρυπτογράφησης από άκρο σε άκρο, καθώς επίσης και στην ελευθερία της έκφρασης εξαιτίας της εφαρμογής μέτρων σάρωσης περιεχομένου σε ευρεία κλίμακα. Η παρούσα

διπλωματική εργασία αφιερώνεται στην ανάλυση των επιπτώσεων της Πρότασης Κανονισμού CSAR στα θεμελιώδη δικαιώματα, με έμφαση στην αξιολόγηση τήρησης της αρχής της αναλογικότητας.

Λέξεις Κλειδιά: Πρόταση Κανονισμού για τη σεξουαλική κακοποίηση παιδιών, ιδιωτικότητα, προσωπικά δεδομένα, τεχνολογίες κατακερματισμού, τεχνολογίες ΤΝ, κρυπτογράφηση από άκρο σε άκρο, αρχή της αναλογικότητας.

Abstract

Child sexual abuse constitutes an increasingly growing problem worldwide, with material depicting the sexual abuse of minors being circulated and stored through online services. The expanded use of digital platforms by young people, combined with the capabilities of the modern digital era—which facilitates communication through social networks and messaging applications—has also led to a significant increase in cases of child grooming for sexual abuse.

Until today, the detection and reporting of the above-mentioned crimes by providers of information society services in the EU has been carried out primarily on a voluntary basis. Consequently, the measures and procedures applied by providers have shown significant heterogeneity, resulting in uneven application between Member States, creating a fragmented landscape and effectively leaving gaps in the protection of children from sexual abuse.

In response to the existing deficiencies of the measures, the CSAR Regulation is proposed, aiming at the prevention and combat of child sexual abuse online. The key provisions introduced by the Regulation include the mandatory detection, reporting, and removal of online child sexual abuse material and grooming by providers, in the event of the issuance of a relevant detection, removal, or blocking order, and the creation of the EU Centre on Child Sexual Abuse, whose operations will aim at the exchange of expertise and the coordination of the actors involved in the prevention and combat of child sexual abuse, particularly online.

The Proposal, however, has generated substantial concern, as its implementation entails risks to fundamental rights. The main concerns relate to the protection of personal data and user privacy affected by mandatory detection orders, the confidentiality of communications potentially compromised by measures such as client-side scanning in cases where end-to-end encryption is weakened, and the freedom of expression threatened by large-scale content scanning measures. This thesis analyzes the implications of the CSAR Regulation Proposal on fundamental rights, with a focus on assessing compliance with the principle of proportionality.

Keywords: Child Sexual Abuse Regulation (CSAR), privacy, personal data, hashing, AI technologies, end-to-end encryption, principle of proportionality.

1. ΕΙΣΑΓΩΓΗ

Η σεξουαλική κακοποίηση παιδιών και η διαδικτυακή διακίνηση του αντίστοιχου υλικού συγκαταλέγονται στα πλέον ανησυχητικά εγκλήματα της ψηφιακής εποχής, ενώ η εύκολη πρόσβαση στο διαδίκτυο και η ανωνυμία των χρηστών δημιουργούν ευνοϊκό έδαφος που αυξάνει συνεχώς τον κίνδυνο για την τέλεσή τους. Το πρόβλημα δεν εξαντλείται μόνο στην διακίνηση υλικού που απεικονίζει σεξουαλική κακοποίηση παιδιών, αλλά επεκτείνεται και σε συμπεριφορές προσεταιρισμού ανηλίκων, οι οποίες συχνά αποτελούν τον προθάλαμο για κακοποίηση στον πραγματικό κόσμο. Η φύση των εγκλημάτων που δεν έχουν γεωγραφικούς περιορισμούς δημιουργεί επιπλέον πολυπλοκότητες, όσον αφορά τη δικαιοδοσία, καθώς η συνύπαρξη διαφορετικών νομικών συστημάτων δυσχεραίνει σημαντικά τον συντονισμό των διωκτικών αρχών και την αποτελεσματική δίωξη των δραστών, αφού μεσολαβούν χρονοβόρες διαδικασίες διεθνούς συνεργασίας και δικαστικής συνδρομής.

Σε ευρωπαϊκό επίπεδο, το νομικό πλαίσιο ενοποιήθηκε μέσω της Οδηγίας 2011/93/ΕΕ, ενώ ο περιορισμός της διάδοσης τέτοιου είδους περιεχομένου στο διαδίκτυο βασίστηκε σε εθελοντικές πρωτοβουλίες των παρόχων υπηρεσιών του διαδικτύου, μέσω χρήσης τεχνολογιών εντοπισμού και αναφοράς παράνομου περιεχομένου στις διωκτικές αρχές. Η συνέχιση της πρακτικής αυτής εξασφαλίστηκε μέσω υιοθέτησης προσωρινών παρεκκλίσεων από την Οδηγία για την ιδιωτική ζωή στις ηλεκτρονικές επικοινωνίες (e-Privacy Directive), προκειμένου να επιτρέπεται στους παρόχους να προβαίνουν σε ελέγχους χωρίς να παραβιάζουν το απόρρητο των επικοινωνιών.

Παρά ταύτα, η υφιστάμενη προσέγγιση αποδείχθηκε ανεπαρκής. Η εθελοντική φύση των μέτρων οδήγησε σε άνιση εφαρμογή και σημαντικά κενά προστασίας, καθώς ορισμένοι πάροχοι απέφυγαν πλήρως την υιοθέτηση τέτοιων πρακτικών. Παράλληλα, η ταχεία διάδοση της κρυπτογράφησης από άκρο σε άκρο, η χρήση ανώνυμων δικτύων και ο διαμοιρασμός αρχείων μέσω cloud υπηρεσιών με περιορισμένη παρακολούθηση περιεχομένου, περιόρισαν τη δυνατότητα εντοπισμού παράνομου υλικού με τα μέχρι τώρα διαθέσιμα εργαλεία.

Στις 11 Μαΐου 2022 η Ευρωπαϊκή Επιτροπή δημοσίευσε Πρόταση Κανονισμού[1] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών[2] («Πρόταση). Βασικό στόχο της πρότασης αποτέλεσε η θέσπιση ενιαίων κανόνων για την αντιμετώπιση της κατάχρησης υπηρεσιών της κοινωνίας της πληροφορίας που προσφέρονται στην Ένωση, για σκοπούς σεξουαλικής κακοποίησης και άγρας παιδιών[3]. Με τις βασικές διατάξεις που εισάγει υποχρεώνονται οι πάροχοι υπηρεσιών της κοινωνίας της πληροφορίας να ελαχιστοποιούν τον κίνδυνο κατάχρησης των υπηρεσιών τους για σκοπούς σεξουαλικής κακοποίησης παιδιών, θεσπίζεται η υποχρέωση αφαίρεσης και απενεργοποίησης της πρόσβασης σε υλικό παιδικής σεξουαλικής κακοποίησης από πλευράς των παρόχων υπηρεσιών φιλοξενίας, ενώ παράλληλα εισάγονται διαδικασίες με βάση τις οποίες πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών υποχρεούνται να εντοπίζουν και να αφαιρούν υλικό διαδικτυακής σεξουαλικής κακοποίησης παιδιών[4] από τις υπηρεσίες τους.

Η Πρόταση προβλέπει επίσης τη δημιουργία ενός νέου οργανισμού, του «Κέντρου της ΕΕ κατά της σεξουαλικής κακοποίησης παιδιών» («Κέντρο της ΕΕ»), καθώς επίσης και τη σύσταση εθνικών συντονιστικών αρχών για σχετικά ζητήματα, προκειμένου να καταστεί δυνατή η εφαρμογή του κανονισμού. Προβλέπεται μάλιστα ότι το Κέντρο της ΕΕ θα προβεί στη δημιουργία και τη λειτουργία βάσεων δεδομένων με δείκτες για τη διαδικτυακή σεξουαλική κακοποίηση, τους οποίους οι πάροχοι θα πρέπει να χρησιμοποιούν προκειμένου να ανταποκρίνονται στις επιβαλλόμενες από την Πρόταση υποχρεώσεις. Παράλληλα, εισάγονται κανόνες για τη λειτουργία των αρμόδιων αρχών των Κρατών μελών[5].

Επιπροσθέτως, η Πρόταση προβλέπει κατάργηση του Κανονισμού (ΕΕ) 2021/1232 («προσωρινός κανονισμός») περί προσωρινής παρεκκλίσεως από ορισμένες διατάξεις της οδηγίας 2002/58/ΕΚ[6], και συνεπώς από την ημερομηνία εφαρμογής της Πρότασης δεν θα επιτρέπεται στους παρόχους ο οικειοθελής εντοπισμός διαδικτυακής σεξουαλικής κακοποίησης παιδιών. Λαμβανομένης υπόψιν της ρύθμισης που θα υποχρεώνει μόνο τους αποδέκτες εντολών εντοπισμού υλικού να προβαίνουν σε διερεύνηση αυτού, η οικειοθελής χρήση τεχνολογιών από πλευράς παρόχων με σκοπό τον εντοπισμό υλικού σεξουαλικής κακοποίησης παιδιών και περιστατικών άγρας θα επιτρέπεται μονάχα αν αυτό προβλέπεται στην εκάστοτε εθνική νομοθεσία που μεταφέρει την Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, σύμφωνα με το άρθρο 15 παράγραφος 1 της εν λόγω οδηγίας.

[1] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών{SEC(2022) 209 final}.

Δεδομένου ωστόσο ότι οι τεχνολογίες που προβλέπεται να χρησιμοποιηθούν για την εκτέλεση των εντολών εντοπισμού πρόκειται να επηρεάσουν την άσκηση των θεμελιωδών δικαιωμάτων των χρηστών των εν λόγω υπηρεσιών και συγκεκριμένα του απορρήτου των επικοινωνιών, της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ελευθερίας έκφρασης, η εκτέλεση των εντολών εντοπισμού θα πρέπει να διενεργείται με τις λιγότερο επεμβατικές τεχνολογίες στην ιδιωτική ζωή.

Παρά την ειδική πρόνοια που έχει ληφθεί ώστε να προληφθεί η προώθηση εσφαλμένων αναφορών στις αρχές επιβολής του νόμου και μολονότι η Πρόταση εγγυάται ότι η παρέμβαση στα θεμελιώδη δικαιώματα περιορίζεται στο απολύτως απαραίτητο για την αποτελεσματική καταπολέμηση της διαδικτυακής σεξουαλικής κακοποίησης παιδιών, έχει επισημανθεί ότι λόγω των μεθόδων που πρόκειται να χρησιμοποιηθούν, των ποσοστών σφαλμάτων των τεχνολογιών, καθώς και της ασάφειας ορισμένων όρων της Πρότασης, ελλοχεύει έντονα ο κίνδυνος εγκαθίδρυσης καθεστώτος γενικής παρακολούθησης των επικοινωνιών.

Οργανώσεις υπέρμαχες των θεμελιωδών δικαιωμάτων της προστασίας των δεδομένων προσωπικού χαρακτήρα και του απορρήτου των επικοινωνιών κάνουν λόγο για Πρόταση κανονισμού-δούρειο ίππο για μαζικές παρακολουθήσεις των επικοινωνιών[7], καθώς επίσης και για ένα αμφιλεγόμενο νομικό οικοδόμημα που μπορεί να οδηγήσει σε εξάλειψη της έννοιας της ιδιωτικότητας και της ελεύθερης έκφρασης στο διαδίκτυο[8].

---

[2] Ό.π. άρθρο 2(ιζ), «διαδικτυακή σεξουαλική κακοποίηση παιδιών»: διαδικτυακή διάδοση υλικού σεξουαλικής κακοποίησης παιδιών και άγρα παιδιών, σκέψη 13 προοιμίου: Ο όρος «διαδικτυακή σεξουαλική κακοποίηση παιδιών» θα πρέπει να καλύπτει όχι μόνο τη διάδοση υλικού που έχει προηγουμένως εντοπιστεί και επιβεβαιωθεί ότι συνιστά υλικό σεξουαλικής κακοποίησης παιδιών («γνωστό» υλικό), αλλά και υλικού που δεν έχει εντοπιστεί προηγουμένως και το οποίο είναι πιθανό να συνιστά υλικό σεξουαλικής κακοποίησης παιδιών, αλλά δεν έχει ακόμη επιβεβαιωθεί ως τέτοιο («νέο» υλικό), καθώς και δραστηριότητες που συνιστούν άγρα παιδιών («προσεταιρισμό»).

[3] Ό.π. άρθρο 1.

[4] Ό.π. άρθρο 2(ιβ) «υλικό σεξουαλικής κακοποίησης παιδιών»: υλικό που συνιστά παιδική πορνογραφία ή πορνογραφική παράσταση, κατά το άρθρο 2 στοιχεία γ) και ε), αντίστοιχα, της οδηγίας 2011/93/ΕΕ·

[5] Ό.π. άρθρο 40.

[6] Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με προσωρινή παρέκκλιση από ορισμένες διατάξεις της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τη χρήση τεχνολογιών από παρόχους υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και άλλων δεδομένων, με σκοπό την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο.

[7] Homo Digitalis, «Ο CSAR ως Δούρειος Ίππος για μαζική παρακολούθηση;», διαθέσιμο: https://homodigitalis.gr/posts/130909/

[8] EDRi Network, "Internal market MEPs wrestle with how to fix Commission's CSAR proposal", διαθέσιμο: https://edri.org/our-work/internal-markets-meps-wrestle-with-how-to-fix-commissions-csar- proposal/

Στο απυρόβλητο δεν μένει φυσικά το δικαίωμα στην επιχειρηματική ελευθερία[9], το οποίο υφίσταται περιορισμούς από τις προτεινόμενες διατάξεις, ενώ το ζήτημα της συμβατότητάς τους με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ παραμένει ανοικτό και αμφισβητούμενο κατ' ελάχιστον έως και την τελική μορφή της Πρότασης Κανονισμού. Αξίζει να σημειωθεί ότι οι επιπτώσεις από την εφαρμογή της Πρότασης προκύπτουν και για τα ίδια τα παιδιά-χρήστες διαδικτυακών υπηρεσιών, των οποίων τα δικαιώματα στην προσωπική ανάπτυξη, την ελεύθερη έκφραση και την ιδιωτική ζωή ενδέχεται να επηρεαστούν.

Η καταπολέμηση του ειδεχθούς εγκλήματος της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο συνιστά ζήτημα γενικού συμφέροντος αναγνωριζόμενου από την ενωσιακή έννομη τάξη. Για την προάσπιση των δικαιωμάτων των θυμάτων και προκειμένου να καταπολεμηθεί η διακίνηση γνωστού[10] και νέου[11] υλικού παιδικής σεξουαλικής κακοποίησης, αλλά και να καταστεί δυνατή η αποτροπή περιστατικών άγρας παιδιών[12] μέσω διαδικτύου, κρίνεται αναγκαία η θεσμοθέτηση ειδικών μέτρων. Οποιοσδήποτε ωστόσο περιορισμός συντελείται σε θεμελιώδη δικαιώματα του ατόμου είναι αναγκαίο να πληροί τις απαιτήσεις που ορίζονται στο άρθρο 52 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕ).

Αντικείμενο της παρούσας διπλωματικής εργασίας αποτελεί η διερεύνηση της Πρότασης Κανονισμού για την σεξουαλική κακοποίηση παιδιών, υπό το πρίσμα της προστασίας των θεμελιωδών δικαιωμάτων. Η ανάλυση εστιάζει στις δομικές ρυθμίσεις της Πρότασης, με έμφαση στις διατάξεις που αφορούν στην υποχρεωτική ανίχνευση, αναφορά και αφαίρεση υλικού παιδικής σεξουαλικής κακοποίησης, αλλά και στον ρόλο του προβλεπόμενου Κέντρου της ΕΕ στην υποστήριξη και τον συντονισμό κρατών μελών, παρόχων υπηρεσιών και αρμόδιων εθνικών αρχών για την εφαρμογή του Κανονισμού. Στόχος της σχετικής ανάλυσης είναι η εξέταση ενδεχόμενων συγκρούσεων των εν λόγω μέτρων με θεμελιώδη ατομικά δικαιώματα, όπως το δικαίωμα στην ιδιωτικότητα, την προστασία δεδομένων προσωπικού χαρακτήρα, την ελευθερία της έκφρασης, το δικαίωμα στην επιχειρηματική ελευθερία, αλλά και στα δικαιώματα των ίδιων των παιδιών-χρηστών των διαδικτυακών υπηρεσιών. Μέσω μιας συνδυαστικής προσέγγισης που περιλαμβάνει την ανάλυση της λειτουργίας των προτεινόμενων τεχνολογικών εργαλείων εντοπισμού και αναφοράς και τη νομική αποτίμηση της εφαρμογής τους στην πράξη, επιχειρείται η αξιολόγηση της αναλογικότητας και της συμβατότητας των σχετικών διατάξεων με τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης.

Παράλληλα με την εξέταση κρίσιμων επιμέρους διατάξεων, όπως αυτών που διέπουν τη λειτουργία του Κέντρου της ΕΕ, αλλά και την επισκόπηση της σχέσης της Πρότασης με θεμελιώδη μέτρα προστασίας της ιδιωτικότητας, όπως η κρυπτογράφηση από άκρο σε άκρο, επιχειρείται η συνολική

αποτίμηση του προτεινόμενου πλαισίου υπό το πρίσμα της προστασίας των θεμελιωδών δικαιωμάτων. Παρά το γεγονός ότι κατά το χρονικό σημείο εκπόνησης της παρούσας Διπλωματικής Εργασίας έχουν προταθεί τροποποιήσεις στο κείμενο της πρότασης[13] και έχουν μεσολαβήσει τα Συμβιβαστικά Κείμενα πολλών Προεδριών του Συμβουλίου, τα οποία εισάγουν αλλαγές στο αρχικό κείμενο της Πρότασης Κανονισμού[14], στην παρούσα ανάλυση θα επιχειρηθεί σχολιασμός των ρυθμίσεων του αρχικού κειμένου της Πρότασης της Επιτροπής. Παρ' όλα αυτά, για λόγους πληρότητας και σύνδεσης με τα τρέχοντα δεδομένα, ακολουθεί μία συνοπτική αποτύπωση των τελευταίων εξελίξεων.

Ειδικότερα, το τελευταίο Συμβιβαστικό Κείμενο που προτάθηκε είναι αυτό της δανικής Προεδρίας του Συμβουλίου, επί του οποίου επετεύχθη τελικώς συμφωνία μεταξύ των κρατών μελών της ΕΕ την 26η Νοεμβρίου 2025[15], γεγονός που ανοίγει τον δρόμο για την εκκίνηση του τριμερούς διαλόγου με το Ευρωπαϊκό Κοινοβούλιο και την Ευρωπαϊκή Επιτροπή. Έπειτα από χρόνιες διαπραγματεύσεις και αποτυχημένες προσπάθειες των διαδοχικών προεδριών της Τσεχίας, της Ισπανίας, του Βελγίου, της Ουγγαρίας και της Πολωνίας να καταλήξουν σε συναίνεση για το τελικό κείμενο, η Δανική προεδρία κατάφερε να εξασφαλίσει την επίτευξη συμβιβαστικής λύσης.

[9] ΧΘΔΕ άρθρο 16.

[10] Ό.π. άρθρο 2 (ιγ) «γνωστό υλικό σεξουαλικής κακοποίησης παιδιών»: υλικό πιθανής σεξουαλικής κακοποίησης παιδιών που εντοπίζεται με τη χρήση των δεικτών που περιέχονται στη βάση δεδομένων δεικτών η οποία αναφέρεται στο άρθρο 44 παράγραφος 1 στοιχείο α)·

[11] Ό.π. άρθρο 2 (ιδ) «νέο υλικό σεξουαλικής κακοποίησης παιδιών»: υλικό πιθανής σεξουαλικής κακοποίησης παιδιών που εντοπίζεται με τη χρήση των δεικτών που περιέχονται στη βάση δεδομένων δεικτών η οποία αναφέρεται στο άρθρο 44 παράγραφος 1 στοιχείο β)·

[12] Ό.π. άρθρο 2 (ιε) «άγρα παιδιών»: η άγρα παιδιών για σεξουαλικούς σκοπούς όπως αναφέρεται στο άρθρο 6 της οδηγίας 2011/93/ΕΕ·

[13] Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, European Parliament, διαθέσιμο: https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html

[14] EDRi, CSA Regulation Document Pool, 2025, διαθέσιμο: https://edri.org/our-work/csa-regulation-document-pool/

[15] Council of the European Union, Child sexual abuse: Council reaches position on law protecting children from online abuse, 2025, διαθέσιμο: https://www.consilium.europa.eu/en/press/press-releases/2025/11/26/child-sexual-abuse-council-reaches-position-on-law-protecting-children-from-online-abuse/?utm_source=brevo&utm_campaign=AUTOMATED%20-%20Alert%20-%20Newsletter&utm_medium=email&utm_id=3318

Το τελικό κείμενο του Κανονισμού[16] εισάγει υποχρεώσεις εκτίμησης και μετριασμού του κινδύνου των υπηρεσιών, με συνακόλουθη ταξινόμησή τους σε κατηγορίες με βάση τον κίνδυνο, ενώ η χρήση της παρέκκλισης δυνάμει του Κανονισμού (ΕΕ) 2021/1232, μέσω του οποίου οι πάροχοι μπορούν να προβαίνουν σε εθελοντικές έρευνες για την εύρεση υλικού παιδικής σεξουαλικής κακοποίησης συνιστά πλέον πιθανό μέτρο μετριασμού του κινδύνου. Οι διατάξεις που αφορούσαν στις υποχρεωτικές εντολές ανίχνευσης καταργούνται, ενώ ως νέο μέτρο εισάγεται η εντολή διαγραφής περιεχομένου από τα αποτελέσματα των μηχανών αναζήτησης (delisting). Ταυτόχρονα, οι διαδικτυακές μηχανές αναζήτησης προστίθενται στον κατάλογο των σχετικών υπηρεσιών της Κοινωνίας της Πληροφορίας. Όσον αφορά στο Κέντρο της ΕΕ, οι βασικές αρμοδιότητές του όπως αυτές είχαν εισαχθεί στο αρχικό κείμενο της Πρότασης, διατηρούνται.

Αναφορικά με την διατερματική κρυπτογράφηση, στο πεδίο εφαρμογής του Κανονισμού υπό άρθρο 1, εισάγεται ρητή διάταξη υπέρ της αδιαμφισβήτητης προστασίας της, αφού προβλέπεται ότι ο Κανονισμός δεν συνεπάγεται υποχρέωση σε βάρος των παρόχων υπηρεσιών φιλοξενίας ή διαπροσωπικών επικοινωνιών να καθιστούν δυνατή την πρόσβαση σε δεδομένα που είναι κρυπτογραφημένα από άκρο σε άκρο, ούτε υποχρέωση να προσφέρουν υπηρεσίες με ασθενέστερη κρυπτογράφηση.

2. ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ CSAR: ΕΠΙΣΚΟΠΗΣΗ ΔΟΜΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Ο προτεινόμενος Κανονισμός αποτελείται από δύο βασικά δομικά στοιχεία[17]: πρώτον, εισάγει συγκεκριμένες υποχρεώσεις στους παρόχους αναφορικά με τον εντοπισμό, την αναφορά, την αφαίρεση και τον αποκλεισμό γνωστού και νέου υλικού παιδικής σεξουαλικής κακοποίησης, καθώς και της άγρας παιδιών, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται στις διαδικτυακές συναλλαγές, και δεύτερον, ιδρύει το Κέντρο της ΕΕ ως αποκεντρωμένο οργανισμό, προκειμένου να καταστεί εφικτή η εφαρμογή του Κανονισμού.

[16] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Partial mandate for negotiations with the European Parliament, 2025, διαθέσιμο: https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf

[17] Ό.π. Αιτιολογική Έκθεση Πρότασης, στοιχείο 5.

Ειδικότερα, η Πρόταση Κανονισμού εισάγει υποχρεώσεις για τους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας που προσφέρονται στην Ένωση, ανεξαρτήτως του τόπου εγκατάστασής τους, προκειμένου να αντιμετωπιστεί το ζήτημα κατάχρησης των υπηρεσιών τους για σκοπούς σεξουαλικής κακοποίησης και άγρας παιδιών. Οι πάροχοι υπηρεσιών φιλοξενίας και υπηρεσιών διαπροσωπικών επικοινωνιών υποχρεούνται να εντοπίζουν και να αξιολογούν τον κίνδυνο χρήσης των υπηρεσιών τους για σκοπούς διαδικτυακής σεξουαλικής κακοποίησης παιδιών[18] και εν συνεχεία να λαμβάνουν εύλογα μέτρα μετριασμού του. Τα εν λόγω μέτρα απαιτείται να είναι αποτελεσματικά[19] για τον μετριασμό του εντοπισθέντος κινδύνου, στοχευμένα και αναλογικά, και να τίθενται σε εφαρμογή κατόπιν συνεκτίμησης πιθανών συνεπειών στην άσκηση των θεμελιωδών δικαιωμάτων άλλων θιγόμενων προσώπων. Τέτοιου είδους μέτρα μπορεί να συνιστούν ενδεικτικά[20] η ενίσχυση του συστήματος εσωτερικής εποπτείας της λειτουργίας της υπηρεσίας ή ακόμη και η συνεργασία με άλλους παρόχους ή οντότητες στις οποίες έχει χορηγηθεί καθεστώς αξιόπιστων πηγών επισήμανσης περιεχομένου.

Σε περίπτωση που από την εκτίμηση κινδύνου προκύψει κίνδυνος χρήσης των υπηρεσιών για σκοπούς άγρας παιδιών, οι πάροχοι υποχρεούνται να λαμβάνουν μέτρα επαλήθευσης της ηλικίας των ανήλικων χρηστών, προκειμένου να τίθενται σε εφαρμογή κατάλληλα μέτρα μετριασμού του κινδύνου[21]. Τα αποτελέσματα της αξιολόγησης κινδύνου, καθώς και τυχόν μέτρα μετριασμού του θα πρέπει να κοινοποιούνται στην αρμόδια για θέματα σεξουαλικής κακοποίησης παιδιών Συντονιστική Αρχή του εκάστοτε κράτους μέλους[22].

Εν συνεχεία, η εν λόγω αρχή εξουσιοδοτούμενη να ελέγξει αν η εκτίμηση κινδύνου και τα αναγκαία μέτρα μετριασμού ελήφθησαν με βάση τα οριζόμενα στα άρθρα 3 και 4[23], δύναται να ζητήσει από την αρμόδια δικαστική ή διοικητική αρχή να εκδώσει[24] εντολή εντοπισμού σε βάρος του παρόχου υπηρεσιών φιλοξενίας ή του παρόχου υπηρεσιών διαπροσωπικών επικοινωνιών που υπάγεται στη δικαιοδοσία του εν λόγω κράτους μέλους, προκειμένου να ληφθούν από πλευράς παρόχου τα περιγραφόμενα στο άρθρο 10 μέτρα ώστε να εντοπισθεί διαδικτυακή σεξουαλική κακοποίηση παιδιών σε μία συγκεκριμένη υπηρεσία.

---

[18] Ό.π. άρθρο 3.

[19] Ό.π. άρθρο 4 παρ. 2.

[20] Ό.π. άρθρο 4 παρ. 1.

[21] Ό.π. άρθρο 4 παρ. 3.

[22] Ό.π. άρθρα 5 και 25.

[23] Ό.π. άρθρο 5 παρ. 2.

[24] Ό.π. άρθρο 7 παρ. 1.

Η αρμόδια δικαστική ή ανεξάρτητη διοικητική αρχή, αφότου λάβει υπόψη τη γνώμη του παρόχου, του Κέντρου της ΕΕ και της Αρχής Προστασίας Δεδομένων[25] εκδίδει εντολή εντοπισμού εάν υπάρχουν αποδείξεις ότι υφίσταται «σημαντικός κίνδυνος» κατάχρησης της υπηρεσίας με σκοπό την τέλεση αδικημάτων διαδικτυακής σεξουαλικής κακοποίησης παιδιών και εάν οι λόγοι για την έκδοσή της υπερκεράζουν τις αρνητικές συνέπειες για τα δικαιώματα και τα έννομα συμφέροντα των θιγόμενων μερών.

Η διαπίστωση ύπαρξης «σημαντικού κινδύνου» εξαρτάται από τον τύπο του υλικού διαδικτυακής σεξουαλικής κακοποίησης παιδιών[26] για το οποίο εκδίδεται εντολή εντοπισμού[27]. Σημαντικός κίνδυνος για τη διάδοση γνωστού υλικού σεξουαλικής κακοποίησης παιδιών υφίσταται όταν παρά τα μέτρα μετριασμού πιθανολογείται ότι μία υπηρεσία χρησιμοποιείται «σε σημαντικό βαθμό[28]» για τη διάδοση τέτοιου υλικού και υπάρχουν παράλληλα αποδεικτικά στοιχεία ότι η υπηρεσία[29] έχει χρησιμοποιηθεί κατά τους τελευταίους 12 μήνες και σε σημαντικό βαθμό για τη διάδοση γνωστού υλικού σεξουαλικής κακοποίησης παιδιών[30].

Σημαντικός κίνδυνος αναφορικά με τη διάδοση νέου υλικού σεξουαλικής κακοποίησης παιδιών θεωρείται ότι υφίσταται όταν παρά τα μέτρα μετριασμού είναι πιθανόν υπηρεσία να χρησιμοποιείται σε σημαντικό βαθμό για τη διάδοση νέου υλικού σεξουαλικής κακοποίησης παιδιών και υπάρχουν αποδεικτικά στοιχεία σύμφωνα με τα οποία η υπηρεσία[31], έχει πράγματι χρησιμοποιηθεί τους τελευταίους 12 μήνες και σε σημαντικό βαθμό για τη διάδοση νέου υλικού σεξουαλικής κακοποίησης παιδιών. Για υπηρεσίες εκτός εκείνων που επιτρέπουν τη ζωντανή μετάδοση πορνογραφικών παραστάσεων[32] τέτοιος κίνδυνος υφίσταται όταν έχει εκδοθεί εντολή εντοπισμού διάδοσης γνωστού υλικού και ο πάροχος έχει υποβάλει σημαντικό αριθμό αναφορών για γνωστό υλικό σεξουαλικής

[25] Ό.π. άρθρο 7 παρ. 3 και 4.

[26] «υλικό σεξουαλικής κακοποίησης παιδιών»: υλικό που συνιστά παιδική πορνογραφία ή πορνογραφική παράσταση, κατά το άρθρο 2 στοιχεία γ) και ε), αντίστοιχα, της οδηγίας 2011/93/ΕΕ·

[27] Ό.π. άρθρο 7 παρ. 5.

[28] Ό.π. προοίμιο, σκέψη 21 «ένα από τα στοιχεία που πρέπει να λαμβάνονται υπόψη στο πλαίσιο αυτό είναι η πιθανότητα η υπηρεσία να χρησιμοποιείται σε σημαντικό βαθμό, δηλαδή, πέραν μεμονωμένων και σχετικά σπάνιων περιπτώσεων, με σκοπό την εν λόγω κακοποίηση».

[29] ή ανάλογη αυτής υπηρεσία εάν η υπηρεσία αυτή δεν έχει προσφερθεί στην Ένωση κατά το χρόνο υποβολής της αίτησης έκδοσης εντολής εντοπισμού.

[30] Ό.π. άρθρο 7 παρ. 6.

[31] ή ανάλογη υπηρεσία εάν η υπηρεσία δεν έχει ακόμη προσφερθεί στην Ένωση κατά την ημερομηνία υποβολής της αίτησης για την έκδοση της εντολής εντοπισμού.

[32] κατά τα οριζόμενα στο άρθρο 2 στοιχείο ε) της οδηγίας 2011/93/ΕΕ.

κακοποίησης παιδιών, το οποίο ανιχνεύθηκε μέσω των μέτρων που ελήφθησαν σύμφωνα με το άρθρο 12.

Αναφορικά με τις εντολές εντοπισμού άγρας παιδιών[33], σημαντικός κίνδυνος να χρησιμοποιηθεί η υπηρεσία για διαδικτυακή σεξουαλική κακοποίηση παιδιών υφίσταται όταν ο πάροχος μπορεί να χαρακτηριστεί πάροχος υπηρεσιών διαπροσωπικών επικοινωνιών, όταν είναι πιθανό παρά τα μέτρα μετριασμού η υπηρεσία να χρησιμοποιείται σε σημαντικό βαθμό για σκοπούς άγρας παιδιών και παράλληλα υπάρχουν αποδεικτικά στοιχεία σύμφωνα με τα οποία η υπηρεσία[34] έχει χρησιμοποιηθεί κατά τους προηγούμενους 12 μήνες και σε βαθμό σημαντικό για την άγρα παιδιών.

Σημειώνεται ότι η Συντονιστική Αρχή θα πρέπει να προσδιορίζει την αίτηση έκδοσης εντολής εντοπισμού κατά τρόπο ώστε τυχόν αρνητικές συνέπειες να παραμένουν περιορισμένες στο απολύτως απαραίτητο για την αποτελεσματική αντιμετώπιση του σημαντικού κινδύνου. Επί παραδείγματι, η εντολή ανίχνευσης θα πρέπει να περιορίζεται σε ένα μέρος της υπηρεσίας, να λαμβάνεται υπόψη η παράμετρος της διαθεσιμότητας επαρκώς αξιόπιστων τεχνολογιών, καθώς και ο αντίκτυπος των μέτρων στα δικαιώματα των θιγόμενων χρηστών[35]. Οι εντολές εντοπισμού για γνωστό και νέο υλικό παιδικής σεξουαλικής κακοποίησης προβλέπεται ότι μπορούν να διαρκέσουν έως και 24 μήνες και για άγρα παιδιών έως και 12 μήνες[36]. Οι πάροχοι και οι χρήστες που επηρεάζονται από τα μέτρα έχουν δικαίωμα αποτελεσματικής προσφυγής, συμπεριλαμβανομένου του δικαιώματος αμφισβήτησης της εντολής εντοπισμού ενώπιον των δικαστηρίων του κράτους μέλους της αρχής που εξέδωσε την εντολή[37].

Για την υποστήριξη της εφαρμογής του προτεινόμενου κανονισμού, το Κέντρο ΕΕ θα ιδρυθεί ως ανεξάρτητο όργανο της Ένωσης[38] και προορίζεται να διευκολύνει τις διαδικασίες ανίχνευσης περιεχομένου μέσω της λειτουργίας βάσεων δεδομένων δεικτών διαδικτυακής σεξουαλικής κακοποίησης παιδιών, τις οποίες πρέπει να χρησιμοποιούν οι πάροχοι για να συμμορφώνονται με τις εντολές εντοπισμού. Μεταξύ άλλων, θα υποστηρίζει τον συντονισμό μεταξύ των εθνικών αρχών[39]

---

[33] Ό.π. άρθρο 7 παρ. 7.

[34] ή ανάλογη υπηρεσία εάν η υπηρεσία δεν έχει ακόμη προσφερθεί στην Ένωση κατά την ημερομηνία υποβολής της αίτησης για την έκδοση της εντολής εντοπισμού

[35] Ό.π. άρθρο 7 παρ. 8.

[36] Ό.π. άρθρο 7 παρ. 9.

[37] Ό.π. άρθρο 9.

[38] Ό.π. άρθρο 41 παρ. 1.

[39] Ό.π. άρθρο 43.

και θα διαβιβάζει στην Europol και στις εθνικές αρχές επιβολής του νόμου σχετικές αναφορές, κατόπιν ελέγχου για ψευδώς θετικά αποτελέσματα[40].

2.1. ΣΧΕΣΗ ΤΗΣ ΠΡΟΤΑΣΗΣ ΜΕ ΤΗΝ ΥΦΙΣΤΑΜΕΝΗ ΝΟΜΟΘΕΣΙΑ

Με βάση το κείμενο της Πρότασης, οι κανόνες που απορρέουν από τον ΓΚΠΔ[41] και την οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[42] δεν θίγονται από την εφαρμογή του προτεινόμενου Κανονισμού. Θα πρέπει ωστόσο να σημειωθεί ότι ο προσωρινός κανονισμός[43] προέβλεπε προσωρινή παρέκκλιση από τις διατάξεις του άρθρου 5 παράγραφος 1 και του άρθρου 6 παράγραφος 1 και όχι από το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[44]. Αντίθετα, η πρόταση προβλέπει τελικώς περιορισμό της άσκησης των δικαιωμάτων και των υποχρεώσεων που προβλέπονται στο άρθρο 5 παράγραφοι 1 και 3 και στο άρθρο 6 παράγραφος 1 της οδηγίας 2002/58/ΕΚ.

Στην Πρόταση επισημαίνεται μάλιστα ότι το άρθρο 15 παράγραφος 1 της οδηγίας 2002/58/ΕΚ, με βάση το οποίο επιτρέπεται στα κράτη μέλη η θέσπιση μέτρων που περιορίζουν την εφαρμογή των δικαιωμάτων στην προστασία του απορρήτου, όταν ο εν λόγω περιορισμός συνιστά αναγκαίο, κατάλληλο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία με σκοπό τη διερεύνηση και τη δίωξη ποινικών αδικημάτων, εφαρμόζεται κατ' αναλογία στις κανονιστικές προβλέψεις της πρότασης που

---

[40] Ό.π. άρθρο 48 παρ. 3.

[41] 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 της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679

[42] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32002L0058

[43] Ό.π.

[44] Κανονισμός (ΕΕ) 2021/1232 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Ιουλίου 2021, περί προσωρινής παρεκκλίσεως από ορισμένες διατάξεις της οδηγίας 2002/58/ΕΚ όσον αφορά τη χρήση τεχνολογιών από παρόχους υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών για την επεξεργασία προσωπικών και άλλων δεδομένων, προς καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο (ΕΕ [2021] L 274/41), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R1232, σκέψη 12 προοιμίου: «Ο παρών κανονισμός προβλέπει προσωρινή παρέκκλιση από το άρθρο 5 παράγραφος 1 και από το άρθρο 6 παράγραφος 1 της οδηγίας 2002/58/ΕΚ, τα οποία προστατεύουν το απόρρητο των επικοινωνιών και των δεδομένων κίνησης».

περιορίζουν τα προβλεπόμενα στα άρθρα 5 παράγραφοι 1 και 3 και 6 παράγραφος 1 δικαιώματα της οδηγίας 2002/58/ΕΚ[45].

Η άσκηση δηλαδή των δικαιωμάτων και η ανάληψη των υποχρεώσεων που προβλέπονται στα ανωτέρω άρθρα θα πρέπει να περιορίζεται στον βαθμό που είναι απολύτως αναγκαίο για την εκτέλεση εντολών εντοπισμού με σκοπό την πρόληψη και την καταπολέμηση της διαδικτυακής σεξουαλικής κακοποίησης παιδιών. Περαιτέρω, η Πρόταση αποσκοπεί στη θέσπιση νομικής βάσης, κατά την έννοια του ΓΚΠΔ, για την επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό τον εντοπισμό υλικού σεξουαλικής κακοποίησης παιδιών[46].

3. ΑΠΑΓΟΡΕΥΣΗ ΓΕΝΙΚΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Η προσέγγιση της ευρωπαϊκής έννομης τάξης αναφορικά με τη διακυβέρνηση της πλατφόρμας βασίζεται στην περιορισμένη ευθύνη των παρόχων για το περιεχόμενο που δημοσιεύουν οι χρήστες. Συγκεκριμένα, η οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο[47] εισήγαγε διατάξεις απαλλαγής των παρόχων από την ευθύνη σε περίπτωση που δεν υπήρχε γνώση ύπαρξης παράνομου περιεχομένου στις υπηρεσίες τους[48], και παράλληλα απαλλαγή τους από την υποχρέωση καθολικού ελέγχου των διαμοιραζόμενων πληροφοριών[49].

Δεδομένου ότι η απαγόρευση οποιασδήποτε γενικής υποχρέωσης παρακολούθησης διασφαλίζει την προστασία θεμελιωδών δικαιωμάτων όπως η ελευθερία της έκφρασης, το απόρρητο και η προστασία δεδομένων, το άρθρο 8 της Πράξης για τις Ψηφιακές Υπηρεσίες (DSA) συνιστά διάταξη που αποσκοπεί στην προστασία των δικαιωμάτων του Χάρτη της ΕΕ[50], όπως αντιστοίχως προέβλεπε το άρθρο 15 της Οδηγίας για το Ηλεκτρονικό Εμπόριο. Η εν λόγω μεταχείριση θεμελιώθηκε στο γεγονός

[45] Ό.π. προοίμιο, σκέψη 9.

[46] Ο.π. αιτιολογική έκθεση, ενότητα: «Συνέπεια με άλλες πολιτικές της Ένωσης», σελ. 5.

[47] 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 («e-Commerce Directive»), διαθέσιμο σε: https://eur-lex.europa.eu/legal- content/EL/ALL/?uri=CELEX:32000L0031

[48] E-Commerce Directive, άρθρο 14.

[49] E-Commerce Directive, άρθρο 15.

[50] Expert Workshop on the EU Proposed Regulation on preventing and Combatting Child sexual Abuse, jointly organized by the Center for Law and Digital Technologies of Leiden University and ECPAT International Leiden University, 2022, Ενότητα 4.1., σελ. 10., διαθέσιμο: https://www.universiteitleiden.nl/en/news/2023/02/report-launch-workshop-on-eu-proposed-regulation-onpreventing-and-combatting-child-sexual-abuse

ότι οι ενδιάμεσοι πάροχοι δεν δύνανται πρακτικά να ελέγχουν τον τεράστιο όγκο δεδομένων που αποθηκεύεται σε αυτούς ή διακινείται μέσω των υπολογιστών τους[51].

Ζητήματα ωστόσο εννοιολογικής φύσεως που ανέκυψαν από την ενσωμάτωση της οδηγίας 2000/31/ΕΚ στις επιμέρους έννομες τάξεις προσπάθησε να επιλύσει η Πράξη για τις Ψηφιακές Υπηρεσίες[52] (DSA), η οποία εξακολουθεί να μεταφέρει την αρχή της απαγόρευσης γενικής υποχρέωσης παρακολούθησης, θεσπίζοντας στο άρθρο 8 την μη επιβολή γενικής υποχρέωσης παρακολούθησης ή ενεργητικής αναζήτησης γεγονότων. Με βάση το άρθρο 9 της DSA οι πάροχοι υποχρεούνται να ενεργήσουν προς κατάργηση συγκεκριμένου παράνομου περιεχομένου, ωστόσο η έκταση παρέμβασης που διατάσσεται με δικαστική απόφαση αφορά σε συγκεκριμένο περιεχόμενο και δεν σχετίζεται με γενική παρακολούθηση[53].

Στην υπόθεση SABAM κατά Netlog[54], το Δικαστήριο της Ευρωπαϊκής Ένωσης («ΔΕΕ») έκρινε ότι η εντολή σε πάροχο φιλοξενίας να εγκαταστήσει σύστημα που φιλτράρει αδιάκριτα όλο το περιεχόμενο που ανέβασε κάθε χρήστης για απροσδιόριστο χρονικό διάστημα συνιστούσε παραβίαση της απαγόρευσης γενικής υποχρέωσης παρακολούθησης, ικανή μάλιστα να θίξει θεμελιώδη δικαιώματα των χρηστών που κατοχυρώνονται από τα άρθρα 8 και 11 του ΧΘΔΕ. Ωστόσο, με βάση την Πρόταση του Γενικού Εισαγγελέα στις συνεκδικασθείσες υποθέσεις C-682/18 και C-683/18[55], ένας πάροχος μπορεί να υποχρεωθεί να εντοπίζει και να αφαιρεί όχι μόνο παράνομο περιεχόμενο αλλά και «ισοδύναμο» αυτού, κατόπιν έκδοσης ασφαλιστικών μέτρων. Ο Γενικός Εισαγγελέας σημείωσε επιπλέον ότι υποχρεώσεις αφαίρεσης ισοδύναμου περιεχομένου δεν μπορούν να επιβληθούν σε όλους τους παρόχους σε περίπτωση που δεν διαθέτουν τους πόρους να ενσωματώσουν τέτοιου είδους τεχνολογία. Με βάση τις ανωτέρω κρίσεις έχει υποστηριχθεί η άποψη ότι η τεχνολογία που αντιστοιχίζει το περιεχόμενο που δημιουργείται από τους χρήστες με μια κεντρική βάση δεδομένων

---

[51] Γιώργος Ν. Γιαννόπουλος, Η ευθύνη των παρόχων υπηρεσιών του Internet, σελ. 113.

[52] Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών (πράξη για τις ψηφιακές υπηρεσίες) και την τροποποίηση της οδηγίας 2000/31/ΕΚ, διαθέσιμο: https://eur-lex.europa.eu/legal

[53] E-commerce Directive, σκέψη 47: "Τα κράτη μέλη δεν μπορούν να επιβάλουν γενική υποχρέωση ελέγχου στους φορείς παροχής υπηρεσιών. Αυτό δεν αφορά τις υποχρεώσεις ελέγχου σε συγκεκριμένες περιπτώσεις, και ειδικότερα δεν θίγει τυχόν εντολές των εθνικών αρχών σύμφωνα με την εθνική νομοθεσία".

[54] ΔΕΕ, SABAM v. Netlog NV, Case C-360/10, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=D4467091242228CE5FADC98767BEA97A?text=&docid=119512&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=3348323

[55] Πρόταση του Γενικού Εισαγγελέα Henrik Saugmandsgaard ØE της 16ης Ιουλίου 2020, συνεκδικαζόμενες υποθέσεις C-682/18 και C-683/18, διαθέσιμο: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CC0682#t-ECR_62018CC0682_EN_01-E0188

γνωστού παράνομου περιεχομένου αποτελεί επιτρεπόμενη εξαίρεση από την απαγόρευση μιας γενικής υποχρέωσης παρακολούθησης[56].

4. ΠΡΟΛΗΨΗ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ ΠΑΙΔΙΩΝ

4.1. ΑΝΑΓΚΗ ΘΕΣΠΙΣΗΣ ΜΕΤΡΩΝ

Δεδομένου ότι το υλικό σεξουαλικής κακοποίησης παιδιών αποτελεί προϊόν πραγματικής σεξουαλικής κακοποίησης, η θέσπιση ρυθμίσεων για τον εντοπισμό του κρίνεται απαραίτητη προκειμένου να υπάρξει αποτελεσματική πρόληψη της παραγωγής και της διάδοσής του, αλλά και να εντοπιστούν τα παιδιά θύματα, τα οποία συνήθως υφίστανται περισσότερες της μίας μορφές κακοποίησης[57]. Στο πλαίσιο της καταπολέμησης ποινικών αδικημάτων σε βάρος των ανηλίκων, το ΔΕΕ έχει μάλιστα υπογραμμίσει τις θετικές υποχρεώσεις των αρμόδιων αρχών να επιβάλλουν τη λήψη μέτρων για την προστασία των δικαιωμάτων των παιδιών στον σεβασμό της ιδιωτικής και οικογενειακής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα[58].

Αναφορικά με τον περιορισμό του δικαιώματος των χρηστών των υπηρεσιών στην ιδιωτική ζωή, σε σχέση με τις αναγκαίες για την εκτέλεση εντολών εντοπισμού ενέργειες, η Επιτροπή υπογραμμίζει την ανάγκη ισορροπίας μεταξύ αφενός των στόχων δημοσίου συμφέροντος που εκπληρώνονται μέσω της λήψης μέτρων για την προστασία των παιδιών και αφετέρου των θεμελιωδών δικαιωμάτων των χρηστών των εν λόγω υπηρεσιών, τονίζοντας τον σημαντικό αντίκτυπο των προτεινόμενων μέτρων στα θεμελιώδη δικαιώματα των θυμάτων[59].

Παρά το γεγονός ότι η αυτόματη αναζήτηση στις διαπροσωπικές επικοινωνίες για σκοπούς εντοπισμού άγρας παιδιών αποτελεί την πιο παρεμβατική μέθοδο όλων σε βάρος των δικαιωμάτων των χρηστών, η Ευρωπαϊκή Επιτροπή τονίζει ότι η μέθοδος αυτή αποτελεί το μοναδικό τρόπο εντοπισμού τέτοιου είδους υλικού. Θεωρεί μάλιστα ότι οι υποχρεώσεις περιορίζονται στο απολύτως αναγκαίο[60] για την επίτευξη των στόχων προστασίας των ανηλίκων, επισημαίνοντας τις

---

[56] Ό.π. Expert Workshop, ενότητα 4.1., σελ.12.

[57] Katrin Chauviré-Geib and Jörg M. Fegert, Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review, Sage Journals, Volume 25, Issue 2, 2024, διαθέσιμο: https://doi.org/10.1177/15248380231178754

[58] ΔΕΕ, C-511/18 - La Quadrature du Net κλπ., συνεκδικασθείσες υποθέσεις C-511/18, C-512/18 και C-520/18, σκέψη 126, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=6898

[59] Ό.π. Αιτιολογική Έκθεση Πρότασης, «αιτιολόγηση και στόχοι της πρότασης».

[60] Ό.π. Αιτιολογική Έκθεση Πρότασης, «Νομική βάση, επικουρικότητα, αναλογικότητα».

παρεχόμενες διασφαλίσεις για την ελαχιστοποίηση της παρέμβασης στα θεμελιώδη δικαιώματα των χρηστών, όπως την πρόσβαση των παρόχων σε αξιόπιστες τεχνολογίες εντοπισμού που θα προσφέρεται από το Κέντρο της ΕΕ προκειμένου να μειωθούν τα ψευδώς θετικά αποτελέσματα.

Παρά την ύπαρξη της Οδηγίας 2011/93/ΕΕ[61] που θεσπίζει το αξιόποινο των αδικημάτων που σχετίζονται με υλικό σεξουαλικής κακοποίησης παιδιών[62] στην ΕΕ, αποδεικνύεται ότι δεν έχει επιτευχθεί αποτελεσματική προστασία, κάτι που επιβεβαιώνεται και από τις ετήσιες αναφορές οργανώσεων προστασίας δικαιωμάτων των παιδιών. Σύμφωνα με το Εθνικό Κέντρο των ΗΠΑ για τα αγνοούμενα παιδιά και τα παιδιά που πέφτουν θύματα εκμετάλλευσης (NCMEC), το 2022 υποβλήθηκαν στην γραμμή CyberTipline αναφορές για πάνω από 49,4 εκατομμύρια εικόνες, εκ των οποίων 18,8 εκατομμύρια (38%) ήταν μοναδικές. Παράλληλα, σύμφωνα με τα στατιστικά στοιχεία του Διεθνούς Συνδέσμου Ανοικτών Γραμμών του διαδικτύου (INHOPE) για το 2022, το 84% των αναφορών που προωθήθηκαν μεταξύ των ανοικτών γραμμών του προκειμένου να αναληφθεί δράση από την αντίστοιχη δικαιοδοσία ήταν νέο[63]. Παρά την συμβολή ορισμένων παρόχων και τη δράση οργανώσεων προστασίας του παιδιού, η αποσπασματική αντιμετώπιση του φαινομένου, καθώς επίσης και οι μεμονωμένες νομοθετικές πρωτοβουλίες κρατών μελών, οδηγούν τελικώς σε ανάπτυξη αποκλινουσών ρυθμίσεων και πρακτικών.

Η αναγκαιότητα υιοθέτησης της Πρότασης δες την παραπάνω παρατήρηση . Αν την ακολουθήσεις πρέπει σε μερικά σημεία να τροποποιήσεις τις διατυπώσεις υπογραμμίζεται και από τον συνασπισμό ECLAG[64], ο οποίος αποτελείται από περισσότερες από 60 οργανώσεις που δραστηριοποιούνται στην κατεύθυνση του τερματισμού της σεξουαλικής κακοποίησης των παιδιών. Στοχεύοντας στην αποδόμηση των επιχειρημάτων περί δημιουργίας καθεστώτος γενικής παρακολούθησης των επικοινωνιών, ο ECLAG τονίζει[65] ότι η εκάστοτε εντολή εντοπισμού θα εκτελείται σε συγκεκριμένο

---

[61] Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαισίου 2004/68/ΔΕΥ του Συμβουλίου, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32011L0093

[62] Ό.π. Προοίμιο, σκέψη 12: «για λόγους συνέπειας και τεχνολογικής ουδετερότητας, ο όρος 'υλικό σεξουαλικής κακοποίησης παιδιών' θα πρέπει, για τους σκοπούς του παρόντος κανονισμού, να ορίζεται ως αναφερόμενος σε κάθε είδους υλικό που συνιστά παιδική πορνογραφία ή πορνογραφική παράσταση κατά την έννοια της οδηγίας 2011/93/ΕΕ, το οποίο μπορεί να διαδοθεί μέσω της χρήσης υπηρεσιών φιλοξενίας ή διαπροσωπικών επικοινωνιών.

[63] INHOPE, Annual Report 2022, διαθέσιμο: https://www.inhope.org/EN/articles/inhope-annual-report-2022#:~:text=INHOPE's%20Impact%20a%20brief%20look,down%20on%20the%20same%20day

[64] ECLAG, A coalition of more than 60 organisations working to end child sexual abuse on and offline, διαθέσιμο σε: https://www.childsafetyineurope.com/eclag/

[65] ECLAG Steering Group, "Myth Busting & Facts on the proposed Regulation on Child Sexual Abuse: addressing the privacy concerns with data and facts", διαθέσιμο: https://www.eurochild.org/news/learn-thefacts-key-insights-on-the-eus-proposed-csa-regulation

μέρος μίας υπηρεσίας και για συγκεκριμένο χρόνο, ενώ ταυτόχρονα τονίζει ότι οι χρησιμοποιούμενες τεχνολογίες δεν δύνανται να εξαγάγουν την ουσία του περιεχομένου των συνομιλιών. Μάλιστα, ως δικλείδα ασφαλείας έναντι της εσφαλμένης κατηγοριοποίησης περιεχομένου ως υλικό σεξουαλικής κακοποίησης αναδεικνύει την υποβολή του εντοπισθέντος υλικού σε διαδικασία πολλαπλών βημάτων επαλήθευσης διαμέσου ανθρώπινου ελέγχου.

Από την πλευρά του, ο Διεθνής Σύνδεσμος Ανοικτών Γραμμών διαδικτύου (INHOPE), του οποίου η προσφορά είναι εγνωσμένη στην μάχη για την καταπολέμηση της διακίνησης υλικού παιδικής σεξουαλικής κακοποίησης, υποστηρίζει την αναγκαιότητα ψήφισης της Πρότασης με σκοπό την προώθηση της συλλογικής δράσης της ΕΕ για την αντιμετώπιση του φαινομένου. Συστήνει μεταξύ άλλων να αναγνωρισθεί ρητά στην Πρόταση η δυνατότητα των χρηστών να αναφέρουν υλικό σεξουαλικής κακοποίησης παιδιών στις ανοικτές γραμμές, ως κρίσιμο στοιχείο για τον εντοπισμό νέου υλικού και να δημιουργηθεί πλαίσιο νομιμοποίησης των γραμμών να ερευνούν εθελοντικά τέτοιου είδους υλικό[66] στο διαδίκτυο.

4.2. ΕΠΗΡΕΑΖΟΜΕΝΑ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

Η Πρόταση Κανονισμού για την σεξουαλική κακοποίηση παιδιών αποτελεί ένα ρυθμιστικό πλαίσιο με αναμφίβολα σημαντικές επιπτώσεις σε θεμελιώδη δικαιώματα, υπό το πρίσμα πιθανών περιορισμών. Από τη μία πλευρά, προάγει την ουσιαστική εφαρμογή του άρθρου 24 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, διασφαλίζοντας το δικαίωμα του παιδιού στην προστασία από κάθε μορφή κακοποίησης και εκμετάλλευσης. Από την άλλη, ωστόσο, εγείρει ερωτήματα ως προς τη συμβατότητά της με το άρθρο 7 (σεβασμός της ιδιωτικής και οικογενειακής ζωής), το άρθρο 8 (προστασία δεδομένων προσωπικού χαρακτήρα) και το άρθρο 11 (ελευθερία έκφρασης και πληροφόρησης) του Χάρτη, καθόσον εισάγει μηχανισμούς που ενδέχεται να οδηγήσουν σε γενικευμένη παρακολούθηση των ηλεκτρονικών επικοινωνιών. Πέραν των ανωτέρω δικαιωμάτων των χρηστών, η Πρόταση εγείρει ερωτήματα και ως προς τη συμβατότητά της με το άρθρο 16 του ΧΘΔΕ, το οποίο κατοχυρώνει την ελευθερία του επιχειρείν. Οι επιβαλλόμενες υποχρεώσεις στους παρόχους ηλεκτρονικών υπηρεσιών ενδέχεται να περιορίσουν ουσιωδώς την επιχειρηματική τους αυτονομία και να δημιουργήσουν δυσανάλογες επιβαρύνσεις δυνάμενες να πλήξουν τον ελεύθερο ανταγωνισμό και την καινοτομία στην ψηφιακή οικονομία.

[66] INHOPE, "The European Union CSAM Regulation", διαθέσιμο: https://inhope.org/EN/articles/the-european-union-csam-regulation?locale=en

Η αναλογικότητα των προβλεπόμενων μέτρων, καθώς και η ύπαρξη ουσιαστικών θεσμικών και τεχνολογικών εγγυήσεων, καθίστανται καθοριστικής σημασίας για την αποτροπή υπέρμετρων περιορισμών και για τη διασφάλιση της συμβατότητας της Πρότασης με το ευρύτερο πλαίσιο της ευρωπαϊκής προστασίας θεμελιωδών δικαιωμάτων. Για την ουσιαστική αξιολόγηση των επιπτώσεων της προτεινόμενης κανονιστικής ρύθμισης επί των θεμελιωδών δικαιωμάτων, κρίνεται σκόπιμο να προηγηθεί η εννοιολογική αποσαφήνιση και ερμηνευτική προσέγγιση των επίμαχων δικαιωμάτων.

4.2.1. ΙΔΙΩΤΙΚΟΤΗΤΑ

Στην ευρωπαϊκή έννομη τάξη, η προστασία των δεδομένων προσωπικού χαρακτήρα αναγνωρίζεται ως αυτοτελές θεμελιώδες δικαίωμα που κατοχυρώνεται ρητά στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, καθώς και στο πρωτογενές δίκαιο της ΕΕ και συγκεκριμένα στο άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ). Σε επίπεδο παράγωγου δικαίου διασφαλίζεται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Μολονότι φέρει στενή σύνδεση με το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής (άρθρο 7 ΧΘΔΕΕ), εντούτοις έχει διακριτή νομική υπόσταση και προστασία, γεγονός που αντικατοπτρίζεται και στη σχετική νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης[67].

Ειδικότερα, το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, προστατεύει και το απόρρητο των επικοινωνιών, ενώ σε επίπεδο παράγωγου δικαίου η Οδηγία 2002/58/ΕΚ (Οδηγία ePrivacy) εξειδικεύει την υποχρέωση προστασίας του θεμελιώδους αυτού δικαιώματος. Αποτελεί στην ουσία το νομοθετικό εργαλείο εφαρμογής του στον ψηφιακό τομέα, καθιερώνοντας εγγυήσεις για την εμπιστευτικότητα του περιεχομένου και των μεταδεδομένων των επικοινωνιών, τις προϋποθέσεις νόμιμης επεξεργασίας τους και την ασφάλεια των δικτύων εν γένει.

Το δικαίωμα του άρθρου 8 είναι ευρύτερο από το δικαίωμα του άρθρου 7, διότι ενεργοποιείται κάθε φορά που πραγματοποιείται επεξεργασία προσωπικών δεδομένων, ανεξαρτήτως από τον αντίκτυπο της πράξης στην ιδιωτική ζωή[68]. Είναι δικαίωμα ενεργό, καθώς απαιτεί την καθιέρωση ενός συστήματος ελέγχων και ισορροπιών για την προστασία των προσώπων κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Από την άλλη, η έννοια της ιδιωτικής ζωής έχει

[67] Βλ. Digital Rights Ireland (C-293/12). ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ., Τμήμα μείζονος συνθέσεως, 8 Απριλίου 2014, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62012CJ0293

[68] FRA, European Union Agency for Fundamental Rights, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, διαθέσιμο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

ερμηνευθεί με ευρύτητα από τη νομολογία, ώστε να καλύπτει «προσωπικές καταστάσεις, ευαίσθητες ή εμπιστευτικές πληροφορίες, οι οποίες θα μπορούσαν να επηρεάσουν αρνητικά την αντίληψη του κοινού για ένα πρόσωπο, αλλά ακόμη και πτυχές της επαγγελματικής ζωής και της δημόσιας συμπεριφοράς προσώπου»[69].

Περαιτέρω, η έννοια της ιδιωτικότητας είναι στενά συνυφασμένη με την αυτονομία και την ικανότητα του ατόμου να διαμορφώνει και να ζει τη ζωή του σύμφωνα με τις αποφάσεις και τις επιλογές του[70], ενώ παράλληλα υποδηλώνει την αξίωση του ατόμου στο «δικαίωμα στην απομόνωση» ή «απόσυρση» - "the right to be left alone"[71]. Η ραγδαία εξέλιξη ωστόσο της Κοινωνίας της Πληροφορίας και των Τηλεπικοινωνιών έχει οδηγήσει σε μετεξέλιξη της παραδοσιακής έννοιας της ιδιωτικής ζωής στη νέα διάστασή της που απαντάται στο «δικαίωμα στην πληροφοριακή αυτοδιάθεση». Ταυτόχρονα, το «δικαίωμα του πληροφοριακού αυτοκαθορισμού», η διακήρυξη[72] του οποίου έλαβε χώρα από το Γερμανικό Συνταγματικό Δικαστήριο, συνίσταται στην αναγνώριση στο άτομο της εξουσίας να αποφασίζει μόνο του ως προς την αποκάλυψη και τη χρήση των προσωπικών του δεδομένων. Σύμφωνα με την Λ. Μήτρου, πρόκειται για «το δικαίωμα του πολίτη να αποφασίζει και να συμπροσδιορίζει ποιες πληροφορίες που τον αφορούν θα αποκαλύπτει στους άλλους και να έχει εποπτεία του πληροφοριακού και αξιολογικού ορίζοντα των επικοινωνιακών εταίρων του[73]»

Στην ελληνική έννομη τάξη, το δικαίωμα αυτό αναγνωρίστηκε με το άρθρο 9Α του Συντάγματος, το οποίο ρυθμίστηκε με τον εκτελεστικό αυτού νόμο 2472/1997, ενώ κατόπιν κατακερματισμού της θεωρίας στην σχέση ιδιωτικότητας, προσωπικών δεδομένων και πληροφοριακού αυτοκαθορισμού, κυριάρχησε η άποψη ότι ο πληροφοριακός αυτοκαθορισμός ήταν η συνταγματική προμετωπίδα της προστασίας δεδομένων[74]. Η παραπομπή στο νόμο συνιστά θετική υποχρέωση προστασίας του

---

[69] Ό.π. FRA, Εγχειρίδιο.

[70] Day, G. and Stemler, A. (2020), "Are Dark Patterns Anticompetitive?", Alabama Law Review, Vol. 72/1, διαθέσιμο: https://doi.org/10.2139/ssrn.3468321

[71] BradeisNOW, To be let alone: Brandeis foresaw privacy problems What would the privacy-law champion make of surveillance programs like PRISM?, 2013, διαθέσιμο: https://www.brandeis.edu/now/2013/july/privacy.html

[72] Έχει υποστηριχθεί ότι το έδαφος για την απόφαση αυτήν είχε προετοιμάσει η Mikrozensus Entsheidung (BVerfGE 27, 1 (6)), σύμφωνα με την οποία το Σύνταγμα απαγορεύει την καταχώριση όλων των πτυχών της ανθρώπινης προσωπικότητας σε ένα αρχείο (BVerfGE 27, 1 (6)), καθώς επίσης και οι αποφάσεις BVerfGE 27, 344, BVerfGE 44, 353, BVerfGE 32, 373, με βάση τις οποίες τέθηκαν αυστηρές προϋποθέσεις για την διαβίβαση πληροφοριών που σε μεταγενέστερο στάδιο κατηγοριοποιούνται ως ευαίσθητες, όπως πληροφορίες για το διαζύγιο ή πληροφορίες ιατρικού περιεχομένου. Βλ. Β. Χρήστου, Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων, 2017, σελ. 25-32, υποσ. 60, και Ι. Ιγγλεζάκη, Ευαίσθητα προσωπικά δεδομένα, 2004, σελ. 51.

[73] Λ. Μήτρου, Προστασία του περιβάλλοντος εναντίον της προστασίας πληροφοριών;, [Νόμος και Φύση 3/1996: 9-31].

[74] Lawspot, Δ. Βέρρας, Πληροφοριακός αυτοκαθορισμός και προστασία προσωπικών δεδομένων, διαθέσιμο: https://www.lawspot.gr/nomika-blogs/dimitris_verras/pliroforiakos-aytokathorismos-kai-prostasia-prosopikon-dedomenon#_ftn6

δικαιώματος που βαρύνει το Κράτος, η οποία επιβεβαιώνεται και από τη νομολογία του ΕΔΔΑ[75] επί του άρθρου 8 της ΕΣΔΑ. Αξίζει να επισημανθεί, ότι προ της ρητής συνταγματικής κατοχύρωσης του δικαιώματος προστασίας προσωπικών δεδομένων[76], η προστασία αυτή διασφαλιζόταν από γενικότερες διατάξεις, όπως το άρθρο 9 παρ. 1 Σ., το άρθρο 5 παρ. 1 Σ. , ή μέσω του συνδυασμού των δύο αυτών διατάξεων σε συνάρτηση με την προστασία της ανθρώπινης αξίας (άρ. 1 παρ. 1 του Συντάγματος). Η συσχέτιση πάντως προστασίας προσωπικών δεδομένων και της προστασίας της ιδιωτικής ζωής ήταν δικαιολογημένη[77], καθώς ο ιδιωτικός βίος εμπεριέχει την πληροφοριακή ιδιωτικότητα, χωρίς ωστόσο να εξαντλείται σε αυτή[78].

Σύμφωνα πάντως με τη νομολογία[79], δεδομένα προσωπικού χαρακτήρα θεωρούνται «όχι μόνον εκείνα που αναφέρονται στην ιδιωτική ζωή, αλλά και εκείνα που προορίζονται για εξωτερίκευση στη δημόσια σφαίρα». Ενδιαφέρον ωστόσο παρουσιάζει το γεγονός ότι όταν ένας χρήστης επιλέγει σε μία εφαρμογή να περιορίσει την προβολή του περιεχομένου του σε συγκεκριμένους «ακολούθους», τότε το σχετικό περιεχόμενο αποτελεί μέρος της ιδιωτικής του ζωής και είναι άξιο προστασίας. Σε αντίθετη περίπτωση, σύμφωνα με πάγια νομολογία των ελληνικών δικαστηρίων[80], η χρήση των εν λόγω πληροφοριών δεν προσβάλει το δικαίωμα στην ιδιωτική ζωή ή την πληροφοριακή αυτοδιάθεση, καθώς δεν πρόκειται πλέον για «προσωπικά δεδομένα», αφού το ίδιο το πρόσωπο αναρτά ηθελημένα δημόσια τις πληροφορίες του και αποδέχεται την δημόσια πρόσβαση σε αυτές.

Στην εποχή του σύγχρονου καπιταλισμού, έχει επισημανθεί ότι[81] τα προσωπικά δεδομένα έχουν αναδειχθεί σε ένα νέο «ψευδο-εμπόρευμα», το οποίο δημιουργείται τυχαία από τους χρήστες των πλατφορμών, μέσω της διαδικτυακής τους δραστηριότητας. Η εξάρτηση των ψηφιακών πλατφορμών από τα εν λόγω δεδομένα ως πρώτη ύλη, έχει οδηγήσει σε εκτεταμένες και συγκαλυμένες πρακτικές επιτήρησης. Ειδικότερα, πρακτικές όπως εκείνες των NSA και Cambridge Analytica απέδειξαν ότι η απόλαυση της ιδιωτικότητας απειλείται άμεσα σε αυτά τα πλαίσια. Τέτοιου είδους πρακτικές

---

[75] I. Roagna, Protecting the right to respect for private and family life under the European Convention on Human Rights, Council of Europe human rights handbooks, διαθέσιμο: https://www.echr.coe.int/documents/d/echr/Roagna2012_EN

[76] Φ. Παναγοπούλου, Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 9Α, Ηλεκτρονική Έκδοση, Επιμέλεια Σπ. Βλαχόπουλος, Ξ. Κοντιάδης, Γ. Τασόπουλος, Ιανουάριος 2023.

[77] Για το δικαιωμα στον ιδιωτικο βιο, βλ. Κ. Μαυριά, Το συνταγματικο δικαιωμα του ιδιωτικου βιου, 1982, σελ. 21 επ.

[78] Βλ. Λ. Μήτρου, «Ερμηνεία Άρθρου 9Α Σ», σε Φ. Σπυρόπουλος/Ξ. Κοντιάδης/Χ. Ανθόπουλος/Γ. Γεραπετρίτης, Σύνταγμα, Κατ' άρθρο ερμηνεία, 2017, σελ. 216.

[79] ΣτΕ 1616/2012

[80] ΤριμΕφΑθ 175/2014, ΕιρΘεσσαλ 6981/2018, ΕιρΑθ 5551/2019

[81] Manokha, Ivan. 2018. Surveillance, Panopticism, and Self-Discipline in the Digital Age. Surveillance & Society 16(2): 219-237, διαθέσιμο: https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

παρήγαγαν ένα «πανοπτικό αποτέλεσμα», όπου τα άτομα γνωρίζοντας ότι παρακολουθούνται συνεχώς, άλλαζαν τη συμπεριφορά τους, με αποτέλεσμα τον περιορισμό της αυτοδιάθεσής τους.

Σοβαρές συνέπειες στην ιδιωτικότητα των χρηστών διαφάνηκαν και από την τροποποίηση των πολιτικών απορρήτου της Facebook και την ενοποίηση των πλατφορμών της Google (χάρτες, Gmail, YouTube, μηχανή αναζήτησης), μεταξύ 2009 και 2012[82]. Οι αλλαγές αυτές επέτρεψαν τη μαζική συλλογή και εμπορία προσωπικών δεδομένων από εταιρείες όπως οι Axiom, Equifax και TomTom. Η χρήση αλγορίθμων ανάλυσης δεδομένων που ακολούθησε, οδήγησε σε πρακτικές όπου η πιστοληπτική ικανότητα χιλιάδων πελατών μειωνόταν αιφνιδίως με βάση τις καταναλωτικές τους συνήθειες και όχι την πραγματική τους ικανότητα αποπληρωμής.

4.2.2. ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Όπως αναλύθηκε ανωτέρω, το δικαίωμα στον σεβασμό της ιδιωτικής και της οικογενειακής ζωής συνιστά δικαίωμα έτερο της προστασίας δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, η προστασία των προσωπικών δεδομένων εν στενή εννοία διαφυλάσσεται στο άρθρο 8 του ΧΘΔΕ, καθώς επίσης και στο άρθρο 16 της ΣΛΕΕ. Η πρώτη ωστόσο διεθνής νομικά δεσμευτική συνθήκη που είχε ως σκοπό την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, ήταν η Σύμβαση 108 του Συμβουλίου της Ευρώπης[83]. Η Σύμβαση αυτή παραμένει μέχρι και σήμερα η μόνη νομικά δεσμευτική διεθνής πράξη στον τομέα της προστασίας δεδομένων και αφορά σε κάθε επεξεργασία δεδομένων, είτε αφορά τον δημόσιο ή ιδιωτικό τομέα, είτε ακόμη και τις δικαστικές αρχές και άλλες αρχές επιβολής του νόμου. Το 2001 εκδόθηκε πρόσθετο πρωτόκολλο σε αυτή σχετικά με τις εποπτικές αρχές και την διασυνοριακή ροή δεδομένων σε τρίτες χώρες, οι διατάξεις του οποίου ενσωματώθηκαν στην επικαιροποιημένη σύμβαση 108.

Οι γενικές αρχές προστασίας των προσωπικών δεδομένων που αποτυπώθηκαν για πρώτη φορά στην Σύμβαση αυτή ενσωματώθηκαν αργότερα στην Οδηγία 95/46/ΕΚ «για την προστασία του ατόμου έναντι της επεξεργασίας προσωπικών δεδομένων και την ελεύθερη κυκλοφορία αυτών των δεδομένων». Το ΕΔΔΑ μάλιστα έχει χρησιμοποιήσει ως οδηγό τις αρχές της Σύμβασης 108 σε περιπτώσεις που έχει κληθεί να προσδιορίσει αν υπάρχει ή όχι επέμβαση στο δικαίωμα προστασίας

[82] Sanjay Sharma, Data Privacy and GDPR Handbook, PhD with research associate Pranav Menon, διαθέσιμο: https://cdn.oujdalibrary.com/books/614/614-data-privacy-and-gdpr-handbook-(www.tawcer.com).pdf

[83] Council of Europe, Convention 108 and Protocols, διαθέσιμο: https://www.coe.int/en/web/data-protection/convention108-and-protocol

προσωπικών δεδομένων[84], ενώ έχει αποφανθεί[85] ότι η προστασία των δεδομένων προσωπικού χαρακτήρα είναι μια σημαντική πτυχή του δικαιώματος στον σεβασμό της ιδιωτικής ζωής (άρθρο 8).

Τον Μάιο του 2018 τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), 2016/679, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο Κανονισμός εφαρμόζεται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στην μη αυτοματοποιημένη επεξεργασία των δεδομένων αυτών, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης[86]. Οι βασικές αρχές που διέπουν τον Κανονισμό περιλαμβάνουν την νομιμότητα, τη διαφάνεια, τον περιορισμό του σκοπού, την ελαχιστοποίηση των δεδομένων, την ακρίβεια, την περιορισμένη αποθήκευση και την ασφάλεια της επεξεργασίας[87]. Παράλληλα, ο ΓΚΠΔ κατοχυρώνει σημαντικά δικαιώματα για τα υποκείμενα των δεδομένων, όπως το δικαίωμα πρόσβασης, διόρθωσης, διαγραφής, περιορισμού και εναντίωσης στην επεξεργασία, καθώς και το δικαίωμα στη φορητότητα των δεδομένων[88]. Μάλιστα, ο Κανονισμός επιβάλλει αυστηρές υποχρεώσεις ασφάλειας και κοινοποίησης παραβιάσεων, ενώ προβλέπει υψηλά διοικητικά πρόστιμα για παραβάσεις.

Αξίζει επίσης να αναφερθεί και η Οδηγία 2002/58/ΕΚ (e-Privacy Directive) για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η εν λόγω Οδηγία επρόκειτο να αντικατασταθεί από τον Κανονισμό για την Ιδιωτικότητα στις Ηλεκτρονικές Επικοινωνίες (ePrivacy Regulation), η Πρόταση του οποίου αποσύρθηκε από την Ευρωπαϊκή Επιτροπή τον Φεβρουάριο του 2025[89] εξαιτίας της αδυναμίας επίτευξης συμφωνίας στις διαπραγματεύσεις μεταξύ των θεσμικών οργάνων της ΕΕ και την παρωχημένη φύση της πρότασης λόγω των τεχνολογικών εξελίξεων.

---

[84] Ό.π. FRA, Εγχειρίδιο.

[85] Βλ. ΕΔΔΑ, Z κατά Φινλανδίας, προσφυγή αριθ. 22009/93, 25 Φεβρουαρίου 1997, διαθέσιμο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58033%22]}

[86] Ό.π. ΓΚΠΔ, άρθρο 2.

[87] Ό.π. ΓΚΠΔ, άρθρο 5.

[88] Ό.π. ΓΚΠΔ, άρθρα 15-22.

[89] EDRi, The ePrivacy Regulation proposal has been withdrawn, but the fight for your privacy is far from over, διαθέσιμο: https://edri.org/our-work/the-eprivacy-regulation-proposal-has-been-withdrawn-but-the-fight-for-your-privacy-is-far-from-over/

4.2.3. ΕΛΕΥΘΕΡΙΑ ΤΗΣ ΕΚΦΡΑΣΗΣ

Το δικαίωμα της ελευθερίας της έκφρασης προβλέπεται στο άρθρο 1 παρ. 1 του ΧΘΔΕ της Ευρωπαϊκής Ένωσης: «Κάθε πρόσωπο έχει δικαίωμα στην ελευθερία έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων». Η νομική κατοχύρωση του δικαιώματος αυτού διασφαλίζεται και στο άρθρο 10 της ΕΣΔΑ, ενώ στις παραγράφους 1 και 2 του άρθρου 19 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα του ΟΗΕ ορίζεται ότι: «Κανείς δεν πρέπει να υπόκειται σε διακριτική μεταχείριση και να παρενοχλείται για τις απόψεις του», «κάθε πρόσωπο έχει δικαίωμα στην ελευθερία της έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία της αναζήτησης, της λήψης και της μετάδοσης πληροφοριών και απόψεων κάθε είδους, ανεξαρτήτως συνόρων, προφορικά, γραπτά, σε έντυπα, σε κάθε μορφή τέχνης ή με κάθε άλλο μέσο της επιλογής του». Στο ελληνικό Σύνταγμα, η ελευθερία έκφρασης του ατόμου κατοχυρώνεται στο άρθρο 14 παρ. 1, σύμφωνα με το οποίο «Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του τηρώντας τους νόμους του Κράτους».

Νομολογιακά, απόφαση ορόσημο του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) για την ερμηνεία του άρθρου 10 της ΕΣΔΑ αποτέλεσε η εκδοθείσα επί της υπόθεσης Handyside v. United Kingdom (1976) απόφαση[90]. Συγκεκριμένα, το ΕΔΔΑ αναγνώρισε την ελευθερία της έκφρασης ως θεμέλιο λίθο της δημοκρατικής κοινωνίας, η οποία εκτείνεται ακόμη και σε πληροφορίες που σοκάρουν ή για κάποιους είναι προσβλητικές. Παράλληλα, ωστόσο, δέχθηκε ότι η ελευθερία της έκφρασης δεν είναι απόλυτο δικαίωμα και ότι μπορεί να υπόκειται σε περιορισμούς προβλεπόμενους από το νόμο, οι οποίοι επιδιώκουν θεμιτό σκοπό και είναι αναγκαίοι σε μία δημοκρατική κοινωνία. Στην υπόθεση αυτή, κρίθηκε αποδεκτός ο περιορισμός της κυκλοφορίας ενός σχολικού εγχειριδίου που περιείχε σεξουαλικό περιεχόμενο, με σκοπό την προστασία της ανηλικότητας.

Μεταγενέστερα, τόσο στην υπόθεση SABAM[91] όσο και στην υπόθεση Πολωνία κατά Κοινοβουλίου και Συμβουλίου[92], το ΔΕΕ επεσήμανε ότι η απαίτηση από τους παρόχους να εφαρμόσουν ένα σύστημα προληπτικού φιλτραρίσματος ενδέχετο να περιορίσει την ελευθερία πληροφόρησης των χρηστών, καθώς η χρησιμοποιούμενη τεχνολογία πιθανολογήθηκε ότι δεν μπορούσε να διακρίνει επαρκώς το νόμιμο περιεχόμενο από το παράνομο και εκ του αποτελέσματος θα οδηγούσεσε αποκλεισμό

[90] Case of Handyside v. The United Kingdom, Application no. 5493/72, διαθέσιμο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]}

[91] Ό.π. SABAM.

[92] Judgment of the Court (Grand Chamber) of 26 April 2022, Republic of Poland v European Parliament and Council of the European Union, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0401

νόμιμων επικοινωνιών. Αντίστοιχα, στην απόφαση Telekabel[93], το ΔΕΕ επεσήμανε ότι, προκειμένου να μη στερηθούν αδικαιολόγητα οι χρήστες του διαδικτύου τη δυνατότητα νόμιμης πρόσβασης σε διαθέσιμες πληροφορίες, κάθε μέτρο αποκλεισμού περιεχομένου θα πρέπει να είναι αυστηρά στοχευμένο.

Ο Γενικός Εισαγγελέας Szpunar, στην υπόθεση Glawischnig[94], εξέφρασε την άποψη ότι η επιβολή υποχρέωσης φιλτραρίσματος για προκαθορισμένο και συγκεκριμένο περιεχόμενο δεν θα έπληττε την ελευθερία έκφρασης των χρηστών του διαδικτύου, εφόσον δεν απαιτούνταν η ενεργός συμμετοχή του ενδιάμεσου παρόχου στη νομική αξιολόγηση του περιεχομένου. Ενδιαφέρον παρουσιάζει το γεγονός ότι το ΔΕΕ δεν έκανε καμία αναφορά στον κίνδυνο υπερβολικού αποκλεισμού (over-blocking) λόγω απουσίας υψηλής ακρίβειας των τεχνολογιών φιλτραρίσματος, όπως είχε συμβεί στην υπόθεση SABAM[95]. Αντίστοιχα, η απόφαση στην υπόθεση YouTube/Cyando υπογραμμίζει τη σημασία της ουδετερότητας του παρόχου στη διαδικασία λήψης αποφάσεων[96], και συνεπώς απαιτεί οποιαδήποτε γνωστοποίηση παραβίασης να περιλαμβάνει «επαρκείς πληροφορίες, ώστε ο ενδιάμεσος να μπορεί να πείθεται, χωρίς να απαιτείται λεπτομερής νομική εξέταση, ότι το περιεχόμενο είναι παράνομο και ότι η αφαίρεσή του είναι συμβατή με την ελευθερία έκφρασης».

Η ερμηνεία αυτή επιβεβαιώνεται περαιτέρω από το ΔΕΕ στην υπόθεση Πολωνία κατά Κοινοβουλίου και Συμβουλίου[97], όπου το Δικαστήριο αναγνώρισε ότι η χρήση εργαλείων αυτόματης αναγνώρισης και φιλτραρίσματος, όπως η τεχνολογία ψηφιακών αποτυπωμάτων, αποτελεί το μόνο διαθέσιμο μέσο συμμόρφωσης με την υποχρέωση παρακολούθησης για την πρόληψη εκ των προτέρων εντοπισμένων παραβιάσεων, όταν πρόκειται για ενδιάμεσους παρόχους που φιλοξενούν μεγάλο όγκο καθημερινά αναρτώμενου περιεχομένου[98]. Ωστόσο, το Δικαστήριο επιβεβαίωσε ότι αυτή η μέθοδος παρακολούθησης και φιλτραρίσματος συνιστά, εξ ορισμού, περιορισμό ενός σημαντικού μέσου

---

[93] JUDGMENT OF THE COURT (Fourth Chamber) 27 March 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf?docid=149924&doclang=EN

[94] Judgment of the Court (Third Chamber) of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-18/18

[95] Toygar Hasan Oruç, The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it?, 2022, διαθέσιμο: https://www.jipitec.eu/jipitec/article/view/354/347

[96] Peterson/Elsevier v Youtube/Cyando, Joined Cases C-682/18 and C-683/18, παράγραφος 116, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf?docid=243241&doclang=en

[97] Ό.π. Republic of Poland v European Parliament and Council of the European Union, παράγραφος 54.

[98] Ό.π. παράγραφος 54.

διάδοσης διαδικτυακού περιεχομένου και, συνεπώς, συνιστά περιορισμό της ελευθερίας έκφρασης και πληροφόρησης των χρηστών των εν λόγω παρόχων[99].

Στην υπόθεση Delfi κατά Εσθονίας, το ΕΔΔΑ έκρινε ότι η επιβολή υποχρέωσης παρακολούθησης σε έναν διαδικτυακό ενδιάμεσο πάροχο για φιλτράρισμα συγκεκριμένου παράνομου περιεχομένου, δηλαδή ρητορικής μίσους και υποκίνησης σε βία, δεν θα παραβίαζε την ελευθερία έκφρασης και πληροφόρησης, εφόσον το στοχευμένο παράνομο περιεχόμενο είναι σαφώς αναγνωρίσιμο σε τέτοιο βαθμό ώστε «η διαπίστωση της παράνομης φύσης του δεν απαιτούσε καμία γλωσσική ή νομική ανάλυση, καθώς οι παρατηρήσεις ήταν εκ πρώτης όψεως προδήλως παράνομες».

4.2.4. ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΕΛΕΥΘΕΡΙΑ

Το δικαίωμα στην επιχειρηματική ελευθερία κατοχυρώνεται στο άρθρο 16 του ΧΘΔΕ[100]. Έχει υποστηριχθεί ότι μαζί με τα υπόλοιπα θεμελιώδη δικαιώματα που κατοχυρώνονται στον ΧΘΔΕ, το άρθρο αυτό μπορεί να λειτουργήσει ως περιορισμός και των Κρατών Μελών, όχι δηλαδή μόνο των αρμοδιοτήτων της ΕΕ[101]. Παράλληλα, θεωρείται ότι το δικαίωμα στην επιχειρηματική ελευθερία φέρει οριζόντια άμεση ισχύ[102] καθώς συνιστά γενική αρχή του ενωσιακού δικαίου. Το εννοιολογικό περιεχόμενο της ελευθερίας του επιχειρείν δεν ορίζεται ρητά στο ανωτέρω άρθρο. Αντιθέτως, καταλείπεται χώρος ερμηνείας του καθώς το δικαίωμα αναγνωρίζεται «σύμφωνα με το δίκαιο της Ένωσης και τις εθνικές νομοθεσίες και πρακτικές». Δεν είναι ωστόσο απόλυτο δικαίωμα και μπορεί να υπόκειται σε περιορισμούς, σύμφωνα πάντοτε με το άρθρο 52 παρ. 1 του ΧΘΔΕ.

Νομολογιακά, σε αποφάσεις του το ΔΕΕ έχει επισημάνει ότι η ελευθερία του επιχειρείν μπορεί να τύχει περιορισμών, οι οποίοι προβλέπονται από το νόμο, εξυπηρετούν θεμιτούς σκοπούς και τηρούν την αρχή της αναλογικότητας. Στην απόφαση Sky Österreich[103], το ΔΕΕ έχει τονίσει ότι η ελευθερία

---

[99] Ό.π. παράγραφος 55.

[100] Ό.π. FRA, Εγχειρίδιο.

[101] Βλ. Marco Gestri, Regolamentazione del mercato e libertà d'iniziativa privata: L'incidenza del diritto comunitario sulla costituzione económica, in ISTITUZIONI E DINAMICHE DEL DIRITTO: MERCATO, AMMINISTRAZIONE, DIRITTI 141–76 (A. Vignudelli ed., 2006).

[102] Andrea Usai, The Freedom to Conduct a Business in the EU, Its Limitations and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration

, Cambridge University Press, διαθέσιμο: https://www.cambridge.org/core/journals/german-law-journal/article/freedom-to-conduct-a-business-in-the-eu-its-limitations-and-its-role-in-the-european-legal-order-a-new-engine-for-deeper-and-stronger-economic-social-and-political-integration/CBB67ACD4D5D633A5D5D19B460538921

[103] Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 22ας Ιανουαρίου 2013 Sky Österreich GmbH κατά Österreichischer Rundfunk, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-283/11&language=EL

του επιχειρείν μπορεί να περιοριστεί για λόγους πολυφωνίας της πληροφόρησης, ενώ στην απόφαση της 6ης Νοεμβρίου 2018 για τις υποθέσεις Bauer και Broßonn[104], το ΔΕΕ έκρινε ότι περιορισμοί στην ελευθερία του επιχειρείν μπορούν να επιβληθούν για την προστασία των εργαζομένων, υπό την προϋπόθεση ότι οι περιορισμοί αυτοί προβλέπονται από το νόμο, εξυπηρετούν θεμιτό σκοπό δημοσίου συμφέροντος, είναι αναγκαίοι και αναλογικοί. Αξίζει να σημειωθεί ότι στις υποθέσεις Scarlet Extended[105] και Netlog[106], το ΔΕΕ έκρινε ότι η επιβολή υποχρέωσης στους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας να εγκαθιστούν και να συντηρούν δαπανηρά πληροφοριακά συστήματα για την παρακολούθηση όλων των ηλεκτρονικών επικοινωνιών στο δίκτυό τους παραβιάζει την ελευθερία άσκησης επιχειρηματικής δραστηριότητας.

[104] Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 6ης Νοεμβρίου 2018, Stadt Wuppertal κατά Maria Elisabeth Bauer και Volker Willmeroth κατά Martina Broßonn, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62016CJ0569

[105] Judgment of the Court (Third Chamber) of 24 November 2011,

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10

[106] Ό.π. ΔΕΕ, SABAM v. Netlog NV, Case C-360/10.

5. ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΠΡΟΤΑΣΗΣ ΚΑΙ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

Δεδομένων των προβλεπόμενων στην Πρόταση παρεμβάσεων σε θεμελιώδη δικαιώματα των χρηστών και της εγνωσμένης σημασίας των εν λόγω ρυθμίσεων για την προστασία των δικαιωμάτων των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η Επιτροπή αποφάσισε στις 12 Μαΐου 2022 να διαβουλευτεί με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («ΕΣΠΔ») και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων («ΕΕΠΔ»)[107]. Η κοινή Γνωμοδότηση των ΕΣΠΔ και ΕΕΠΔ[108] εστίασε μεταξύ άλλων σε πτυχές ρυθμίσεων της Πρότασης η εφαρμογή των οποίων εγείρει ανησυχία αναφορικά με την αναγκαιότητα και την αναλογικότητα των επιβαλλόμενων παρεμβάσεων στην ιδιωτική ζωή, και οι οποίες δεν εγγυώνται επαρκή προστασία των θεμελιωδών δικαιωμάτων και συνεπώς χρήζουν τροποποίησης προκειμένου να εναρμονιστούν με το νομοθετικό πλαίσιο της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

Μολονότι στην κοινή Γνωμοδότηση αποτυπώνεται η αντίληψη ότι η Πρόταση θα μπορούσε να οδηγήσει σε γενικευμένη σάρωση του περιεχομένου όλων των ηλεκτρονικών επικοινωνιών, αναγνωρίζεται ωστόσο ότι τα τρία διαφορετικά είδη εντολών εντοπισμού[109] συνεπάγονται διαφορετικό επίπεδο παρεμβατικότητας και διαφορετικής έντασης αντίκτυπο στα δικαιώματα της ιδιωτικής ζωής και της προστασίας προσωπικών δεδομένων των χρηστών, αφού η εκτέλεσή τους προϋποθέτει τη χρήση διαφορετικής τεχνολογίας. Ως εκ τούτου προκειμένου να αξιολογηθεί αν η παρέμβαση στα θεμελιώδη δικαιώματα βρίσκεται σε συμφωνία με το άρθρο 52 παρ. 1 του ΧΘΔΕ, το ΕΣΠΔ και ο ΕΕΠΔ υπογράμμισαν ότι επιβάλλεται η διενέργεια ελέγχου αναγκαιότητας και αναλογικότητας των προβλεπόμενων μέτρων χωριστά[110]. Επιπλέον, εξέφρασαν άποψη και για την λειτουργία του Κέντρου της ΕΕ, αλλά και κριτική στην Πρόταση στο σύνολό της.

Στις ενότητες που ακολουθούν, επιχειρείται η ανάλυση των χρησιμοποιούμενων τεχνολογιών για την εκτέλεση των μέτρων εντοπισμού υλικού σεξουαλικής κακοποίησης παιδιών με βάση την Πρόταση Κανονισμού, η περιγραφή του ρόλου του Κέντρου της ΕΕ όπως προβλέπεται στα σχετικά άρθρα,

---

[107] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Οκτωβρίου 2018 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ, άρθρο 42 παρ. 2, διαθέσιμο: https://eur-lex.europa.eu/eli/reg/2018/1725/oj

[108] ΕΣΠΔ-ΕΕΠΔ, Κοινή γνωμοδότηση 4/2022 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, διαθέσιμο: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_el

[109] Ό.π. άρθρο 7 παρ. 5-7.

[110] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 24.

καθώς επίσης και η ανάδειξη των επιπτώσεων στα θεμελιώδη δικαιώματα όλων των επηρεαζόμενων μερών από τις ανωτέρω διαδικασίες.

5.1. ΤΕΧΝΟΛΟΓΙΕΣ ΕΝΤΟΠΙΣΜΟΥ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ ΠΑΙΔΙΩΝ ΚΑΙ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

5.1.1. ΜΕΤΡΑ ΕΝΤΟΠΙΣΜΟΥ ΓΝΩΣΤΟΥ ΥΛΙΚΟΥ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ ΠΑΙΔΙΩΝ

Οι χρησιμοποιούμενες για τον εντοπισμό γνωστού υλικού σεξουαλικής κακοποίησης παιδιών τεχνολογίες είναι συνήθως τεχνολογίες αντιστοίχισης οι οποίες βασίζονται σε ήδη υπάρχουσα βάση δεδομένων γνωστού υλικού σεξουαλικής κακοποίησης παιδιών, μέσω της οποίας μπορεί να γίνει σύγκριση και αντιστοίχιση ψηφιακών εικόνων, αφότου έχει προηγηθεί η μετατροπή τους σε τιμές κατακερματισμού. Όπως αναφέρεται στην Έκθεση Εκτίμησης Επιπτώσεων που συνοδεύει την Πρόταση Κανονισμού, η τεχνολογία κατακερματισμού έχει εκτιμώμενο ποσοστό ψευδώς θετικών αποτελεσμάτων 0,000000002 %[111].

Ειδικότερα, "hashing", σύμφωνα με την Έκθεση Εκτίμησης Επιπτώσεων[112], συνιστά έναν μοναδικό ψηφιακό κωδικό που παράγεται από έναν μαθηματικό αλγόριθμο και αποτελεί την μοναδική ψηφιακή υπογραφή ενός αρχείου. Παράλληλα όμως, ο όρος "hashing"[113] αποτελεί έναν γενικό όρο – ομπρέλα για τις τεχνικές δημιουργίας δακτυλικών αποτυπωμάτων (fingerprints) αρχείων σε ένα υπολογιστικό σύστημα. Ένας αλγόριθμος, γνωστός ως συνάρτηση κατακερματισμού (hash function), χρησιμοποιείται για να υπολογίσει ένα δακτυλικό αποτύπωμα, το οποίο είναι γνωστό ως hash, από ένα αρχείο. Η σύγκριση ενός τέτοιου αποτυπώματος (hash) με ένα ψηφιακό αποτύπωμα που είναι αποθηκευμένο σε μια βάση δεδομένων ονομάζεται «αντιστοίχιση αποτυπωμάτων» (hash matching).
Στο πεδίο αυτό υπάρχουν δύο δημοφιλείς συναρτήσεις κατακερματισμού: η κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function) και η αντιληπτική συνάρτηση

---

[111] Ευρωπαϊκή Επιτροπή, Έγγραφο εργασίας των υπηρεσιών της Επιτροπής, Έκθεση εκτίμησης επιπτώσεων που συνοδεύει την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, (2022), σ. 281, υποσημείωση 511, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209

[112] Ό.π. σελ. 39 και 96.

[113] Ofcom, Overview of Perceptual Hashing Technology, (2022), σ. 3, διαθέσιμο σε: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/perceptual-hashing-technology.pdf?v=328806

κατακερματισμού (perceptual hash function)[114]. Η κρυπτογραφική συνάρτηση κατακερματισμού χαρακτηρίζεται από την λειτουργία του «φαινομένου της χιονοστιβάδας» ("avalanche effect"). Η εν λόγω λειτουργία συνεπάγεται ότι η παραμικρή αλλαγή σε ένα δεδομένο αρχείο (παραδείγματος χάριν ενός pixel σε μία εικόνα) έχει ως αποτέλεσμα την παραγωγή εντελώς διαφορετικού hash. Ως εκ τούτου, προκύπτει αδυναμία επίτευξης ταύτισης μεταξύ όμοιων αντιληπτικά από τον άνθρωπο εικόνων, λόγω της απουσίας ευαισθησίας του αλγορίθμου σε μικρές μετατροπές των εικόνων. Συνεπώς, αν δύο κρυπτογραφικά hashes διαφέρουν έστω και ελάχιστα, υποθέτουμε ότι υπολογίστηκαν από δύο διαφορετικά αρχεία εισόδου, ενώ, αν δύο κρυπτογραφικά hashes είναι ίδια, υποθέτουμε ότι υπολογίστηκαν από το ίδιο αρχείο εισόδου.

Με βάση τα παραπάνω, οδηγούμαστε στο συμπέρασμα ότι εύκολα μπορεί κανείς να παρακάμψει τέτοιες τεχνικές ανίχνευσης τροποποιώντας ελάχιστα μία εικόνα[115]. Μία ακόμη ιδιότητα των κρυπτογραφικών συναρτήσεων κατακερματισμού είναι η αδυναμία αναστροφής της hash τιμής. Καθίσταται, δηλαδή, αδύνατον να ανακτηθεί το αρχικό αρχείο από την hash τιμή που του έχει απονεμηθεί. Αναφορικά με τους περιορισμούς αυτής της τεχνολογίας, υπάρχει η πιθανότητα επέλευσης «σύγκρουσης κατακερματισμού» ("hash collision"), η οποία διαγιγνώσκεται όταν δύο διαφορετικά αρχεία φέρουν το ίδιο hash. Ενδέχεται δηλαδή, δύο εικόνες εκ των οποίων η μία αποτυπώνει παράνομη δραστηριότητα, ενώ η άλλη αποτυπώνει περιεχόμενο αδιάφορο ποινικά, να φέρουν την ίδια hash τιμή[116].

Στον αντίποδα των κρυπτογραφικών συναρτήσεων κατακερματισμού βρίσκονται οι αντιληπτικές συναρτήσεις κατακερματισμού, στόχος των οποίων είναι η παραγωγή παρόμοιων hashes για εικόνες αντιληπτικά παρόμοιες από τον άνθρωπο[117]. Εν προκειμένω, αν μία εικόνα προκύπτει από μία άλλη μέσω τροποποίησης, τα hashes που θα προκύπτουν για αυτές θα είναι παρόμοια, κάτι που θα υποδεικνύει την συνάφεια των συγκεκριμένων εικόνων. Τέτοιου είδους τροποποιήσεις μπορεί να είναι η μετατροπή από μία μορφή αρχείου σε άλλη, μικρή μείωση του μεγέθους του αρχείου ή της ποιότητάς

---

[114] Ό.π. σ.3.

[115]ActiveFence, Detecting Novel CSAM – Why Image Hash Matching Isn't Enough Anymore, διαθέσιμο σε: https://www.activefence.com/blog/detecting-csam-hash-matching/

[116] Zulfany Erlisa Rasjid et al., A review of collisions in cryptographic hash function used in digital forensic tools (2017), διαθέσιμο σε: https://www.sciencedirect.com/science/article/pii/S1877050917321221

[117] Martin Steinebach et al., Image Hashing Robust Against Cropping and Rotation, διαθέσιμο σε: https://www.researchgate.net/publication/370500036_Image_Hashing_Robust_Against_Cropping_and_Rotation

του, προσθήκη ή αφαίρεση υδατογραφημάτων ή αλλαγή εικονοστοιχείων ή περιοχών εικονοστοιχείων (pixel-regions) μιας εικόνας[118].

Το ποσοστό ομοιότητας μεταξύ δύο hashes διαπιστώνεται με την χρήση ενός τρόπου μέτρησης της απόστασης μεταξύ δύο σημείων. Λόγου χάριν, με χρήση της Ευκλείδειας Απόστασης[119]. Όσο μικρότερη είναι η ευκλείδεια απόσταση, τόσο πιο παρόμοιες είναι οι εικόνες. Ομοίως, με χρήση της απόστασης Hamming (Hamming Distance) μπορεί να υπολογιστεί η εγγύτητα δύο hashes, μέσω μέτρησης των bits που είναι διαφορετικά μεταξύ τους. Αξίζει να σημειωθεί ότι βάσει προηγούμενων ερευνών η χρήση αντιληπτικών συναρτήσεων κατακερματισμού και η ανάλυση μεταδεδομένων συνιστούν τους πιο αποτελεσματικούς τρόπους ανίχνευσης υλικού παιδικής σεξουαλικής κακοποίησης στο διαδίκτυο[120]. Είναι σημαντικό να σημειώσουμε ότι το αποδεκτό όριο ομοιότητας που τίθεται μπορεί να διαφέρει ανάλογα με το πλαίσιο. Για παράδειγμα, οι αντιληπτικές συναρτήσεις κατακερματισμού ενδέχεται να προσαρμόζονται από την εκάστοτε πλατφόρμα ώστε να αντανακλούν το επίπεδο ομοιότητας που θεωρείται αποδεκτό αναλόγως την δεδομένη περίπτωση χρήσης[121].

Ωστόσο, και οι αντιληπτικές συναρτήσεις κατακερματισμού υπόκεινται σε ορισμένους εγγενείς περιορισμούς. Ένας τέτοιος περιορισμός είναι η περίπτωση «σύγκρουσης κατακερματισμού» όπου δύο διαφορετικά αρχεία παράγουν το ίδιο hash. Αυτό μπορεί να συμβεί στην περίπτωση που οι λειτουργίες κατακερματισμού θεωρήσουν εσφαλμένα δύο ανόμοια δεδομένα παρόμοια, βάσει συγκεκριμένων χαρακτηριστικών: λ.χ. εξαιτίας ομοιότητας περιοχών pixels. Αξίζει να σημειωθεί ότι ο περιορισμός αυτός ενδέχεται να εγείρει ζητήματα ασφάλειας δεδομένων σε περίπτωση που παράγονται παραπλανητικά αποτελέσματα[122].

Ένας ακόμη περιορισμός αφορά στη δυνατότητα αναστροφής της αντιληπτικής hash τιμής. Σημειώνεται πάντως ότι δεν υπάρχει η δυνατότητα πλήρους ανάκτησης του αρχικού αρχείου εισόδου. Μπορεί ωστόσο να εξευρεθεί μία σειρά από υποψήφια αρχεία, κάτι που εξαρτάται από τη λειτουργία

---

[118] Hany Farid, An Overview of Perceptual Hashing, Journal of Online Trust and Safety, Vol. 1 No. 1 (2021), διαθέσιμο: https://tsjournal.org/index.php/jots/article/view/24

[119] Ό.π. Ofcom, σ. 8.

[120] Guerra, E., & Westlake, B. G. (2021). Detecting child sexual abuse images: traits of child sexual exploitation hosting and displaying websites. Child Abuse & Neglect, 122, 105336, διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S0145213421004051

[121] Ό.π. Ofcom, σ. 9.

[122] Leblanc-Albarel D. & Preneel B., Black-box Collision Attacks on Widely Deployed Perceptual Hash Functions, διαθέσιμο: https://eprint.iacr.org/2024/1869.pdf

του κατακερματισμού και τον αριθμό των υποψήφιων αρχείων που επιθυμεί κανείς να ανεύρει[123]. Υπάρχει, συνεπώς, ένας μη αμελητέος κίνδυνος διαρροής της ιδιωτικότητας και της εμπιστευτικότητας του αρχείου εισόδου, εφόσον ενδέχεται να καταστεί δυνατόν να διακριθούν περιεχόμενα σε κάποιο βαθμό μόνον του αρχικού αρχείου, όχι όμως και το αρχικό αρχείο στο σύνολό του.

Στις ευρέως χρησιμοποιούμενες συναρτήσεις κατακερματισμού για σκοπούς εντοπισμού υλικού παιδικής σεξουαλικής κακοποίησης, ανήκουν ο MD5 - Message Digest Algorithm 5[124], ο SHA-1 - Secure Hash Algorithm 1[125] και SHA-256 - Secure Hash Algorithm 256[126]. Στις δημοφιλείς αντιληπτικές συναρτήσεις κατακερματισμού για τον ίδιο σκοπό εντοπίζονται το PhotoDNA της Microsoft και του Dartmouth College[127], το CSAI Match της YouTube για εντοπισμό βίντεο[128] που απεικονίζουν παιδική σεξουαλική κακοποίηση, το NeuralHash της Apple[129], το PDQ της Meta[130], το TMK+PDQF[131] που αποτελεί συνδυασμός του PDQ και τεχνικής TMK της Meta και το Videntifier της Videntifier Technologies[132].

Σύμφωνα με την Έκθεση Εκτίμησης Επιπτώσεων, το εργαλείο PhotoDNA της Microsoft είναι η πιο ευρέως χρησιμοποιούμενη τεχνολογία στο πεδίο ανίχνευσης υλικού παιδικής σεξουαλικής κακοποίησης. Το PhotoDNA[133] δημιουργεί ένα μοναδικό ψηφιακό αποτύπωμα μίας εικόνας ή βίντεο

---

[123] Medium, Black-Box Attacks on Perceptual Image Hashes with GANs, διαθέσιμο: https://medium.com/data-science/black-box-attacks-on-perceptual-image-hashes-with-gans-cc1be11f277

[124] Farhad Ahmed Sagar, Cryptographic Hashing Functions - MD5, διαθέσιμο: https://cs.indstate.edu/~fsagar/doc/paper.pdf

[125] Morales F. et. al., PHVSpec: A Benchmark-based Analysis of Perceptual Hash Systems for Videos, διαθέσιμο: https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/Tech-Coalition-Video-Hash-Benchmark-Paper.pdf

[126] Cometchat, Understanding Hash Matching Technology: A Guide for Trust & Safety Professionals, διαθέσιμο: https://www.cometchat.com/blog/what-is-hash-matching

[127] Microsoft, PhotoDNA, How does PhotoDNA technology work?, διαθέσιμο: https://www.microsoft.com/en-us/photodna

[128] Youtube CSAI Match, Protect your content and online community from child exploitation videos, διαθέσιμο: https://www.youtube.com/csai-match/

[129] CSAM Detection Technical Summary, διαθέσιμο: https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

[130] Facebook, Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer, διαθέσιμο: https://about.fb.com/news/2019/08/open-source-photo-video-matching/

[131] Ό.π. Facebook.

[132] Videntifier, Hash Matching Will Save Content Moderation, Faster Than AI Currently Can On Its Own, διαθέσιμο: https://www.videntifier.com/post/ai-and-hash-matching

[133] NYTimes, Child Abusers Run Rampant as Tech Companies Look the Other Way, διαθέσιμο: https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html

και το συγκρίνει με μία βάση δεδομένων που περιέχει hash τιμές υλικού που αποτελεί επαληθευμένα υλικό παιδικής σεξουαλικής κακοποίησης. Σε περίπτωση που δεν υπάρξει αντιστοίχιση hashes από την εν λόγω διαδικασία, δεν διατηρείται στη βάση καμία σχετική πληροφορία. Το PhotoDNA χρησιμοποιείται για πάνω από 10 χρόνια από οργανισμούς παγκοσμίως, περιλαμβανομένων παρόχων υπηρεσιών, μη κυβερνητικών οργανώσεων (ΜΚΟ) και αρχών επιβολής του νόμου στην ΕΕ.

Το ποσοστό των ψευδώς θετικών αποτελεσμάτων του (false positives) εκτιμάται ότι δεν υπερβαίνει το 1 στα 50 δισεκατομμύρια, σύμφωνα με τις δοκιμές[134], ωστόσο ορισμένοι ειδικοί στο πεδίο έχουν αμφισβητήσει το ποσοστό αυτό[135]. Ταυτόχρονα, όμως, έχει επισημανθεί ότι η ενδεχόμενη μεταφορά εργαλείων αντιληπτικού κατακερματισμού σε συσκευές χρηστών συνεπάγεται κίνδυνο τα εργαλεία αυτά να υποστούν αντίστροφη μηχανική (reverse engineering). Η τεχνική αυτή ενέχει κίνδυνο αποκωδικοποίησης των εργαλείων με σκοπό την εξαγωγή ευαίσθητων πληροφοριών, που σε ορισμένες περιπτώσεις φτάνουν μέχρι και την αναγνώριση προσώπων σε μία εικόνα[136].

Δοθείσης της χρόνιας εφαρμογής αυτών των τεχνολογιών εντοπισμού και της αποδεδειγμένης αποτελεσματικότητάς τους στην αναχαίτιση της συνεχιζόμενης κακοποίησης παιδιών, τα μέτρα αυτά όχι μόνο φαίνονται αναγκαία αλλά υποστηρίζεται ότι απαιτείται και η υιοθέτηση συνδυαστικών λύσεων για την αντιμετώπιση του ειδεχθούς φαινομένου. Και τούτο διότι τα άτομα που κατέχουν υλικό παιδικής σεξουαλικής κακοποίησης ενδέχεται να δραστηριοποιούνται και στη διανομή τέτοιου υλικού. Αντίστοιχα, δράστες που παράγουν ή διανέμουν τέτοιο υλικό, ενδέχεται να εμπλέκονται και σε σεξουαλικές αξιόποινες πράξεις σε βάρος παιδιών[137].

Στο πλαίσιο της Ποιοτικής Εκτίμησης των προτεινόμενων μέτρων πολιτικής της Έκθεσης Εκτίμησης Επιπτώσεων, η Ευρωπαϊκή Επιτροπή προσεγγίζει το ζήτημα των επιπτώσεων των προτεινόμενων διατάξεων στα θεμελιώδη δικαιώματα. Εν προκειμένω, υπογραμμίζεται ότι ο επιδιωκόμενος από την Πρόταση στόχος, δηλαδή η πρόληψη και η καταπολέμηση του ιδιαίτερα σοβαρού αυτού εγκλήματος, συνιστά στόχο γενικού συμφέροντος σύμφωνα με το Άρθρο 52(1) του Χάρτη[138], ενώ παράλληλα

---

[134] Farid H., House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, διαθέσιμο: https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf

[135] Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων της Πρότασης Κανονισμού για τη θέσπιση κανόνων πρόληψης και καταπολέμησης της σεξουαλικής κακοποίησης παιδιών, Υπηρεσία Έρευνας Ευρωπαϊκού Κοινοβουλίου, 2023, διαθέσιμο: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

[136] Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, διαθέσιμο: https://arxiv.org/pdf/2110.07450

[137] Cale, J. et al., (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. Trends and issues in crime and criminal justice, (617), 1-22), διαθέσιμο: https://www.aic.gov.au/publications/tandi/tandi617

[138] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕ), άρθρο 52, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT

επιδιώκει την προστασία των δικαιωμάτων των άλλων, και συγκεκριμένα των παιδιών. Αφορά ιδιαίτερα τα θεμελιώδη δικαιώματα στην ανθρώπινη αξιοπρέπεια[139], στην ακεραιότητα του προσώπου[140] και την απαγόρευση απάνθρωπης ή εξευτελιστικής μεταχείρισης[141], καθώς επίσης και το σύνολο των δικαιωμάτων του παιδιού[142].

Τονίζεται επίσης ότι τα αδικήματα παιδικής σεξουαλικής κακοποίησης που επιδιώκεται να καταπολεμηθούν μέσω της Πρότασης, επηρεάζουν τα δικαιώματα των παιδιών για σεβασμό στην ιδιωτική και οικογενειακή ζωή και στην προστασία των προσωπικών τους δεδομένων. Στο πλαίσιο της καταπολέμησης των εγκλημάτων κατά των ανηλίκων, το ΔΕΕ έχει σημειώσει ότι τουλάχιστον κάποια από τα θεμελιώδη δικαιώματα που αναφέρονται μπορεί να δημιουργήσουν θετικές υποχρεώσεις για τις αρμόδιες δημόσιες αρχές να υιοθετήσουν νομικά μέτρα για την προστασία των εν λόγω δικαιωμάτων[143].

Ταυτόχρονα, στην Ποιοτική Εκτίμηση της Ευρωπαϊκής Επιτροπής αναγνωρίζεται η επίδραση των προβλεπόμενων μέτρων στην άσκηση των θεμελιωδών δικαιωμάτων των χρηστών των υπηρεσιών που βρίσκονται εντός του πεδίου εφαρμογής της Πρότασης. Αυτά τα δικαιώματα περιλαμβάνουν, ιδίως, τα θεμελιώδη δικαιώματα για σεβασμό της ιδιωτικής ζωής[144] (συμπεριλαμβανομένης της εμπιστευτικότητας των επικοινωνιών, ως μέρος του ευρύτερου δικαιώματος σεβασμού της ιδιωτικής και οικογενειακής ζωής), για προστασία των προσωπικών δεδομένων[145] και για ελευθερία έκφρασης και πληροφόρησης[146]. Σημειώνεται, ωστόσο, ότι παρά τη σημασία των ανωτέρω δικαιωμάτων, κανένα από αυτά δεν είναι απόλυτο και πρέπει να εξετάζονται σε σχέση με τη λειτουργία τους στην κοινωνία και πάντοτε υπό τους όρους της διάταξης του άρθρου 52(1) του Χάρτη[147]. Το ίδιο ισχύει και για το δικαίωμα της ελευθερίας του επιχειρείν.

Ειδικότερα, τα μέτρα που στοχεύουν στην επίτευξη του προαναφερθέντος στόχου, συνεπάγονται διάφορους βαθμούς παρεμβατικότητας στα θεμελιώδη δικαιώματα των χρηστών. Στην περίπτωση

---

[139] Ό.π. Χάρτης, άρθρο 1.

[140] Ό.π. Χάρτης, άρθρο 3.

[141] Ό.π. Χάρτης, άρθρο 4.

[142] Ό.π. Χάρτης, άρθρο 24.

[143] Βλ. ΔΕΕ, La Quadrature du Net, Joined Cases C-511/18, C-512/18 and C-520/18, παρ. 126., διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL

[144] Ό.π. Χάρτης, άρθρο 7.

[145] Ό.π. Χάρτης, άρθρο 8.

[146] Ό.π. Χάρτης, άρθρο 11.

[147] Βλ. ΔΕΕ, Joined Cases C-511/18, C-512/18 and C-520/18, παράγραφος 120, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL

περιεχομένου που είναι προσβάσιμο στο κοινό, σημειώνεται ότι η επίδραση στο δικαίωμα στην ιδιωτικότητα, είναι γενικά μικρότερη δεδομένου του ρόλου αυτών των υπηρεσιών ως «εικονικών δημόσιων χώρων» για σκοπούς έκφρασης και οικονομικών συναλλαγών[148]. Ωστόσο, η επίδραση στο δικαίωμα στην ιδιωτικότητα σε σχέση με τις ιδιωτικές επικοινωνίες εκτιμάται ότι θα είναι μεγαλύτερη. Υπογραμμίζεται όμως ότι θα πρέπει να είναι αναγκαία και αναλογική του επιδιωκόμενου στόχου και να μετριάζεται με τα κατάλληλα προστατευτικά μέτρα.

Στην Έκθεση τονίζεται επίσης ότι η λανθασμένη αφαίρεση-στη βάση ψευδώς θετικών αναφορών-περιεχομένου χρηστών, μπορεί να επιφέρει σημαντική επίδραση στην ελευθερία της έκφρασης και της πληροφόρησης[149]. Ταυτόχρονα όμως, υλικό σεξουαλικής κακοποίησης παιδιών που δεν αφαιρείται, θα έχει σημαντική αρνητική επίδραση στα θεμελιώδη δικαιώματα των παιδιών. Ως εκ τούτου, εκτιμάται ότι η υποχρέωση ανίχνευσης γνωστού υλικού παιδικής σεξουαλικής κακοποίησης, θα είχε σημαντικά θετική επίδραση στα θεμελιώδη δικαιώματα των θυμάτων, ιδίως στο δικαίωμά τους για σεβασμό της ιδιωτικής ζωής και των δικαιωμάτων τους ως παιδιά γενικότερα.

Περαιτέρω, τονίζεται ότι ενώ τα δικαιώματα στην ελευθερία έκφρασης και πληροφόρησης δεν εκτείνονται στην προστασία παράνομων δραστηριοτήτων που αποσκοπούν στην καταστρατήγηση οποιωνδήποτε από τα βασικά θεμελιώδη δικαιώματα και ελευθερίες, η ανίχνευση εκ των πραγμάτων θα εκτείνεται και στον έλεγχο νόμιμου υλικού και περιεχομένου επικοινωνιών για την διαπίστωση ύπαρξης υλικού παιδικής σεξουαλικής κακοποίησης. Ως εκ τούτου, απαιτείται ισχυρή τεκμηρίωση και αιτιολόγηση προκειμένου να διασφαλιστεί η κατάλληλη ισορροπία των διαφορετικών θεμελιωδών δικαιωμάτων. Η αιτιολόγηση συνίσταται ουσιαστικά με βάση την σχετική Έκθεση στα ιδιαίτερα σοβαρά εγκλήματα που στοχεύεται να καταπολεμηθούν και να αποτραπούν με τα προτεινόμενα μέτρα και στην προστασία των παιδιών που αποσκοπούν να εξασφαλίσουν.

Ταυτόχρονα, η διαθεσιμότητα αξιόπιστων και επαληθευμένων εργαλείων θα μπορούσε να διασφαλίσει ότι η επίδραση στα δικαιώματα των χρηστών δεν ξεπερνά το αυστηρώς αναγκαίο, περιορίζοντας την παρέμβαση και μειώνοντας τον κίνδυνο λανθασμένων θετικών αποτελεσμάτων και τη δυνατότητα κατάχρησης. Ειδικότερα, δεν προβλέπεται ανθρώπινη αλληλεπίδραση με τις προσωπικές επικοινωνίες των χρηστών πέρα από τις επικοινωνίες που έχουν αναγνωριστεί αυτόματα ως περιέχουσες υλικό παιδικής σεξουαλικής κακοποίησης[150].

Επιπλέον, σημειώνεται ότι η υποχρεωτική φύση της ανίχνευσης έχει σημαντική επίδραση στην ελευθερία των παρόχων να ασκούν τις επιχειρηματικές τους δραστηριότητες. Αυτό μπορεί να

[148] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 94.

[149] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 94.

[150] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 97.

δικαιολογηθεί μόνο εν όψει της θεμελιώδους σημασίας της καταπολέμησης των ιδιαίτερα σοβαρών εγκλημάτων και της πιο αποτελεσματικής προστασίας των παιδιών. Ειδικά στο πλαίσιο των διαπροσωπικών επικοινωνιών, οι πάροχοι είναι οι μόνοι που έχουν ορατότητα για την κακοποίηση που λαμβάνει χώρα. Δεδομένου ότι μέχρι και το 80% των ερευνών σε ορισμένα κράτη μέλη είναι δυνατές μόνο χάρη σε αναφορές από παρόχους, ένα τέτοιο μέτρο είναι αντικειμενικά αναγκαίο[151]. Επιπλέον, οι πάροχοι θα έχουν πρόσβαση σε δωρεάν και επαληθευμένα εργαλεία ανίχνευσης, ενώ η υποχρέωση ανίχνευσης του γνωστού υλικού παιδικής σεξουαλικής κακοποίησης θα εξασφάλιζε ίσους όρους ανταγωνισμού[152].

Αναφορικά με τον κίνδυνο κατάχρησης των τεχνολογιών που προορίζονται για ανίχνευση γνωστού υλικού για αλλότριους σκοπούς, σημειώνεται από την Έκθεση Εκτίμησης Επιπτώσεων ότι ο κίνδυνος αυτός ενυπάρχει σε κάθε είδους τεχνολογία, όπως για παράδειγμα στην χρήση της τεχνολογίας GPS ή της κάμερας του κινητού τηλεφώνου για σκοπούς παρακολούθησης[153]. Η ίδια η τεχνολογία κατακερματισμού (hashing) χρησιμοποιήθηκε αρχικώς για την ανίχνευση κακόβουλου λογισμικού. Ωστόσο, σύμφωνα με την Έκθεση, στην περίπτωση των τεχνικών για την ανίχνευση υλικού σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο, τα σχετικά εργαλεία υπάρχουν για πάνω από μια δεκαετία (π.χ. το PhotoDNA) και μέχρι στιγμής δεν υπάρχει απόδειξη ότι ο κίνδυνος κατάχρησης έχει υλοποιηθεί. Τα εργαλεία έχουν διατεθεί με συμφωνία άδειας που περιορίζει τη χρήση τους στην ανίχνευση περιεχομένου κακοποίησης παιδιών, κάτι που φαίνεται να έχει τηρηθεί. Συν τοις άλλοις, θα προβλέπονται μέτρα προστασίας σχετικά για τον περιορισμό του σκοπού, τον τρόπο διάθεσης των εργαλείων και την εποπτεία από τις αρμόδιες αρχές και το Κέντρο της ΕΕ, ώστε να διατηρηθεί ο κίνδυνος κατάχρησης στο απολύτως ελάχιστο.

Περαιτέρω, δεδομένης της υποχρεωτικής φύσης της ανίχνευσης και της οριζόντιας εφαρμογής της, προβλέπεται ότι οι χρήστες θα αντιμετωπίσουν περιορισμούς στην επιλογή υπηρεσιών που δεν εκτελούν ανίχνευση παιδικής σεξουαλικής κακοποίησης, αν επιθυμούν να αποφεύγουν να υποβάλλονται σε τέτοια μέτρα. Η επίδραση στους χρήστες είναι, συνεπώς, σημαντική[154]. Τονίζεται ωστόσο, ότι δεδομένου του σημαντικού αντικτύπου στους χρήστες, η πρωτοβουλία περιλαμβάνει μια σειρά από προϋποθέσεις για να διασφαλισθεί ο σεβασμός των δικαιωμάτων των παιδιών και των δικαιωμάτων όλων των χρηστών. Οι κυριότερες διασφαλίσεις περιλαμβάνουν την υποχρέωση των παρόχων υπηρεσιών να χρησιμοποιούν τεχνολογίες που εγγυώνται ακρίβεια, περιορίζοντας τον αριθμό των ψευδών θετικών όσο το δυνατόν περισσότερο, ώστε να μειώσουν τον κίνδυνο

[151] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 193.

[152] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 185.

[153] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 97.

[154] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 175.

αδικαιολόγητης υποψίας συμμετοχής σε σεξουαλική κακοποίηση παιδιών. Επιπλέον, η πρωτοβουλία επιδιώκει να δημιουργήσει μεγαλύτερη διαφάνεια στα μέτρα ανίχνευσης, εξασφαλίζοντας ότι οι χρήστες θα είναι πλήρως ενημερωμένοι για τα μέτρα και τις πιθανές συνέπειες σε περίπτωση που εντοπιστεί υλικό παιδικής σεξουαλικής κακοποίησης.

Επιπλέον, υπογραμμίζεται ότι η μείωση των ψευδώς θετικών αποτελεσμάτων θα υποβοηθείται από την λειτουργία του Κέντρου της ΕΕ, έργο του οποίου θα είναι η παροχή αξιόπιστων πληροφοριών στους παρόχους. Το Κέντρο θα μπορούσε να διασφαλίσει ότι δεν θα υπάρξει λανθασμένη αφαίρεση περιεχομένου ή κατάχρηση των εργαλείων για ανίχνευση νόμιμου περιεχομένου, ενώ θα διευκολύνει και την υποβολή καταγγελιών από χρήστες που θεωρούν ότι το περιεχόμενό τους αφαιρέθηκε εσφαλμένα. Τα εν λόγω μέτρα αναμένεται να διασφαλίσουν ότι η επίδραση στους χρήστες περιορίζεται στο απολύτως απαραίτητο για την επίτευξη του νόμιμου στόχου.

ΕΣΠΔ και ΕΕΠΔ[155], μελετώντας στο πλαίσιο της Κοινής τους Γνωμοδότησης τις τεχνολογικές απαιτήσεις που εισάγει η Πρόταση για σκοπούς εντοπισμού[156], αποφάνθηκαν ότι οι μόνες τεχνολογίες που προς το παρόν διαφαίνεται ότι πληρούν τις σχετικές απαιτήσεις είναι εκείνες που προορίζονται για τον εντοπισμό γνωστού υλικού σεξουαλικής κακοποίησης παιδιών[157]. Δεν παραλείπουν ωστόσο να σημειώσουν ότι οι συνθήκες έκδοσης εντολών ανίχνευσης σύμφωνα με την Πρόταση, όπως για παράδειγμα η εφαρμογή μιας τέτοιας εντολής σε ολόκληρη την υπηρεσία και όχι μόνο σε επιλεγμένες επικοινωνίες και η διάρκεια μέχρι και 24 μήνες για γνωστό υλικό, ενδέχεται να οδηγήσουν σε ένα πολύ ευρύ πεδίο εφαρμογής της εντολής στην πράξη. Αυτή η συνθήκη, μπορεί σύμφωνα με την Κοινή Γνωμοδότηση να οδηγήσει σε γενική και αδιάκριτη παρακολούθηση στην πράξη και όχι σε στοχευμένη. Εν όψει των ανωτέρω, μάλιστα, ΕΣΠΔ και ΕΕΠΔ εκφράζουν ανησυχία για τις ενδεχόμενες αποτρεπτικές επιδράσεις στην άσκηση της ελευθερίας της έκφρασης, γνωστές και ως «chilling effect»[158].

Επισημαίνουν επίσης ότι ενώ σύμφωνα με την Σκέψη 4, η Πρόταση θα είναι «τεχνολογικά ουδέτερη», τόσο η αποτελεσματικότητα των μέτρων ανίχνευσης όσο και ο αντίκτυπός τους στα άτομα θα εξαρτηθούν σε μεγάλο βαθμό από την επιλογή της εφαρμοζόμενης τεχνολογίας[159]. Η διαπίστωση

---

[155] ΕΣΠΔ-ΕΕΠΔ, Κοινή γνωμοδότηση 4/2022 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, διαθέσιμο: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_el

[156] Ό.π. άρθρο 10.

[157] Ό.π. Κοινή Γνωμοδότηση, σελ. 24.

[158] Ό.π. Κοινή Γνωμοδότηση, σελ. 20.

[159] Ό.π. Κοινή Γνωμοδότηση, σελ. 21.

αυτή αναγνωρίζεται και από την Έκθεση Εκτίμησης Επιπτώσεων της Επιτροπής, όσο και από την Μελέτη Εκτίμησης Επιπτώσεων του Ευρωπαϊκού Κοινοβουλίου για την Πρόταση της Επιτροπής αναφορικά με την προσωρινή παρέκκλιση από την Οδηγία e-Privacy για τον σκοπό καταπολέμησης της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο[160].

5.1.2. ΜΕΤΡΑ ΕΝΤΟΠΙΣΜΟΥ ΝΕΟΥ ΥΛΙΚΟΥ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ ΠΑΙΔΙΩΝ

Για τον εντοπισμό νέου υλικού σεξουαλικής κακοποίησης παιδιών χρησιμοποιείται συνήθως διαφορετικό είδος τεχνολογίας, μεταξύ άλλων αλγόριθμοι ταξινόμησης και τεχνητή νοημοσύνη (ΤΝ). Ένα τέτοιο εργαλείο είναι αυτό του Thorn[161], το οποίο σύμφωνα με την Έκθεση Εκτίμησης Επιπτώσεων μπορεί να χρησιμοποιηθεί από έναν πάροχο για την ανίχνευση γνωστού αλλά και νέου υλικού παιδικής σεξουαλικής κακοποίησης. Ορισμένες εταιρίες προχωρούν σε αναζήτηση νέου υλικού με την χρήση αυτών των τεχνολογιών όταν έχει ήδη εντοπιστεί γνωστό υλικό στις επικοινωνίες συγκεκριμένου χρήστη, ενώ άλλες προχωρούν σε αναζήτηση γνωστού και νέου υλικού παράλληλα[162]. Στην πρώτη περίπτωση, μόλις το γνωστό υλικό εντοπιστεί σε έναν λογαριασμό, χρησιμοποιούνται ταξινομητές για να εκτιμήσουν το περιεχόμενο του λογαριασμού και να εντοπίσουν αν υπάρχει υψηλή πιθανότητα να περιέχει υλικό σεξουαλικής κακοποίησης παιδιών. Συνήθως όμως, οι τεχνολογίες που χρησιμοποιούνται για τον εντοπισμό νέου υλικού βασίζονται σε μοντέλα πρόγνωσης μέσω της χρήσης τεχνητής νοημοσύνης.

Ειδικότερα, ένας ταξινομητής (classifier) είναι οποιοσδήποτε αλγόριθμος κατατάσσει δεδομένα σε ετικετοποιημένες κατηγορίες ή κατηγορίες πληροφοριών μέσω αναγνώρισης προτύπων[163]. Οι ταξινομητές χρειάζονται δεδομένα για να εκπαιδευτούν και η ακρίβειά τους βελτιώνεται όσο περισσότερα δεδομένα τους παρέχονται. Ο ταξινομητής της Thorn, για παράδειγμα, διαθέτει ποσοστό ακρίβειας 99,9%, το οποίο ωστόσο δύναται να εντοπίσει μονάχα το 80% του συνολικού υλικού σεξουαλικής κακοποίησης παιδιών στο σχετικό σύνολο δεδομένων[164]. Τέτοιου είδους τεχνολογίες είναι πιθανόν φυσικά να βελτιώνονται με την πάροδο του χρόνου μέσω της αυξανόμενης χρήσης και

---

[160] Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment (European Parliamentary Research Service, February 2021), παράγραφος 14, διαθέσιμο: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662598

[161] Thorn, How Safer's detection technology stops the spread of CSAM, διαθέσιμο: https://www.thorn.org/blog/how-safers-detection-technology-stops-the-spread-of-csam/

[162] WhatsApp, «How WhatsApp Helps Fight Child Exploitation», διαθέσιμο: https://faq.whatsapp.com/5704021823023684/?locale=el

[163] Ό.π. έκθεση εκτίμησης επιπτώσεων, σελ. 281.

[164] Ό.π. έκθεση εκτίμησης επιπτώσεων, σελ. 282.

ανατροφοδότησης με δεδομένα. Άλλα εργαλεία που χρησιμοποιούν τεχνολογία ταξινομητών και Τεχνητή Νοημοσύνη για την ανίχνευση νέου υλικού είναι το Content Safety API της Google[165] και η AI τεχνολογία της Facebook[166].

Ωστόσο, η αξιοπιστία των αλγορίθμων εξαρτάται σε μεγάλο βαθμό από την διαθεσιμότητα ποιοτικών δεδομένων εκπαίδευσης, δηλαδή από περιεχόμενο που έχει ήδη αναγνωριστεί αξιόπιστα ως υλικό σεξουαλικής κακοποίησης ανηλίκων. Δεδομένων των μεγάλων όγκων γνωστού υλικού, η αυτοματοποιημένη αναγνώριση νέου υλικού διαθέτει μία καλή βάση ανάπτυξης[167] και προβλέπεται ότι θα καταστεί πιο αποτελεσματική μέσω της συνεχούς επέκτασης της βάσης δεδομένων του γνωστού υλικού που επιβεβαιώνεται από ανεξάρτητες αρχές.

Το νέο υλικό σεξουαλικής κακοποίησης παιδιών δεν μπορεί να αναγνωριστεί μέσω τεχνολογιών αντιστοίχισης, καθώς οι εικόνες που έχουν ανιχνευθεί και οι μοναδικές hash τιμές τους δεν θα αντιστοιχηθούν σε βάση δεδομένων hashes[168]. Επομένως, το νέο υλικό μπορεί να ανιχνευθεί μόνο μέσω της χρήσης ταξινομητών και τεχνητής νοημοσύνης. Σημειώνεται ωστόσο ότι ένα ιδιαίτερο πρόβλημα στην ανίχνευση νέου υλικού είναι η δυνατότητα αξιόπιστης εκτίμησης της ηλικίας του ατόμου που εμφανίζεται στο περιεχόμενο, ιδιαίτερα όταν πρόκειται για άτομα κοντά στην ηλικία σεξουαλικής συναίνεσης (λ.χ. ενδέχεται να χαρακτηριστούν λανθασμένα είτε ως ενήλικες είτε ως παιδιά[169]).

Είναι σημαντικό να σημειώσουμε ότι η διαδικασία είναι παρόμοια με αυτήν για την ανίχνευση γνωστού υλικού, καθώς οι ταξινομητές δεν είναι σε θέση να συμπεράνουν την ουσία του περιεχομένου των επικοινωνιών, αλλά είναι ικανοί μόνο να ανιχνεύουν μοτίβα που υποδεικνύουν πιθανό υλικό σεξουαλικής κακοποίησης. Ωστόσο, μετά την επισήμανση νέου υλικού από το λογισμικό, απαιτείται ανθρώπινος έλεγχος και ανασκόπηση του περιεχομένου προκειμένου να εξακριβωθεί η πιθανή παρανομία του. Παρόλο που η μηχανική μάθηση γίνεται ολοένα και πιο ακριβής, η ανθρώπινη επαλήθευση εξακολουθεί να παραμένει απαραίτητη σύμφωνα με ειδικούς

---

[165] Google, Fighting child sexual abuse online, διαθέσιμο: https://protectingchildren.google/intl/en/

[166] Facebook, New Technology to Fight Child Exploitation, διαθέσιμο: https://about.fb.com/news/2018/10/fighting-child-exploitation/ και NBC News, Facebook touts use of artificial intelligence to fight child exploitation, διαθέσιμο: https://www.nbcnews.com/tech/tech-news/facebook-touts-use-artificial-intelligence-fight-child-exploitation-n923906

[167] Ό.π. έκθεση εκτίμησης επιπτώσεων, σελ. 78.

[168] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 15.

[169] Peersman et al., Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study', 2023, σ. 23, διαθέσιμο: https://research-information.bris.ac.uk/en/publications/towards-a-framework-for-evaluating-csam-prevention-and-detection-

εμπειρογνώμονες, προκειμένου να προσδώσει αποχρώσεις που η μηχανική μάθηση αδυνατεί να εισφέρει[170].

Περαιτέρω, ανησυχίες εκφράζονται όσον αφορά τη διαφάνεια και τη δικαιοσύνη λόγω της εφαρμογής αλγορίθμων στις διαδικασίες ελέγχου και διαχείρισης περιεχομένου (content moderation) στις πλατφόρμες[171]. Οι ειδικοί επισημαίνουν τις προκλήσεις αναφορικά με τον προσδιορισμό του φορέα που θα σχεδιάσει και θα συντηρήσει τον αλγόριθμο, καθώς και τον επαπειλούμενο κίνδυνο διακρίσεων κατά ορισμένων ομάδων. Δεδομένης της πολυπλοκότητας αυτών των αλγορίθμων μηχανικής μάθησης, η διαφάνειά τους σε σύγκριση με τους αλγορίθμους που χρησιμοποιούνται σε εργαλεία όπως το PhotoDNA είναι μικρότερη. Το PhotoDNA απεναντίας, βασίζεται σε μία λιγότερο σύνθετη τεχνολογία και επομένως συνιστά εργαλείο πιο διαφανές. Ως εκ τούτου, η ανεξάρτητη αξιολόγηση των αλγορίθμων μηχανικής μάθησης για τον μετριασμό περιεχομένου είναι πιο περίπλοκη και δεν μπορεί να γίνει τόσο ενδελεχής όσο η ανεξάρτητη αξιολόγηση εργαλείων σαν το PhotoDNA[172].

Στην Έκθεση Εκτίμησης Επιπτώσεων αναγνωρίζεται από την Επιτροπή ότι η υποχρεωτική ανίχνευση νέου υλικού πέραν του γνωστού θα συνεπαγόταν μεγαλύτερη επίδραση στην ελευθερία των παρόχων υπηρεσιών να διεξάγουν τις επιχειρήσεις τους και θα παρενέβαινε περισσότερο στο δικαίωμα των χρηστών στην ιδιωτικότητα, την προστασία των προσωπικών δεδομένων και την ελευθερία έκφρασης[173]. Ταυτόχρονα όμως εκτιμάται ότι θα επέλθει σημαντική αύξηση των μορφών σεξουαλικής κακοποίησης παιδιών που θα αντιμετωπίζονται και ως εκ τούτου καλύτερη επίτευξη του στόχου της καταπολέμησης των σχετικών ιδιαίτερα σοβαρών εγκλημάτων σε βάρος των παιδιών. Παρά την παρόμοια φύση γνωστού και νέου υλικού και μολονότι η ανίχνευση και των δύο τύπων εξαρτάται από επαληθευμένους δείκτες που θα παρέχονται από το Κέντρο της ΕΕ, οι χρησιμοποιούμενες τεχνικές ανίχνευσης ενέχουν πάντως διαφορετικό επίπεδο παρεμβατικότητας. Και τούτο διότι τα επίπεδα ακριβείας των εργαλείων ανίχνευσης νέου υλικού, ενώ παραμένουν πολύ πάνω από το 90%, είναι χαμηλότερα από εκείνα για την ανίχνευση γνωστού υλικού, και ως εκ τούτου η ανθρώπινη επιβεβαίωση κρίνεται απαραίτητη[174]. Παρά την αύξηση του φόρτου στους παρόχους υπηρεσιών που θα προέκυπτε από την προαναφερθείσα προϋπόθεση, η τήρησή της θεωρείται απαραίτητη για την αποφυγή αρνητικών συνεπειών προερχόμενων από μία εσφαλμένη πρόβλεψη.

---

[170] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 16.

[171] Gorwa, R., Binns, R. and Katzenbach, C., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', 2020, σ. 10., διαθέσιμο: https://journals.sagepub.com/doi/full/10.1177/2053951719897945

[172] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 16.

[173] Ό.π. έκθεση εκτίμησης επιπτώσεων, σελ. 98.

[174] Ό.π. έκθεση εκτίμησης επιπτώσεων, σελ. 98.

Περαιτέρω, η ταυτοποίηση των παρόχων που υπόκεινται στην υποχρέωση ανίχνευσης θα γίνεται μέσω εντολών εκδιδόμενων από τις εθνικές αρχές των κρατών μελών. Αυτό εξασφαλίζει σύμφωνα με την Έκθεση μια προσέγγιση κατ' αρχήν, βασισμένη στον κίνδυνο και περιορισμένη χρονικά, συμβάλλοντας στην επίτευξη αναλογικότητας[175]. Στην Έκθεση υποστηρίζεται ακόμη ότι για την ανίχνευση νέου υλικού το κατώφλι των εντολών ανίχνευσης θα είναι υψηλότερο και θα περιλαμβάνει υπηρεσίες με υψηλό και αντικειμενικό κίνδυνο κατάχρησης για την ανταλλαγή και διάδοση νέου υλικού. Η επιλογή αυτή μάλιστα θα ενείχε θετική επίδραση στα θύματα συνεχιζόμενης κακοποίησης.

Επιπλέον, η έγκαιρη ανίχνευση και επιβεβαίωση νέου υλικού και η ταχεία προσθήκη του στη βάση δεδομένων γνωστού υλικού θα μπορούσε να βοηθήσει στον περιορισμό της εξάπλωσης του υλικού παιδικής κακοποίησης μέσω των παρόχων υπηρεσιών, ενώ έτσι θα προστατεύονταν τα θεμελιώδη δικαιώματα των θυμάτων σχετικά με το απόρρητο και την προστασία των δεδομένων τους. Ταυτόχρονα, οι εν λόγω βάσεις δεδομένων, πέραν της τροφοδότησής τους με εργαλεία για την ανίχνευση γνωστού υλικού, χρησιμεύουν και για την περαιτέρω εκπαίδευση των εργαλείων για την αυτοματοποιημένη ανίχνευση του νέου υλικού. Η επακόλουθη ανίχνευση που βασίζεται στην σύγκριση με αυτές τις βάσεις δεδομένων μπορεί επίσης να παρέχει σημαντικές πληροφορίες σχετικά με τον τρόπο διάδοσης αυτού του τύπου παράνομου υλικού στο διαδίκτυο και τους κύκλους των κακοποιών, διευκολύνοντας την ανίχνευση και την αποτελεσματική δράση κατά αυτών των ομάδων.

Το ΕΣΠΔ και ο ΕΕΠΔ με τη σειρά τους, εκτιμώντας τις προταθείσες ρυθμίσεις σε συνδυασμό με την Έκθεση Εκτίμησης Επιπτώσεων (ΕΕΕ) της Πρότασης, επισημαίνουν ότι η πρόβλεψη εντολών εντοπισμού για νέο υλικό χρήζουν βελτίωσης, καθώς οι δείκτες επιδόσεων που περιλαμβάνονται στην ΕΕΕ της Πρότασης δεν παρέχουν εξαντλητικές πληροφορίες ως προς την καταλληλότητά τους σε πραγματικές συνθήκες. Ένα υψηλότερο ποσοστό «ψευδώς θετικών» αποτελεσμάτων σε σχέση με το υπολογιζόμενο στην ΕΕΕ θα μπορούσε μάλιστα να συνεπάγεται σοβαρές συνέπειες για τους χρήστες, αφού προβλέπεται ότι τα εμπλεκόμενα μέρη θα λαμβάνουν αυτόματη επισήμανση στο εσωτερικό των επικοινωνιών τους μέσω της οποίας θα τους γνωστοποιείται ότι ενδεχομένως έχουν διαπράξει ένα πολύ σοβαρό αδίκημα[176]. Επισημαίνουν μάλιστα ότι δεν υπάρχει βεβαιότητα ότι οι διαδικαστικές προϋποθέσεις που θα πρέπει να πληρούνται προκειμένου να επιβεβαιωθεί η ύπαρξη σημαντικού κινδύνου κατάχρησης υπηρεσιών[177] για σκοπούς διάδοσης υλικού σεξουαλικής κακοποίησης παιδιών είναι επαρκείς, ώστε να αντισταθμιστούν οι επαπειλούμενοι κίνδυνοι για τα δικαιώματα.

[175] Ό.π.

[176] Κοινή Γνωμοδότηση 4/2022, σελ. 25.

[177] Ό.π. άρθρο 7 παρ. 6.

Παράλληλα, η ύπαρξη αφηρημένων όρων που αφορούν στα επίπεδα κινδύνου, όπως για παράδειγμα ο όρος «σημαντικός βαθμός» ή ο όρος «πιθανότητα», ενδέχεται να οδηγήσουν σε ανασφάλεια δικαίου και σε ανομοιόμορφη εφαρμογή της Πρότασης στην Ένωση. Η ανησυχία αυτή στηρίζεται στο γεγονός ότι η ερμηνεία των προαναφερθέντων όρων θα επαφίεται αποκλειστικά στις αρμόδιες δικαστικές ή άλλες ανεξάρτητες αρχές των κρατών μελών, ενώ η έλλειψη σαφήνειας θα επηρεάζει τελικώς τον τρόπο έκδοσης των εντολών εντοπισμού οι οποίες εκ του αποτελέσματος αποτελούν περιορισμό του δικαιώματος στο απόρρητο[178]. Ανησυχία προκαλείται και σε σχέση με το γεγονός ότι οι διατάξεις για τις εντολές ανίχνευσης αποτελούν περιορισμό στην αρχή του απορρήτου, όπως καθορίζεται από άρθρο 5 της Οδηγίας e-Privacy, για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Ως εκ τούτου, η σαφήνεια και η προβλεψιμότητά τους θα πρέπει να βελτιωθούν στον προτεινόμενο Κανονισμό.

Επιπλέον, οι δείκτες απόδοσης θα πρέπει να λαμβάνονται υπόψιν σε συγκεκριμένο πλαίσιο χρήσης των εργαλείων ανίχνευσης και να παρέχεται μία εξαντλητική περιγραφή της συμπεριφοράς των εργαλείων αυτών. Όταν χρησιμοποιούνται αλγόριθμοι ΤΝ σε εικόνες ή κείμενα, είναι ευρέως καταγεγραμμένο ότι μπορεί να προκύψει μεροληψία και διάκριση λόγω της έλλειψης αντιπροσωπευτικότητας ορισμένων πληθυσμιακών ομάδων στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του αλγορίθμου. Αυτές οι μεροληψίες θα πρέπει να εντοπίζονται και να μειώνονται σε αποδεκτό επίπεδο, προκειμένου τα συστήματα ανίχνευσης να είναι πραγματικά ωφέλιμα για την κοινωνία στο σύνολό της[179].

5.1.3. ΜΕΤΡΑ ΕΝΤΟΠΙΣΜΟΥ ΑΓΡΑΣ ΠΑΙΔΙΩΝ

Όσον αφορά περιστατικά άγρας παιδιών σε επικοινωνίες που βασίζονται σε κείμενο, η σχετική εντολή στηρίζεται συνήθως στον εντοπισμό μοτίβων τα οποία καταδεικνύουν πιθανά στοιχεία υποψίας σεξουαλικής κακοποίησης παιδιών, χωρίς ωστόσο να είναι σε θέση να συναγάγουν την ουσία του περιεχομένου μίας συνομιλίας. Συγκεκριμένα, οι συνομιλίες βαθμολογούνται βάσει ορισμένων χαρακτηριστικών και τους απονέμεται μία συνολική βαθμολογία η οποία καταδεικνύει την εκτιμώμενη πιθανότητα μία επικοινωνία να συνιστά άγρα παιδιών στο διαδίκτυο. Στην ΕΕΕ επισημαίνεται ότι ορισμένες από τις υφιστάμενες τεχνολογίες για τον εντοπισμό προσεταιρισμού παιδιών έχουν ποσοστό ακρίβειας 88%[180]. Στην συγκεκριμένη κατηγορία περιλαμβάνεται το εργαλείο του Project Artemis της Microsoft, το οποίο αναπτύχθηκε σε συνεργασία με τις The Meet Group, Roblox,

[178] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 26.

[179] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 22.

[180] Έκθεση εκτίμησης επιπτώσεων, σελ. 283.

Kik και Thorn. Ωστόσο, έχει επισημανθεί ότι δεν διατίθενται ανεξάρτητες αξιολογήσεις εμπειρογνωμόνων του επιπέδου ακριβείας αυτών των τεχνολογιών[181], ενώ παράλληλα επισημαίνεται ότι αυτές τις τεχνολογίες είναι δύσκολο να επιτύχουν ποσοστά σφαλμάτων κάτω του 5-10%[182]. Ως εκ τούτου, εκτιμάται ότι τέτοια ποσοστά ακριβείας θα οδηγούσαν σε υψηλά ποσοστά ψευδών αποτελεσμάτων που θα απαιτούσαν σημαντικούς ανθρώπινους πόρους προκειμένου να επαληθευτεί αν πράγματι οι εκάστοτε ειδοποιήσεις συνιστούν παιδική σεξουαλική κακοποίηση.

Περαιτέρω, δεδομένου ότι η Πρόταση προορίζεται για εφαρμογή και επί των ακουστικών επικοινωνιών παρά το γεγονός ότι κάτι τέτοιο βρίσκεται σε αντίθεση με τον Προσωρινό Κανονισμό, ΕΣΠΔ και ΕΕΠΔ τονίζουν ότι απουσιάζει από την Έκθεση Εκτίμησης Επιπτώσεων σχετική αναφορά στην τεχνολογία που στοχεύεται να χρησιμοποιηθεί σε περιπτώσεις άγρας παιδιών[183]. Ένα ακόμη ζήτημα που εγείρεται είναι η δυσκολία προσδιορισμού της ηλικίας των ατόμων που συμμετέχουν στις επισημασμένες συνομιλίες. Σχετική μελέτη της Εθνικής Επιτροπής για την Πληροφορική και τις Ελευθερίες (National Commission on Informatics and Liberty – CNIL) της Γαλλίας ανέδειξε ότι οι τρέχουσες μέθοδοι επαλήθευσης ηλικίας είναι αρκετά παρεμβατικές[184], σημειώνοντας ότι λιγότερο παρεμβατικές μέθοδοι θα μπορούσαν να εφαρμοστούν προς το σκοπό αυτό, οι οποίες θα βασίζονταν σε τεχνικές αυθεντικοποίησης των χρηστών με βάση ορισμένα χαρακτηριστικά. Μια τέτοια λύση, όμως, σύμφωνα με την Εθνική Επιτροπή θα απαιτούσε την υιοθέτηση ενιαίου ευρωπαϊκού προτύπου τόσο για τους παρόχους όσο και για τα Κράτη Μέλη. Δεν παραλείπει ωστόσο να επισημάνει ότι ορισμένες από αυτές της μεθόδους δεν παύουν να επιτρέπουν τη σύνδεση της επίσημης ταυτότητας με προσωπικές πληροφορίες, επηρεάζοντας έτσι την ιδιωτικότητα των χρηστών. Επιπροσθέτως, ειδικοί υποστηρίζουν ότι οι τεχνολογίες ανίχνευσης άγρας παιδιών μπορούν εύκολα να παρακαμφθούν ή να χειραγωγηθούν, κάτι που μπορεί να επηρεάσει περαιτέρω τα επίπεδα ακρίβειας της τεχνολογίας[185].

Καθώς η αποπλάνηση βασίζεται κυρίως σε κείμενο, είναι ουσιώδες οι τεχνολογίες αυτές να προσαρμοστούν στις τοπικές γλώσσες των κρατών μελών και να είναι απαλλαγμένες από προκαταλήψεις. Αυτή τη στιγμή, τα εργαλεία που αναφέρθηκαν παραπάνω είναι κυρίως διαθέσιμα

---

[181] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 17.

[182] Vu et al., 'ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data', 2021, σ. 4, διαθέσιμο: https://arxiv.org/abs/2111.04479); και Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, σ. 4, διαθέσιμο: https://arxiv.org/pdf/2110.07450.

[183] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 19.

[184] CNIL, Online age verification: balancing privacy and the protection of minors, διαθέσιμο:

https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[185] I. Shumailov et. al., Manipulating SGD with Data Ordering Attacks, Cornell University, διαθέσιμο: https://arxiv.org/abs/2104.09667

και δοκιμασμένα στα αγγλικά. Ομοίως, για να είναι αποτελεσματικές οι τεχνολογίες που χρησιμοποιούνται για την ανίχνευση της αποπλάνησης σε όλη την ΕΕ, θα πρέπει επίσης να είναι σχεδιασμένες ώστε να ανιχνεύουν τις πολιτισμικές διαφορές στην επικοινωνία[186]. Σε κάθε περίπτωση, τα ανιχνευόμενα περιστατικά άγρας απαιτούν ανθρώπινο έλεγχο για να επαληθευτεί αν το εντοπισμένο κείμενο αφορά πραγματικά προσεταιρισμό παιδιών, κάτι που δεδομένα αυξάνει την παρεμβατικότητα αυτών των εργαλείων.

Στην Έκθεση Εκτίμησης Επιπτώσεων αναγνωρίζεται η μεγαλύτερη επίδραση στα θεμελιώδη δικαιώματα που συνεπάγεται η υποχρεωτική ανίχνευση προσεταιρισμού παιδιών, υπογραμμίζεται ωστόσο ότι θα εξισορροπείται από αυστηρότερες εγγυήσεις για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, παρέχοντας παράλληλα διορθωτικά μέτρα, λογοδοσία και διαφάνεια. Στο πλαίσιο αυτό η βελτίωση της αξιοπιστίας των σχετικών δεικτών με την πάροδο του χρόνου, δεδομένου ότι οι αλγόριθμοι μαθαίνουν ακολουθώντας την ανθρώπινη ανασκόπηση[187], δεν απομειώνει το επίπεδο παρεμβατικότητας στα δικαιώματα των χρηστών που απορρέει από την ανίχνευση μοτίβων σε κειμενικές επικοινωνίες, το οποίο είναι σαφώς υψηλότερο σε σχέση με την ανάλυση μιας εικόνας ή ενός βίντεο για την ανίχνευση υλικού σεξουαλικής κακοποίησης παιδιών. Τονίζεται ωστόσο ότι αυτή η υποχρέωση θα περιορίζεται μόνο σε συγκεκριμένους παρόχους υπηρεσιών που σημειώνουν υψηλό κίνδυνο κατάχρησης των υπηρεσιών τους για το συγκεκριμένο αδίκημα, μειώνοντας περαιτέρω την επίδραση στα θεμελιώδη δικαιώματα μόνο για τους χρήστες αυτών των υπηρεσιών και τους παρόχους που εμπλέκονται. Δεδομένης της διασφάλισης των αναγκαίων εγγυήσεων, η εφαρμογή και αυτού του μέτρου πιστεύεται από την Επιτροπή ότι θα έχει σημαντικά μεγαλύτερη θετική επίδραση στα δικαιώματα των θυμάτων.

Συνολικά, οι νομοθετικές διατάξεις για την υποχρεωτική ανίχνευση και των τριών τύπων υλικού παιδικής σεξουαλικής κακοποίησης, σε συνδυασμό με την υποστήριξη του Κέντρου της ΕΕ που εισάγεται ως δικλείδα ασφαλείας για την ανίχνευση και αφαίρεση του παράνομου περιεχομένου, υπολογίζεται από την Επιτροπή ότι θα μειώσουν το νομικό κατακερματισμό της ποινικής νομοθεσίας σε επίπεδο ΕΕ και θα διευκολύνουν τη συνεργασία των Κρατών-Μελών.

Τίθεται ωστόσο το ερώτημα αν η αξιοπιστία των δεικτών που θα παρέχονται για τον εντοπισμό περιστατικών άγρας παιδιών είναι επαρκής τη δεδομένη χρονική στιγμή ώστε να δικαιολογηθεί ο περιορισμός του δικαιώματος των παρόχων να ασκούν την επιχειρηματική τους δραστηριότητα.

---

[186] Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, 2023, σ. 31, διαθέσιμο: https://rm.coe.int/outcome-report-of-the-expert-workshop-on-eu-proposed-regulation-on-pre/1680aa00e4

[187] Έκθεση εκτίμησης επιπτώσεων, σελ. 99.

Δοθέντος ότι η αρχή της απαγόρευσης γενικής υποχρέωσης παρακολούθησης εδράζεται στην ανάγκη αποφυγής δυσανάλογου φόρτου σε βάρος των παρόχων, αμφισβητείται αν μπορεί να επιτευχθεί δίκαιη ισορροπία των δικαιωμάτων εν προκειμένω. Νομολογιακά, στην υπόθεση Glawischnig[188], ο Γενικός Εισαγγελέας θεώρησε ότι η υποχρέωση παρακολούθησης των ενδιάμεσων παρόχων για την ανίχνευση πανομοιότυπου δυσφημιστικού περιεχομένου που έχει ήδη κριθεί δικαστικά δεν παραβιάζει την αρχή της δίκαιης ισορροπίας, καθώς δεν απαιτεί προηγμένες τεχνολογίες. Αντιθέτως, η παρακολούθηση ισοδύναμου περιεχομένου θα απαιτούσε νομική αξιολόγηση από τον πάροχο, προκαλώντας αυξημένο κόστος και τεχνικές δυσκολίες. Το ΔΕΕ υιοθέτησε αυτήν την ανησυχία, ορίζοντας ότι η παρακολούθηση πρέπει να περιορίζεται σε περιεχόμενο με σαφή χαρακτηριστικά, το οποίο μπορεί να αναγνωριστεί μέσω αυτοματοποιημένων εργαλείων χωρίς να απαιτείται περαιτέρω νομική εκτίμηση από τον πάροχο.

Λαμβάνοντας υπόψιν την Πρόταση και την ΕΕΕ που την συνοδεύει, ΕΣΠΔ και ΕΕΠΔ αντιμετωπίζουν τα μέτρα εντοπισμού άγρας παιδιών με επιφυλακτικότητα, δεδομένου μάλιστα ότι προϋποθέτουν αυτοματοποιημένη ανάλυση κειμένου ή ομιλίας όλων των επικοινωνιών που βρίσκονται εντός του πεδίου εφαρμογής μίας εντολής εντοπισμού, ενώ παράλληλα συνεπάγονται μεγαλύτερη παρέμβαση στο απόρρητο των χρηστών και στην προστασία των δεδομένων προσωπικού χαρακτήρα[189]. Η ίδια η αιτιολογική έκθεση της πρότασης μάλιστα περιορίζεται σε απλή αναφορά της αξιοπιστίας των δεικτών προσεταιρισμού[190]. Επιπλέον, δεδομένης της χρήσης ασαφών όρων στην Πρόταση, όπως προαναφέρθηκε, τονίζεται η επίδραση των μέτρων αυτών στην ελευθερία της έκφρασης, αφού η γενικευμένη σάρωση επικοινωνιών σε ένα τμήμα μίας υπηρεσίας πιθανολογείται ότι θα λειτουργεί αποτρεπτικά στην άσκηση του δικαιώματος αυτού. Ως εκ τούτου, το ΕΣΠΔ και ο ΕΕΠΔ καταλήγουν ότι η αυτοματοποιημένη σάρωση των επικοινωνιών για σκοπούς εντοπισμού άγρας παιδιών δεν συνιστά αναγκαίο και αναλογικό μέτρο, καθώς η αδιάκριτη χρήση τέτοιας τεχνολογίας ενδέχεται να επηρεάσει την ουσία του θεμελιώδους δικαιώματος στην ιδιωτική ζωή[191].

5.2. ΚΕΝΤΡΟ ΤΗΣ ΕΕ ΚΑΙ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

5.2.1. Ο ΡΟΛΟΣ ΤΟΥ ΚΕΝΤΡΟΥ ΤΗΣ ΕΕ

[188] Ό.π. Eva Glawischnig-Piesczek v Facebook, Opinion of AG Spunzar, παρ. 62, 63, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-18/18

[189] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 26.

[190] Ό.π. αιτιολογική έκθεση, ενότητα «αποτελέσματα των εκ των υστέρων αξιολογήσεων, των διαβουλεύσεων με τα ενδιαφερόμενα μέρη και των εκτιμήσεων επιπτώσεων», σελ. 18.

[191] Ό.π. ΧΘΔΕ, άρθρο 7.

Η Πρόταση προβλέπει επίσης την ίδρυση ενός νέου οργανισμού της Ευρωπαϊκής Ένωσης, του «Κέντρου της ΕΕ»[192], για την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών. Το Κέντρο της ΕΕ προορίζεται να διευκολύνει τις διαδικασίες εκτίμησης κινδύνου[193], εντοπισμού, αναφοράς και αφαίρεσης. Βασική αποστολή του[194] θα είναι η δημιουργία και λειτουργία βάσεων δεδομένων με δείκτες διαδικτυακής σεξουαλικής κακοποίησης παιδιών, τους οποίους οι πάροχοι θα πρέπει να χρησιμοποιούν για να συμμορφώνονται με τις εντολές εντοπισμού, ενώ παράλληλα θα πρέπει να διαθέτει τεχνολογίες στους παρόχους για την εκτέλεση των εντολών αυτών. Το υλικό της εν λόγω βάσης θα προέρχεται από ποικίλες πηγές[195], συμπεριλαμβανομένων των προηγούμενων αναφορών από παρόχους υπηρεσιών, στοιχεία ερευνών από τις αρχές επιβολής του νόμου, γραμμών βοηθείας ή άμεσων αναφορών από το κοινό στο Κέντρο της ΕΕ (π.χ. από επιζώντες που ζητούν υποστήριξη από το Κέντρο για να αφαιρεθεί υλικό που απεικονίζει την κακοποίησή τους).

Περαιτέρω, στην Πρόταση προβλέπεται στενή συνεργασία του Κέντρου της ΕΕ με την Europol[196]. Μετά τη λήψη αναφορών από τους παρόχους και την επαλήθευσή τους, οι αναφορές που δεν είναι προδήλως αβάσιμες θα προωθούνται στην Europol και στις εθνικές αρχές επιβολής του νόμου[197]. Στο πλαίσιο αυτό, το Κέντρο της ΕΕ θα αναλαμβάνει την εξέταση αναφορών προκειμένου να διασφαλίζεται ότι οι δημόσιες αρχές δεν θα χρειάζεται να σπαταλούν χρόνο και πόρους φιλτράροντας αναφορές, ενώ παράλληλα θα διευκολύνει την επικοινωνία παρόχων υπηρεσιών και δημόσιων αρχών σε περίπτωση που οι τελευταίες αιτούνται την παροχή επιπλέον πληροφοριών από τους παρόχους[198]. Προβλέπεται επίσης ότι η Europol και το Κέντρο της ΕΕ θα παρέχουν αμοιβαία τη μέγιστη δυνατή πρόσβαση σε σχετικές πληροφορίες και πληροφοριακά συστήματα.

Στην Πρόταση ορίζεται επιπροσθέτως, ότι προκειμένου να διευκολυνθεί η παρακολούθηση της συμμόρφωσης με τον παρόντα κανονισμό, το Κέντρο της ΕΕ μπορεί, υπό ορισμένες περιστάσεις, να διενεργεί διαδικτυακές αναζητήσεις υλικού σεξουαλικής κακοποίησης παιδιών ή να κοινοποιεί το εν λόγω υλικό στους οικείους παρόχους υπηρεσιών φιλοξενίας, ζητώντας την αφαίρεσή του ή την απενεργοποίηση της πρόσβασης σ' αυτό[199]. Και αντιστρόφως, οι πάροχοι υπηρεσιών φιλοξενίας ή διαπροσωπικών επικοινωνιών οι οποίοι έχουν αντιληφθεί, ανεξαρτήτως τρόπου, οποιαδήποτε

---

[192] Ό.π. Πρόταση, άρθρο 40.

[193] όπως προβλέπονται στο άρθρο 3 παράγραφος 8, στο άρθρο 4 παράγραφος 5, στο άρθρο 6 παράγραφος 4 και στο άρθρο 11.

[194] όπως προβλέπονται στο άρθρο 44 (σύμφωνα με το άρθρο 46 και το άρθρο 50 παράγραφος 1).

[195] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 56.

[196] Ό.π. Πρόταση, άρθρο 48 (3).

[197] Ό.π. Πρόταση, άρθρο 48

[198] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 57.

[199] Ό.π. Πρόταση, άρθρο 49.

περίπτωση πιθανής διαδικτυακής σεξουαλικής κακοποίησης παιδιών στις υπηρεσίες τους που παρέχονται στην Ένωση, θα πρέπει να την αναφέρουν αμέσως στο Κέντρο της ΕΕ[200].

Ακόμη, προβλέπεται το δικαίωμα των παιδιών θυμάτων σεξουαλικής κακοποίησης να λαμβάνουν από το Κέντρο της ΕΕ[201], μέσω της συντονιστικής αρχής του τόπου διαμονής τους, πληροφορίες σχετικά με αναφορές γνωστού υλικού σεξουαλικής κακοποίησης που τα απεικονίζει. Θεσπίζεται επιπλέον το δικαίωμα των θυμάτων να ζητούν βοήθεια από τους οικείους παρόχους υπηρεσιών φιλοξενίας ή, μέσω της συντονιστικής αρχής του τόπου διαμονής τους, τη στήριξη του Κέντρου της ΕΕ, όταν επιδιώκουν την αφαίρεση του εν λόγω υλικού ή την απενεργοποίηση της πρόσβασης σ' αυτό[202].

5.2.2. ΚΟΙΝΗ ΓΝΩΜΟΔΟΤΗΣΗ ΕΣΠΔ ΚΑΙ ΕΕΠΔ

Οι ΕΣΠΔ και ΕΕΠΔ επισημαίνουν στην Κοινή τους Γνωμοδότηση ότι εγείρεται προβληματισμός για τα θεμελιώδη δικαιώματα αναφορικά με το Άρθρο 48 της Πρότασης το οποίο προβλέπει την διαβίβαση όλων των αναφορών που δεν είναι «προδήλως αβάσιμες» στην Europol και στις αρμόδιες αρχές επιβολής του νόμου, με σκοπό την αποφυγή επιβάρυνσης των τελευταίων με τον ογκώδη φόρτο φιλτραρίσματος περιεχομένου που έχει εσφαλμένα επισημανθεί ως υλικό σεξουαλικής κακοποίησης παιδιών[203]. Ειδικότερα, επισημαίνουν ότι δεν καθίσταται σαφές για ποιους λόγους το Κέντρο της ΕΕ δεν θα μπορούσε να προβαίνει σε πιο ενδελεχή νομική αξιολόγηση των αναφορών, ώστε να περιοριστεί ο κίνδυνος αποστολής δεδομένων προσωπικού χαρακτήρα αθώων προσώπων στις αρχές επιβολής του νόμου. Το όριο αναφορών «όχι προδήλως αβάσιμων» κρίνεται επομένως πολύ χαμηλό, δοθέντος ότι σκοπός του Κέντρου της ΕΕ είναι και η διασφάλιση της προστασίας των προσωπικών δεδομένων.

Περαιτέρω, κρίνουν ότι η διάταξη που αφορά στη διάρκεια αποθήκευσης προσωπικών δεδομένων από το Κέντρο της ΕΕ είναι αρκετά ευρεία, δεδομένου του ευαίσθητου χαρακτήρα των δεδομένων αυτών[204]. Ακόμη και αν δεν είναι δυνατόν να οριστεί μέγιστη περίοδος αποθήκευσης, ΕΣΠΔ και ΕΕΠΔ προτείνουν να οριστεί τουλάχιστον ένα μέγιστο χρονικό όριο για την αξιολόγηση της αναγκαιότητας συνέχισης αποθήκευσης των δεδομένων και να απαιτείται αιτιολόγηση για την παρατεταμένη διατήρηση μετά από αυτήν την περίοδο.

---

[200] Ό.π. Πρόταση, άρθρο 12.

[201] Ό.π. Πρόταση, άρθρο 20.

[202] Ό.π. Πρόταση, άρθρο 21.

[203] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 31.

[204] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 31.

Επιπλέον, δεδομένης της εξαιρετικά υψηλής ευαισθησίας των προσωπικών δεδομένων που θα επεξεργάζεται το Κέντρο της ΕΕ, οι ΕΣΠΔ και ΕΕΠΔ εκτιμούν ότι η επεξεργασία θα πρέπει να υπόκειται σε επιπρόσθετα μέτρα προστασίας με σκοπό τη διασφάλιση αποτελεσματικής εποπτείας. Επί παραδείγματι[205], τέτοιου είδους μέτρα θα συνιστούσαν την υποχρέωση του Κέντρου της ΕΕ να διατηρεί αρχεία (logs) για τις λειτουργίες επεξεργασίας σε αυτοματοποιημένα συστήματα επεξεργασίας των δεδομένων, με τις εν λόγω καταγραφές να χρησιμεύουν στην επαλήθευση της νομιμότητας, της ακεραιότητας και της ασφάλειας της επεξεργασίας.

Σημειώνουν επίσης ότι σύμφωνα με το Άρθρο 50 της Πρότασης, το Κέντρο της ΕΕ θα έχει την ευθύνη να προσδιορίσει τη λίστα των τεχνολογιών που μπορεί να χρησιμοποιηθούν για την εκτέλεση των εντολών ανίχνευσης. Ωστόσο, σύμφωνα με το Άρθρο 12(1) της Πρότασης[206], οι πάροχοι υποχρεούνται να αναφέρουν όλες τις πληροφορίες που υποδεικνύουν ενδεχόμενη διαδικτυακή σεξουαλική κακοποίηση παιδιών στις υπηρεσίες τους, όχι δηλαδή μονάχα αυτές που προκύπτουν από την εκτέλεση μιας εντολής εντοπισμού. Δεδομένου, λοιπόν, ότι είναι πολύ πιθανόν σημαντικός αριθμός των πληροφοριών αυτών να προέρχεται από τη λειτουργία των μέτρων μετριασμού των παρόχων[207], ΕΣΠΔ και ΕΕΠΔ θεωρούν κρίσιμο να διευκρινιστεί ποια μπορεί να είναι τα εν λόγω μέτρα, η αποτελεσματικότητά τους, το ποσοστό σφαλμάτων τους και ο αντίκτυπός τους στα δικαιώματα και τις ελευθερίες των ατόμων. Ως εκ τούτου, θεωρούν σημαντικό ο νομοθέτης να περιλάβει στο άρθρο 50 ως αποστολή του Κέντρου της ΕΕ την υποχρέωση να παράσχει μία λίστα συνιστώμενων μέτρων μετριασμού, αφού ζητήσει προηγουμένως τη γνώμη του ΕΕΠΔ, καθώς ενδέχεται τα μέτρα αυτά να επηρεάσουν τα θεμελιώδη δικαιώματα προστασίας προσωπικών δεδομένων και της ιδιωτικότητας.

Προβληματισμοί εγείρονται επίσης αναφορικά με την συνεργασία που προβλέπεται από την Πρόταση μεταξύ Κέντρου της ΕΕ και της Europol[208]. ΕΣΠΔ και ΕΕΠΔ επισημαίνουν ότι αρκετές πτυχές που αφορούν στη συνεργασία αυτή προκαλούν ανησυχία και απαιτούν περαιτέρω εξειδίκευση[209]. Συγκεκριμένα, μολονότι το άρθρο 48 αποδίδει στην Europol τον ρόλο της αναγνώρισης της αρμόδιας εθνικής αρχής όταν δεν είναι σαφές ποια αρχή είναι υπεύθυνη, η διάταξη προβλέπει στην πράξη ότι όλες οι αναφορές θα διαβιβάζονται στην Europol, ανεξαρτήτως αν η εθνική αρχή έχει ήδη εξευρεθεί. Ωστόσο, η Πρόταση δεν διευκρινίζει τον αναμενόμενο ρόλο της Europol κατά την λήψη των αναφορών, ιδιαίτερα στις περιπτώσεις όπου η εθνική αρχή επιβολής του νόμου έχει ήδη προσδιοριστεί και ειδοποιηθεί.

---

[205] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 31, 32.

[206] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 32.

[207] Ό.π. Πρόταση, άρθρο 4.

[208] Ό.π. Πρόταση, Κεφάλαιο IV.

[209] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 33.

Υπογραμμίζουν επίσης ότι η εντολή της Europol περιορίζεται στην στήριξη των αρμόδιων αρχών των Κρατών Μελών και της αμοιβαίας συνεργασίας τους στην πρόληψη και καταπολέμηση σοβαρών εγκλημάτων που επηρεάζουν δύο ή περισσότερα Κράτη Μέλη. Συγκεκριμένα, βάσει του άρθρου 19 του Κανονισμού (ΕΕ) 2016/794[210], όπως τροποποιήθηκε από τον Κανονισμό (ΕΕ) 2022/991, σώμα της Ένωσης που παρέχει πληροφορίες στην Europol υποχρεούται να καθορίσει τον σκοπό και τις συνθήκες επεξεργασίας πληροφοριών από την Europol. Είναι επίσης υπεύθυνο για την εξασφάλιση της ακρίβειας των προσωπικών δεδομένων που μεταφέρονται. Η μαζική προώθηση αναφορών στην Europol θα παραβίαζε, συνεπώς, τον τροποποιημένο Κανονισμό της και θα συνεπαγόταν κινδύνους για την προστασία των δεδομένων.

Επισημαίνεται ακόμη ότι η επαναλαμβανόμενη επεξεργασία προσωπικών δεδομένων θα μπορούσε να οδηγήσει στην αποθήκευση πολλαπλών αντιγράφων ευαίσθητων προσωπικών δεδομένων σε διάφορες τοποθεσίες[211] (π.χ. στο Κέντρο της ΕΕ, στην Europol, στην εθνική αρχή επιβολής του νόμου), προκαλώντας κινδύνους για την ακρίβεια των δεδομένων λόγω ενδεχόμενης έλλειψης συγχρονισμού των βάσεων δεδομένων, καθώς και για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων. Επιπλέον, το χαμηλό όριο που καθορίζεται στην Πρόταση για την διαβίβαση αναφορών στις αρχές επιβολής του νόμου (αναφορές που δεν είναι «προδήλως αβάσιμες») υποδηλώνει μεγάλη πιθανότητα να αποθηκευτούν ψευδώς θετικές αναφορές στα συστήματα πληροφοριών της Europol, ενδεχομένως για παρατεταμένες περιόδους. Ως εκ τούτου[212], ΕΣΠΔ και ΕΕΠΔ συνιστούν να διευκρινιστούν οι σκοποί προώθησης αναφορών από το Κέντρο της ΕΕ στην Europol, σύμφωνα με τον τροποποιημένο Κανονισμό της τελευταίας και να εξαιρεθούν ρητά οι περιπτώσεις όπου οι αναφορές έχουν ήδη διαβιβαστεί στην αρμόδια εθνική αρχή επιβολής του νόμου, οι οποίες δεν συνεπάγονται διασυνοριακή διάσταση. Επιπροσθέτως, η Πρόταση θα πρέπει να περιλαμβάνει την απαίτηση το Κέντρο της ΕΕ να διαβιβάζει στην Europol μόνο προσωπικά δεδομένα που είναι επαρκή, συναφή και περιορισμένα στο αυστηρά αναγκαίο.

Εν συνεχεία, κριτική ασκείται στο πνεύμα του άρθρου 53(2) της Πρότασης, αναφορικά με την παροχή αμοιβαία από πλευράς Europol και Κέντρου της ΕΕ «της πλησιέστερης δυνατής πρόσβασης στις σχετικές πληροφορίες και συστήματα πληροφοριών, εφόσον απαιτείται για την εκτέλεση των αντίστοιχων καθηκόντων τους και σύμφωνα με τις πράξεις του ενωσιακού δικαίου που διέπουν την

[210] Κανονισμός 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαΐου 2016 για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0794&from=EN

[211] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 34.

[212] Ό.π.

πρόσβαση αυτή»[213]. Το εν λόγω άρθρο αποτελεί την μοναδική αναφορά στην Πρόταση για την πρόσβαση του Κέντρου της ΕΕ στα συστήματα πληροφοριών της Europol και ως εκ τούτου παραμένουν ασαφείς οι σκοποί πραγματοποίησης αυτής της πρόσβασης. Συγκεκριμένα, τα κριτήρια και τα μέτρα προστασίας που καθορίζουν την πρόσβαση της Europol και την επακόλουθη χρήση των δεδομένων που αποκτώνται από τα συστήματα πληροφοριών του Κέντρου της ΕΕ δεν έχουν διευκρινιστεί. Επιπλέον, δεν εξηγείται γιατί είναι απαραίτητο να παραχωρηθεί στην Europol άμεση πρόσβαση στα συστήματα πληροφοριών ενός μη επιχειρησιακού οργανισμού, που περιέχουν εξαιρετικά ευαίσθητα προσωπικά δεδομένα, τα οποία ενδέχεται να μην σχετίζονται άμεσα με εγκληματική δραστηριότητα ή πρόληψη εγκλήματος. Για να διασφαλιστεί υψηλό επίπεδο προστασίας των δεδομένων και συμμόρφωση με την αρχή του περιορισμού του σκοπού, η ΕΣΠΔ και ο ΕΕΠΔ συνιστούν η μετάδοση προσωπικών δεδομένων από το Κέντρο της ΕΕ στην Europol να πραγματοποιείται μόνο κατά περίπτωση, κατόπιν αξιολογημένου αιτήματος, μέσω ασφαλούς καναλιού επικοινωνίας, όπως το SIENA[214].

ΕΣΠΔ και ΕΕΠΔ υπενθυμίζουν ότι δεδομένου ότι το προτεινόμενο Κέντρο της ΕΕ δεν αποτελεί όργανο επιβολής του νόμου, δεν θα πρέπει να του παραχωρείται άμεση πρόσβαση στα συστήματα πληροφοριών της Europol υπό κανέναν όρο. Οι ΕΔΠΠ και ΕΕΠΔ σημειώνουν περαιτέρω ότι ένα μεγάλο ποσοστό των πληροφοριών που ενδιαφέρουν τόσο το Κέντρο της ΕΕ όσο και την Europol θα αφορά προσωπικά δεδομένα που σχετίζονται με θύματα φερόμενων εγκλημάτων, προσωπικά δεδομένα ανηλίκων και προσωπικά δεδομένα που αφορούν τη σεξουαλική ζωή, τα οποία χαρακτηρίζονται ως ειδικές κατηγορίες προσωπικών δεδομένων σύμφωνα με τον τροποποιημένο Κανονισμό της Europol[215]. Ο τροποποιημένος Κανονισμός της Europol επιβάλλει αυστηρούς όρους όσον αφορά την πρόσβαση σε ειδικές κατηγορίες προσωπικών δεδομένων. ΕΣΠΔ και ΕΕΠΔ συνιστούν, επομένως, να διευκρινιστεί η διατύπωση του Άρθρου 53(2) της Πρότασης ώστε να αντικατοπτρίζει σωστά τους περιορισμούς που ισχύουν σύμφωνα με τον τροποποιημένο Κανονισμό της Europol και να προσδιορίσει τις διαδικασίες για την πρόσβαση του Κέντρου της ΕΕ. Συγκεκριμένα, οποιαδήποτε πρόσβαση σε προσωπικά δεδομένα που επεξεργάζονται τα συστήματα πληροφοριών της Europol, όταν κρίνεται αυστηρά απαραίτητη για την εκτέλεση των καθηκόντων του Κέντρου της ΕΕ, θα πρέπει να παραχωρείται μόνο κατά περίπτωση, μετά την υποβολή ενός σαφούς αιτήματος που τεκμηριώνει τον συγκεκριμένο σκοπό. Η Europol θα πρέπει να είναι υπεύθυνη για τη σχολαστική αξιολόγηση αυτών των αιτημάτων και να μεταβιβάζει προσωπικά δεδομένα στο Κέντρο της ΕΕ μόνο όταν είναι αυστηρά αναγκαίο και αναλογικό με τον απαιτούμενο σκοπό.

---

[213] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 35.

[214] Secure Information Exchange Network Application (SIENA).

[215] Ό.π. Κοινή Γνωμοδότηση.

Η ΕΣΠΔ και ο ΕΕΠΔ χαιρετίζουν καταρχήν την απαίτηση ενημέρωσης των χρηστών των οποίων τα προσωπικά δεδομένα ενδέχεται να επηρεαστούν από την εκτέλεση της εντολής ανίχνευσης, σύμφωνα με τα οριζόμενα στο Άρθρο 10(6) της Πρότασης[216]. Σημειώνεται ότι η εν λόγω ενημέρωση πρέπει να λαμβάνει χώρα μονάχα κατόπιν επιβεβαίωσης από την Europol ή την εθνική αρχή επιβολής του νόμου ενός Κράτους Μέλους που έλαβε την αναφορά[217] ότι η σχετική πράξη δεν θα επηρεάσει τις δραστηριότητες για την πρόληψη, διερεύνηση και δίωξη των αδικημάτων σεξουαλικής κακοποίησης παιδιών. Ωστόσο, ΕΔΠΠ και ΕΕΠΔ εντοπίζουν ελλείψεις αναφορικά με την πρακτική εφαρμογή της διάταξης αυτής. Ειδικότερα, όταν οι αναφορές διαβιβάζονται τόσο στην Europol όσο και στην εθνική αρχή επιβολής του νόμου ενός Κράτους Μέλους, η Πρόταση δεν διευκρινίζει αν απαιτείται επιβεβαίωση από τον έναν ή και τους δύο παραλήπτες, ούτε καθορίζονται οι διαδικασίες διαβίβασης της επιβεβαίωσης αυτής στην Πρόταση. Λαμβάνοντας υπόψη τον μεγάλο όγκο υλικού σεξουαλικής κακοποίησης που μπορεί να απαιτηθεί να επεξεργαστούν η Europol και οι εθνικές αρχές επιβολής του νόμου, καθώς επίσης και την έλλειψη σαφούς χρονικού περιορισμού για την παροχή επιβεβαίωσης («χωρίς αδικαιολόγητη καθυστέρηση»), ΕΔΠΠ και ΕΕΠΔ συνιστούν να διευκρινιστούν οι εφαρμοστέες διαδικασίες προκειμένου να διασφαλιστεί η εφαρμογή αυτής της προστασίας στην πράξη.

5.2.3 ΚΕΝΤΡΟ ΤΗΣ ΕΕ ΚΑΙ ΑΠΑΓΟΡΕΥΣΗ ΓΕΝΙΚΕΥΜΕΝΗΣ ΔΙΑΤΗΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ

Αναφορικά με την διάταξη της Πρότασης που αφορά στην διάρκεια αποθήκευσης προσωπικών δεδομένων από το Κέντρο της ΕΕ, ΕΣΠΔ και ΕΕΠΔ κρίνουν ότι η εν λόγω διάρκεια είναι αρκετά ευρεία, δεδομένου του ευαίσθητου χαρακτήρα των δεδομένων αυτών.[218] Όπως τονίστηκε και ανωτέρω, σε περίπτωση που δεν είναι δυνατόν να οριστεί μέγιστη περίοδος αποθήκευσης, προτείνουν να οριστεί ένα μέγιστο χρονικό όριο για την αξιολόγηση της αναγκαιότητας συνέχισης αποθήκευσης των δεδομένων και να απαιτείται αιτιολόγηση για την παρατεταμένη διατήρησή τους μετά την περίοδο αυτή.

Συναφής με το ζήτημα διατήρησης δεδομένων προσωπικού χαρακτήρα στο πλαίσιο αντιμετώπισης σοβαρών εγκλημάτων είναι η υπόθεση La Quadrature du Net[219], όπου το ΔΕΕ ερμήνευσε τον όρο «στοχευμένη παρακολούθηση» και αναφέρθηκε ειδικά σε εγκλήματα «παιδικής πορνογραφίας» ιδιαίτερης σοβαρότητας. Συγκεκριμένα, το ΔΕΕ διευκρίνισε ότι η γενική και αδιάκριτη διατήρηση διευθύνσεων IP όλων των προσώπων που διαθέτουν τερματικό εξοπλισμό με δυνατότητα πρόσβασης

[216] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 36.

[217] Ό.π. Πρόταση, άρθρο 48.

[218] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 31.

[219] Ό.π. La Quadrature du Net.

στο διαδίκτυο, χωρίς εκ πρώτης όψεως σύνδεση με τους επιδιωκόμενους σκοπούς, και χωρίς να υπάρχει υποψία για σοβαρό έγκλημα, είναι επιτρεπτή. Κι αυτό, επειδή οι διευθύνσεις IP μπορεί να είναι το μοναδικό μέσο ταυτοποίησης του προσώπου στο οποίο είχε ανατεθεί η διεύθυνση τη στιγμή τέλεσης της αξιόποινης πράξης.

Ωστόσο, η περίοδος διατήρησης των δεδομένων τονίστηκε ότι δεν θα πρέπει να υπερβαίνει αυτό που είναι απολύτως αναγκαίο με βάση τον επιδιωκόμενο σκοπό, και θα πρέπει να προβλέπονται ουσιαστικές και διαδικαστικές προϋποθέσεις για τη χρήση αυτών των δεδομένων[220]. Το ΔΕΕ κατέληξε επίσης ότι η κατεπείγουσα διατήρηση δεδομένων κίνησης και τοποθεσίας, τα οποία επεξεργάζονται και αποθηκεύουν πάροχοι υπηρεσιών της Κοινωνίας της Πληροφορίας, για συγκεκριμένο χρονικό διάστημα, είναι επιτρεπτή για την καταπολέμηση σοβαρού εγκλήματος και την προστασία της εθνικής ασφάλειας. Η σε πραγματικό χρόνο διατήρηση των δεδομένων κίνησης και τοποθεσίας θεωρείται ιδιαίτερα ευαίσθητη και επιτρέπεται μόνο για την πρόληψη τρομοκρατικών ενεργειών, και μόνο για πρόσωπα για τα οποία υπάρχουν βάσιμες υπόνοιες ότι εμπλέκονται σε τρομοκρατική δραστηριότητα[221].

Τέλος, το ΔΕΕ εξέτασε και το ενδεχόμενο αυτοματοποιημένης ανάλυσης όλων των δεδομένων κίνησης και τοποθεσίας που διατηρούνται από παρόχους, κατόπιν αιτήματος των εθνικών αρχών, μέσω εφαρμογής αλγορίθμων για τον εντοπισμό ύποπτων μοτίβων και συμπεριφορών στο πλαίσιο προστασίας της εθνικής ασφάλειας. Το Δικαστήριο έκρινε ότι μια τέτοια πράξη θα συνιστούσε γενική και αδιάκριτη επεξεργασία, η οποία θα ισοδυναμούσε με σοβαρή παρέμβαση στα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, ανεξαρτήτως του τρόπου χρησιμοποίησης των δεδομένων αυτών στη συνέχεια[222].

Με βάση τα προβλεπόμενα στην απόφαση La Quadrature du Net, υποστηρίζεται ότι για σοβαρά εγκλήματα όπως τα αδικήματα παιδικής σεξουαλικής κακοποίησης, τα μέτρα διατήρησης δεν θα πρέπει να είναι γενικά και αδιάκριτα αλλά περισσότερο στοχευμένα[223]. Διαφορετικά, σε περίπτωση που δεν αποκλείεται από το λεκτικό της Πρότασης η γενική διατήρηση δεδομένων, εγείρονται ανησυχίες ως προς την αναλογικότητα, ιδιαίτερα όταν δεν ορίζονται τα πρόσωπα που στοχεύονται.

[220] Ό.π. παρ. 154 - 155.

[221] Ό.π. παρ. 164 – 165.

[222] Ό.π. παρ. 172-173

[223] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 50.

5.3. ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ ΤΗΣ ΠΡΟΤΑΣΗΣ

5.3.1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΠΟ ΑΚΡΟ ΣΕ ΑΚΡΟ

Στο Προοίμιο της Πρότασης[224] σημειώνεται ότι η επιλογή τεχνολογιών με σκοπό την εκτέλεση εντολών εντοπισμού καταλείπεται στους παρόχους, υπό την προϋπόθεση ότι πληρούν τις απαιτήσεις του Κανονισμού και ότι μέσω αυτών θα εξασφαλίζεται η αποτελεσματικότητα των μέτρων. Επισημαίνεται παράλληλα ότι μεταξύ των απαιτήσεων που πρέπει να πληρούνται βάσει της ίδιας της Πρότασης είναι «η χρήση τεχνολογίας διατερματικής κρυπτογράφησης (E2EE), που αποτελεί σημαντικό εργαλείο για τη διασφάλιση της προστασίας του απορρήτου των επικοινωνιών των χρηστών, συμπεριλαμβανομένων των παιδιών[225]». Η Πρόταση Κανονισμού συνεπώς, είναι τεχνολογικά ουδέτερη και δεν περιλαμβάνει ειδικές διατάξεις για κρυπτογραφημένες επικοινωνίες. Ωστόσο στην διάρκεια της διαδικασίας νομοθέτησης έχουν προταθεί συμβιβαστικές λύσεις που ενδεχομένως επηρεάσουν την κρυπτογράφηση από άκρο σε άκρο.

Αξίζει να σημειωθεί ότι η υποχρέωση σάρωσης των επικοινωνιών των χρηστών με σκοπό τον εντοπισμό υλικού παιδικής σεξουαλικής κακοποίησης, θα μπορούσε να συνεπάγεται την ενσωμάτωση από πλευράς παρόχων μίας μεθόδου παράκαμψης του ενσωματωμένου ελέγχου κρυπτογράφησης στην αρχιτεκτονική των συστημάτων τους, η οποία θα επέτρεπε εξαιρετική πρόσβαση στην επικοινωνίες ή σάρωση από την πλευρά του πελάτη, άλλως σάρωση εξερχόμενης επικοινωνίας στην προσωπική συσκευή[226]. Ένα τέτοιο οικοδόμημα ωστόσο έχει σημειωθεί ότι θα ενείχε σοβαρές επιπτώσεις στο δικαίωμα στην ιδιωτικότητα.

Σύμφωνα με το NCMEC[227], πάνω από τις μισές καταγγελίες που λαμβάνει μέσω της πλατφόρμας CyberTipline θα εξαφανιστούν σε περίπτωση που εφαρμοστεί ευρέως διατερματική κρυπτογράφηση. Κάτι τέτοιο θα οδηγούσε σε αδυναμία εντοπισμού της κακοποίησης, εκτός εάν οι πάροχοι υιοθετούσαν μέτρα προστασίας των παιδιών ακόμη και στις υπηρεσίες που εφαρμόζουν διατερματική κρυπτογράφηση. Παράλληλα, οργανώσεις για τα δικαιώματα των παιδιών τονίζουν ότι οι διαπράττοντες αδικήματα σεξουαλικής κακοποίησης παιδιών μετέρχονται μεταξύ άλλων τη μέθοδο «off-platforming»[228], η οποία επί της ουσίας συνίσταται στη μεταφορά της επικοινωνίας τους με παιδιά σε υπηρεσίες ανταλλαγής μηνυμάτων που εγγυώνται κρυπτογράφηση από άκρο σε άκρο.

---

[224] Ό.π. προοίμιο, σκ. 26.

[225] Ό.π. προοίμιο.

[226] Ό.π. Expert Workshop, ενότητα 5.1., σελ.26.

[227] NCMEC, The issues, End-to-end encryption, διαθέσιμο: https://www.missingkids.org/theissues/end-to-end-encryption

[228] Ό.π. ECLAG Steering Group, σελ. 4.

Οι ίδιες οργανώσεις ωστόσο, υποστηρίζουν τη λύση της σάρωσης από την πλευρά του πελάτη, η οποία δεν επηρεάζει την διατερματική κρυπτογράφηση, καθώς διενεργείται σε στάδιο προτού μεταφερθεί η επικοινωνία στο κρυπτογραφημένο κανάλι. Μία τέτοιου είδους λύση θα μπορούσε να συνεπάγεται τη σύνδεση της προσωπικής συσκευής του χρήστη με μία εξωτερική βάση δεδομένων, του Κέντρου της ΕΕ επί παραδείγματι, μέσω της οποίας θα διενεργούνταν αντιστοίχιση με επιβεβαιωμένο γνωστό υλικό παιδικής κακοποίησης[229]. Επισημαίνουν μάλιστα ότι τέτοιου είδους τεχνολογία έχει χρησιμοποιηθεί ευρέως με χαρακτηριστικό παράδειγμα εργαλείο το οποίο σαρώνει περιεχόμενο τοπικά τις συσκευές των παιδιών και εμφανίζει ένδειξη επί ειλημμένου και απεσταλμένου περιεχομένου που περιέχει γυμνό[230].

Μέρος, πάντως, των εν λόγω οργανώσεων υποστηρίζει ότι ο εντοπισμός υλικού μπορεί να πραγματοποιηθεί και σε περιβάλλοντα διατερματικής κρυπτογράφησης, μέσω ομομορφικής κρυπτογράφησης, με μεθόδους υπολογισμού πολλαπλών μερών (multi-party computation)[231] ή μέσω ασφαλών θυλάκων (secure enclaves)[232]. Αξίζει να σημειωθεί ότι ως μέθοδος ανίχνευσης υλικού σεξουαλικής κακοποίησης παιδιών σε συστήματα διατερματικής κρυπτογράφησης συστήνεται στην Έκθεση Εκτίμησης Επιπτώσεων η πραγματοποίηση της διαδικασίας κατακερματισμού στην συσκευή με μετέπειτα αντιστοίχιση στον διακομιστή[233], ενώ παράλληλα συστήνεται μεταξύ άλλων η επένδυση στην έρευνα ταξινομητών (classifiers) που θα συμπληρώσουν τον κατακερματισμό και την αντιστοίχιση, καθώς επίσης και στην ομομορφική κρυπτογράφηση αναφορικά με την αντιστοίχιση εικόνων.

Στον αντίποδα των ισχυρισμών οργανώσεων για τα δικαιώματα του παιδιού, οργανώσεις που προασπίζονται το δικαίωμα στην ιδιωτικότητα σημειώνουν ότι παρόλο που σύμφωνα με την Πρόταση οι εντολές εντοπισμού εκδίδονται μονάχα όταν μία τέτοια παρέμβαση «υπερτερεί των αρνητικών συνεπειών» στα δικαιώματα των χρηστών, δεν υπάρχει σαφής δήλωση αναφορικά με το αν η υπονόμευση της κρυπτογράφησης συνιστά μία τέτοιας έντασης αρνητική συνέπεια. Συνακόλουθα, υπογραμμίζουν ότι οι αιτιολογικές σκέψεις 22, 23 και 26 είναι πολύ ασαφείς, χωρίς να παρέχουν ειδική

---

[229] Ό.π.

[230] Wired, Apple Expands Its On-Device Nudity Detection to Combat CSAM, διαθέσιμο: https://www.wired.com/story/apple-communication-safety-nude-detection/

[231] Inpher Computing Company, What is Secure Multiparty Computation?, διαθέσιμο: https://inpher.io/technology/what-is-secure-multiparty-computation/

[232] «Ως ασφαλής θύλακας ορίζεται μία απομονωμένη διαδικασία, που εκτελείται σε μια πλατφόρμα που παρέχει εμπιστευτικότητα και ακεραιότητα κώδικα και δεδομένων», Beekman, Jethro Gideon, "Improving Cloud Security using Secure Enclaves", ενότητα 2.3., UC Berkeley, Electronic Theses and Dissertations, 2016, διαθέσιμο: https://escholarship.org/uc/item/0jn0n1xs

[233] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, παράρτημα 9.

προστασία στην κρυπτογράφηση από άκρο σε άκρο[234]. Οι ευρωπαϊκές Αρχές προστασίας δεδομένων από την πλευρά τους τάσσονται υπέρ της αδιαμφισβήτητης σημασίας της ισχυρής κρυπτογράφησης και εναντιώνονται σε ενδεχόμενη ενσωμάτωση κάθε είδους κερκόπορτας στα συστήματα ασφαλείας. Σύμφωνα μάλιστα με τον ΕΕΠΔ[235], δεν είναι εφικτό τεχνικά να διενεργηθεί σάρωση για τους σκοπούς εντοπισμού υλικού του παρόντος κανονισμού χωρίς να αποδυναμωθεί η κρυπτογράφηση και να υπονομευτεί το απόρρητο των χρηστών.

Αξίζει πάντως να αναφερθεί ότι στην Έκθεση Εκτίμησης Επιπτώσεων που συνοδεύει την Πρόταση, σημειώνεται ότι η απουσία εργαλείων ανίχνευσης υλικού σεξουαλικής κακοποίησης παιδιών σε συστήματα διατερματικής κρυπτογράφησης μειώνει την ικανότητα στοιχειοθέτησης των εν λόγω αδικημάτων[236]. Στη διαπίστωση αυτή οδηγείται και η Europol αναφορικά με την ευρεία χρήση εφαρμογών που ενσωματώνουν κρυπτογράφηση από άκρο σε άκρο[237].

5.3.2. ΛΥΣΕΙΣ ΑΝΙΧΝΕΥΣΗΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ Ε2ΕΕ

Στην Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων της Πρότασης που ζητήθηκε από την Επιτροπή Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων του Ευρωπαϊκού Κοινοβουλίου[238], η οποία δημοσιεύθηκε τον Απρίλιο του 2023 από την Ευρωπαϊκή Υπηρεσία Ερευνών του Ευρωπαϊκού Κοινοβουλίου, αφιερώνεται ξεχωριστή ενότητα για τις προκλήσεις στην ανίχνευση υλικού παιδικής σεξουαλικής κακοποίησης μέσω διαπροσωπικών επικοινωνιών που είναι διατερματικά κρυπτογραφημένες.

Στην εν λόγω ενότητα, ανασκοπούνται οι εννέα τεχνολογικές λύσεις που προτάθηκαν στην Ευρωπαϊκή Επιτροπή από ειδικούς τεχνικούς εμπειρογνώμονες για την ανίχνευση υλικού σεξουαλικής κακοποίησης σε περιβάλλοντα διατερματικά κρυπτογραφημένα[239]. Τελικώς, τρεις λύσεις προκρίθηκαν από του τεχνικούς εμπειρογνώμονες ως οι πιο εφικτές για τους σκοπούς αυτούς: ο πλήρης κατακερματισμός στη συσκευή (με αντιστοίχιση στον διακομιστή), ο μερικός

---

[234] EDRi network, position paper on the "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse" 2022/0155(COD) (CSA Regulation), διαθέσιμο: https://edri.org/our-work/csa-regulation-document-pool/#position

[235] Ευρωπαίος Επόπτης Προστασίας Δεδομένων, Briefing note on the CSAM proposal: "The Point of No Return", διαθέσιμο: https://www.edps.europa.eu/data-protection/our-work/publications/factsheets/2023-10- 23-briefing-note-csam-point-no-return_en

[236] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 28.

[237] Europol, Europol Serious and Organised Crime Threat Assessment (SOCTA), Απρίλιος 2021, διαθέσιμο: https://www.europol.europa.eu/publications-events/main-reports/socta-report

[238] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων.

[239] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 288.

κατακερματισμός στη συσκευή (με αντιστοίχιση στον διακομιστή), και οι ασφαλείς θύλακες σε διακομιστή παρόχου ηλεκτρονικών υπηρεσιών. Σημειώνεται ότι, παρόλο που οι εν λόγω λύσεις είναι τεχνολογικά εφικτές, δεν θεωρούνται έτοιμες προς εφαρμογή από τους ειδικούς εμπειρογνώμονες που συμβουλεύτηκε η Ευρωπαϊκή Επιτροπή.

Καθώς η κρυπτογράφηση σε επικοινωνίες E2EE δεν επιτρέπει τον κατακερματισμό στον διακομιστή μετά την κρυπτογράφηση της επικοινωνίας, η λύση του πλήρους κατακερματισμού στην συσκευή με αντιστοίχιση στον διακομιστή συνεπάγεται την μετατροπή του περιεχομένου σε κατακερματισμούς σε στάδιο προ της κρυπτογράφησής του. Αφού δημιουργηθούν οι κατακερματισμοί, η συσκευή αποστέλλει τόσο τους κατακερματισμούς όσο και το κρυπτογραφημένο μήνυμα στον διακομιστή. Ο διακομιστής στη συνέχεια συγκρίνει αν οι απεσταλμένοι κατακερματισμοί ταιριάζουν με τους κατακερματισμούς στη βάση δεδομένων. Η λύση αυτή απαιτεί την εγκατάσταση μιας εφαρμογής στη συσκευή του χρήστη για να διευκολυνθεί η αντιστοίχιση στον διακομιστή[240].

Οι εμπειρογνώμονες που συμβουλεύτηκε η Ευρωπαϊκή Επιτροπή θεωρούν αυτή τη λύση υποσχόμενη, καθώς επιτρέπει την ανίχνευση γνωστού υλικού. Ωστόσο, εγείρονται προβληματισμοί σχετικά με την εφαρμογή τεχνολογιών ανίχνευσης στην πλευρά του πελάτη (client-side scanning). Μερικές από τις ανησυχίες που γεννώνται είναι παρόμοιες με εκείνες που διατυπώνονται για την παρακολούθηση σε επικοινωνίες που δεν είναι E2EE. Η πρόσβαση των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας, φερ' ειπείν, σε όλους τους κατακερματισμούς, προκαλεί ανησυχία για την ασφάλεια και την ιδιωτικότητα[241]. Επίσης, υπάρχει έλλειψη συνεπούς εποπτείας από κάποια αρμόδια αρχή, γεγονός που επηρεάζει τη διαφάνεια της τεχνολογίας[242].

Στο ίδιο πλαίσιο, εκφράζονται ανησυχίες που σχετίζονται με την παρακολούθηση E2EE επικοινωνιών. Πρώτον, η ανίχνευση στην πλευρά του πελάτη έχει σημαντικό αντίκτυπο στα όρια μεταξύ της ιδιωτικής και της ημιδημόσιας σφαίρας του χρήστη. Μέσω της εφαρμογής αυτής της τεχνολογικής λύσης, το περιεχόμενο που προηγουμένως ήταν ιδιωτικό για τον χρήστη μπορεί να γίνει προσβάσιμο στις Αρχές επιβολής του νόμου, χωρίς προϋπόθεση έκδοσης εντάλματος. Δεύτερον, η ανίχνευση στην πλευρά του πελάτη ενέχει σημαντικούς κινδύνους επιθέσεων και καταχρήσεων[243].

---

[240] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 23.

[241] CEPS (Centre for European Policy Studies), Towards a principled level playing field for an open and secure online environment, σ. 46, διαθέσιμο: https://www.ceps.eu/ceps-publications/towards-a-principled-level-playing-field-for-an-open-and-secure-online-environment/

[242] Ό.π. CEPS, σ. 289.

[243] Jain et al., Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based clientside scanning, 2023, σ. 2318, διαθέσιμο: https://openreview.net/forum?id=CQbqeGAM_Ki και Hao et al., It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications, 2021, σ. 81, διαθέσιμο: https://www.usenix.org/system/files/sec22-jain.pdf

Με την επέκταση της τεχνολογίας από την παρακολούθηση στην πλευρά του διακομιστή στην παρακολούθηση στην πλευρά του πελάτη, δημιουργούνται νέες ευπάθειες για επιθέσεις στις συσκευές. Επιθέσεις μπορούν να εκπορεύονται από διάφορα σημεία, όπως από κυβερνήσεις ή μη κρατικούς δρώντες[244]. Επιπλέον, η ανίχνευση στην πλευρά του πελάτη ενέχει τον κίνδυνο κατάχρησης. Ενώ οι τεχνολογίες ανίχνευσης θα προγραμματίζονται να εντοπίζουν μόνο υλικό σεξουαλικής κακοποίησης παιδιών σε ορισμένες εφαρμογές που είναι εγκατεστημένες στη συσκευή (λ.χ. μόνο σε επικοινωνίες μέσω WhatsApp ή Facebook Messenger), υπάρχει κίνδυνος οι παράμετροι αυτές να τροποποιηθούν ώστε να παρακολουθούνται και άλλες εφαρμογές στη συσκευή[245].

Ακόμη, εμπειρογνώμονες έχουν επισημάνει ορισμένα ζητήματα που πιθανότατα θα προκύψουν από την εφαρμογή μεθόδων ανίχνευσης στην πλευρά του πελάτη (client-side scanning). Το βασικό εξ αυτών σχετίζεται με την εξεύρεση αξιόπιστου φορέα που θα επιφορτίζεται με την δημιουργία κώδικα για τις εφαρμογές ανίχνευσης στην πλευρά του πελάτη. Ο προσδιορισμός του κατάλληλου φορέα[246] ή του οργανισμού που θα αναπτύξει τον κώδικα είναι κρίσιμος, καθώς θα πρέπει να υπάρχει εμπιστοσύνη στην ακεραιότητα και την ασφάλεια του λογισμικού. Ένα ακόμη ζήτημα αφορά στον τρόπο ενημέρωσης αυτών των κωδίκων. Η διαρκής συντήρηση και ενημέρωση των εφαρμογών είναι απαραίτητη για την αντιμετώπιση νέων απειλών και για τη βελτίωση της τεχνολογίας. Επιπλέον, θα ήταν δύσκολο να περιοριστούν οποιαδήποτε μέτρα σχετικά με την κρυπτογράφηση μόνο στους χρήστες υπηρεσιών εντός της ΕΕ[247]. Ακόμη, οι εμπειρογνώμονες προειδοποιούν ότι η τεχνολογία εξελίσσεται γρήγορα, γεγονός που δεν συνεπάγεται μόνο την βελτίωση των εργαλείων ανίχνευσης, αλλά και την ανάπτυξη αποδοτικότερων μεθόδων παράκαμψης των εργαλείων αυτών από τους παραβάτες.

Η δεύτερη πιθανή λύση που προκρίθηκε από τους εμπειρογνώμονες είναι ο μερικός κατακερματισμός στη συσκευή, με αντιστοίχιση στον διακομιστή. Η λύση αυτή συνιστά μία προηγμένη μορφή της προηγούμενης, που προσφέρει τη δυνατότητα ανίχνευσης γνωστού υλικού. Η ειδοποιός της διαφορά εντοπίζεται στις διεργασίες πραγματοποίησης του αντιληπτικού κατακερματισμού, ο οποίος πραγματοποιείται σε δύο στάδια[248]. Το πρώτο στάδιο λαμβάνει χώρα στη συσκευή του χρήστη, όπου

---

[244] Levy, I. και Robinson, C., Thoughts on Child Safety on Commodity Platforms, 2022, σ. 35, διαθέσιμο: https://arxiv.org/pdf/2207.09506

[245] Client-Side Scanning And Winnie The-Pooh Redux (Plus Some Thoughts On Zoom), The Center for Internet and Society, διαθέσιμο: https://cyberlaw.stanford.edu/blog/2020/05/client-side-scanning-and-winnie-pooh-redux-plus-some-thoughts-zoom/

[246] Bartusek et al., End-to-End Secure Messaging with Traceability Only for Illegal Content, 2022, σ. 7, διαθέσιμο: https://eprint.iacr.org/2022/1643

[247] EDRi, Private and secure communications attacked by European Commission's latest proposal, διαθέσιμο: https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/

[248] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 23.

η συνάρτηση κατακερματισμού θα μπορούσε να καταστεί δημόσια μέσω τεχνικής αντίστροφης μηχανικής (reverse engineering), επιτρέποντας στους χρήστες να επαληθεύσουν την υπολογιστική διαδικασία. Η διεργασία αυτή υποστηρίζεται ότι θα συνέβαλε στην επίτευξη καθεστώτος διαφάνειας. Το δεύτερο στάδιο της λύσης αυτής πραγματοποιείται στον διακομιστή, όπου ο μερικός κατακερματισμός κατακερματίζεται εκ νέου με μια δεύτερη συνάρτηση και το αποτέλεσμα συγκρίνεται με τη βάση δεδομένων που περιέχει γνωστό περιεχόμενο. Το πλεονέκτημα αυτής της προσέγγισης είναι ότι το δεύτερο μέρος της διαδικασίας κατακερματισμού πραγματοποιείται στους διακομιστές, και επομένως μπορεί να παραμείνει μυστικό. Προσφέρεται επίσης αυξημένη διαφάνεια, καθώς ο χρήστης μπορεί να επαληθεύσει την υπολογιστική διαδικασία του μερικού κατακερματισμού.

Οι εμπειρογνώμονες που συνέβαλαν στην Εκτίμηση Επιπτώσεων για την Πρόταση[249] και οι ειδικοί που συνέπραξαν στην Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων[250], αντιμετωπίζουν με επιφύλαξη την λύση αυτή ως προς την αποτελεσματικότητά της, καθώς είναι πολύ πιο πρόσφατη από αυτήν του πλήρους κατακερματισμού στη συσκευή. Υποστηρίζουν ότι βρίσκεται ακόμη υπό ανάπτυξη και ότι τα επίπεδα ακρίβειας αυτής της τεχνολογίας δεν είναι υψηλά, οπότε δεν μπορεί να εφαρμοστεί στην πράξη. Επιπλέον, όλες οι ανησυχίες που εκφράστηκαν για τη λύση του πλήρους κατακερματισμού στη συσκευή ισχύουν και για αυτή τη λύση.

Η τρίτη πιθανή λύση που προκρίθηκε από τους εμπειρογνώμονες είναι η χρήση ασφαλών θυλάκων στους διακομιστές των παρόχων ηλεκτρονικών υπηρεσιών. Στην περίπτωση αυτή, το περιεχόμενο θα κρυπτογραφηθεί και θα αποσταλεί σε έναν διακομιστή για να αποκρυπτογραφηθεί μετέπειτα σε ασφαλές περιβάλλον[251]. Μόλις αποκρυπτογραφηθεί η επικοινωνία, είναι δυνατή η εκτέλεση όλων των λειτουργιών που εφαρμόζονται και σε επικοινωνίες που δεν είναι E2EE. Οι πάροχοι μπορούν να αποκτήσουν πρόσβαση στο περιεχόμενο στον ασφαλή θύλακα, να το κρυπτογραφήσουν και να το στείλουν όταν θεωρηθεί ασφαλές[252]. Ωστόσο, μέχρι σήμερα, καμία εταιρεία δεν έχει εφαρμόσει αυτή τη λύση για την ανίχνευση υλικού σεξουαλικής κακοποίησης παιδιών.

Οι εμπειρογνώμονες που αξιολόγησαν τις διάφορες λύσεις στο πλαίσιο της Έκθεσης Εκτίμησης Επιπτώσεων θεωρούν αυτή τη λύση υποσχόμενη, καθώς μπορεί να ανιχνεύσει τόσο γνωστό όσο και νέο υλικό[253]. Παρ' όλα αυτά, στο παρόν στάδιο υπάρχουν σημαντικές ανησυχίες ως προς την εφαρμοσιμότητα της λύσης αυτής, καθώς το απαιτούμενο υλικό και λογισμικό είναι λειτουργικά

[249] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 298.

[250] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 23.

[251] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 24.

[252] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 289.

[253] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 24.

περίπλοκα. Ως εκ τούτου, ελάχιστες εταιρείες μπορούν αυτή τη στιγμή να υλοποιήσουν τη λύση αυτή (για σκοπούς άλλους από την ανίχνευση του υλικού σεξουαλικής κακοποίησης παιδιών). Η υλοποίηση, μάλιστα, αυτής της λύσης από μικρότερους παρόχους πιθανότατα θα είναι δύσκολη ή ακόμα και μη ρεαλιστική.

Όσον αφορά στην ιδιωτικότητα, την ασφάλεια και τη διαφάνεια, οι ανησυχίες είναι παρόμοιες με εκείνες για τις λύσεις κατακερματισμού στη συσκευή. Υποστηρίζεται ότι ενώ η τεχνολογία αυτή δεν είναι απρόσβλητη, εντούτοις δύσκολα μπορεί να παρακαμφθεί. Οι πάροχοι υπηρεσιών της Κοινωνίας της Πληροφορίας μπορεί να δημιουργήσουν τροποποιημένους ασφαλείς θύλακες που δεν είναι δυνατόν να ανιχνευθούν από τους πελάτες. Στη συνέχεια, μπορούν να έχουν πλήρη πρόσβαση στην επικοινωνία μετά την αποκρυπτογράφησή της. Το Κέντρο της ΕΕ[254] που προβλέπεται να ιδρυθεί σύμφωνα με την Πρόταση θα μπορούσε, ενδεχομένως, να διαδραματίσει ρόλο στην προώθηση τέτοιων τεχνολογικών εξελίξεων. Παρόλα αυτά, για να προσφέρει προστιθέμενη αξία στις υπάρχουσες δραστηριότητες έρευνας και ανάπτυξης, θα απαιτούνταν επαρκής χρηματοδότηση για τις τεχνολογικές δραστηριότητές του.

Μερίδα παρόχων υπηρεσιών της Κοινωνίας της Πληροφορίας έχουν εκφράσει την άποψη ότι οι λύσεις που βασίζονται σε τεχνολογία μη E2EE έχουν μεγαλύτερη αναπτυξιακή δυναμική[255]. Παραδείγματα τέτοιων λύσεων περιλαμβάνουν την ανάλυση συμπεριφοράς και σημάτων δικτύου (network signals), ενώ πολλοί εμπειρογνώμονες έχουν τονίσει την ανάγκη ενδυνάμωσης των χρηστών υπηρεσιών διαδικτυακής επικοινωνίας ώστε να αναφέρουν περιεχόμενο που εντοπίζουν. Οι επακόλουθες έρευνες από τις αρχές επιβολής του νόμου θα μπορούσαν να βασιστούν σε μεταδεδομένα για να συνδέσουν αναφορές με ένα συγκεκριμένο δίκτυο. Σημειώνεται πάντως ότι τεχνολογικές λύσεις για τον εντοπισμό URL με υλικό σεξουαλικής κακοποίησης παιδιών σε επικοινωνίες E2EE χρησιμοποιούνται ήδη σήμερα[256]: για παράδειγμα, υπηρεσίες όπως το WhatsApp ή το Signal σαρώνουν τα URL ενός μηνύματος πριν αυτό κρυπτογραφηθεί, για ανεπιθύμητο περιεχόμενο και κακόβουλο λογισμικό, καθώς και για να εμφανίσουν στον χρήστη προεπισκόπηση της ιστοσελίδας στην οποία οδηγεί το URL.

Αξίζει να σημειωθεί ότι η συμμόρφωση με τις επιταγές της Πρότασης θα επηρεάσει το κίνητρο των παρόχων να καινοτομήσουν, καθώς επίσης και να αναπτύσσουν την επιχειρηματική τους δραστηριότητα στην ΕΕ[257]. Καθώς η συμμόρφωση με την Πρόταση ενδέχεται να προϋποθέτει την ανάπτυξη τεχνολογιών που επιτρέπουν την παρακολούθηση των E2EE επικοινωνιών σε έναν βαθμό,

---

[254] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 25.

[255] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 25.

[256] Ό.π. Έκθεση Εκτίμησης Επιπτώσεων, σ. 74.

[257] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 29.

ενδέχεται να περιοριστεί το κίνητρο των παρόχων να επενδύσουν στην περαιτέρω ανάπτυξη τέτοιου είδους τεχνολογίας, ιδιαίτερα εκείνων που προσφέρουν ως κύριο πλεονέκτημα στους πελάτες τους την προστασία της ιδιωτικότητας. Υπό αυτό το πρίσμα, υπάρχει αυξανόμενη αντίσταση[258], ιδίως από παρόχους λογισμικού, οι οποίοι έχουν έννομο συμφέρον να διασφαλίζουν την εμπιστοσύνη των χρηστών στην ασφάλεια και την αξιοπιστία των προϊόντων τους.

Τον Αύγουστο του 2021, η Apple ανακοίνωσε πρωτοβουλία της για την Ασφάλεια των Παιδιών, στην οποία περιλαμβανόταν η ανίχνευση γνωστού υλικού απευθείας στην συσκευή[259]. Η αναγνώριση και η αναφορά χρηστών iCloud που αποθηκεύουν γνωστό υλικό στους λογαριασμούς iCloud Photos τους, περιλάμβανε τα παρακάτω κατά σειρά βήματα. Πρώτο βήμα θα αποτελούσε η σάρωση της εικόνας στην συσκευή, με χρήση μιας βάσης δεδομένων γνωστών κατακερματισμένων εικόνων σεξουαλικής κακοποίησης παιδιών του NCMEC (Εθνικό Κέντρο για τα Αγνοούμενα και Εκμεταλλευόμενα Παιδιά), με συνακόλουθη μετατροπή της βάσης δεδομένων σε ένα ακατάληπτο σύνολο κατακερματισμένων τιμών που αποθηκεύεται με ασφάλεια στις συσκευές των χρηστών. Κατόπιν, θα λάμβανε χώρα ανάλυση εικόνας και μετατροπή της σε έναν μοναδικό αριθμό, με συνακόλουθη κωδικοποίηση ενός "safety voucher" (πιστοποιητικού ασφαλείας) που περιέχει το αποτέλεσμα της αντιστοίχισης, το οποίο θα μεταφορτωνόταν στο iCloud Photos μαζί με την εικόνα.

Στη συνέχεια, με χρήση μιας άλλης τεχνολογίας που ονομάζεται “threshold secret sharing”, το σύστημα θα εξασφάλιζε ότι το περιεχόμενο των safety vouchers δεν μπορεί να ερμηνευτεί από την Apple, εκτός αν ο λογαριασμός iCloud Photos υπερβεί ένα κατώφλι γνωστού περιεχομένου. Το κατώφλι επιλέχθηκε έτσι ώστε να παρέχει μια εξαιρετικά χαμηλή πιθανότητα (1 στα 1 τρισεκατομμύριο) να επισημανθεί λανθασμένα ένας λογαριασμός. Ο σχετικός κίνδυνος θα μειωνόταν περαιτέρω μέσω μιας διαδικασίας χειροκίνητης ανασκόπησης, κατά την οποία η Apple θα έλεγχε κάθε αναφορά για να επιβεβαιώσει την ύπαρξη αντιστοίχισης, να απενεργοποιήσει τον λογαριασμό του χρήστη και να στείλει μια αναφορά στο NCMEC. Η ακολουθία αυτή συνιστούσε μία προσέγγιση που θα στόχευε στην ανίχνευση υλικού με σεβασμό στην ιδιωτικότητα του χρήστη και θα ελαχιστοποιούσε τις περιπτώσεις λανθασμένων αναφορών.

Ωστόσο, τον Σεπτέμβριο του 2021, η Apple ανακοίνωσε ότι η υλοποίηση αυτής της λύσης θα καθυστερούσε, προκειμένου να συγκεντρωθούν επιπλέον σχόλια οργανώσεων για την προστασία της ιδιωτικότητας και ερευνητών, πριν από την κυκλοφορία της, λόγω κριτικής που είχε δεχθεί. Έκτοτε, η Apple έχει υλοποιήσει την ανίχνευση εικόνων που περιέχουν γυμνό και αποστέλλονται ή

---

[258] Meredith Whittacker, New Branding, Same Scanning: “Upload Moderation” Undermines End-to-End Encryption, διαθέσιμο: https://signal.org/blog/pdfs/upload-moderation.pdf

[259] Apple, CSAM Detection, Technical Summary, August 2021, διαθέσιμο: https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

λαμβάνονται από παιδιά, μέσω ανάλυσης στην ίδια τη συσκευή για τις εισερχόμενες και εξερχόμενες εικόνες, παρέχοντας μια προειδοποίηση στα παιδιά να μην τις δουν ή να μην τις στείλουν. Όταν αποστέλλουν ή λαμβάνουν τέτοιες εικόνες, τα παιδιά έχουν τη δυνατότητα να ειδοποιήσουν κάποιον που εμπιστεύονται και να ζητήσουν βοήθεια[260].

Η WhatsApp της Meta, η οποία χρησιμοποιεί κρυπτογράφηση E2EE, έχει επίσης εφαρμόσει εργαλεία για την αναγνώριση υλικού σεξουαλικής κακοποίησης στην υπηρεσία μηνυμάτων της, βασισμένα σε μη κρυπτογραφημένα δεδομένα που σχετίζονται με την επικοινωνία[261]. Ωστόσο, η Meta έχει αναγνωρίσει και τους περιορισμούς των τωρινών εργαλείων ανίχνευσής της σε δημόσιες ακροάσεις της αμερικανικής κυβέρνησης, δηλώνοντας ότι αναμένει χαμηλότερους αριθμούς ανίχνευσης σε σχέση με τις μη κρυπτογραφημένες επικοινωνίες[262].

5.3.3. ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ E2EE ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Το ζήτημα της E2EE κρυπτογράφησης απασχόλησε ιδιαίτερα την ΕΣΠΔ και ΕΕΠΔ στην Κοινή τους Γνωμοδότηση επί των διατάξεων της Πρότασης. Σημειώνουν ειδικότερα ότι, η αποθάρρυνση της χρήσης E2EE με οποιονδήποτε τρόπο στο πλαίσιο των διαπροσωπικών επικοινωνιών, η επιβολή στους παρόχους υπηρεσιών υποχρέωσης επεξεργασίας δεδομένων ηλεκτρονικών επικοινωνιών για σκοπούς άλλους από την παροχή των υπηρεσιών τους, ή η υποχρέωσή τους να προωθούν ηλεκτρονικές επικοινωνίες σε τρίτους, θα είχε ως αποτέλεσμα οι πάροχοι να προσφέρουν λιγότερο κρυπτογραφημένες υπηρεσίες για να συμμορφωθούν καλύτερα με τις υποχρεώσεις τους, εξασθενίζοντας έτσι τον ρόλο της κρυπτογράφησης γενικά και υπονομεύοντας τον σεβασμό των θεμελιωδών δικαιωμάτων των Ευρωπαίων πολιτών[263]. Η ανάπτυξη εργαλείων για την παρέμβαση και ανάλυση διαπροσωπικών ηλεκτρονικών επικοινωνιών είναι θεμελιωδώς αντίθετη με την E2EE, καθώς η τελευταία στοχεύει να εγγυηθεί τεχνικά ότι μια επικοινωνία παραμένει εμπιστευτική μεταξύ του αποστολέα και του παραλήπτη.

Ως εκ τούτου, ΕΣΠΔ και ΕΕΠΔ κρίνουν ότι μολονότι η Πρόταση δεν καθιερώνει υποχρέωση συστηματικής παρέμβασης για τους παρόχους (μέσω ενσωμάτωσης κάποιας κερκόπορτας που ανοίγει με «ειδικό κλειδί» αποκρυπτογράφησης που έχει στη διάθεσή του ο πάροχος για «εξαιρετικές

---

[260] Cnet, Apple to beta test iMessage feature that warns kids about nude imagery, διαθέσιμο: https://www.cnet.com/tech/mobile/apple-to-beta-test-imessage-feature-that-warns-kids-about-nude-imagery/

[261] Whatsapp, How WhatsApp Helps Fight Child Exploitation, διαθέσιμο: https://faq.whatsapp.com/5704021823023684/?locale=en_US

[262] Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, διαθέσιμο: https://www.wired.com/story/whatsapp-encryption-child-abuse/

[263] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 27.

περιπτώσεις»), η απλή πιθανότητα έκδοσης εντολής ανίχνευσης ενδέχεται να επηρεάσει σημαντικά τις τεχνικές επιλογές που θα κάνουν οι πάροχοι, ειδικά δεδομένου του περιορισμένου χρονικού πλαισίου που θα έχουν για να συμμορφωθούν με αυτή την εντολή και των επιπτώσεων που θα αντιμετωπίσουν αν δεν το πράξουν[264]. Στην πράξη, αυτό μπορεί να οδηγήσει ορισμένους παρόχους να σταματήσουν να χρησιμοποιούν Ε2ΕΕ.

Επισημαίνουν επιπλέον ότι κάθε μία από τις τεχνικές για την παράκαμψη της προστατευτικής φύσης της ιδιωτικότητας της Ε2ΕΕ θα δημιουργούσε κενά ασφαλείας. Για παράδειγμα, η ανίχνευση στην πλευρά του πελάτη θα οδηγούσε πιθανότατα σε σημαντική, αδιάκριτη πρόσβαση και επεξεργασία μη κρυπτογραφημένου περιεχομένου στις συσκευές των τελικών χρηστών[265]. Μια τέτοια σημαντική υποβάθμιση της εμπιστευτικότητας θα επηρέαζε ιδιαίτερα τα παιδιά, καθώς οι υπηρεσίες που χρησιμοποιούν είναι πιο πιθανό να υπόκεινται σε εντολές ανίχνευσης, καθιστώντας τα ευάλωτα σε παρακολούθηση ή υποκλοπή. Ταυτόχρονα, η ανίχνευση στην πλευρά του διακομιστή είναι επίσης θεμελιωδώς ασύμβατη με την Ε2ΕΕ, καθώς το κρυπτογραφημένο κανάλι επικοινωνίας μεταξύ των χρηστών θα πρέπει να σπάσει, οδηγώντας έτσι σε μαζική επεξεργασία προσωπικών δεδομένων στους διακομιστές των παρόχων.

Ενώ η Πρόταση αναφέρει ότι «αφήνει στον οικείο πάροχο την επιλογή των τεχνολογιών που θα χρησιμοποιηθούν για την αποτελεσματική συμμόρφωση με τις εντολές εντοπισμού και δεν θα πρέπει να θεωρείται ότι ενθαρρύνει ή αποθαρρύνει τη χρήση οποιασδήποτε τεχνολογίας»[266], η δομική ασυμβατότητα ορισμένων εντολών ανίχνευσης με την Ε2ΕΕ καθίσταται στην πράξη ισχυρό αποτρεπτικό στοιχείο για τη χρήση της Ε2ΕΕ. Η αδυναμία πρόσβασης και χρήσης υπηρεσιών που χρησιμοποιούν Ε2ΕΕ θα μπορούσε να έχει αποτρεπτική επίδραση στην ελευθερία της έκφρασης και στη νόμιμη ιδιωτική χρήση υπηρεσιών ηλεκτρονικής επικοινωνίας[267]. Η αμοιβαία αποκλειόμενη σχέση μεταξύ της ανίχνευσης υλικού παιδικής σεξουαλικής κακοποίησης και της Ε2ΕΕ αναγνωρίζεται επίσης από την Επιτροπή, όταν επισημαίνει στην Έκθεση Εκτίμησης Επιπτώσεων ότι η εφαρμογή της Ε2ΕΕ από το Facebook το 2023 θα μπορούσε να οδηγήσει στο τέλος της εθελοντικής σάρωσης στις υπηρεσίες του. Εν κατακλείδι, ΕΣΠΔ και ΕΕΠΔ θεωρούν ότι οι όροι εφαρμογής της Πρότασης θα πρέπει να δηλώνουν ξεκάθαρα ότι τίποτα στον προτεινόμενο Κανονισμό δεν θα πρέπει να ερμηνεύεται ως απαγόρευση ή εξασθένηση της κρυπτογράφησης, σύμφωνα με όσα αναφέρονται στην σκέψη 25 του Προοιμίου του Προσωρινού Κανονισμού. Και τούτο με σκοπό να διασφαλιστεί ότι

[264] Ό.π.

[265] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 28.

[266] Ό.π. Πρόταση, Σκ. 26.

[267] Ό.π. Κοινή Γνωμοδότηση 4/2022, σελ. 28.

η Πρόταση δεν πρόκειται να υπονομεύσει την ασφάλεια ή την εμπιστευτικότητα των ηλεκτρονικών επικοινωνιών των Ευρωπαίων πολιτών.

Αναφορικά με την διατερματική κρυπτογράφηση, προβληματισμοί έχουν εγερθεί και από πλευράς παρόχων υποδομών υπολογιστικού νέφους στην Ευρώπη. Ειδικότερα, η Ένωση CISPE (Cloud Infrastructure Services Providers in Europe) έχει επισημάνει[268] ότι οι υποδομές υπολογιστικού νέφους (cloud) θα πρέπει να αντιμετωπίζονται αναλογικά με τη θέση τους στην τεχνολογική αλυσίδα, ώστε να διασφαλίζεται μία αναλογική συνεισφορά τους στη μάχη ενάντια στο διακινούμενο υλικό σεξουαλικής κακοποίησης παιδιών. Ειδικότερα, η Ένωση επισημαίνει ότι οι πάροχοι υποδομών cloud παρέχουν τη δυνατότητα στους πελάτες τους να χρησιμοποιούν και να ελέγχουν την κρυπτογράφηση, όπως επιθυμούν. Τονίζουν ότι η απαίτηση από τους παρόχους να δημιουργούν αδυναμίες στα προϊόντα και τις υπηρεσίες τους θα υπονόμευε την ασφάλεια και την ιδιωτικότητα των δεδομένων των πελατών και προτείνουν να εισαχθεί ρύθμιση που θα διασφαλίζει ότι οι πάροχοι δεν θα υποχρεούνται να υπονομεύουν την κρυπτογράφηση προκειμένου να συμμορφωθούν με μια εντολή ανίχνευσης.

5.3.4. ΕΝΤΟΠΙΣΜΟΣ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ ΜΕ ΧΡΗΣΗ ΜΕΤΑΔΕΔΟΜΕΝΩΝ

Εκτός των μεθόδων αξιολόγησης καθαυτού του περιεχομένου, έχουν αναπτυχθεί εναλλακτικοί τρόποι ανίχνευσης υλικού παιδικής σεξουαλικής κακοποίησης με χρήση μεταδεδομένων. Συγκεκριμένα, έχει προταθεί μία μέθοδος ανίχνευσης τέτοιου είδους υλικού στο διαδίκτυο με χρήση μοντέλων μηχανικής μάθησης, τα οποία έχουν εκπαιδευτεί με βάση διαδρομές αρχείων (file paths)[269]. Σε σχετική έρευνα που πραγματοποιήθηκε[270], οι διαδρομές αρχείων εξήχθησαν από πραγματικό σύνολο δεδομένων με περισσότερες από 1 εκατομμύριο διαδρομές αρχείων οι οποίες είχαν συλλεγεί στο πλαίσιο ποινικής διερεύνησης εγκλημάτων. Το μοντέλο αυτό παρουσίασε ψευδώς θετικό ποσοστό 0,002 όταν αξιολογήθηκε σε διαδρομές αρχείων κοινών δεδομένων που προέκυψαν κατόπιν

---

[268] CISPE, CISPE position paper on the European Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse ("CSA"), διαθέσιμο: https://cispe.cloud/website_cispe/wp-content/uploads/2022/10/CISPE-CSAM-position-paper-06-09-22.pdf

[269] «Μια διαδρομή αρχείου περιγράφει τη θέση ενός αρχείου στη δομή φακέλων μιας τοποθεσίας web», W3schools, διαθέσιμο: https://www.w3schools.com/html/html_filepaths.asp#:~:text=HTML%20File%20Paths-,A%20file%20path%20describes%20the%20location%20of%20a%20file%20in,Images

[270] Hee-Eun Lee et al., Detecting child sexual abuse material: A comprehensive survey, διαθέσιμο: https://www.sciencedirect.com/science/article/abs/pii/S2666281720301554?casa_token=D75TTQhANbwAAAAA:GmQLmNLY1SYjYyYQ9gO8cwFM-zcK6rwTKPFvo2b6bClUMusy5GtAhFJSfmwN17hhzYCgYs8

ανίχνευσης του παγκόσμιου ιστού, κάτι που καταδεικνύει την υψηλή λειτουργικότητα του μοντέλου σε διακριτές κατανομές δεδομένων.

Στην πράξη, τέτοιου είδους μοντέλα μηχανικής μάθησης προβαίνουν σε ανάλυση διαδρομών και ονομάτων αρχείων από συστήματα αποθήκευσης αρχείων προκειμένου να προσδιορίσουν την πιθανότητα ένα αρχείο να περιλαμβάνει σεξουαλική κακοποίηση παιδιών. Δοθέντος ότι έχει εντοπιστεί ότι οι δράστες τέτοιων αδικημάτων χρησιμοποιούν συγκεκριμένο λεξιλόγιο για να ονοματίσουν αρχεία[271], θεωρείται ότι ο έλεγχος διαδρομών αρχείων, που συνδυάζει έλεγχο θέσης και ονόματος αρχείου, αποτελεί μία σημαντική πρακτική για τον εντοπισμό παράνομου υλικού, με παράλληλη αποφυγή άμεσης επαφής με το περιεχόμενο. Μία τέτοια μέθοδος εντοπισμού θα μπορούσε να συνιστά ένα λιγότερο παρεμβατικό μέτρο στα θεμελιώδη δικαιώματα των χρηστών και ένα εξίσου αποτελεσματικό μέτρο με τα προβλεπόμενα στην Πρόταση. Προκειμένου ωστόσο να οδηγηθούμε σε ένα ασφαλές συμπέρασμα ως προς αυτό, ο τομέας αυτός χρήζει επισταμένης έρευνας.

Παρά το γεγονός ότι η Πρόταση δεν κάνει λόγο για κρυπτογραφημένες επικοινωνίες, έχει υποστηριχθεί ότι διερεύνηση για ύπαρξη υλικού παιδικής σεξουαλικής κακοποίησης σε κρυπτογραφημένα περιβάλλοντα μπορεί να διενεργηθεί με ανάλυση μεταδεδομένων χωρίς να συντελείται υπέρμετρη παρέμβαση στα θεμελιώδη δικαιώματα. Η ανάλυση μεταδεδομένων που αφορούν σε κρυπτογραφημένο μήνυμα με χρήση τεχνικών μηχανικής μάθησης μπορούν να συμβάλουν στην πρόβλεψη του βαθμού που ένας συγκεκριμένος χρήστης μοιράζεται προβληματικό περιεχόμενο σε μία υπηρεσία με κρυπτογράφηση από άκρο σε άκρο. Για παράδειγμα, η ανάλυση μη κρυπτογραφημένων δεδομένων, όπως μία φωτογραφία προφίλ ή περιγραφή μίας ομαδικής συνομιλίας, με την μέθοδο της ταξινόμησης μέσω μηχανικής μάθησης, μπορεί να συμβάλει στον εντοπισμό λογαριασμών που εμπλέκονται στη διανομή υλικού σεξουαλικής κακοποίησης παιδιών σε υπηρεσίες που εφαρμόζουν διατερματική κρυπτογράφηση[272].

Συνακόλουθα, με χρήση τέτοιων τεχνικών μπορούν να εκπαιδευτούν μοντέλα συμπεριφοράς χρηστών που έχουν μπλοκαριστεί από μία υπηρεσία που προσφέρει κρυπτογράφηση από άκρο σε άκρο, μέσω αξιοποίησης των χρησιμοποιούμενων πρακτικών δημιουργίας προφίλ ή του πλήθους αναφορών από άλλους χρήστες για προβληματικό περιεχόμενο. Ενδεχομένως η εντολή εντοπισμού τέτοιου είδους περιεχομένου σε ήδη επισημασμένο ως ύποπτο λογαριασμό, με παράλληλη χρήση μεταδεδομένων, να μπορούσε να αποτελέσει ένα στοχευμένο και όχι γενικευμένης φύσεως μέτρο.

---

[271] Claudia Peersman et al., Live forensics to reveal previously unknown criminal media on p2p networks. Digital Investigation, διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S1742287616300779

[272] Σύμφωνα με το WhatsApp, περισσότεροι από 300.000 λογαριασμοί μπλοκάρονται μηνιαίως για ύποπτη κοινή χρήση υλικού παιδικής σεξουαλικής κακοποίησης, χρησιμοποιώντας τέτοιου είδους προσεγγίσεις, Whatsapp, "How WhatsApp Helps Fight Child Exploitation", διαθέσιμο: https://faq.whatsapp.com/5704021823023684/?locale=en_US

Και σε αυτή τη μέθοδο διερεύνησης ωστόσο έχουν εντοπιστεί αδύναμα σημεία. Ένα από αυτά είναι το γεγονός ότι η επισήμανση περιεχομένου ως μηνύματος προωθημένου αρκετές φορές δεν καταδεικνύει απαραίτητα περιεχόμενο ύποπτο, αλλά ενδεχομένως απλώς ενδιαφέρον[273]. Επιπλέον, η πρόσβαση στα μεταδεδομένα από πλευράς παρόχων, παρόλο που δεν συνιστά πρόσβαση στην ουσία του περιεχομένου, ενδέχεται να οδηγήσει στην αποκάλυψη της ταυτότητας του αποστολέα ή του παραλήπτη. Δοθέντος μάλιστα ότι η δημιουργία προφίλ χρήστη από άλλους απλούς χρήστες είναι εξορισμού ευχερής με χρήση δημόσια διαθέσιμων δεδομένων των χρηστών[274], επί παραδείγματι μέσω της χρήσης μεταδεδομένων για σκοπούς παρακολούθησης μοτίβων χρήσης των πλατφορμών ή ανίχνευσης προσωπικότητας, και δεδομένου ότι τέτοιου είδους πρακτικές συνιστούν παρέμβαση στο δικαίωμα των χρηστών στην ιδιωτικότητα, απαιτείται προσοχή στον τρόπο υιοθέτησης μέτρων ανίχνευσης περιεχομένου από πλευράς παρόχου που διακινείται μέσω διαπροσωπικών επικοινωνιών. Η ανάλυση ωστόσο των μεταδεδομένων που περιορίζεται επί παραδείγματι σε μία εγκατεστημένη στην συσκευή του ίδιου του χρήστη εφαρμογή και δεν αποθηκεύει ή αποστέλλει αποκρυπτογραφημένα μηνύματα, υποστηρίζεται ότι μπορεί να θωρακίσει το απόρρητο και να συνεχίσει να τηρεί τις εγγυήσεις της E2EE[275].

Υπέρμαχοι πάντως της διατήρησης της διατερματικής κρυπτογράφησης υποστηρίζουν ότι η καλύτερη μέθοδος αντιμετώπισης τέτοιου είδους περιεχομένου, ο διαμοιρασμός του οποίου πραγματοποιείται μέσω κρυπτογραφημένων επικοινωνιών, συνίσταται στην υιοθέτηση παραδοσιακών συστημάτων αυτορρύθμισης των πλατφορμών[276] που εκκινούν από αναφορές χρηστών και μετέπειτα ανάλυση μεταδεδομένων, χωρίς να απαιτείται η επέμβαση διαχειριστών περιεχομένου[277]. Κάτι τέτοιο ωστόσο δεν θα επέλυε το ζήτημα διαμοιρασμού υλικού παιδικής σεξουαλικής κακοποίησης μεταξύ δύο χρηστών που διαπράττουν ως συναυτουργοί ή ως συνεργοί τα σχετικά αδικήματα μέσω E2EE περιβάλλοντος. Αξίζει να αναφερθεί, ότι στην Έκθεση Εκτίμησης Επιπτώσεων της Πρότασης περιλαμβάνεται απλώς η αναφορά ότι οι πάροχοι δεν θεωρούν τη χρήση μεταδεδομένων ένα

---

[273] Ό.π. Whatsapp.

[274] L. Mitrou et al, Social Media Profiling: a Panopticon or Omniopticon tool?, 2014, διαθέσιμο: https://api.semanticscholar.org/CorpusID:49362390

[275] Seny Kamara et al., Outside looking in approaches to content moderation in end-to-end encrypted systems, διαθέσιμο: https://www.researchgate.net/publication/358488067_Outside_Looking_In_Approaches_to_Content_Moderation_in_End-to-End_Encrypted_Systems

[276] Murdoch Watney, Law Enforcement Access to End-to-End Encrypted Social Media Communications, διαθέσιμο: https://books.google.gr/books?hl=en&lr=&id=FCAEEAAAQBAJ&oi=fnd&pg=PA322&dq=info:W1NNBcUZG_0J:scholar.google.com&ots=UiL-vtuyHh&sig=ei020OFYBmIja9x8mksi53YjBQ&redir_esc=y#v=onepage&q&f=false

[277] Bleakley Paul et al., Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed?, European Journal of Criminology, 2023, διαθέσιμο: https://doi.org/10.1177/147737082311813

αποτελεσματικό εργαλείο εντοπισμού τέτοιου υλικού[278], ενώ παράλληλα η χρήση μεταδεδομένων αναφέρεται ως ανεπαρκής πρακτική για την εκκίνηση διαδικασιών έρευνας[279].

Ανάλογα τον τύπο των υπηρεσιών της Κοινωνίας της Πληροφορίας που αφορά η εκάστοτε εντολή ανίχνευσης, ενδέχεται να διενεργείται παρακολούθηση τόσο των δεδομένων κυκλοφορίας και τοποθεσίας (traffic and location data), όσο και του περιεχομένου των διαπροσωπικών επικοινωνιών[280]. Το Δικαστήριο της Ευρωπαϊκής Ένωσης έχει κρίνει σε διάφορες υποθέσεις ότι η διατήρηση και ανάλυση, τόσο των δεδομένων κυκλοφορίας και τοποθεσίας (μεταδεδομένα)[281], όσο και των δεδομένων περιεχομένου[282] από τις κρατικές αρχές εμπίπτει στο πεδίο εφαρμογής του Άρθρου 7 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Και τούτο διότι, όπως τονίστηκε και στην Digital Rights Ireland[283], η διατήρηση ακόμη και των δεδομένων κυκλοφορίας και τοποθεσίας επιτρέπει την εξαγωγή εξαιρετικά ακριβών συμπερασμάτων σχετικά με την ιδιωτική ζωή των ατόμων των οποίων τα δεδομένα διατηρούνται. Συνεπώς, η συλλογή μεταδεδομένων συνιστά παρέμβαση στο δικαίωμα του άρθρου 7 του ΧΘΔΕ. Ωστόσο, μπορεί να υποστηριχθεί ότι τα μέτρα της Πρότασης για την καταπολέμηση του υλικού σεξουαλικής κακοποίησης παιδιών, τα οποία απευθύνονται σε υπηρεσίες της κοινωνίας της πληροφορίας και περιλαμβάνουν την παρακολούθηση του περιεχομένου των επικοινωνιών, θα μπορούσαν να συνιστούν ακόμη σοβαρότερη παρέμβαση στο εν λόγω δικαίωμα και πολύ πιθανόν να παραβίαζαν την ίδια την ουσία του δικαιώματος.

5.3.5. ΔΙΑΜΟΙΡΑΣΜΟΣ ΣΥΝΑΙΝΕΤΙΚΟΥ ΥΛΙΚΟΥ ΣΕΞΟΥΑΛΙΚΗΣ ΦΥΣΗΣ ΜΕΤΑΞΥ ΕΦΗΒΩΝ ΧΡΗΣΤΩΝ

Ζήτημα επίσης αποτελεί ο τρόπος με τον οποίο θα αντιμετωπιστεί υλικό σεξουαλικού περιεχομένου παραγόμενο και διαμοιραζόμενο συναινετικά από τους ίδιους τους ανηλίκους, στα πλαίσια εξερεύνησης της σεξουαλικότητάς τους. Η αξιολόγηση μίας εικόνας χωρίς πρόσθετα στοιχεία δεν οδηγεί πάντοτε σε ασφαλή συμπεράσματα ως προς το αν πρόκειται για σεξουαλική κακοποίηση ή για

[278] Pfefferkorn, R., Stanford Internet Observatory, 2021, σελ. 10, διαθέσιμο: https://doi.org/10.54501/jots.v1i2.14

[279] WeProtect Global Alliance to end child sexual exploitation online, Global Threat Assessment, 2021, διαθέσιμο: https://www.weprotect.org/global-threat-assessment-21/#report

[280] Ό.π. Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων, σ. 38.

[281] Βλ. υποθέσεις Digital Rights Ireland και Tele2 Sverige.

[282] Βλ. υπόθεση Schrems.

[283] Ό.π.

συναινετική σεξουαλική πράξη εφήβου, πόσο μάλλον όταν η τεχνολογία που χρησιμοποιείται για τον εντοπισμό νέου υλικού ή άγρας παιδιών δεν διακρίνει μεταξύ συναινετικών και μη συναινετικών εικόνων ή συνομιλιών[284]. Γεννάται λοιπόν το ερώτημα με ποιον τρόπο θα μπορούσε η Πρόταση να αντιμετωπίσει τέτοιου είδους περιεχόμενο, καθώς επίσης και να συμβάλει στην αξιολόγηση επικοινωνιών που θα εντοπίζονται στα πλαίσια εντολής ανίχνευσης άγρας παιδιών, θα αποτυπώνουν ωστόσο συναινετικές συνομιλίες εφήβων σεξουαλικού περιεχομένου.

Το ζήτημα περιπλέκεται περισσότερο αν ληφθεί υπόψη ότι το Κέντρο της ΕΕ δεν εξουσιοδοτείται να αποκλείσει τέτοιου είδους περιεχόμενο από την κατηγορία υλικού παιδικής σεξουαλικής κακοποίησης, καθώς εφαρμόζει τους ορισμούς της Οδηγίας 2011/93/ΕΕ[285]. Εναπόκειται στην ευχέρεια των κρατών μελών να προχωρήσουν στην ποινικοποίηση της παραγωγής, της απόκτησης ή της κατοχής υλικού στο οποίο απεικονίζονται παιδιά πέραν του ηλικιακού ορίου της σεξουαλικής συναίνεσης, με την προϋπόθεση ότι η παραγωγή και η κατοχή του εν λόγω υλικού πραγματοποιήθηκε με τη συναίνεση των παιδιών και μόνο για σκοπούς ιδίας χρήσης από τα συγκεκριμένα πρόσωπα, στον βαθμό που οι αποτυπωνόμενες πράξεις δεν περιλαμβάνουν κακοποίηση[286]. Αξίζει να επισημανθεί ότι μονάχα ελάχιστα κράτη έχουν αποποινικοποιήσει ορισμένες συναινετικές σεξουαλικές δραστηριότητες μεταξύ εφήβων[287]. Η εξέταση, πάντως, του εν λόγω ζητήματος συμπαρασύρει και ζητήματα παραβίασης των δεδομένων προσωπικού χαρακτήρα των παιδιών, ενώ ταυτόχρονα η αδιάκριτη έκθεση της σεξουαλικότητάς τους ενδέχεται να συνιστά παραβίαση του δικαιώματος στο σεβασμό της ιδιωτικής ζωής[288].

Ο περιορισμός αυτών των δικαιωμάτων μπορεί να έχει επιπτώσεις στην προσωπική ανάπτυξη των παιδιών και στον ασφαλή χώρο τους για να εξελιχθούν, ενώ παράλληλα ενδέχεται να περιοριστούν τα δικαιώματά τους ως χρηστών διαδικτυακών υπηρεσιών, και ειδικότερα του δικαιώματος στην προστασία των προσωπικών δεδομένων[289] και στην ελευθερία της έκφρασης[290][291]. Στο απυρόβλητο δεν μένει φυσικά και το δικαίωμα του άρθρου 24 του ΧΘΔΕ, το οποίο κατοχυρώνει ειδική προστασία στα δικαιώματα του παιδιού, ενσωματώνοντας θεμελιώδεις αρχές της διεθνούς σύμβασης του ΟΗΕ για

---

[284] Ό.π. Expert Workshop, ενότητα 4.3., σελ.19.

[285] Ό.π. πρόταση, άρθρο 2 (ιβ): «υλικό σεξουαλικής κακοποίησης παιδιών»: υλικό που συνιστά παιδική πορνογραφία ή πορνογραφική παράσταση, κατά το άρθρο 2 στοιχεία γ) και ε), αντίστοιχα, της οδηγίας 2011/93/ΕΕ.

[286] Ό.π. Οδηγία 2011/93/ΕΕ, άρθρο 8 παρ. 3.

[287] Ό.π. Expert Workshop, ενότητα 4.1., σελ. 21.

[288] ΧΘΔΕ, άρθρο 7.

[289] ΧΘΔΕ, άρθρο 8.

[290] ΧΘΔΕ, άρθρο 11.

[291] Ό.π. Συμπληρωματική, σ. 34.

τα δικαιώματά του. Συγκεκριμένα, τα προτεινόμενα μέτρα ενδέχεται να επηρεάσουν την ικανότητα των παιδιών να διαμορφώσουν την ταυτότητά τους, ενώ το αίσθημα ότι παρακολουθούνται μπορεί να τα οδηγήσει σε αυτολογοκρισία, λόγω ανησυχιών σχετικά με σεξουαλικό περιεχόμενο και ενδεχόμενη προσέγγιση από τρίτους[292]. Το ίδιο πνεύμα αντικατοπτρίζεται και στην Συμπληρωματική Έκθεση, όπου αναγνωρίζεται η ανάγκη προστασίας των παιδιών από την σεξουαλική κακοποίηση, τονίζεται όμως παράλληλα η επιταγή να μπορούν να απολαμβάνουν τα θεμελιώδη δικαιώματά τους, ως βάση για την ανάπτυξη και τη μετάβασή τους στην ενήλικη ζωή[293].

6. ΣΥΝΟΛΙΚΗ ΘΕΩΡΗΣΗ ΚΑΙ ΚΡΙΤΙΚΗ ΑΠΟΤΙΜΗΣΗ ΤΗΣ ΠΡΟΤΑΣΗΣ

Σε γενικές γραμμές, το ΕΣΠΔ και ο ΕΕΠΔ εκφράζουν ιδιαίτερο προβληματισμό και ανησυχία αναφορικά με την αναγκαιότητα και την αναλογικότητα των προβλεπόμενων μέτρων για τον εντοπισμό νέου υλικού σεξουαλικής κακοποίησης και περιστατικών άγρας παιδιών. Υπογραμμίζουν ότι τα εν λόγω μέτρα καταρχήν συνεπάγονται δυνητικά γενικευμένη πρόσβαση σε περιεχόμενο επικοινωνιών και όχι στοχευμένη, βασιζόμενη πρακτικά σε τεχνολογίες που σημειώνουν προς στιγμήν σημαντικά ποσοστά σφάλματος. Επισημαίνουν μάλιστα ότι, με βάση τη νομολογία του ΔΕΕ, μέτρα που επιτρέπουν στις αρχές επιβολής του νόμου γενικευμένη πρόσβαση στο περιεχόμενο των επικοινωνιών είναι πιθανόν να θίξουν το βασικό περιεχόμενο των δικαιωμάτων που κατοχυρώνονται στα άρθρα 7 και 8 του ΧΘΔΕ[294].

Αναλύοντας την χρήση λιγότερο παρεμβατικών μέτρων, προτείνουν μία βελτιωτική τροποποίηση της κατασκευής του άρθρου 4 της Πρότασης, στο οποίο προβλέπεται η λήψη μέτρων μετριασμού του κινδύνου κατάχρησης των υπηρεσιών για σκοπούς διαδικτυακής σεξουαλικής κακοποίησης παιδιών, στάδιο που προηγείται της δυνατότητας έκδοσης εντολής εντοπισμού. Συγκεκριμένα, τονίζουν ότι αν ένα λιγότερο παρεμβατικό μέτρο μετριασμού του κινδύνου δεν τίθεται σε εφαρμογή οικειοθελώς από πλευράς παρόχου[295], τότε δεν θα πρέπει εκδίδεται απευθείας εντολή εντοπισμού, αλλά θα πρέπει να εξουσιοδοτείται η εκάστοτε αρμόδια ανεξάρτητη διοικητική ή δικαστική αρχή να καθιστά την εφαρμογή των μέτρων μετριασμού υποχρεωτική για τους παρόχους[296].

---

[292] Powell et al., Child Protection and Freedom of Expression Online, 2010, σ. 3, διαθέσιμο: https://www.oii.ox.ac.uk/wp-content/uploads/old-docs/FD17.pdf

[293] Ό.π. Συμπληρωματική, σ. 39.

[294] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 27.

[295] Φερ' ειπείν η παρεμπόδιση μετάδοσης γνωστού υλικού από πλευράς πελάτη, με αποτροπή αναφόρτωσής του και εκ νέου αποστολής.

[296] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 21.

Αναφορικά με το πεδίο εφαρμογής των εντολών εντοπισμού, ΕΣΠΔ και ΕΕΠΔ διατυπώνουν την άποψη ότι η δυνατότητα έκδοσης σχετικής εντολής εντοπισμού σε μία ολόκληρη υπηρεσία, καθώς επίσης και η προβλεπόμενη ανώτατη διάρκεια εφαρμογής της, μπορεί να καταστήσουν το πεδίο εφαρμογής της εντολής αρκετά ευρύ, οδηγώντας σε γενικευμένη, χωρίς διακρίσεις, παρακολούθηση[297]. Η απουσία σαφήνειας ορισμένων όρων σε συνδυασμό με την εφαρμογή της Πρότασης σε όλους τους παρόχους σχετικών υπηρεσιών της κοινωνίας της πληροφορίας που προσφέρουν τις υπηρεσίες τους στην Ένωση δεν εγγυώνται στοχευμένη προσέγγιση του ζητήματος της καταπολέμησης τέτοιου είδους παράνομου υλικού.

Επιπροσθέτως, η αυτοματοποιημένη επεξεργασία του περιεχομένου των επικοινωνιών που εφαρμόζεται και στα τρία είδη εντολών εντοπισμού, τα υψηλά ποσοστά σφαλμάτων που παρουσιάζουν οι τεχνολογίες για εντοπισμό νέου υλικού και άγρας παιδιών, καθώς επίσης και ο κίνδυνος υποβολής αναφοράς στο Κέντρο της ΕΕ σύμφωνα με το άρθρο 12 παράγραφος 1 και το άρθρο 48 παράγραφος 1 της πρότασης, περί εντοπισμού «πιθανού» υλικού σεξουαλικής κακοποίησης παιδιών, είναι στοιχεία της πρότασης που αυξάνουν τον προβληματισμό των δύο οργάνων[298].

Στην Κοινή Γνωμοδότηση των ΕΣΠΔ και ΕΕΠΔ, επισημαίνεται επίσης ότι οι πάροχοι υπηρεσιών διαδικτύου μπορούν να έχουν πρόσβαση στην ακριβή διεύθυνση URL του περιεχομένου, μονάχα αν το κείμενο δεν είναι κρυπτογραφημένο ("clear text"). Αν όμως το περιεχόμενο μιας ιστοσελίδας προστατεύεται με κρυπτογράφηση (όπως συμβαίνει με χρήση HTTPS), ο πάροχος δεν έχει πρόσβαση στο πλήρες URL και τα δεδομένα επικοινωνίας, παρά μόνο αν σπάσει την κρυπτογράφηση και παραβιάσει την ασφάλεια της επικοινωνίας. Ως εκ τούτου, οι ΕΣΠΔ και ΕΕΠΔ αμφιβάλλουν κατά πόσον θα ήταν αποτελεσματικό να μπλοκάρουν υλικό παιδικής σεξουαλικής κακοποίησης κατ' αυτόν τον τρόπο. Η απαίτηση δηλαδή να αποκρυπτογραφούν οι πάροχοι επικοινωνίες για να μπλοκάρουν τέτοιου είδους περιεχόμενο δεν θα ήταν αναλογική με το πρόβλημα που πρέπει να επιλυθεί[299].

Επισημαίνουν επίσης ότι ο αποκλεισμός ή η απενεργοποίηση της πρόσβασης σε ψηφιακό περιεχόμενο είναι μία διαδικασία που λαμβάνει χώρα σε επίπεδο δικτύου και η εφαρμογή της ενδέχεται να αποδειχθεί αναποτελεσματική, σε περίπτωση που υπάρχουν πολλά αντίγραφα του ίδιου περιεχομένου. Επιπλέον, μία τέτοια ενέργεια μπορεί να αποδειχθεί δυσανάλογη σε περιπτώσεις όπου ο αποκλεισμός επηρεάζει και άλλο μη παράνομο ψηφιακό περιεχόμενο, το οποίο είναι αποθηκευμένο στον ίδιο διακομιστή και καθίσταται μη προσβάσιμο μέσω εντολών δικτύου (π.χ. αποκλεισμός διεύθυνσης IP ή μαύρη λίστα DNS). Επίσης, δεν είναι όλες οι προσεγγίσεις αποκλεισμού

[297] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 23.

[298] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 23.

[299] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 22.

στο επίπεδο του δικτύου εξίσου αποτελεσματικές, ενώ κάποιες μπορεί να παρακαμφθούν εύκολα με βασικές τεχνικές γνώσεις.

Περαιτέρω, ΕΣΠΔ και ΕΕΠΔ επισημαίνουν ότι απαιτήσεις της Πρότασης που αφορούν στις τεχνολογίες για την ανίχνευση υλικού σεξουαλικής κακοποίησης και άγρας παιδιών δεν φαίνεται να είναι επαρκώς αυστηρές. Ειδικότερα, στην Κοινή Γνωμοδότηση σημειώνεται ότι[300] – σε αντίθεση με τις αντίστοιχες διατάξεις στον Προσωρινό Κανονισμό – η Πρόταση δεν κάνει καμία ρητή αναφορά στην αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, και δεν προβλέπει ότι οι τεχνολογίες που χρησιμοποιούνται για την ανάλυση κειμένων στις επικοινωνίες δεν θα πρέπει να είναι σε θέση να συμπεραίνουν την ουσία του περιεχομένου των επικοινωνιών. Η Πρόταση απλώς προβλέπει στο Άρθρο 10(3)(β) ότι οι τεχνολογίες δεν πρέπει να είναι σε θέση να «εξάγουν» οποιαδήποτε άλλη πληροφορία από τις σχετικές επικοινωνίες πέρα από την πληροφορία που είναι απολύτως απαραίτητη για την ανίχνευση. Ωστόσο, αυτό το πρότυπο δεν φαίνεται να είναι αρκετά αυστηρό, καθώς μπορεί να είναι δυνατόν να συμπεράνει κανείς άλλες πληροφορίες από την ουσία του περιεχομένου μιας επικοινωνίας χωρίς να εξάγει πληροφορίες από την επικοινωνία καθαυτή.

Συστήνουν, συνεπώς, να εισαχθεί στην Πρόταση αιτιολογική σκέψη που να ορίζει ότι η αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού[301], ισχύει για τις τεχνολογίες που ρυθμίζονται από το Άρθρο 10 της Πρότασης. Επιπλέον[302], το Άρθρο 10(3)(β) θα πρέπει να τροποποιηθεί έτσι ώστε να διασφαλίζεται ότι δεν εξάγεται καμία άλλη πληροφορία, ούτε συνάγεται η ουσία του περιεχομένου των επικοινωνιών, όπως προβλέπεται επί του παρόντος στο Άρθρο 3(1)(β) του Προσωρινού Κανονισμού.

Σε αντίθεση με τον Προσωρινό Κανονισμό[303], η Πρόταση δεν εξαιρεί από το πεδίο εφαρμογής της τη σάρωση των ακουστικών επικοινωνιών στο πλαίσιο της ανίχνευσης άγρας παιδιών. ΕΣΠΔ και ΕΕΠΔ φρονούν ότι η σάρωση ηχητικών επικοινωνιών είναι ιδιαίτερα επεμβατική, καθώς θα απαιτούσε ενεργή, συνεχιζόμενη και «ζωντανή» παρεμβολή στην επικοινωνία. Ταυτόχρονα, θα πρέπει να ληφθεί υπόψη ότι σε ορισμένα Κράτη Μέλη, η ιδιωτικότητα του προφορικού λόγου απολαμβάνει ειδικής προστασίας[304]. Επιπλέον, λόγω του γεγονότος ότι, κατ' αρχήν, το σύνολο του περιεχομένου της ηχητικής επικοινωνίας θα πρέπει να αναλυθεί, αυτό το μέτρο ενδέχεται να επηρεάσει την ουσία των δικαιωμάτων που εγγυώνται τα Άρθρα 7 και 8 του Χάρτη. Ως εκ τούτου, αυτή η μέθοδος ανίχνευσης θα πρέπει να παραμείνει εκτός του πεδίου εφαρμογής των υποχρεώσεων ανίχνευσης που

[300] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 24.

[301] η οποία καθορίζεται στο Άρθρο 25 του Κανονισμού (ΕΕ) 2016/679.

[302] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 25.

[303] Ό.π. Κανονισμός (ΕΕ) 2021/1232, άρθρο 1(2).

[304] Βλ. Γερμανικό Ποινικό Κώδικα, άρθρο 201.

καθορίζονται στην προτεινόμενη ρύθμιση, τόσο για τα ηχητικά μηνύματα όσο και για τις ζωντανές επικοινωνίες.

Ειδική μνεία γίνεται και στο Άρθρο 22 της Πρότασης, το οποίο περιορίζει τους σκοπούς για τους οποίους οι πάροχοι μπορούν να διατηρούν τα δεδομένα περιεχομένου και άλλα δεδομένα που επεξεργάζονται σε σχέση με τα μέτρα που λαμβάνονται, με σκοπό να συμμορφωθούν με τις υποχρεώσεις που καθορίζονται στην Πρόταση[305]. Η Πρόταση, ωστόσο, υποδεικνύει ότι οι πάροχοι μπορούν επίσης να διατηρούν αυτές τις πληροφορίες για τον σκοπό της βελτίωσης της αποτελεσματικότητας και της ακρίβειας των τεχνολογιών που χρησιμοποιούνται για την εκτέλεση εντολής ανίχνευσης, αλλά δεν επιτρέπεται να αποθηκεύουν προσωπικά δεδομένα για αυτόν τον σκοπό[306]. ΕΣΠΔ και ΕΕΠΔ θεωρούν ότι μόνο οι πάροχοι που χρησιμοποιούν τις δικές τους τεχνολογίες ανίχνευσης πρέπει να επιτρέπεται να διατηρούν δεδομένα για τη βελτίωση της αποτελεσματικότητας και της ακρίβειας των τεχνολογιών, ενώ εκείνοι που χρησιμοποιούν τεχνολογίες που παρέχονται από το Κέντρο της ΕΕ δεν πρέπει να επωφελούνται από αυτή τη δυνατότητα. Επιπλέον, ΕΣΠΔ και ΕΕΠΔ σημειώνουν ότι μπορεί να είναι δύσκολο να εξασφαλιστεί στην πράξη ότι δεν θα αποθηκευτούν προσωπικά δεδομένα για αυτόν τον σκοπό, καθώς τα περισσότερα δεδομένα περιεχομένου και άλλα δεδομένα που υπόκεινται σε επεξεργασία για σκοπούς ανίχνευσης είναι πιθανό να θεωρούνται προσωπικά δεδομένα[307].

Προκειμένου να εξετασθεί εάν τα εν λόγω μέτρα τηρούν την αρχή της αναλογικότητας υπό στενή εννοία[308], θα πρέπει τα μειονεκτήματα που προκύπτουν από την εφαρμογή τους για την άσκηση των θεμελιωδών δικαιωμάτων στην προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα να μην υπερτερούν των πλεονεκτημάτων που προκύπτουν από αυτά. Για την αξιολόγηση των επιπτώσεων ενός μέτρου στα εν λόγω δικαιώματα, λαμβάνεται υπόψη[309] κυρίως το πεδίο εφαρμογής του μέτρου, η διενέργεια επεξεργασίας δεδομένων ειδικών κατηγοριών, ο βαθμός παρεμβατικότητας, η κατάρτιση προφίλ των επηρεαζόμενων προσώπων, η σύνδεση του μέτρου με την χρήση αυτοματοποιημένου συστήματος για την λήψη αποφάσεων, καθώς επίσης και η ενδεχόμενη επίδραση σε άλλα θεμελιώδη δικαιώματα.

---

[305] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 27.

[306] Ό.π. Πρόταση, άρθρο 22(1).

[307] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 22.

[308] ΧΘΔΕ, άρθρο 52 παρ. 1.

[309] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, σελ. 20, διαθέσιμο: https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

Το γεγονός μάλιστα ότι δεν διαφαίνεται η ύπαρξη ειδικής τεχνολογίας για τον εντοπισμό υλικού που εμπεριέχεται σε κρυπτογραφημένη επικοινωνία, εγείρει τον προβληματισμό κατά πόσο πρόκειται για μέτρα που πράγματι θα οδηγήσουν σε αύξηση των αναφορών. Αξίζει να σημειωθεί ότι το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων αποφάνθηκε πρόσφατα στην υπόθεση Podchasov κατά Ρωσίας ότι η κρυπτογράφηση από άκρο σε άκρο αποτελεί θεμελιώδες δικαίωμα και είναι παράνομο να αποδυναμώνεται αυτή η προστασία προληπτικά[310]. Η ανεπάρκεια πόρων των αρχών επιβολής του νόμου αποτελεί επίσης ένα στοιχείο αποθαρρυντικό που χρήζει συνεκτίμησης προκειμένου να απαντηθεί το ερώτημα αν πράγματι η υλοποίηση των εντολών εντοπισμού συνεπάγεται αποτελεσματική διερεύνηση αδικημάτων παιδικής σεξουαλικής κακοποίησης[311].

Ελλείψει ασφάλειας δικαίου που προκύπτει από την απουσία σαφήνειας ορισμένων διατάξεων και δοθέντος ότι το πεδίο εφαρμογής της Πρότασης είναι αρκετά ευρύ, το ΕΣΠΔ και ο ΕΕΠΔ θεωρούν ότι η Πρόταση θα μπορούσε να αποτελέσει «τη βάση για de facto γενικευμένη σάρωση του περιεχομένου σχεδόν όλων των ειδών ηλεκτρονικών επικοινωνιών όλων των χρηστών στην ΕΕ[312]». Δεδομένου, ωστόσο, ότι οι τεχνολογίες για την εκτέλεση εντολών εντοπισμού συνεπάγονται διαφορετικά επίπεδα παρεμβατικότητας, αποφαίνονται τελικώς ότι μονάχα τα προοριζόμενα για τον εντοπισμό γνωστού υλικού μέσα πληρούν τις σχετικές απαιτήσεις αναλογικότητας, ενώ ταυτόχρονα οι τεχνολογίες που συνεπάγονται αυτοματοποιημένη ανάλυση ομιλίας ή κειμένου με σκοπό τον εντοπισμό άγρας συνιστούν την σημαντικότερη παρέμβαση όλων στα θεμελιώδη δικαιώματα.

Τα μέτρα ανίχνευσης νέου υλικού και επικοινωνιών που συνιστούν άγρα παιδιών έχουν επικριθεί ευρέως ως αναποτελεσματικά και μη πληρούντα την αρχή της αναλογικότητας λόγω των τεχνικών περιορισμών που συγκεντρώνουν τα συγκεκριμένα εργαλεία, όπως αναλύθηκε προηγουμένως. Και τούτο διότι, εξαιτίας του τεράστιου όγκου των δεδομένων που εξετάζονται, ακόμα και ένα μικρό ποσοστό ψευδώς θετικών αποτελεσμάτων μπορεί να οδηγήσει σε μεγάλο αριθμό εσφαλμένων υποψιών τέλεσης εγκλημάτων. Έχει υποστηριχθεί ότι δεδομένου ότι η ανίχνευση συνδέεται με υποχρέωση αναφοράς, υπάρχει ο κίνδυνος παρεμβατικών ενεργειών από τις αρχές επιβολής του νόμου, οι οποίες μπορεί να παραβιάσουν θεμελιώδη δικαιώματα και να επιβαρύνουν τους πόρους των αρμόδιων αρχών[313]. Ακόμα και όταν οι αναφορές είναι ορθά ταξινομημένες, ο μεγάλος όγκος των

---

[310] ECtHR, Podchasov v. Russia, Application No. 33696/19, διαθέσιμο: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

[311] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 21.

[312] Ό.π. Κοινή γνωμοδότηση 4/2022, σελ. 22.

[313] Quaisser Charlotte, Effective Enforcement or Excessive Surveillance? New Technologies, New Crimes, and the Search for a New Equilibrium in EU Law Enforcement Illustrated by the Example of the Combat against Child Sexual Abuse, Jean Monnet Network on EU Law Enforcement Working Paper Series Conference: Enforcement of European Union Law: New Horizons, 19-20 September 2024 at King's College London.

αυτοματοποιημένων αναφορών απειλεί να κατακλύσει τις αρχές και να επιφέρει το αντίθετο από το επιθυμητό αποτέλεσμα, ενώ παράλληλα ζητήματα σεξουαλικής κακοποίησης παιδιών εκτός του ψηφιακού χώρου υποστηρίζεται ότι ενδέχεται να χάσουν την ορατότητά τους[314].

Αναφορικά, ωστόσο, και με την λιγότερο παρεμβατική μέθοδο κατακερματισμού (hashing) για την ανίχνευση μη κρυπτογραφημένου περιεχομένου έχουν εγερθεί προβληματισμοί, καθώς μεταβάλλει εκ βάθρων τις πρακτικές καταπολέμησης του εγκλήματος: όλες οι μέθοδοι ανίχνευσης που προβλέπονται από την Έκθεση Εκτίμησης Επιπτώσεων της Πρότασης, ισοδυναμούν με προληπτική, γενική και αδιάκριτη επιτήρηση, χωρίς να υπάρχει αρχική υπόνοια τέλεσης εγκλήματος[315]. Και τούτο υποστηρίζεται ότι υπονομεύει έναν από τους παραδοσιακούς περιορισμούς των μέτρων επιβολής του νόμου.

Περαιτέρω, το προτεινόμενο οικοδόμημα έχει επικριθεί καθώς οι μηχανισμοί προστασίας της ιδιωτικότητας παρακάμπτονται από το γεγονός ότι η επιτήρηση διενεργείται από ιδιωτικούς φορείς[316]. Τα μέτρα επιτήρησης από πλευράς του Κράτους, εν αντιθέσει με τα διενεργούμενα από ιδιωτικές εταιρίες, υπόκεινται σε αυστηρούς ελέγχους και απαιτήσεις λογοδοσίας. Οι χρήστες μάλιστα, έχουν πρόσβαση σε μηχανισμούς προστασίας κατά των κρατικών μέτρων, όπως επί παραδείγματι ένδικα μέσα, κάτι που δεν συμβαίνει με τα εκπορευόμενα από ιδιωτικούς φορείς μέτρα. Αντίστοιχα, η σάρωση του περιεχομένου δεν λαμβάνει χώρα κατόπιν έκδοσης δικαστικής απόφασης, όπως συμβαίνει συνήθως με τα κρατικά μέτρα παρακολούθησης.

Δεδομένου ότι τα προβλεπόμενα μέτρα καλύπτουν διαπροσωπικές επικοινωνίες, η επέμβαση στα Άρθρα 7 και 8 του ΧΘΔΕ σύμφωνα με ορισμένες εκτιμήσεις, «υπερβαίνει κατά πολύ οποιαδήποτε επέμβαση έχει μέχρι στιγμής εξεταστεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης»[317], ακόμη και σε σχέση με την πρόσφατη απόφαση La Quadrature du Net II[318]. Η εγκαθίδρυση ενός είδους «chat control» εξαιτίας της πρόσβασης στο ίδιο το περιεχόμενο της επικοινωνίας απέχει πολύ από τις μέχρι τώρα αποφάσεις του ΔΕΕ που αφορούσαν σε μεταδεδομένα. Σύμφωνα με μία άποψη, το γεγονός ότι η περαιτέρω επεξεργασία περιεχομένου λαμβάνει χώρα μόνο σε περίπτωση θετικού ευρήματος, δεν

---

[314] Erik Tuchtfeld, '"Vielen Dank, Ihre Post ist unbedenklich": Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte' (VerfBlog, 25 May 2022), Robert Bongen, 'Pädokriminelle Bilder im Netz: EU-Abgeordnete fordern Aufklärung'.

[315] Nena Decoster, 'The policing and reporting of online child sexual abuse material: a scoping review' (2024) 95(2) RIDP, 323 347, διαθέσιμο: https://biblio.ugent.be/publication/01J717F469T6DJTHNVHNM8NP85

[316] Ό.π. Quaisser Charlotte, σ. 10.

[317] Christopher Vajda, 'Legal opinion commissioned by MEP Patrick Breyer, member of the Greens/EFA Group in the European Parliament', 2023, διαθέσιμο: https://www.patrick-breyer.de/wp-content/uploads/2023/11/Vajda-Legal-Opinion-ChatControl-CSAR-2023-11-19.pdf

[318] CJEU, Case C-470/21, La Quadrature du Net II (30 April 2024), διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0470

αναιρεί το γεγονός της προηγηθείσας γενικής και αδιάκριτης επέμβασης στις επικοινωνίες που τυχαίνουν αντικείμενο εντολών εντοπισμού. Κατά πόσον αυτό λοιπόν μπορεί να θεωρηθεί «απολύτως αναγκαίο και αναλογικό» είναι αμφισβητήσιμο[319].

Λαμβάνοντας υπόψη ότι ο στόχος της Πρότασης είναι η προστασία των παιδιών, θα πρέπει επίσης να ληφθεί υπόψιν ότι επηρεάζονται και τα δικαιώματα των ίδιων των παιδιών που είναι ενεργά στο διαδίκτυο. Τα θεμελιώδη δικαιώματά τους στην πληροφοριακή αυτοδιάθεση και την ιδιωτικότητα περιορίζονται εξίσου, ενώ παράλληλα έχει υποστηριχθεί ότι θα επηρεαστεί σε μεγάλο βαθμό η υγιής ανάπτυξή τους και η επικοινωνιακή τους συμπεριφορά, καθώς παραβιάζονται ο ιδιωτικός τους χώρος και τα προστατευμένα περιβάλλοντα στα οποία κινούνται.

Αντιρρήσεις επί της Πρότασης έχουν εγερθεί και από παρόχους υποδομών υπολογιστικού νέφους (cloud providers), ορισμένοι εκ των οποίων υποστηρίζουν ότι δεν είναι σε θέση να εφαρμόσουν αποτελεσματικά εντολές ανίχνευσης[320]. Και τούτο διότι οι πάροχοι υποδομών cloud δεν ελέγχουν το περιεχόμενο που φιλοξενούν οι πελάτες τους, ούτε έχουν πρόσβαση στο περιεχόμενο σε επίπεδο εφαρμογής εντολής ανίχνευσης. Απεναντίας, οι πάροχοι υποδομών υπολογιστικού νέφους προσφέρουν στους πελάτες τους υπηρεσίες υπολογιστικής ισχύος και αποθήκευσης βάσεων δεδομένων, με αποτέλεσμα τα συστήματα που βασίζονται σε cloud και δημιουργούνται από τους πελάτες να είναι σχεδιασμένα, ελεγχόμενα και διαχειριζόμενα από τον ίδιο τον πελάτη, ο οποίος είναι συχνά «υπεύθυνος επεξεργασίας δεδομένων», αλλά και «εκτελών την επεξεργασία». Πελάτες των παρόχων αυτών είναι επί παραδείγματι οι πάροχοι διαπροσωπικής επικοινωνίας, χρηματοπιστωτικά ιδρύματα, νοσοκομεία, ακόμη και κυβερνήσεις, που έχουν πλήρη έλεγχο και ευθύνη για το περιεχόμενο των υπηρεσιών που λειτουργούν. Μονάχα οι πελάτες, λοιπόν, έχουν άμεση σχέση με τους τελικούς χρήστες των πλατφορμών όπου μπορεί να διανέμεται υλικό σεξουαλικής κακοποίησης παιδιών.

Οι πάροχοι cloud δεν δύνανται συνεπώς να ελέγξουν το περιεχόμενο, τον τρόπο διανομής του ή τα πρόσωπα που αποκτούν πρόσβαση σε αυτό, γεγονός που σημαίνει ότι δεν μπορούν να εφαρμόσουν αποτελεσματικά μία εντολή ανίχνευσης με τρόπο που δεν θα ξεπερνούσε το απολύτως αναγκαίο, ώστε να αντιμετωπιστεί αποτελεσματικά ο κίνδυνος διάδοσης υλικού σεξουαλικής κακοποίησης παιδιών. Επιπλέον, λόγω των μέτρων ασφάλειας και εμπιστευτικότητας που οφείλουν οι πάροχοι υποδομών cloud να προσφέρουν στους πελάτες τους βάσει συμβατικής ενοχής, οι πελάτες έχουν πλήρη έλεγχο των προτιμήσεων κρυπτογράφησής τους. Συνεπώς, η CISPE προτείνει οι εντολές ανίχνευσης να απευθύνονται στους φορείς που δύνανται να ελέγξουν το διακινούμενο υλικό

[319] Ό.π. Quaisser Charlotte, σ. 8.

[320] Ό.π. CISPE.

σεξουαλικής κακοποίησης παιδιών, στους παρόχους δηλαδή υπηρεσιών οι οποίοι ενεργούν ως υπεύθυνοι επεξεργασίας δεδομένων σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Πέραν των εντολών ανίχνευσης, οι cloud πάροχοι εκφράζουν προβληματισμούς και για τις εντολές αφαίρεσης, τις οποίες θεωρούν μέτρο έσχατης λύσης. Υπογραμμίζουν ότι είναι σπάνια τεχνικά εφικτό για έναν πάροχο υποδομών cloud να αφαιρέσει ή να απενεργοποιήσει την πρόσβαση σε ένα συγκεκριμένο κομμάτι περιεχομένου, καθώς ο cloud πάροχος δεν έχει πρόσβαση στο λεπτομερές περιεχόμενο των πελατών του. Το εν λόγω οικοδόμημα αποτελεί μάλιστα την ουσία του επιχειρηματικού μοντέλου των υποδομών cloud. Όταν οι πάροχοι υποδομών cloud λαμβάνουν εντολές αφαίρεσης, θα πρέπει σε ορισμένες περιπτώσεις να καταργήσουν μια ολόκληρη υπηρεσία, αντί για «συγκεκριμένο περιεχόμενο». Συνεπώς, είναι πολύ πιο γρήγορο να εκδίδονται εντολές αφαίρεσης προς τους «υπεύθυνους επεξεργασίας δεδομένων», καθώς σε αντίθετη περίπτωση οι πάροχοι υποδομών cloud θα είναι υποχρεωμένοι να ανακατευθύνουν την εντολή στους πελάτες τους για να αφαιρέσουν εκείνοι το περιεχόμενο.

Επισημαίνουν επίσης ότι η «αφαίρεση» και η «απενεργοποίηση», αν και παρόμοιες έννοιες, συνεπάγονται ελαφρώς διαφορετικές υποχρεώσεις. Οι πάροχοι υποδομών cloud είναι πιο κατάλληλοι για να απενεργοποιούν περιεχόμενο, καθώς η λέξη «αφαίρεση» υποδηλώνει ότι το περιεχόμενο απομακρύνεται εντελώς από το διαδίκτυο. Ως εκ τούτου, σημειώνουν ότι είναι τεχνικά αδύνατο για έναν πάροχο υποδομών cloud να διασφαλίσει ότι όλα τα αντίγραφα του εκάστοτε περιεχομένου έχουν εξαλειφθεί. Ως εκ τούτου, υπογραμμίζουν ότι είναι αναγκαίο να διασφαλιστεί ότι ο Κανονισμός, όπου είναι κατάλληλο, θα εφαρμόζει την επιλογή για «αφαίρεση ή απενεργοποίηση της πρόσβασης», όπως αναφέρεται ήδη στο Άρθρο 1(γ), με συνέπεια σε όλο τον Κανονισμό.

Η Πρόταση αναμένεται επίσης ότι θα επιφέρει σημαντικές επιπτώσεις στους παρόχους υπηρεσιών της Κοινωνίας της Πληροφορίας καθώς θα αυξήσει σημαντικά τον φόρτο εργασίας τους λόγω των υποχρεώσεων που εισάγονται, ενώ παράλληλα ενδέχεται να αναστείλει την καινοτομία, καθώς κατευθύνει προς την υιοθέτηση τεχνολογιών που συγκρούονται με την ιδιωτικότητα στις επικοινωνίες[321]. Ταυτόχρονα όμως, επισημαίνεται ότι η ανάγκη εντοπισμού νέου υλικού και περιστατικών άγρας παιδιών δημιουργεί ευκαιρίες καινοτομίας. Παρόλο που στις υποθέσεις Scarlet Extended[322] και Netlog[323] το ΔΕΕ έκρινε ότι η επιβολή γενικής υποχρέωσης στους παρόχους υπηρεσιών της Κοινωνίας της Πληροφορίας να εγκαθιστούν και να συντηρούν δαπανηρά πληροφοριακά συστήματα για την παρακολούθηση όλων των ηλεκτρονικών επικοινωνιών στο δίκτυό τους παραβιάζει την ελευθερία άσκησης επιχειρηματικής δραστηριότητας των παρόχων, υποστηρίζεται

[321] Ό.π. Συμπληρωματική Έκθεση, σ. 83.

[322] Ό.π. Scarlet Extended.

[323] Ό.π. Netlog.

ότι δεν είναι δυνατόν να αξιολογηθεί με ακρίβεια ο βαθμός στον οποίο θίγεται το δικαίωμα στην επιχειρηματική δραστηριότητα, με βάση την Πρόταση και την Έκθεση Εκτίμησης Επιπτώσεων[324]. Παρά τις προβλεπόμενες αρνητικές επιπτώσεις, ωστόσο, έχει επισημανθεί ότι η Πρόταση περιλαμβάνει δικονομικές εγγυήσεις και δίνει τη δυνατότητα στις πλατφόρμες να προσβάλουν τις εντολές εντοπισμού, περιορίζοντας έτσι την παρέμβαση στο δικαίωμα της επιχειρηματικής ελευθερίας[325].

Ακόμη, μολονότι η τεχνολογία hashing και ειδικότερα ο αντιληπτικός κατακερματισμός αποτελεί έναν από τους αποτελεσματικότερους τρόπους ανίχνευσης υλικού παιδικής σεξουαλικής κακοποίησης στο διαδίκτυο[326], η αδυναμία εντοπισμού τέτοιου είδους υλικού σε διατερματικά κρυπτογραφημένες επικοινωνίες εμμένει. Το γεγονός μάλιστα ότι οι εντολές δεν προβλέπεται να εκτελούνται στοχευμένα σε χρήστες ενώ παράλληλα προορίζονται για εφαρμογή ακόμη και σε E2EE επικοινωνίες, αποτελούν στοιχεία της Πρότασης που εγείρουν ζητήματα αναλογικότητας.

Παρά τις όποιες ανησυχίες ωστόσο για την επίδραση της Πρότασης στα θεμελιώδη δικαιώματα, πολλές οργανώσεις επιδοκιμάζουν το οικοδόμημα που εισάγεται για την καταπολέμηση της σεξουαλικής κακοποίησης των παιδιών στο διαδίκτυο, αναγνωρίζοντας την ανάγκη εγκαθίδρυσης ενός συνεκτικού νομικού πλαισίου που εμπλέκει όλους τους συναρμόδιους φορείς στην προστασία των παιδιών. Ειδικότερα, ο Οργανισμός Missing Children Europe[327] επιδοκιμάζει την δράση του προτεινόμενου Κέντρου της ΕΕ για την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, αλλά και για την διευκόλυνση της παροχής αρωγής στα θύματα και τους επιζώντες, ενώ ταυτόχρονα επικροτεί τη σκοπούμενη δημιουργία Συντονιστικών Αρχών στα Κράτη Μέλη και την συνεργατική τους σχέση με το Κέντρο της ΕΕ. Από την άλλη, ο Οργανισμός Eurochild[328] υποστηρίζει μεν ότι κάθε εξέταση της αρχής της αναλογικότητας θα πρέπει να θέτει στο επίκεντρο το βέλτιστο συμφέρον του παιδιού, επισημαίνει ωστόσο ότι η ΕΕ θα πρέπει να λαμβάνει υπόψιν επιπρόσθετες βλάβες που μπορεί να προκαλέσει στα ίδια τα παιδιά οποιαδήποτε παρέμβαση επηρεάζει την κρυπτογράφηση. Ως εκ τούτου, θεωρεί ότι η μεγαλύτερη επένδυση στην καινοτομία είναι καθοριστικής σημασίας για τη βελτίωση των υπαρχουσών λύσεων και την ανάπτυξη νέων

---

[324] Ό.π. Συμπληρωματική Έκθεση, σ. 109-110.

[325] Ό.π. Συμπληρωματική Έκθεση, σ. 110.

[326] Ό.π. Guerra, E., & Westlake, B. G. (2021).

[327] Missing Children Europe, Missing Children Europe welcomes the European Commission's new regulation on preventing and combating child sexual abuse, διαθέσιμο: https://missingchildreneurope.eu/mce-welcomes-the-new-regulation-on-child-sexual-abuse/

[328] Eurochild, Eurochild calls for a Child Sexual Abuse Regulation that puts children first, διαθέσιμο: https://eurochild.org/news/eurochild-calls-for-a-child-sexual-abuse-regulation-that-puts-children-first/#:~:text=Eurochild%20welcomes%20the%20clear%20and,against%20child%20sexual%20abuse%20material.

τεχνολογιών που θα καταπολεμούν αποτελεσματικά αλλά και με ασφάλεια τη σεξουαλική κακοποίηση παιδιών.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η Πρόταση Κανονισμού της Ευρωπαϊκής Ένωσης για την σεξουαλική κακοποίηση παιδιών αποσκοπεί στην θέσπιση ενός συνεκτικού πλαισίου για την καταπολέμηση του υλικού παιδικής σεξουαλικής κακοποίησης στο διαδίκτυο, μέσω της θεσμοθέτησης υποχρεωτικών μηχανισμών δράσης από πλευράς των παρόχων υπηρεσιών της Κοινωνίας της Πληροφορίας. Η υποσχόμενη μάλιστα δυναμική της Πρότασης διαφαίνεται σε επίπεδο διατάξεων διακρατικού συντονισμού, δεδομένου ότι το Κέντρο της ΕΕ στοχεύεται να αποτελεί τον ασφαλή δίαυλο διαβίβασης επαληθευμένων αναφορών στην Europol και στις εθνικές αρχές επιβολής του νόμου. Ο ρόλος μάλιστα του Κέντρου στην άρση των εμποδίων στην εσωτερική αγορά, ιδιαίτερα σε σχέση με τις υποχρεώσεις των παρόχων που απορρέουν από την Πρόταση, αναμένεται ότι θα πολλαπλασιάσει τη χρήση της εμπειρογνωσίας για την καταπολέμηση της διαδικτυακής σεξουαλικής κακοποίησης των παιδιών.

Μολονότι η Ευρωπαϊκή Επιτροπή παρουσιάζει την Πρόταση ως αναπόσπαστο μέρος μίας ολοκληρωμένης στρατηγικής για την αντιμετώπιση του ειδεχθούς αυτού φαινομένου, δεν αμφισβητείται εντούτοις ότι τα προβλεπόμενα σε αυτήν μέτρα εντοπισμού συνιστούν σημαντική παρέμβαση στα θεμελιώδη δικαιώματα των χρηστών. Συγκεκριμένα, τα μέτρα εντοπισμού νέου υλικού και άγρας παιδιών, σε συνδυασμό με το ευρύ πεδίο εφαρμογής τους, την προβλεπόμενη ανώτατη διάρκειά τους και την ασάφεια ορισμένων όρων της Πρότασης, υποστηρίζεται ότι μπορούν να οδηγήσουν σε γενικευμένη παρακολούθηση των επικοινωνιών και να θίξουν το βασικό περιεχόμενο των δικαιωμάτων που κατοχυρώνονται στα άρθρα 7 και 8 του ΧΘΔΕ. Η τεχνολογική αξιοπιστία των προτεινόμενων εργαλείων, μάλιστα, έχει αποτελέσει αντικείμενο αντιπαράθεσης μεταξύ εμπειρογνωμόνων, εγείροντας ζητήματα αναφορικά με την αποτελεσματικότητα και την ακρίβεια των σχετικών μεθόδων.

Ο αμφιλεγόμενος χαρακτήρας της Πρότασης εντείνεται ακόμη περισσότερο με τη θέση της διατερματικής κρυπτογράφησης των επικοινωνιών υπό διακινδύνευση. Στο πλαίσιο αυτό, επισημαίνεται ευρέως ότι η υπονόμευση της ιδιωτικότητας και της ασφάλειας των επικοινωνιών μπορεί κάλλιστα να δημιουργήσει τις προϋποθέσεις για γενικευμένη ψηφιακή επιτήρηση, ενώ ταυτόχρονα, τεχνολογικές λύσεις που έχουν δημιουργηθεί για σκοπούς σάρωσης περιεχομένου σε διατερματικά κρυπτογραφημένα περιβάλλοντα, βρίσκονται επί του παρόντος σε πρώιμο στάδιο ανάπτυξης.

Η ευρεία κριτική στο κανονιστικό οικοδόμημα της Πρότασης, καταδεικνύει ότι η αναμενόμενη αποτελεσματικότητά της θα είναι περιορισμένη, εξαιτίας διαφόρων παραγόντων, όπως η χαμηλή ακρίβεια των τεχνολογιών εντοπισμού νέου υλικού και άγρας παιδιών, η πιθανή μεταπήδηση των δραστών σε πιο δυσπρόσιτα δίκτυα με σκοπό την αποφυγή εντοπισμού τους, καθώς επίσης και τα σοβαρά ζητήματα που προβλέπεται ότι θα προκύψουν για τα θεμελιώδη δικαιώματα των χρηστών από την αποδυνάμωση της διατερματικής κρυπτογράφησης.

Η ίδρυση πάντως του Κέντρου της ΕΕ κατά της σεξουαλικής κακοποίησης πιστεύεται ότι αποτελεί ένα θετικό βήμα για την ενίσχυση του αγώνα ενάντια στο φαινόμενο και την βελτίωση της συνεργασίας των εμπλεκόμενων μερών. Ο ρόλος μάλιστα που πρόκειται να διαδραματίσει για την υποστήριξη των παρόχων υπηρεσιών διαμέσου της παροχής τεχνογνωσίας, παράλληλα με τις δικονομικές εγγυήσεις που η Πρόταση προσφέρει στους παρόχους για προσβολή των εντολών εντοπισμού, φαίνεται ότι περιορίζουν σημαντικά την παρέμβαση στο δικαίωμα της επιχειρηματικής ελευθερίας. Σε συνδυασμό μάλιστα με βελτιωτικές τροποποιήσεις που έχουν προταθεί από όργανα της Ευρωπαϊκής Ένωσης, η Πρόταση μπορεί να καταστεί αποτελεσματικότερη, διασφαλίζοντας παράλληλα τον σεβασμό στα θεμελιώδη δικαιώματα της προστασίας δεδομένων προσωπικού χαρακτήρα, της ιδιωτικότητας και της ελευθερίας της έκφρασης.

Πέραν της ανάγκης τροποποίησης ορισμένων διατάξεων, κρίνεται επίσης απαραίτητη η εξέταση της πιθανότητας ύπαρξης εξίσου αποτελεσματικών μέτρων εντοπισμού υλικού σεξουαλικής κακοποίησης παιδιών, τα οποία θα συνιστούν μικρότερης έντασης επέμβαση στα θεμελιώδη δικαιώματα των χρηστών. Προς τον σκοπό αυτό, χρήζει περαιτέρω εξέτασης η δυνατότητα εντοπισμού υλικού που βασίζεται στη χρήση μεταδεδομένων, η οποία δεν συνεπάγεται καταρχήν επέμβαση στο περιεχόμενο, και η οποία υπό ορισμένες συνθήκες μπορεί να υποστηριχθεί και σε κρυπτογραφημένα από άκρο σε άκρο περιβάλλοντα. Στο ίδιο πλαίσιο, κρίνεται αναγκαία η επένδυση στη βελτίωση καινοτόμων προσεγγίσεων που θα καταστήσουν δυνατή την ανίχνευση υλικού παιδικής σεξουαλικής κακοποίησης χωρίς να χρειάζεται να παραβιαστεί η αρχή της κρυπτογράφησης από άκρο σε άκρο.

Δεδομένης μάλιστα της αμφισβητούμενης αξιοπιστίας των υπαρχόντων τεχνολογιών εντοπισμού νέου υλικού και δοθέντος ότι το ανεξερεύνητο υλικό παιδικής σεξουαλικής κακοποίησης στο διαδίκτυο εκτιμάται ότι είναι υπερμέγεθες σε σχέση με το ήδη γνωστό, η χρήση μεταδεδομένων για τον εντοπισμό του θα μπορούσε να συνιστά ένα λιγότερο παρεμβατικό μέτρο στα θεμελιώδη δικαιώματα των χρηστών. Μια τέτοια λύση θα μπορούσε να κριθεί πρόσφορη σε περιπτώσεις στοχευμένης εφαρμογής της σε ύποπτους χρήστες, ή ακόμη και σε ευρύτερη κλίμακα υπό συγκεκριμένες ουσιαστικές και διαδικαστικές εγγυήσεις.

Εν κατακλείδι, ο σκοπός της Πρότασης για προστασία των παιδιών από την σεξουαλική κακοποίηση αναγνωρίζεται πανευρωπαϊκά ως ύψιστης σημασίας, τα προτεινόμενα μέσα για την επίτευξή του

ωστόσο σε συνδυασμό με ανεπαρκείς εγγυήσεις ενδέχεται να υπονομεύσουν σημαντικά θεμελιώδη δικαιώματα. Κατά συνέπεια, η υιοθέτηση του Κανονισμού προϋποθέτει μελετημένο επανασχεδιασμό με έμφαση στα νευραλγικά σημεία που επισημάνθηκαν, ώστε να επιτευχθεί η εξισορρόπηση της προστασίας των παιδιών με τον σεβασμό των ατομικών δικαιωμάτων και να διασφαλιστούν οι εκπορευόμενες από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ένωσης εγγυήσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ
ΕΛΛΗΝΙΚΗ

Δ. Βέρρας, Πληροφοριακός αυτοκαθορισμός και προστασία προσωπικών δεδομένων, διαθέσιμο: https://www.lawspot.gr/nomika-blogs/dimitris_verras/pliroforiakos-aytokathorismos-kai-prostasia-prosopikon-dedomenon#_ftn6

Για το δικαιωμα στον ιδιωτικο βιο, βλ. Κ. Μαυριά, Το συνταγματικο δικαιωμα του ιδιωτικου βιου, 1982.

Γιώργος Ν. Γιαννόπουλος, Η ευθύνη των παρόχων υπηρεσιών του Internet.

Ευρωπαϊκή Επιτροπή, Έγγραφο εργασίας των υπηρεσιών της Επιτροπής, Έκθεση εκτίμησης επιπτώσεων που συνοδεύει την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, (2022), σ. 281, υποσημείωση 511, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209

Ι. Ιγγλεζάκης, Ευαίσθητα προσωπικά δεδομένα, 2004.

Κ. Μαυριά, Το συνταγματικο δικαιωμα του ιδιωτικου βιου, 1982, σελ. 21 επ.

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 της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679

Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Οκτωβρίου 2018 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ, διαθέσιμο σε: https://eur-lex.europa.eu/eli/reg/2018/1725/oj

Κανονισμός (ΕΕ) 2021/1232 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Ιουλίου 2021, περί προσωρινής παρεκκλίσεως από ορισμένες διατάξεις της οδηγίας 2002/58/ΕΚ όσον αφορά τη χρήση τεχνολογιών από παρόχους υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών για την επεξεργασία προσωπικών και άλλων δεδομένων, προς καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο (ΕΕ [2021] L 274/41), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R1232

Κανονισμός 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαΐου 2016 για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0794&from=EN

Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με προσωρινή παρέκκλιση από ορισμένες διατάξεις της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τη χρήση τεχνολογιών από παρόχους υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και άλλων δεδομένων, με σκοπό την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52020PC0568

Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών (Πράξη για τις ψηφιακές υπηρεσίες) και την τροποποίηση της οδηγίας 2000/31/ΕΚ, διαθέσιμο: https://eur-lex.europa.eu/legal

Λ. Μήτρου, «Ερμηνεία Άρθρου 9Α Σ», σε Φ. Σπυρόπουλος/Ξ. Κοντιάδης/Χ. Ανθόπουλος/Γ. Γεραπετρίτης, Σύνταγμα, Κατ' άρθρο ερμηνεία, 2017.

Λ. Μήτρου, «Ερμηνεία Άρθρου 9Α Σ», σε Φ. Σπυρόπουλος/Ξ. Κοντιάδης/Χ. Ανθόπουλος/Γ. Γεραπετρίτης, Σύνταγμα, Κατ' άρθρο ερμηνεία, 2017, σελ. 216.

Λ. Μήτρου, Προστασία του περιβάλλοντος εναντίον της προστασίας πληροφοριών;, [Νόμος και Φύση 3/1996: 9-31].

Λ. Μήτρου, Προστασία του περιβάλλοντος εναντίον της προστασίας πληροφοριών;, [Νόμος και Φύση 3/1996: 9-31].

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 («e-Commerce Directive»), διαθέσιμο σε: https://eur-lex.europa.eu/legal- content/EL/ALL/?uri=CELEX:32000L0031

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32002L0058

Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης

παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαισίου 2004/68/ΔΕΥ του Συμβουλίου, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32011L0093

Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, 2022/0155(COD), διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0209

Συμπληρωματική Έκθεση Εκτίμησης Επιπτώσεων της Πρότασης Κανονισμού για τη θέσπιση κανόνων πρόληψης και καταπολέμησης της σεξουαλικής κακοποίησης παιδιών, Υπηρεσία Έρευνας Ευρωπαϊκού Κοινοβουλίου, 2023, διαθέσιμο: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

Φ. Παναγοπούλου, Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 9Α, Ηλεκτρονική Έκδοση, Επιμέλεια Σπ. Βλαχόπουλος, Ξ. Κοντιάδης, Γ. Τασόπουλος, Ιανουάριος 2023.

Φ. Παναγοπούλου, Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 9Α, Ηλεκτρονική Έκδοση, Επιμέλεια Σπ. Βλαχόπουλος, Ξ. Κοντιάδης, Γ. Τασόπουλος, Ιανουάριος 2023.

Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕ), άρθρο 52, διαθέσιμο: https://eur- lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT

ΞΕΝΟΓΛΩΣΣΗ

Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, σ. 4, διαθέσιμο: https://arxiv.org/pdf/2110.07450.

ActiveFence, Detecting Novel CSAM – Why Image Hash Matching Isn't Enough Anymore, διαθέσιμο σε: https://www.activefence.com/blog/detecting-csam-hash-matching/

Andrea Usai, The Freedom to Conduct a Business in the EU, Its Limitations and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration

Apple, CSAM Detection, Technical Summary, August 2021, διαθέσιμο: https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

Bartusek et al., End-to-End Secure Messaging with Traceability Only for Illegal Content, 2022, σ. 7, διαθέσιμο: https://eprint.iacr.org/2022/1643

Beekman, Jethro Gideon, "Improving Cloud Security using Secure Enclaves", ενότητα 2.3., UC Berkeley, Electronic Theses and Dissertations, 2016, διαθέσιμο: https://escholarship.org/uc/item/0jn0n1xs

Bleakley Paul et al., Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed?, European Journal of Criminology, 2023, διαθέσιμο: https://doi.org/10.1177/147737082311813

BradeisNOW, To be let alone: Brandeis foresaw privacy problems What would the privacy-law champion make of surveillance programs like PRISM?, 2013, διαθέσιμο σε: https://www.brandeis.edu/now/2013/july/privacy.html

Brussels Signal, EU's 'chat control' vote scrapped amid continuing opposition, Οκτώβιος 2025, διαθέσιμο: https://brusselssignal.eu/2025/10/eus-chat-control-vote-scrapped-amid-continuing-opposition/?utm_source=

Cale, J. et al., (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. Trends and issues in crime and criminal justice, (617), 1-22), διαθέσιμο: https://www.aic.gov.au/publications/tandi/tandi617

Cambridge University Press, διαθέσιμο: https://www.cambridge.org/core/journals/german-law-journal/article/freedom-to-conduct-a-business-in-the-eu-its-limitations-and-its-role-in-the-european-legal-order-a-new-engine-for-deeper-and-stronger-economic-social-and-political-integration/CBB67ACD4D5D633A5D5D19B460538921

CEPS (Centre for European Policy Studies), Towards a principled level playing field for an open and secure online environment, σ. 46, διαθέσιμο: https://www.ceps.eu/ceps-publications/towards-a-principled-level-playing-field-for-an-open-and-secure-online-environment/

Christopher Vajda, 'Legal opinion commissioned by MEP Patrick Breyer, member of the Greens/EFA Group in the European Parliament', 2023, διαθέσιμο: https://www.patrick-breyer.de/wp-content/uploads/2023/11/Vajda-Legal-Opinion-ChatControl-CSAR-2023-11-19.pdf

CISPE, CISPE position paper on the European Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse ("CSA"), διαθέσιμο: https://cispe.cloud/website_cispe/wp-content/uploads/2022/10/CISPE-CSAM-position-paper-06-09-22.pdf

Claudia Peersman et al., Live forensics to reveal previously unknown criminal media on p2p networks. Digital Investigation, διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S1742287616300779

Client-Side Scanning And Winnie The-Pooh Redux (Plus Some Thoughts On Zoom), The Center for Internet and Society, διαθέσιμο: https://cyberlaw.stanford.edu/blog/2020/05/client-side-scanning-and-winnie-pooh-redux-plus-some-thoughts-zoom/

Cnet, Apple to beta test iMessage feature that warns kids about nude imagery, διαθέσιμο: https://www.cnet.com/tech/mobile/apple-to-beta-test-imessage-feature-that-warns-kids-about-nude-imagery/

CNIL, Online age verification: balancing privacy and the protection of minors, διαθέσιμο:

Cometchat, Understanding Hash Matching Technology: A Guide for Trust & Safety Professionals, διαθέσιμο:

Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment (European Parliamentary Research Service, February 2021), παράγραφος 14, διαθέσιμο: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662598

Council of Europe, Convention 108 and Protocols, διαθέσιμο σε: https://www.coe.int/en/web/data-protection/convention108-and-protocol

Council of the European Union, Child sexual abuse: Council reaches position on law protecting children from online abuse, διαθέσιμο: https://www.consilium.europa.eu/en/press/press-releases/2025/11/26/child-sexual-abuse-council-reaches-position-on-law-protecting-children-from-online-abuse/?utm_source=brevo&utm_campaign=AUTOMATED%20-%20Alert%20-%20Newsletter&utm_medium=email&utm_id=3318

CSA Regulation Document Pool, EDRi, διαθέσιμο: https://edri.org/our-work/csa-regulation-document-pool/

CSAM Detection Technical Summary, διαθέσιμο: https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

Day, G. and Stemler, A. (2020), "Are Dark Patterns Anticompetitive?", Alabama Law Review, Vol. 72/1, διαθέσιμο: https://doi.org/10.2139/ssrn.3468321

Digital Rights Ireland (C-293/12). ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ., Τμήμα μείζονος συνθέσεως, 8 Απριλίου 2014, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62012CJ0293

ECLAG Steering Group, "Myth Busting & Facts on the proposed Regulation on Child Sexual Abuse: addressing the privacy concerns with data and facts", διαθέσιμο σε: https://www.eurochild.org/news/learn-thefacts-key-insights-on-the-eus-proposed-csa-regulation

ECLAG, A coalition of more than 60 organisations working to end child sexual abuse on and offline, διαθέσιμο σε: https://www.childsafetyineurope.com/eclag/

ECtHR, Podchasov v. Russia, Application No. 33696/19, διαθέσιμο: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022, διαθέσιμο: https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

EDPS, Briefing note on the CSAM proposal: "The Point of No Return", https://www.edps.europa.eu/data-protection/our-work/publications/factsheets/2023-10-23-briefing-note-csam-point-no-return_en

EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, σελ. 20, διαθέσιμο: https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

EDRi network, position paper on the "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse" 2022/0155(COD) (CSA Regulation), διαθέσιμο: https://edri.org/our-work/csa-regulation-document-pool/#position

EDRi, Private and secure communications attacked by European Commission's latest proposal, διαθέσιμο: https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/

EDRi, The ePrivacy Regulation proposal has been withdrawn, but the fight for your privacy is far from over, διαθέσιμο σε: https://edri.org/our-work/the-eprivacy-regulation-proposal-has-been-withdrawn-but-the-fight-for-your-privacy-is-far-from-over/

Erik Tuchtfeld, '"Vielen Dank, Ihre Post ist unbedenklich": Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte' (VerfBlog, 25 May 2022), Robert Bongen, 'Pädokriminelle Bilder im Netz: EU-Abgeordnete fordern Aufklärung'.

EU "Chat Control" Regulation Nears Final Vote: Understanding the Proposal, the Process, and What Comes Next, European Crypto Initiative, διαθέσιμο: https://eu.ci/eu-chat-control-regulation/

Eurochild, Eurochild calls for a Child Sexual Abuse Regulation that puts children first, διαθέσιμο: https://eurochild.org/news/eurochild-calls-for-a-child-sexual-abuse-regulation-that-puts-children-first/#:~:text=Eurochild%20welcomes%20the%20clear%20and,against%20child%20sexual%20abuse%20material.

European Union Agency for Fundamental Rights, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018, διαθέσιμο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

Europol, Europol Serious and Organised Crime Threat Assessment (SOCTA), Απρίλιος 2021, διαθέσιμο: https://www.europol.europa.eu/publications-events/main-reports/socta-report

Eva Glawischnig-Piesczek v Facebook, Opinion of AG Spunzar, παρ. 62, 63, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-18/18

Expert Workshop on the EU Proposed Regulation on preventing and Combatting Child sexual Abuse, jointly organized by the Center for Law and Digital Technologies of Leiden University and ECPAT International Leiden University, 2022, διαθέσιμο: https://www.universiteitleiden.nl/en/news/2023/02/report-launch-workshop-on-eu-proposed-regulation-onpreventing-and-combatting-child-sexual-abuse

Facebook, New Technology to Fight Child Exploitation, διαθέσιμο: https://about.fb.com/news/2018/10/fighting-child-exploitation/ και NBC News, Facebook touts use of artificial intelligence to fight child exploitation, διαθέσιμο: https://www.nbcnews.com/tech/tech-news/facebook-touts-use-artificial-intelligence-fight-child-exploitation-n923906

Facebook, Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer, διαθέσιμο: https://about.fb.com/news/2019/08/open-source-photo-video-matching/

Farhad Ahmed Sagar, Cryptographic Hashing Functions - MD5, διαθέσιμο: https://cs.indstate.edu/~fsagar/doc/paper.pdf

Farid H., House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, διαθέσιμο: https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf

Fight Chat Control, The EU (still) wants to scan your private messages and photos, διαθέσιμο: https://fightchatcontrol.eu/

Google, Fighting child sexual abuse online, διαθέσιμο: https://protectingchildren.google/intl/en/

Gorwa, R., Binns, R. and Katzenbach, C., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', 2020, διαθέσιμο σε: https://journals.sagepub.com/doi/full/10.1177/2053951719897945

Guerra, E., & Westlake, B. G. (2021). Detecting child sexual abuse images: traits of child sexual exploitation hosting and displaying websites. Child Abuse & Neglect, 122, 105336, διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S0145213421004051

Hany Farid, An Overview of Perceptual Hashing, Journal of Online Trust and Safety, Vol. 1 No. 1 (2021), διαθέσιμο: https://tsjournal.org/index.php/jots/article/view/24

Hee-Eun Lee et al., Detecting child sexual abuse material: A comprehensive survey, διαθέσιμο: https://www.sciencedirect.com/science/article/abs/pii/S2666281720301554?casa_token=D75TTQhANbwAAAAA:GmQLmNLY1SYjYyYQ9gO8cwFM-zcK6rwTKPFvo2b6bClUMusy5GtAhFJSfmwN17hhzYCgYs8

https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

https://www.cometchat.com/blog/what-is-hash-matching

I. Roagna, Protecting the right to respect for private and family life under the European Convention on Human Rights, Council of Europe human rights handbooks, διαθέσιμο: https://www.echr.coe.int/documents/d/echr/Roagna2012_EN

I. Shumailov et. al., Manipulating SGD with Data Ordering Attacks, Cornell University, διαθέσιμο: https://arxiv.org/abs/2104.09667

INHOPE, Annual Report 2022, διαθέσιμο σε: https://www.inhope.org/EN/articles/inhope-annual-report-2022#:~:text=INHOPE's%20Impact%20a%20brief%20look,down%20on%20the%20same%20day

INHOPE, The European Union CSAM Regulation, διαθέσιμο σε: https://inhope.org/EN/articles/the-european-union-csam-regulation?locale=en

Inpher Computing Company, What is Secure Multiparty Computation?, διαθέσιμο: https://inpher.io/technology/what-is-secure-multiparty-computation/

Jain et al., Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based clientside scanning, 2023, σ. 2318, διαθέσιμο: https://openreview.net/forum?id=CQbqeGAM_Ki και Hao et al., It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications, 2021, σ. 81, διαθέσιμο: https://www.usenix.org/system/files/sec22-jain.pdf

Katrin Chauviré-Geib and Jörg M. Fegert, Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review, Sage Journals, Volume 25, Issue 2, 2024, διαθέσιμο: https://doi.org/10.1177/15248380231178754

L. Mitrou et al, Social Media Profiling: a Panopticon or Omniopticon tool?, 2014, διαθέσιμο: https://api.semanticscholar.org/CorpusID:49362390

Leblanc-Albarel D. & Preneel B., Black-box Collision Attacks on Widely Deployed Perceptual Hash Functions, διαθέσιμο: https://eprint.iacr.org/2024/1869.pdf

Levy, I. και Robinson, C., Thoughts on Child Safety on Commodity Platforms, 2022, σ. 35, διαθέσιμο: https://arxiv.org/pdf/2207.09506

Manokha, Ivan. 2018. Surveillance, Panopticism, and Self-Discipline in the Digital Age. Surveillance & Society 16(2): 219-237, διαθέσιμο: https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

Manokha, Ivan. 2018. Surveillance, Panopticism, and Self-Discipline in the Digital Age. Surveillance & Society 16(2): 219-237, διαθέσιμο: https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

Marco Gestri, Regolamentazione del mercato e libertà d'iniziativa privata: L'incidenza del diritto comunitario sulla costituzione económica, in ISTITUZIONI E DINAMICHE DEL DIRITTO: MERCATO, AMMINISTRAZIONE, DIRITTI 141–76 (A. Vignudelli ed., 2006).

Martin Steinebach et al., Image Hashing Robust Against Cropping and Rotation, διαθέσιμο σε: https://www.researchgate.net/publication/370500036_Image_Hashing_Robust_Against_Cropping_and_Rotation

Medium, Black-Box Attacks on Perceptual Image Hashes with GANs, διαθέσιμο: https://medium.com/data-science/black-box-attacks-on-perceptual-image-hashes-with-gans-cc1be11f277

Meredith Whittacker, New Branding, Same Scanning: "Upload Moderation" Undermines End-to-End Encryption, διαθέσιμο: https://signal.org/blog/pdfs/upload-moderation.pdf

Microsoft, PhotoDNA, How does PhotoDNA technology work?, διαθέσιμο: https://www.microsoft.com/en-us/photodna

Missing Children Europe, Missing Children Europe welcomes the European Commission's new regulation on preventing and combating child sexual abuse, διαθέσιμο: https://missingchildreneurope.eu/mce-welcomes-the-new-regulation-on-child-sexual-abuse/

Morales F. et. al., PHVSpec: A Benchmark-based Analysis of Perceptual Hash Systems for Videos, διαθέσιμο: https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/Tech-Coalition-Video-Hash-Benchmark-Paper.pdf

Murdoch Watney, Law Enforcement Access to End-to-End Encrypted Social Media Communications, διαθέσιμο: https://books.google.gr/books?hl=en&lr=&id=FCAEEAAAQBAJ&oi=fnd&pg=PA322&dq=info:W1NNBcUZG_0J:scholar.google.com&ots=UiL-vtuyHh&sig=ei020OFYBmIja9x8mksi53YjBQ&redir_esc=y#v=onepage&q&f=false

NCMEC, The issues, End-to-end encryption, διαθέσιμο: https://www.missingkids.org/theissues/end-to-end-encryption

Nena Decoster, 'The policing and reporting of online child sexual abuse material: a scoping review' (2024) 95(2) RIDP, 323 347, διαθέσιμο: https://biblio.ugent.be/publication/01J717F469T6DJTHNVHNM8NP85

NYTimes, Child Abusers Run Rampant as Tech Companies Look the Other Way, διαθέσιμο: https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html

Ofcom, Overview of Perceptual Hashing Technology, (2022), σ. 3, διαθέσιμο σε: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/perceptual-hashing-technology.pdf?v=328806

Peersman et al., Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study', 2023, σ. 23, διαθέσιμο: https://research-information.bris.ac.uk/en/publications/towards-a-framework-for-evaluating-csam-prevention-and-detection-

Peterson/Elsevier v Youtube/Cyando, Joined Cases C-682/18 and C-683/18, διαθέσιμο σε: https://curia.europa.eu/juris/document/document.jsf?docid=243241&doclang=en

Pfefferkorn, R., Stanford Internet Observatory, 2021, σελ. 10, διαθέσιμο: https://doi.org/10.54501/jots.v1i2.14

Powell et al., Child Protection and Freedom of Expression Online, 2010, σ. 3, διαθέσιμο: https://www.oii.ox.ac.uk/wp-content/uploads/old-docs/FD17.pdf

Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Presidency compromise texts, Ιούλιος 2025, σελ. 50, διαθέσιμο: https://data.consilium.europa.eu/doc/document/ST-10131-2025-INIT/en/pd

Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Presidency compromise texts, 2025, διαθέσιμο: https://data.consilium.europa.eu/doc/document/ST-5352-2025-INIT/en/pdf

Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Partial mandate for negotiations with the European Parliament, 2025, διαθέσιμο: https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf

Quaisser Charlotte, Effective Enforcement or Excessive Surveillance? New Technologies, New Crimes, and the Search for a New Equilibrium in EU Law Enforcement Illustrated by the Example of the Combat against Child Sexual Abuse, Jean Monnet Network on EU Law Enforcement Working Paper Series Conference: Enforcement of European Union Law: New Horizons, 19-20 September 2024 at King's College London.
Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, European Parliament, διαθέσιμο: https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html

Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, 2023, διαθέσιμο: https://rm.coe.int/outcome-report-of-the-expert-workshop-on-eu-proposed-regulation-on-pre/1680aa00e4

Sanjay Sharma, Data Privacy and GDPR Handbook, PhD with research associate Pranav Menon, διαθέσιμο: https://cdn.oujdalibrary.com/books/614/614-data-privacy-and-gdpr-handbook-(www.tawcer.com).pdf

Sanjay Sharma, Data Privacy and GDPR Handbook, PhD with research associate Pranav Menon, διαθέσιμο: https://cdn.oujdalibrary.com/books/614/614-data-privacy-and-gdpr-handbook-(www.tawcer.com).pdf

Seny Kamara et al., Outside looking in approaches to content moderation in end-to-end encrypted systems, διαθέσιμο: https://www.researchgate.net/publication/358488067_Outside_Looking_In_Approaches_to_Content_Moderation_in_End-to-End_Encrypted_Systems

Thorn, How Safer's detection technology stops the spread of CSAM, διαθέσιμο: https://www.thorn.org/blog/how-safers-detection-technology-stops-the-spread-of-csam/

Toygar Hasan Oruç, The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it?, 2022, διαθέσιμο: https://www.jipitec.eu/jipitec/article/view/354/347

Videntifier, Hash Matching Will Save Content Moderation, Faster Than AI Currently Can On Its Own, διαθέσιμο: https://www.videntifier.com/post/ai-and-hash-matching

Vu et al., 'ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data', 2021, διαθέσιμο: https://arxiv.org/abs/2111.04479)

WeProtect Global Alliance to end child sexual exploitation online, Global Threat Assessment, 2021, διαθέσιμο: https://www.weprotect.org/global-threat-assessment-21/#report

WhatsApp, «How WhatsApp Helps Fight Child Exploitation», διαθέσιμο: https://faq.whatsapp.com/5704021823023684/?locale=el

Whatsapp, How WhatsApp Helps Fight Child Exploitation, διαθέσιμο: https://faq.whatsapp.com/5704021823023684/?locale=en_US

Wired, Apple Expands Its On-Device Nudity Detection to Combat CSAM, διαθέσιμο: https://www.wired.com/story/apple-communication-safety-nude-detection/

Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, διαθέσιμο: https://www.wired.com/story/whatsapp-encryption-child-abuse/

Youtube CSAI Match, Protect your content and online community from child exploitation videos, διαθέσιμο: https://www.youtube.com/csai-match/

Zulfany Erlisa Rasjid et al., A review of collisions in cryptographic hash function used in digital forensic tools (2017), διαθέσιμο σε: https://www.sciencedirect.com/science/article/pii/S1877050917321221

ΝΟΜΟΛΟΓΙΑ

ΕιρΘεσσαλ 6981/2018

ΕιρΑθ 5551/2019

ΣτΕ 1616/2012

ΤριμΕφΑθ 175/2014

ECtHR, Case of Handyside v. The United Kingdom, Application no. 5493/72, διαθέσιμο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]}

CJEU, In Joined Cases C-511/18, C-512/18 and C-520/18, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=6898

ECtHR, Case of Z. v. Finland, application no. 22009/93, διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58033%22]}

CJEU, SABAM v. Netlog NV, Case C-360/10, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=D4467091242228CE5FADC98767BEA97A?text=&docid=119512&pageIndex=0&doclang=el&mode=req&dir=&occ=first&part=1&cid=3348323

CJEU, Judgment of the Court (Third Chamber) of 24 November 2011, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10

CJEU, Judgment of the Court (Grand Chamber), 22 January 2013, Sky Österreich GmbH v Österreichischer Rundfunk, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-283/11&language=EL

CJEU, Judgement of the Court, (Fourth Chamber) 27 March 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, διαθέσιμο: https://curia.europa.eu/juris/document/document.jsf?docid=149924&doclang=EN

CJEU, Judgement of the Court (Grand Chamber), 6 November 2018, in Joined Cases C-569/16 and C-570/16, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62016CJ0569

CJEU, Judgment of the Court (Third Chamber) of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?num=C-18/18

CJEU, Opinion of Advocate General Saugmandsgaard Øe, 16 July 2020, Joined Cases C-682/18 and C-683/18, διαθέσιμο: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CC0682#t-ECR_62018CC0682_EN_01-E0188

CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others, joined Cases C-511/18, C-512/18 and C-520/18., διαθέσιμο: https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL

CJEU, Judgment of the Court (Grand Chamber) of 26 April 2022, Republic of Poland v European Parliament and Council of the European Union, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0401

CJEU, Judgement of the Court (Full Court) of 30 April 2024, Case C-470/21, La Quadrature du Net and Others v Premier ministre and Ministère de la Culture, διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0470