Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών:
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Τεχνικές ανίχνευσης περιεχομένου σε κρυπτογραφημένες επικοινωνίες – Τεχνολογικά και Ηθικά ζητήματα

Χρήστος Καλλίνης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών:

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Τεχνικές ανίχνευσης περιεχομένου σε κρυπτογραφημένες επικοινωνίες – Τεχνολογικά και Ηθικά ζητήματα

Χρήστος Καλλίνης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2022

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή ασχολείται με τεχνικές ανίχνευσης υλικού σεξουαλικής κακοποίησης ή/και παρενόχλησης παιδιών και με τα τεχνολογικά και ηθικά ζητήματα που προκύπτουν. Επικεντρώνεται στην «End-to-End κρυπτογράφηση» (E2EE) γιατί είναι η πιο ασφαλής μέθοδος και δυσχεραίνει πολύ την ανίχνευση τέτοιου υλικού, καθώς επιτρέπει στους κακοποιούς να αποκρύψουν από τις Αρχές το παράνομο περιεχόμενο που διακινούν, την ταυτότητά τους και τα ψηφιακά τους ίχνη.

Ως εκ τούτου, οι Αρχές επιβολής του νόμου «διαμαρτύρονται» στις κυβερνήσεις των χωρών τους ότι με την E2E κρυπτογράφηση, το έργο της καταπολέμησης αυτού του είδους εγκλήματος καθίσταται εξαιρετικά δύσκολο και ζητούν μέτρα παράκαμψής της ή ακόμα και απαγόρευση της διάθεσής της για το ευρύ κοινό. Σε αρκετές περιπτώσεις οι κυβερνήσεις συμφώνησαν και πέρασαν νέους νόμους με περιορισμούς στη χρήση της E2EE, ξεσήκωσαν όμως σφοδρές αντιδράσεις από άτομα και φορείς υπέρ της προστασίας των ανθρωπίνων δικαιωμάτων από οποιαδήποτε προσπάθεια παραβίασης. Διατείνονται ότι οι νόμοι αυτοί θα παραβιάσουν τα θεμελιώδη ατομικά δικαιώματα της «Ιδιωτικότητας», του «Απορρήτου των Επικοινωνιών» κ.α., καθώς θεωρούν σίγουρο ότι οι τεχνικές ανίχνευσης CSAM θα χρησιμοποιηθούν από κυβερνήσεις και για άλλους σκοπούς, εκμεταλλευόμενες «κερκόπορτες» που θα υπάρχουν στην κρυπτογράφηση.

Η διατριβή παρουσιάζει τα σχετικά ισχύοντα νομικά πλαίσια στην Ε.Ε, τις Η.Π.Α. και άλλες χώρες, καθώς και τα ηθικά ζητήματα που εγείρει η εφαρμογή τους. Επίσης περιγράφει συνοπτικά τις πιο σημαντικές τεχνικές που προτάθηκαν και αξιολογεί την αποτελεσματικότητά τους, την εφαρμοσιμότητα τους κ.α., αλλά και τους κινδύνους που ενδεχομένως απορρέουν από τη χρήση τους, για τα θεμελιώδη ανθρώπινα δικαιώματα.

Διαπιστώθηκε μια τάση των κυβερνήσεων παγκοσμίως να επιβάλουν με νόμους στους Παρόχους την εσκεμμένη υποβάθμιση της E2EE στις επικοινωνίες προκειμένου να διευκολυνθεί η ανίχνευση CSAM, η οποία όμως, όπως ειπώθηκε, συναντά ισχυρές αντιδράσεις. Επίσης διαπιστώθηκε, ότι όντως υπάρχουν κάποιες αρκετά υποσχόμενες τεχνικές, αλλά απαιτείται σημαντική περαιτέρω έρευνα και εξέλιξή τους προκειμένου να καταστούν πιο αξιόπιστες, κάτι που προς το παρόν δεν ισχύει.

Συμπερασματικά, καθώς και οι δύο πλευρές έχουν βάσιμα επιχειρήματα, εκτιμάται ότι η καλύτερη λύση θα είναι να υπάρξει σε παγκόσμιο επίπεδο ένα moratorium μεταξύ τους, ώστε να δοθεί στους ερευνητές ο απαραίτητος χρόνος, για να εξελίξουν πιο λειτουργικές και αξιόπιστες τεχνικές, που θα συνδυάζουν τα θετικά σημεία και των δύο πλευρών.

Summary

This postgraduate dissertation deals with the detection techniques of Child Sexual Abuse Material (CSAM) and Child Grooming material, as well as the technical and ethical issues which arise from their use. It focuses on «End-to-End Encryption» (E2EE) since it is the most secure method of encryption and therefore, it is assumed to be a barrier for detecting such material, because it allows criminals to hide from the Law Enforcement Agencies (LEA) the material itself, their identity and their digital traces.

Hence, the Law Enforcement Agencies of many countries "complain" to their governments that E2EE makes their task of fighting this kind of crime exceptionally difficult and ask for measures to circumvent it, or even ban its distribution for the general public. In several cases the governments concurred and passed new laws with limitations to the use of E2EE, but they triggered harsh reactions from people and foundations in favor of the protection of human rights from any violation attempt.

They argue that these laws will violate the fundamental human rights of "Privacy", the "Confidentiality of Communications" etc., as they consider certain that the CSAM detection techniques will be used by governments for other purposes too, exploiting "backdoors" that will exist in encryption.

The dissertation presents the relevant legislation in effect in the EU, USA and other countries, as well as the ethical issues raised by its application. It also describes concisely the most important proposed techniques and assesses their effectiveness, applicability etc., and the possible risks that may derive from their use, for the fundamental human rights.

It was established that there is a tendency of governments worldwide, to impose by law to Providers the deliberate degradation of E2EE in communications, in order to facilitate the detection of CSAM, which is met, as already said, with strong resistance. It was also established that there are indeed some quite promising techniques, but significant further research and development is needed in order to make them more reliable, which is currently not the case.

In conclusion, since both sides have valid arguments, it is considered that the best solution will be to establish a worldwide moratorium between them, in order to provide researchers with the necessary time, to develop techniques that are more operational and reliable and will combine the positive aspects of both views.

Ευχαριστίες

Θα ήθελα πρωτίστως να ευχαριστήσω θερμότατα τον καθηγητή μου κ. **Κωνσταντίνο Λιμνιώτη** που, κατόπιν μιας πολύς σοβαρής περιπέτειας με την υγεία μου που απείλησε έως και τη ζωή μου και τελικά με άφησε με σοβαρή αναπηρία, εξακολούθησε να πιστεύει σε μένα και με παρότρυνε να μην εγκαταλείψω την προσπάθεια (όπως είχα αρχικά αποφασίσει) και να συνεχίσω με την εκπόνηση της διατριβής μου!

Επίσης θα ήθελα να ευχαριστήσω και τη σύζυγο και τα παιδιά μου, που επίσης με παρότρυναν να συνεχίσω και με στήριξαν σε όλη αυτή τη μακρά και δύσκολη περίοδο με την εμβόλιμη ασθένειά μου!

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Μέσω του Διαδικτύου διακινείται σήμερα ένας τεράστιος όγκος πληροφοριών σε όλες τις μορφές πολυμέσων (κείμενο, εικόνα, βίντεο, ήχος) και προσφέρονται ποικίλοι τρόποι επικοινωνίας μεταξύ των ατόμων και εύκολης ανταλλαγής/διαμοιρασμού των πληροφοριών αυτών, ενώ προστίθενται διαρκώς καινούργιοι τρόποι.

Η επικοινωνία γενικότερα καθώς και η ανταλλαγή δεδομένων και πληροφοριών βασίζονται σε τρείς αυτονόητους κανόνες που αποτελούν ταυτόχρονα και θεμελιώδεις πυλώνες των σύγχρονων Δημοκρατιών: την «Ελευθερία της Έκφρασης» και την εξασφάλιση του «Απορρήτου των Επικοινωνιών» και κατά συνέπεια την «Προστασία της Ιδιωτικότητας».

Για την υποστήριξη του πρώτου πυλώνα, στις Δημοκρατίες υφίσταται ένα ευρύ πλαίσιο από νόμους που θέτουν τα όρια εντός των οποίων πρέπει να λειτουργούν τα άτομα.

Στην υποστήριξη του δεύτερου και τρίτου πυλώνα παίζει κρίσιμο ρόλο, μεταξύ άλλων, η κρυπτογράφηση, καθώς επιτυγχάνει σε μεγάλο βαθμό τη διατήρηση του απορρήτου των διακινούμενων στο Διαδίκτυο, δεδομένων και πληροφοριών.

Όμως, σε κάθε κοινωνία υπάρχουν και άτομα που επιλέγουν να δρουν έξω από τα προαναφερθέντα νομικά όρια και εκμεταλλεύονται σε μεγάλο βαθμό την κρυπτογραφία προκειμένου να καλύψουν τη δράση και την ταυτότητά τους.
Χαρακτηριστικά παραδείγματα είναι η φωτογραφία και το βίντεο, δύο μοντέρνες τέχνες που δύνανται να είναι υψηλής αισθητικής, να συμβάλλουν στην καλλιέργεια των ανθρώπων και να τους προσφέρουν ψυχαγωγία και ενημέρωση. Στα χέρια όμως κάποιων ατόμων, μετατρέπονται σε εγκληματικά υποπροϊόντα που αποσκοπούν στο κέρδος από την εξυπηρέτηση και ικανοποίηση αρρωστημένων παθών, όπως συμβαίνει με τις φωτογραφίες και τα βίντεο παιδικής πορνογραφίας. Μάλιστα υπάρχουν πια αδιάσειστα στοιχεία από πολλές χώρες που δείχνουν ότι τα άτομα αυτά επιλέγουν να διακινούν το παράνομο υλικό τους, χρησιμοποιώντας κρυπτογραφημένες υπηρεσίες επικοινωνίας του

Διαδικτύου, με αποτέλεσμα η ανίχνευσή του, καθώς και ο εντοπισμός των ιδίων από τις Αρχές να καθίσταται εξαιρετικά δυσχερής.

Πρόκειται για στυγνούς εγκληματίες που κινούνται σαφέστατα εκτός των ανωτέρω ορίων και νόμων, αλλά και πέραν πάσης ηθικής, καταστρέφοντας παιδικές ψυχές. Κάθε σύγχρονη κοινωνία που σέβεται τα μέλη της και ιδιαίτερα τα παιδιά της, οφείλει να έχει τους κατάλληλους μηχανισμούς για να τους εντοπίζει και να εξαρθρώνει τα κυκλώματά τους, να τους διώκει ποινικά, και να τους τιμωρεί παραδειγματικά.

1.1 Βασικά Ερευνητικά ερωτήματα και Σκοπός της διατριβής

Για την ανωτέρω ανάγκη δεν υφίσταται αμφισβήτηση, αλλά φαίνεται να υπάρχουν δύο αρκετά διαφορετικές απόψεις, πάνω στο θέμα του τρόπου με τον οποίο θα πρέπει να γίνεται η έρευνα για τον εντοπισμό του παιδο-πορνογραφικού υλικού.
Οι δύο διαφορετικές απόψεις έγκεινται στο ότι ουσιαστικά το εν λόγω ζήτημα έχει να κάνει με «σύγκρουση» δύο θεμελιωδών δικαιωμάτων:

Αφενός, το αυτονόητο δικαίωμα κάθε παιδιού στην προστασία του από κάθε μορφή σεξουαλικής εκμετάλλευσης ή/και κακοποίησης, συμπεριλαμβανομένης βέβαια της παιδικής πορνογραφίας και γενικά κάθε παράνομης σεξουαλικής δραστηριότητας (και φυσικά την εξάλειψη τέτοιων παράνομων ενεργειών), και αφετέρου το δικαίωμα όλων στο «απόρρητο των επικοινωνιών» τους, το οποίο είναι, μεταξύ άλλων, στενά συνυφασμένο με το δικαίωμα «προστασίας της ιδιωτικότητάς» τους. Ειδικότερα:

Όπως προαναφέρθηκε, η μία άποψη, που εκφράζεται κυρίως από Διωκτικές αρχές και Κυβερνήσεις, διατείνεται ότι καθώς οι μέθοδοι κρυπτογράφησης διαρκώς εξελίσσονται και κατόπιν γίνονται διαθέσιμες στο ευρύ κοινό, το έργο του εντοπισμού εκ μέρους τους του διακινούμενου στο Διαδίκτυο παράνομου υλικού παιδικής πορνογραφίας και συνεπακόλουθα, της εξάρθρωσης των κυκλωμάτων πίσω απ' αυτό, γίνεται όλο και δυσκολότερο. Για τον λόγο αυτόν προτείνουν τη λήψη δραστικών μέτρων (που περιγράφονται κατωτέρω στη διατριβή αυτή) και φτάνουν έως και την πλήρη εξάλειψη της κρυπτογράφησης δεδομένων για τις διαθέσιμες στο κοινό υπηρεσίες ψηφιακής επικοινωνίας.

Η άλλη άποψη, που εκφράζεται κυρίως από οργανισμούς και ιδρύματα για την προώθηση της Δημοκρατίας και των δικαιωμάτων του ανθρώπου, αναγνωρίζει μεν την ανάγκη καταπολέμησης της διακίνησης παιδικής πορνογραφίας, αλλά αντιτίθεται στα προτεινόμενα από τις Αρχές μέτρα με το σκεπτικό ότι:
α) αφενός τα μέτρα αυτά παραβιάζουν θεμελιώδη δικαιώματα των ατόμων, και
β) αφετέρου υποστηρίζει πως υπάρχουν διαθέσιμες συγκεκριμένες τεχνικές που μπορούν να χρησιμοποιήσουν οι Αρχές για να ανιχνεύουν αποτελεσματικά υλικό παιδικής πορνογραφίας σε κρυπτογραφημένα δεδομένα, χωρίς να παραβιάζουν θεμελιώδη ατομικά δικαιώματα.

Το εν λόγω ζήτημα είναι απόλυτα επίκαιρο, αφού μέσα στο 2022 η Ευρωπαϊκή Επιτροπή ανακοίνωσε σχέδιο Κανονισμού αναφορικά με υποχρεώσεις των Παρόχων τηλεπικοινωνιακών υπηρεσιών που θα πρέπει να ανταποκρίνονται σε αιτήματα των διωκτικών αρχών για εντοπισμό τέτοιου παράνομου υλικού. Ωστόσο, από τις υποχρεώσεις αυτές, διαφαίνεται ότι η εκπλήρωσή τους πιθανότατα απαιτεί την κατάργηση ή έστω την υποβάθμιση της κρυπτογράφησης που χρησιμοποιείται ήδη στις υπηρεσίες αυτές.

Η παρούσα διατριβή στοχεύει στην παρουσίαση:
Α) των υφιστάμενων (αλλά και των προτεινόμενων) σχετικών με το ανωτέρω ζήτημα Νομικών πλαισίων σε χώρες όπως οι Η.Π.Α., η Αυστραλία, η Βρετανία, και φυσικά στις χώρες της Ευρωπαϊκής Ένωσης, και
Β) των προαναφερθέντων τεχνικών (π.χ. Machine Learning, Perceptual Hashing, Client-side scanning κ.α.), προκειμένου να υπάρξει μία συγκριτική αποτίμηση τόσο της αποτελεσματικότητάς τους, όσο και των κινδύνων για την προστασία θεμελιωδών ατομικών δικαιωμάτων που ενδεχομένως απορρέουν από τη χρήση τους. Επίσης, καθώς και η Ελλάδα και η Κύπρος είναι μέλη της Ευρωπαϊκής Ένωσης, τα τεχνολογικά χαρακτηριστικά της κάθε περίπτωσης θα αποτιμηθούν και υπό το φως και των νομικών απαιτήσεων της ΕΕ για την προστασία των προσωπικών δεδομένων.

Απώτερος στόχος είναι η εξαγωγή συμπερασμάτων ως προς το εάν οι υπάρχουσες σήμερα τεχνολογίες αιχμής σε αυτόν τον τομέα, θα μπορούσαν να χρησιμοποιηθούν σε αυτήν την κατεύθυνση ή εάν ακόμα δεν είναι «ώριμες» και θα πρέπει να υπάρξει περαιτέρω έρευνα σε συγκεκριμένες τεχνολογικές κατευθύνσεις.

1.2. Αναγκαιότητα και σπουδαιότητα της διατριβής

Το αντικείμενο της παρούσας διατριβής αποτελεί σήμερα ανοιχτό ερευνητικό πεδίο στο οποίο έχουν εστιάσει αρκετές ομάδες (ερευνητές, νομοθέτες, αρμόδιες αρχές), ακριβώς λόγω του ότι διαμορφώνεται νέο νομικό πλαίσιο που μπορεί να επηρεάσει ουσιωδώς θεμελιώδη ατομικά δικαιώματα.

1.3 Δομή της διατριβής

- Στο 2ο Κεφάλαιο που ακολουθεί γίνεται αναφορά στο τι είναι γενικά η Κρυπτογραφία το Hashing και η End-to-End Κρυπτογράφηση, καθώς είναι έννοιες που εμφανίζονται συχνά στα επόμενα κεφάλαια.
- Στο 3ο Κεφάλαιο εξετάζεται συνοπτικά το νομικό πλαίσιο που ισχύει στην Ευρωπαϊκή Ένωση αναφορικά με την προστασία των δεδομένων και της ιδιωτικότητας (privacy) και γίνεται ιδιαίτερη αναφορά στον GDPR και τα βασικά του άρθρα καθώς και στην «e-Privacy» οδηγία.
- Στο 4ο Κεφάλαιο γίνεται μια γενική επισκόπηση του ζητήματος της ενδεχόμενης ανάγκης(;) για έλεγχο των επικοινωνιών και τίθενται προβληματισμοί ως προς τον βαθμό που αυτός ο έλεγχος θα επηρεάσει αρνητικά τα θεμελιώδη δικαιώματα των χρηστών. Γίνονται ιδιαίτερες αναφορές στο αμφιλεγόμενο παράδειγμα της Αυστραλίας και τον νόμο που πέρασε το κοινοβούλιό της, στην περίπτωση των Η.Π.Α. με τον νόμο EARN IT και τις αντιδράσεις που προκάλεσε, καθώς και στα ισχύοντα στην Βρετανία.
- Στο 5ο Κεφάλαιο εξηγείται η ισχύουσα (κατά τη διάρκεια της πανδημίας και προς το παρόν) κατάσταση στην ΕΕ σε σχέση με τον έλεγχο του περιεχομένου των επικοινωνιών, που διέπεται από τον (προσωρινό) Ευρωπαϊκό Κανονισμό 2021/1232. Επίσης παρουσιάζονται τα προβλεπόμενα σχετικά με το ίδιο θέμα μέτρα που περιέχει η Πρόταση νέου Κανονισμού της ΕΕ για ανίχνευση CSAM και Grooming, καθώς και η άποψη των EDPB και EDPS επί αυτής.
- Στο 6ο Κεφάλαιο παρουσιάζονται οι τεχνικές λύσεις ελέγχου περιεχομένου σε E2E κρυπτογραφημένες επικοινωνίες που περιέχονται σε παράρτημα της προαναφερθείσας Πρότασης Κανονισμού της ΕΕ και αποτιμώνται αφενός ως προς την αποτελεσματικότητά τους και αφετέρου ως προς την (ενδεχόμενη) προσβολή της ιδιωτικότητας των χρηστών.

- Στο 7ο Κεφάλαιο περιγράφονται τα τεχνικά προβλήματα που αντιμετωπίζουν οι λύσεις που παρουσιάστηκαν στο προηγούμενο κεφάλαιο.
- Στο 8ο Κεφάλαιο, παρουσιάζονται τα συμπεράσματα της διατριβής, και
- Στο 9ο Κεφάλαιο ακολουθεί ο Επίλογος.

Κεφάλαιο 2

Κρυπτογραφία, Hashing & End-to-End Κρυπτογράφηση

Ήδη από το προηγούμενο Κεφάλαιο έγινε προφανές πως το θέμα που εξετάζεται στην παρούσα διατριβή σχετίζεται στενά με την Κρυπτογραφία και ειδικότερα με μια συγκεκριμένη μέθοδο κρυπτογράφησης που ονομάζεται End-to-End Encryption ή «Διατερματική Κρυπτογράφηση» στα Ελληνικά και για συντομία E2EE, καθώς επίσης και με το Hashing. Κρίνεται λοιπόν σκόπιμο στο σημείο αυτό να γίνει αναφορά στο τι είναι γενικά η Κρυπτογραφία και τι η End-to-End Κρυπτογράφηση και το Hashing.

2.1. Κρυπτογραφία

Η **Κρυπτογραφία** μελετά (μαθηματικές) τεχνικές με τις οποίες ένα μήνυμα μπορεί να μετασχηματιστεί σε μία **ακατάληπτη μορφή**, ώστε ακόμα και αν υποκλαπεί από κάποιον, να μην μπορεί να αναγνωστεί [15, 23].

Από το παραπάνω συνάγεται ότι η κρυπτογραφία αποσκοπεί πρωτίστως στη διασφάλιση της εμπιστευτικότητας της πληροφορίας, ωστόσο η χρησιμότητά της είναι πολύ ευρύτερη. Συγκεκριμένα, στοχεύει και στη διασφάλιση διαφόρων ζητημάτων που άπτονται της ασφάλειας της πληροφορίας. Επομένως αποσκοπεί στην [15, 23]:

1. **Εμπιστευτικότητα** (**Confidentiality**): μόνο ο παραλήπτης να μπορεί να διαβάσει κάποιο μήνυμα που απευθύνεται μόνο σε αυτόν.
2. **Πιστοποίηση της Ταυτότητας** του αποστολέα (**Authentication**)
3. Διασφάλιση της **Ακεραιότητας** της πληροφορίας (**Integrity**): δηλαδή ότι το μήνυμα δεν έχει αλλοιωθεί από κάποιον τρίτο.

Στο χώρο της κρυπτογραφίας, οι έννοιες της κρυπτογράφησης και αποκρυπτογράφησης ορίζονται ως εξής [15, 23]:

- **Κρυπτογράφηση**: είναι η διαδικασία μετατροπής ενός μηνύματος σε ακατάληπτη μορφή, και
- **Αποκρυπτογράφηση**: είναι η αντίστροφη διαδικασία.

Η κρυπτογραφία παίζει πολύ κρίσιμο ρόλο στην προστασία της ιδιωτικότητας και της ελεύθερης έκφρασης των ατόμων/χρηστών, όταν αυτοί είναι διασυνδεδεμένοι (online). Δεν θα ήταν εφικτό να μεταδοθεί καμία πληροφορία (π.χ. μήνυμα ηλεκτρονικού ταχυδρομείου, μήνυμα κειμένου-chat, βιντεοκλήση) με ασφάλεια, δηλαδή με την σιγουριά ότι δεν θα το δει/υποκλέψει κάποιος τρίτος. Ούτε θα ήταν εφικτό να πραγματοποιηθούν συναλλαγές (π.χ. διαδικτυακές αγορές), χωρίς τη χρήση της κρυπτογραφίας – η οποία μάλιστα πρέπει να είναι και ισχυρή για να είναι αποτελεσματική.

Σε μια τυπική κρυπτογράφηση ενός μηνύματος, ο κρυπταλγόριθμος παίρνει σαν είσοδο το κείμενο του μηνύματος καθώς και ένα ψηφιακό κλειδί (που γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης του μηνύματος) και παράγει ένα κρυπτοκείμενο, δηλαδή μια ακατάληπτη (κρυπτογραφημένη) μορφή του αρχικού κειμένου, η οποία αποστέλλεται στον παραλήπτη. Εκείνος, προκειμένου να το διαβάσει, χρησιμοποιεί το ίδιο ψηφιακό κλειδί και αποκρυπτογραφεί το κρυπτοκείμενο στην αρχική του αναγνώσιμη μορφή [15, 23].

Η Κρυπτογράφηση δεδομένων συνήθως χρησιμοποιείται ως κομμάτι ενός ευρύτερου «συστήματος» όπως μια εφαρμογή «αποστολής Μηνυμάτων» (Messaging) ή μια υπηρεσία «Αποθήκευσης δεδομένων» των χρηστών σε «Νέφος» (Cloud Storage Service). Και επειδή ουσιαστικά βασίζεται στο να μοιράζονται τα δύο μέρη (αποστολέας και παραλήπτης) από κοινού το ίδιο ψηφιακό κλειδί (διαδικασία key exchange and sharing), για την αποτελεσματική εφαρμογή και λειτουργία της, είναι κεφαλαιώδους σημασίας η διαχείριση της διαδικασίας αυτής κατά τρόπο απολύτως ασφαλή. Κατά κανόνα, το κλειδί της «συμμετρικής κρυπτογράφησης» – που είναι η περίπτωση της κρυπτογράφησης που αναφέραμε ανωτέρω – ανταλλάσσεται με ασφάλεια με ένα άλλο είδος κρυπτογράφησης που ονομάζεται «ασύμμετρη».

2.2. Κρυπτογραφικές συναρτήσεις κατακερματισμού

Μια Hashing συνάρτηση ή «συνάρτηση κατακερματισμού» είναι μια κρυπτογραφική λειτουργία που κάθε είσοδο τη μετασχηματίζει σε μια μικρή σχετικά αλφαριθμητική σειρά σταθερού μήκους που ονομάζεται «Hash» (ψηφιακό αποτύπωμα) και είναι μοναδική για την είσοδο αυτή και μη αντιστρεπτή.

Συγκεκριμένα, μία κρυπτογραφική συνάρτηση κατακερματισμού έχει τις εξής ιδιότητες:

- Για συγκεκριμένη έξοδο, δεν είναι πρακτικά εφικτός ο υπολογισμός της αντίστοιχης εισόδου. Η ιδιότητα αυτή αναφέρεται στη βιβλιογραφία ως ανθεκτικότητα ως προς την προ-απεικόνιση (preimage resistance).
- Για συγκεκριμένη έξοδο και μια είσοδο που την παράγει, δεν είναι πρακτικά εφικτή η εύρεση μίας άλλης εισόδου που να παράγει την ίδια έξοδο. Η ιδιότητα αυτή αναφέρεται στη βιβλιογραφία ως δεύτερη ανθεκτικότητα ως προς την προ-απεικόνιση (second preimage resistance).
- Είναι πρακτικά μη εφικτό, να βρεθούν δύο οποιεσδήποτε είσοδοι οι οποίες να παράγουν την ίδια έξοδο. Η ιδιότητα αυτή αναφέρεται στη βιβλιογραφία ως ανθεκτικότητα ως προς τις «συγκρούσεις» (collision resistance).

Ως άμεση απόρροια των ανωτέρω, ακόμα και αν δύο αρχεία διαφέρουν ελάχιστα μεταξύ τους, τα αντίστοιχα αποτυπώματα (cryptographic hashes) θα είναι πολύ διαφορετικά – γενικότερα, κάθε bit του μηνύματος εισόδου επηρεάζει σημαντικά το αποτύπωμα. Το «κρυπτογραφικό Hashing» χρησιμοποιείται για έλεγχο εγκυρότητας (ακεραιότητας) ενός αρχείου, μιας «εικόνας» (image) σκληρού δίσκου, για ανάλυση ψηφιακών πειστηρίων, για παραγωγή ψηφιακών υπογραφών κτλ.

Πέραν του κρυπτογραφικού hashing, τα τελευταία χρόνια έχει αναπτυχθεί το λεγόμενο «αντιληπτικό» - Perceptual Hashing (που μας ενδιαφέρει στην παρούσα διατριβή). Στοχεύει στην αντιστοίχιση παρόμοιων hashes σε παρόμοιο περιεχόμενο (π.χ. εικόνες) και του οποίου οι αλγόριθμοι διαφέρουν σημαντικά από το κρυπτογραφικό. Με άλλα λόγια, τα «αποτυπώματα» μπορούν να καταδεικνύουν ότι πρόκειται για ίδιες εισόδους, ακόμα και αν οι είσοδοι ως αρχεία δεν είναι ολόιδια αλλά έχουν υποστεί κάποιες μεταβολές, απλά και μόνο για να μην ταυτίζονται τα αποτυπώματα μέσω κρυπτογραφικών συναρτήσεων κατακερματισμού (π.χ., αν πρόκειται για αρχείο φωτογραφίας ή video, υλοποίηση αλλαγής φωτισμού στο ένα αρχείο).

Χρησιμοποιείται ευρέως στα μοντέλα Ταύτισης που αποσκοπούν στον εντοπισμό πιθανού CSAM που ταυτίζεται ακριβώς ή σε πολύ μεγάλο βαθμό με ήδη γνωστό CSAM. Αρχικά ο υπολογιστής που εκτελεί τον Hashing αλγόριθμο εξάγει από το υπό έλεγχο περιεχόμενο, για παράδειγμα μια φωτογραφία, το ψηφιακό της αποτύπωμα – hash, καθώς είναι πολύ πιο εύκολα διαχειρίσιμο και καταλληλότερο για αυτόματη (μέσω υπολογιστή) σύγκριση, από το αυθεντικό περιεχόμενο από το οποίο προήλθε, δηλαδή την ίδια την φωτογραφία. Κατόπιν γίνεται η σύγκριση του hash αυτού με hashes από φωτογραφίες με επιβεβαιωμένο περιεχόμενο CSA και εφόσον διαπιστωθεί πλήρης, ή έστω μερική, αλλά σε μεγάλο βαθμό ταύτιση, η εν λόγω φωτογραφία χαρακτηρίζεται ως ύποπτη και αποστέλλεται για περαιτέρω (οπτικό) έλεγχο από άνθρωπο.

2.3 End-to-End (Διατερματική) Κρυπτογράφηση

Η «End-to-End Encryption (E2EE)» είναι μια αρχιτεκτονική κρυπτογράφησης που προστατεύει σε συνεχή βάση τα δεδομένα που ανταλλάσσονται μεταξύ δύο ή περισσοτέρων χρηστών και παρέχει το μέγιστο επίπεδο ασφαλείας. Στην E2EE τα δεδομένα κρυπτογραφούνται στη συσκευή του χρήστη και μπορούν να αποκρυπτογραφηθούν μόνο από εξουσιοδοτημένους χρήστες που έχουν ανταλλάξει μεταξύ τους κλειδιά και είναι οι μόνοι που τα γνωρίζουν. Έτσι οι τυχόν επίδοξοι επιτιθέμενοι στη διαδρομή, δεν μπορούν να τα «διαβάσουν», ούτε καν οι διάφοροι ενδιάμεσοι Πάροχοι Υπηρεσιών Επικοινωνίας [02].

Πιο συγκεκριμένα, μια υπηρεσία επικοινωνίας ή εφαρμογή είναι «End-to-End» κρυπτογραφημένη εφόσον τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που διακινεί ή διαχειρίζεται, είναι γνωστά μόνο στον αποστολέα και στους εξουσιοδοτημένους παραλήπτες αυτών των δεδομένων. Αυτό σημαίνει πως όλα τα ενδιάμεσα μέρη που δρομολογούν, αποθηκεύουν, παίρνουν αντίγραφα ασφαλείας και διαχειρίζονται τα κρυπτογραφημένα αυτά δεδομένα, δεν έχουν πρόσβαση στα κλειδιά και επομένως δεν έχουν τη δυνατότητα να μάθουν οτιδήποτε γι' αυτά. Στην πράξη (π.χ. σε μία εφαρμογή συνομιλίας ή τηλεδιάσκεψης), αυτό σημαίνει ότι οι μόνοι που μπορούν να διαβάσουν τα μηνύματα/αρχεία (ή κάθε άλλου είδους δεδομένα, όπως ήχος ή βίντεο) που ανταλλάσσονται είναι τα δύο συνδιαλεγόμενα μέρη. Ο Πάροχος της υπηρεσίας δεν έχει τη δυνατότητα να αναγνώσει τα δεδομένα,

καθώς δεν μπορεί να αποκτήσει πρόσβαση στο συμμετρικό κλειδί κρυπτογράφησης που έχουν ανταλλάξει οι δύο χρήστες [02].

Κρυπτογράφηση «end-to-end» υλοποιείται από διάφορες γνωστές εφαρμογές όπως οι Viber και Signal, ενώ εφαρμογές όπως το Skype και το Messenger δεν την εφαρμόζουν.

Κεφάλαιο 3

Προστασία προσωπικών δεδομένων και ιδιωτικότητα: Νομικό πλαίσιο ΕΕ

Στο κεφάλαιο αυτό θα εξεταστεί συνοπτικά το νομικό πλαίσιο που ισχύει στην Ευρωπαϊκή Ένωση (ΕΕ) αναφορικά με την προστασία των δεδομένων και της ιδιωτικότητας (privacy) των χρηστών.

3.1. Εισαγωγή

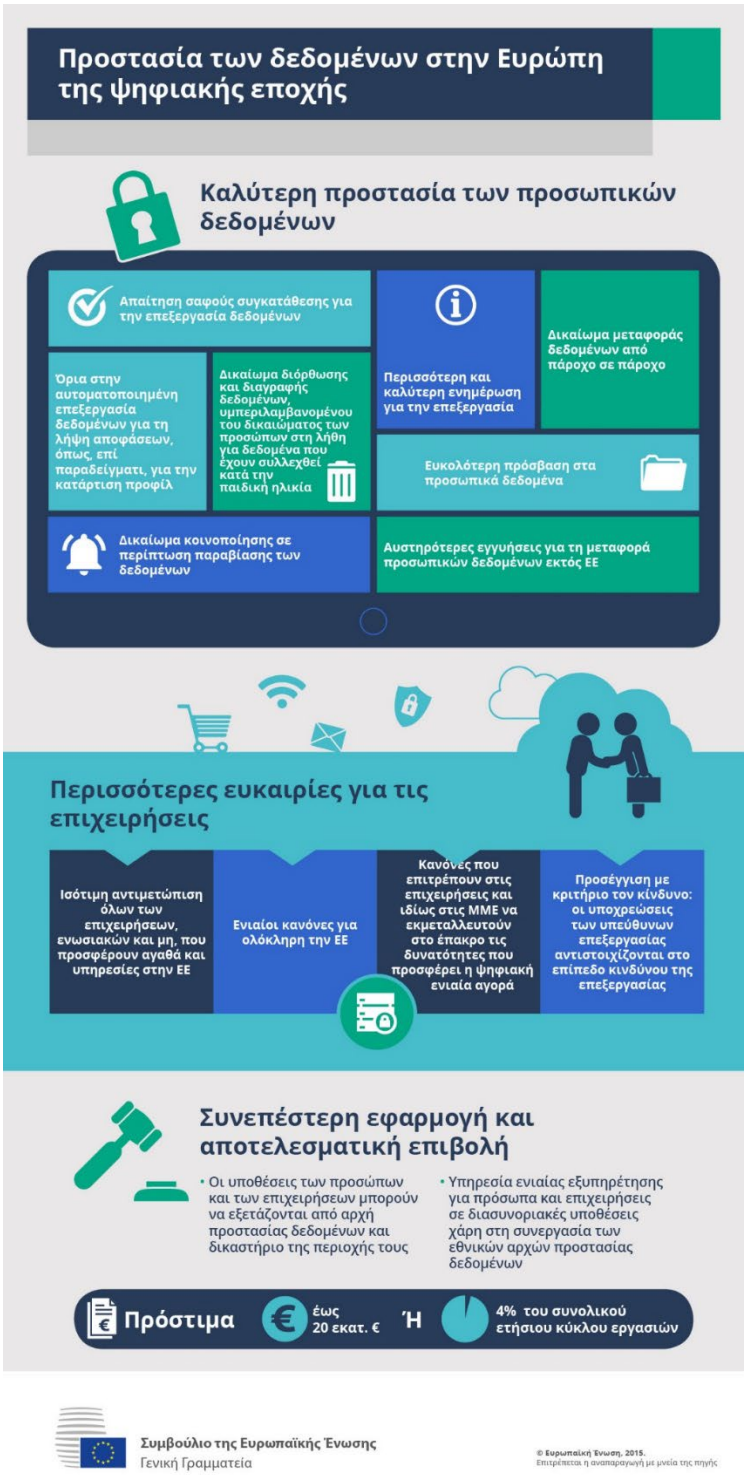
Η προστασία των δεδομένων προσωπικού χαρακτήρα θεωρείται και αποτελεί θεμελιώδες δικαίωμα για την Ευρωπαϊκή Ένωση (από το 2007 - Συνθήκη Λισαβόνας), δηλαδή υπάρχει συγκεκριμένο νομικό υπόβαθρο, πάνω στο οποίο το Ευρωκοινοβούλιο νομοθετεί προκειμένου να το προστατεύει διαχρονικά.
Πιο συγκεκριμένα το άρθρο 7 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ κατοχυρώνει το δικαίωμα της «ιδιωτικότητας» (privacy) καθώς αναφέρει ότι «*κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του*», ενώ στο άρθρο 8 ορίζεται ότι «*κάθε πολίτης της ΕΕ έχει δικαίωμα:*

- *στην προστασία των προσωπικών δεδομένων που τον/την αφορούν*
- *στην πρόσβαση σε δεδομένα που έχουν συλλεγεί και τον/την αφορούν, και στη διόρθωσή τους*» [21].

3.2 Ευρωπαϊκός Γενικός Κανονισμός Προστασίας των Δεδομένων (GDPR)

Το 2018 το όλο πλαίσιο αυστηροποιήθηκε καθώς τέθηκε σε εφαρμογή ο Γενικός Κανονισμός της Ευρωπαϊκής Ένωσης για την Προστασία των Δεδομένων (General Data

Protection Regulation - GDPR). Ο GDPR αποτελεί ένα ενιαίο σύνολο κανόνων, δεσμευτικό για όλα τα κράτη μέλη και όλες τις εταιρίες που τηρούν προσωπικά δεδομένα και δραστηριοποιούνται στην Ένωση (ασχέτως με το πού εδρεύουν), με στόχο την προστασία των πολιτών από την ανεξέλεγκτη διάθεση και χρήση των προσωπικών τους δεδομένων (με ιδιαίτερη έμφαση στα δεδομένα που τηρούνται σε ψηφιακή μορφή).



Σχήμα 1. GDPR [22].

Απώτερος σκοπός του GDPR είναι, οι πολίτες των κρατών – μελών της Ευρωπαϊκής Ένωσης να έχουν καλύτερο έλεγχο των προσωπικών τους δεδομένων, γνωρίζοντας πλήρως και αποφασίζοντας οι ίδιοι ποιες εταιρείες και οργανισμοί θα τα διατηρούν, ποια και τι είδους δεδομένα τους θα υφίστανται επεξεργασία, για πόσο χρονικό διάστημα, για ποια χρήση και για ποιο σκοπό.

Αλλά και οι εταιρείες/οργανισμοί που εκ της φύσης τους τηρούν προσωπικά δεδομένα, έχουν ένα συγκεκριμένο, ευρέως γνωστό και κοινό για όλους πλαίσιο, εντός του οποίου πρέπει να λειτουργούν και φυσικά να συμμορφώνονται με τις επιταγές του. Έτσι, αφενός προστατεύονται αποτελεσματικότερα τα προσωπικά δεδομένα των πολιτών και αφετέρου εξασφαλίζονται σε μεγάλο βαθμό συνθήκες υγιούς ανταγωνισμού για τις εν λόγω εταιρείες.

Ο GDPR δίνει ιδιαίτερη έμφαση στη διαφάνεια της επεξεργασίας, όπως επίσης και στα δικαιώματα των υποκειμένων των δεδομένων, όπως είναι το δικαίωμα πρόσβασης (δικαίωμα του να μάθει ένα πρόσωπο λεπτομερώς πληροφορίες για την επεξεργασία που υφίστανται τα δεδομένα του, αλλά και να λάβει αντίγραφο αυτών), το δικαίωμα διόρθωσης των δεδομένων (εφόσον π.χ. ένας οργανισμός διαθέτει ανακριβείς πληροφορίες για ένα άτομο), το δικαίωμα διαγραφής των δεδομένων, το δικαίωμα μη αυτοματοποιημένης λήψης αποφάσεων (συμπεριλαμβανομένης της δημιουργίας προφίλ) κ.α.

3.3. Βασικά άρθρα του GDPR

Εμβαθύνοντας στον GDPR, παρατίθενται συνοπτικά κατωτέρω τα πιο σημαντικά άρθρα του.

Ας δούμε πρώτα τι νοούνται ως «δεδομένα προσωπικού χαρακτήρα» για τον GDPR, σύμφωνα με το άρθρο 4 του εν λόγω κανονισμού: Είναι «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη*

σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου» [18].

Σύμφωνα με τα παραπάνω, στοιχεία του ατόμου που αποτελούν προσωπικά δεδομένα είναι, ενδεικτικά, το ονοματεπώνυμό του, η εικόνα/φωτογραφία του, η διεύθυνση κατοικίας του, ο αριθμός της ταυτότητάς/διαβατηρίου του, η διεύθυνση IP και η διεύθυνση email, η τοποθεσία που βρίσκεται ανά πάσα στιγμή, δεδομένα που αφορούν την υγεία του κ.α.

Ορίζεται επίσης η έννοια της επεξεργασίας προσωπικών δεδομένων ως εξής: «*επεξεργασία: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*» [18].

Τέλος, στο ίδιο άρθρο, ορίζεται ο «Υπεύθυνος Επεξεργασίας» που κάθε οργανισμός ή εταιρεία που τηρεί δεδομένα προσωπικού χαρακτήρα, οφείλει να έχει προκαθορίσει:

Είναι το «*φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους*» [18].

Ο Υπεύθυνος επεξεργασίας φέρει την ευθύνη να συμμορφώνεται πλήρως με τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που σύμφωνα με το άρθρο 5 του GDPR: «*υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»)»,..,«συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς, …, είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται, ,…, διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται»* και *«υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια» ,…, «την προστασία τους από μη εξουσιοδοτημένη ή*

παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»)» [18].

Το άρθρο 6 του GDPR καθορίζει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα «*είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:*

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία τους για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί» (Σημείωση: δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους).

Ουσιαστικά, για να είναι νόμιμη μία επεξεργασία προσωπικών δεδομένων, πρέπει να πληρούνται σωρευτικά όλες οι προϋποθέσεις νομιμότητας του άρθρου 5, ενώ επιπροσθέτως θα πρέπει να εφαρμόζεται τουλάχιστον μία εκ των νομικών βάσεων του άρθρου 6 του GDPR [18].

Όταν όμως πρόκειται για παιδί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών, το άρθρο 8 του GDPR καθορίζει ότι «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα παιδιού είναι σύννομη εάν το παιδί είναι τουλάχιστον 16 χρονών. Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού*». Απαιτείται μάλιστα από τον υπεύθυνο επεξεργασίας να χρησιμοποιήσει κάθε διαθέσιμη τεχνολογία για να «*επαληθεύσει ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού*». Τέλος, το άρθρο επιτρέπει στα κράτη μέλη να καθορίσουν με νόμο μικρότερη ηλικία, αλλά με κατώτατο όριο τα 13 έτη [18].

Το άρθρο 25 προβλέπει την «*Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού*" (by design & by default). Συγκεκριμένα επιφορτίζει τον υπεύθυνο επεξεργασίας να «*εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων*» και επιπλέον «*να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας*» [18].

Με απλά λόγια, όταν πρόκειται να υλοποιηθεί ένα σύστημα/εφαρμογή μέσω του οποίου θα γίνεται επεξεργασία προσωπικών δεδομένων, η σχεδίαση εξ αρχής πρέπει να λαμβάνει υπόψη τις απαιτήσεις για προστασία των προσωπικών δεδομένων διότι, διαφορετικά, μπορεί να είναι πολύ δύσκολο ή και αδύνατο να ενσωματωθούν εκ των υστέρων.

Το άρθρο 32 μεριμνά για την "Ασφάλεια της επεξεργασίας" αναφέροντας ότι «*κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους*». Επίσης επιφορτίζει τον υπεύθυνο επεξεργασίας καθώς και αυτόν που την εκτελεί να «*εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το*

κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,

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

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

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

Τέλος επιφορτίζει τον υπεύθυνο της επεξεργασίας που θα κάνει την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας που θα πρέπει να εφαρμόζεται (και έχει την σχετική ευθύνη γι' αυτό) να λαμβάνει ιδιαίτερα υπόψη τους κινδύνους «*που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*» [18].

Με άλλα λόγια, ο GDPR προκρίνει σαφώς μία διαχείριση κινδύνων, προκειμένου να ληφθούν οι σωστές αποφάσεις για τα κατάλληλα μέτρα ασφάλειας που θα πρέπει να υλοποιούνται κάθε φορά.

3.4. Οδηγία «E-Privacy»

Πολύ πριν από την εφαρμογή του GDPR, ήδη από το 2002, είχε εκδοθεί από το Ευρωπαϊκό Κοινοβούλιο η Οδηγία 2002/58/ΕΚ γνωστότερη και ως οδηγία «e-Privacy», που εξειδικεύει το θέμα της προστασίας των προσωπικών δεδομένων για τις ηλεκτρονικές επικοινωνίες συγκεκριμένα.

Καταρχάς υποχρεώνει όλα τα κράτη μέλη να κατοχυρώσουν το απόρρητο των επικοινωνιών μέσω της εθνικής τους νομοθεσίας και απαγορεύει «*την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη*

συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια» ή «*όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα*» [17].

Επιτρέπει στις Τηλεπικοινωνιακές εταιρείες και οργανισμούς την αποθήκευση (σε ίδια μέσα ή ακόμα και στον τερματικό εξοπλισμό των συνδρομητών/χρηστών τους) πληροφοριών που τους αφορούν, καθώς και την πρόσβαση σε αυτές, μόνον εφόσον παρέχουν στον συγκεκριμένο συνδρομητή ή χρήστη σαφή και εκτεταμένη ενημέρωση «*μεταξύ άλλων για το σκοπό της επεξεργασίας*», καθώς και το δικαίωμα να αρνείται την επεξεργασία αυτή. Δεν εμποδίζει όμως «*οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, …, είναι αναγκαία για τη διενέργεια ή τη διευκόλυνση μιας επικοινωνίας, ή μόνο για την παροχή υπηρεσίας, …, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής*» [17].

Εφόσον όμως ο εξοπλισμός των χρηστών επιτρέπει σε άλλους να έχουν απομακρυσμένη πρόσβαση σε αυτόν «παρακολουθώντας» τις πράξεις και τις συμπεριφορές τους (π.χ. cookies – καταναλωτική συμπεριφορά) θα πρέπει η όλη διαδικασία να λειτουργεί με τη μεγαλύτερη δυνατή διαφάνεια και υπό τον έλεγχο των χρηστών.

Όσον αφορά τα δεδομένα κίνησης που αποθηκεύονται και υποβάλλονται σε επεξεργασία, ο Τηλεπικοινωνιακός φορέας πρέπει να ενημερώνει τον συνδρομητή ή τον χρήστη σχετικά με το γεγονός αυτό, όπως και για τον τύπο των δεδομένων και τη διάρκεια της επεξεργασίας, ενώ «*πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσής μιας επικοινωνίας*», ή εφόσον «*είναι απαραίτητα για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, μπορούν να υποβάλλονται σε επεξεργασία, …, μόνον έως το τέλος της χρονικής περιόδου εντός της οποίας δύναται να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή*» [17].

Τέλος, επιτρέπει την επεξεργασία των προαναφερθέντων δεδομένων για σκοπούς εμπορικής προώθησης ή για την παροχή υπηρεσιών προστιθέμενης αξίας με την προϋπόθεση ότι ο συνδρομητής ή ο χρήστης τον οποίο αφορούν θα δώσει την συγκατάθεσή του (την οποία έχει τη δυνατότητα να ανακαλέσει οποιαδήποτε στιγμή) και ότι τα πρόσωπα που διενεργούν την επεξεργασία αυτήν λειτουργούν υπό την εποπτεία του Τηλεπικοινωνιακού φορέα και λόγω της θέσης που κατέχουν στον φορέα

αυτόν έχουν την ανάλογη αρμοδιότητα να το πράττουν (π.χ. ασχολούνται με τη διαχείριση της χρέωσης ή της κίνησης, τις απαντήσεις σε ερωτήσεις πελατών, την ανίχνευση της απάτης, την εμπορική προώθηση υπηρεσιών ηλεκτρονικών επικοινωνιών κλπ.) [17].

Σε περιπτώσεις εφαρμογών ανταλλαγής μηνυμάτων, αρχείων, τηλεδιασκέψεων κτλ., εφαρμόζεται κατ' αρχάς, αναφορικά με τις προϋποθέσεις νόμιμης επεξεργασίας, η e-Privacy Οδηγία ως ειδικότερη του GDPR. Αν κάτι δεν καλύπτεται ακριβώς από την e-Privacy Οδηγία (όπως για παράδειγμα σε ποιο βαθμό λεπτομέρειας πρέπει να παρέχεται πληροφόρηση σχετικά με τα χαρακτηριστικά της επεξεργασίας) τότε έχει εφαρμογή ο GDPR. Στην Ελλάδα, η e- Privacy Οδηγία έχει ενσωματωθεί στην εθνική νομοθεσία με το ν. 3471/2006, ενώ στην Κύπρο με τον ν. 112(Ι)/2004.

Κεφάλαιο 4

Το ζήτημα της ανάγκης(;) ελέγχου των επικοινωνιών και συναφείς προβληματισμοί ως προς τα θεμελιώδη δικαιώματα

Στο κεφάλαιο αυτό εξετάζεται το κατά πόσο είναι αναγκαίος ο μαζικός έλεγχος των επικοινωνιών για εντοπισμό υλικού παιδικής πορνογραφίας, πως αντιμετώπισαν το ζήτημα διάφορες χώρες και ποιοι κίνδυνοι προκύπτουν για τα θεμελιώδη ανθρώπινα δικαιώματα από τα μέτρα που νομοθέτησαν.

4.1. Γενική Επισκόπηση του Ζητήματος

Τα τελευταία χρόνια, στις χώρες της Ευρωπαϊκής Ένωσης, καθώς και στις Η.Π.Α, τον Καναδά, Αυστραλία κ.α., έχει προκύψει ένα σοβαρό ζήτημα που διχάζει τουλάχιστον τους ειδικούς και σταδιακά - καθώς γίνεται ευρύτερα γνωστό - και τις κοινωνίες, σε δύο πλευρές.

Οι χώρες αυτές που είναι κατά παράδοση Δημοκρατικές με ελεύθερες εκλογές και εναλλαγή των διαφόρων κομμάτων στην εξουσία, ήταν και πρωτοπόρες στην αναγνώριση και προστασία των θεμελιωδών δικαιωμάτων των ατόμων, έχοντας καταρχάς θεσπίσει το απαραίτητο για τον σκοπό αυτό θεσμικό και νομικό πλαίσιο, το οποίο και εφαρμόζουν σε πολύ ικανοποιητικό βαθμό - με τις όποιες βέβαια δυσλειτουργίες και θλιβερές εξαιρέσεις - που όμως δεν αποτελούν τον κανόνα.

Το γεγονός ότι οι χώρες αυτές είναι γενικά εύπορες και προηγμένες τεχνολογικά, σημαίνει ότι σε πολύ μεγάλο ποσοστό οι πολίτες τους (σε όλο το εύρος των ηλικιών - από παιδιά Δημοτικού έως και ηλικιωμένοι) κατέχουν έξυπνα κινητά τηλέφωνα – (smartphones), Tablets και φορητούς ή επιτραπέζιους υπολογιστές. Τις συσκευές αυτές

τις χρησιμοποιούν ευρέως στην καθημερινότητά τους για επικοινωνία, ενημέρωση, ψυχαγωγία, εργασία καθώς και για τις κάθε είδους γραφειοκρατικές και οικονομικές συναλλαγές είτε μεταξύ τους, είτε με τις Εταιρίες & Οργανισμούς του Δημοσίου, του Ιδιωτικού και του Χρηματοοικονομικού τομέα (Τράπεζες, Πιστωτικές κάρτες κλπ.).

Απολαμβάνουν λοιπόν τις θετικές πλευρές της προηγμένης τεχνολογίας και χάρη στις ψηφιακές επικοινωνίες μπορούν να τα κάνουν σχεδόν όλα από τη συσκευή τους! Φυσικά όμως υπόκεινται και στους κινδύνους που αναπόφευκτα τις συνοδεύουν. Οι ιοί και γενικά τα κακόβουλα λογισμικά, οι Hackers και οι κάθε λογής απατεώνες που χρησιμοποιούν μια πλειάδα τεχνικών (π.χ. phishing) ώστε να εισβάλουν στις συσκευές και να κλέψουν αριθμούς και pin πιστωτικών καρτών, να αδειάσουν τραπεζικούς λογαριασμούς, να κατασκοπεύσουν τα άτομα είτε για «προσωπική τους ικανοποίηση», είτε για να τους βλάψουν προσωπικά ή επαγγελματικά, είναι μερικοί από τους σοβαρότατους αυτούς κινδύνους. Και όλα αυτά τα διαπράττουν χωρίς να παραβιάσουν κάποια «φυσική» πόρτα ή παράθυρο, αλλά μέσα από τον υπολογιστή τους χρησιμοποιώντας τα δίκτυα επικοινωνίας (internet) για να φτάσουν μέχρι το σπίτι του εκάστοτε χρήστη και να εισβάλουν στη συσκευή του (και κατ' επέκταση και στη ζωή του.).

Είναι λοιπόν απολύτως λογικό, την όλο και μεγαλύτερη ανάγκη των πολιτών για ψηφιακή επικοινωνία, να την συνοδεύει και η επίσης λογική απαίτηση η επικοινωνία αυτή να είναι ασφαλής. Ιδιαίτερα όταν διακινούνται δεδομένα προσωπικού χαρακτήρα η ανάγκη αυτή είναι αδήριτη. Προκύπτει λοιπόν το θεμελιώδες δικαίωμα του «Απορρήτου των Επικοινωνιών» », για το οποίο έγινε και συζήτηση στο προηγούμενο κεφάλαιο. Σημαντικότατος αρωγός στην διασφάλιση του δικαιώματος αυτού είναι η κρυπτογραφία, η οποία προσφέρει στους απλούς χρήστες μια πλειάδα προηγμένων ψηφιακών τεχνικών προκειμένου να αποκρύψουν από hackers και επίδοξους υποκλοπείς το πραγματικό περιεχόμενο των δεδομένων που αποστέλλουν ή λαμβάνουν.

Σε αρκετές από τις προαναφερθείσες χώρες δρουν τρομοκρατικές ομάδες (κάποιες με διασυνδέσεις στο εξωτερικό) που διαπράττουν, ή αποπειρώνται να διαπράξουν, τρομοκρατικές ενέργειες. Για την εξάρθρωσή τους και την προστασία του κοινού από σχεδιαζόμενες τέτοιες ενέργειες, εμφανίζεται πολλές φορές ως αναγκαία η παρακολούθηση των επικοινωνιών των μελών τους από τις υπηρεσίες ασφαλείας (και μάλιστα αρκετές φορές διασυνοριακά, που βέβαια απαιτεί διακρατικές συνεργασίες).

Επιπλέον, όπως συμβαίνει στις κοινωνίες όλων των χωρών του πλανήτη, έτσι και στις κοινωνίες των χωρών αυτών, υπάρχει εγκληματικότητα (μεγάλη ή μικρή - ανάλογα την χώρα). Εκτός των περιπτώσεων που οι κάθε λογής εγκληματίες δρουν από μόνοι τους, σε πλείστες περιπτώσεις σχηματίζουν ομάδες ή «συμμορίες» που για να «λειτουργήσουν» απαιτείται συχνή επικοινωνία μεταξύ των μελών τους. Και σε αυτές τις περιπτώσεις, η παρακολούθηση των επικοινωνιών τους μπορεί να είναι καταλύτης προκειμένου, τελικά, οι αρχές επιβολής του νόμου να τους εντοπίσουν.

Καθώς ανωτέρω έγινε μια γενική αναφορά στο «Έγκλημα», το οποίο βέβαια έχει πάρα πολλά παρακλάδια, κρίνεται απαραίτητο στο σημείο αυτό να γίνει ειδική αναφορά στο είδος εγκλήματος που πραγματεύεται η παρούσα διατριβή: αυτό της Παιδικής Πορνογραφίας. Πρόκειται για ένα από τα πιο ειδεχθή εγκλήματα, καθώς δυστυχώς αφορά παιδικές ψυχές και περιλαμβάνει δύο στάδια:

Το πρώτο, που είναι και το ειδεχθέστερο, αφορά αυτή καθαυτή τη δημιουργία του παιδο-πορνογραφικού υλικού (βίντεο και φωτογραφίες) με κατ' εξακολούθηση βιασμούς παιδιών ή/και εξαναγκασμό τους σε διάφορες σεξουαλικές πράξεις μπροστά στην κάμερα, είτε με ενηλίκους, είτε μεταξύ τους. Φυσικά οι εγκληματίες παίρνουν όλα τα απαραίτητα μέτρα προκειμένου να μην αναγνωριστούν κρύβοντας ή καλύπτοντας τα πρόσωπά τους, καθώς και άλλα πιθανώς αναγνωρίσιμα στοιχεία του σώματός τους (π.χ. τατουάζ), ή στοιχεία του χώρου όπου βιντεοσκοπούνται οι βιασμοί, αποφεύγουν να ακουστεί η φωνή τους κ.α.
Όπως είναι προφανές, το έγκλημα αυτό προϋποθέτει την τέλεση και άλλων σοβαρότατων εγκλημάτων, όπως την απαγωγή παιδιών και τον δια της βίας εγκλεισμό τους σε κάποιο κρησφύγετο, την άσκηση ψυχολογικής ή/και φυσικής βίας (ξυλοδαρμοί) και πιθανότατα την δια της βίας χορήγηση στα παιδιά αυτά ψυχοτρόπων ουσιών προκειμένου να μην αντιδρούν και για να μην αποδράσουν. Κάποιες φορές οι κακοποιοί φτάνουν ακόμα και στο «έσχατο έγκλημα», δηλαδή τη δολοφονία των παιδιών αυτών όταν πια δεν τους είναι «χρήσιμα», ή για να «μη μιλήσουν» (π.χ. υπόθεση Ντιτρού στο Βέλγιο).

Το δεύτερο στάδιο που αποτελεί και τον τελικό σκοπό του εν λόγω εγκλήματος, είναι η διακίνηση του υλικού αυτού με σκοπό το κέρδος, εκμεταλλευόμενη μια (απ' ότι δυστυχώς φαίνεται) μεγάλη αγορά «πελατών», διατεθειμένων να πληρώσουν πολλά χρήματα (καθώς πρόκειται για παράνομο, άρα και ακριβό υλικό).

Δεδομένου ότι το υλικό είναι ψηφιακά καταγεγραμμένο, διακινείται μέσω του internet και γενικότερα των ψηφιακών επικοινωνιών. Αυτό σημαίνει ότι οι διωκτικές αρχές βαρύνονται με το ιδιαίτερα δύσκολο έργο του εντοπισμού, αφενός του υλικού αυτού μέσα στον τεράστιο όγκο δεδομένων που διακινείται καθημερινά στο internet και αφετέρου των «ψηφιακών ιχνών» που τυχόν υπάρχουν και τα οποία ενδεχομένως να τις οδηγήσουν στους κακοποιούς (δηλαδή τους παραγωγούς, τους διακινητές αλλά και τους αγοραστές/ λήπτες/κατόχους του παιδο-πορνογραφικού υλικού, καθώς για τον νόμο - αλλά και ηθικά - είναι όλοι συνυπεύθυνοι).

Και στην περίπτωση των τρομοκρατικών ομάδων, αλλά και στην περίπτωση των εγκληματικών (και ειδικότερα τα κυκλώματα διακίνησης παιδικής πορνογραφίας), οι τυχόν υποκλαπείσες επικοινωνίες και τα ψηφιακά καταγεγραμμένα βίντεο, φωτογραφίες και ίχνη διακίνησης, είναι πολύ συχνά τα πιο κρίσιμα, ή από πιο τα κρίσιμα αποδεικτικά στοιχεία για την εξάρθρωσή τους και την μετέπειτα καταδίκη των μελών τους.

Προκύπτει λοιπόν έντονη η ανάγκη, οι υπηρεσίες ασφαλείας των κρατών να μπορούν, κατά κάποιο τρόπο, να παρακολουθούν και να ελέγχουν τις ψηφιακές επικοινωνίες φωνής και δεδομένων για λόγους εθνικής ασφάλειας, πρόληψης τρομοκρατικών ενεργειών και καταπολέμησης του εγκλήματος σε όλες του τις μορφές.

Όμως δημιουργείται σοβαρό πρόβλημα, καθώς η ανάγκη αυτή των Αρχών έρχεται σε ευθεία αντίθεση με το προαναφερθέν θεμελιώδες δικαίωμα των ατόμων στο «Απόρρητο των Επικοινωνιών» τους.

Μέχρι πρόσφατα το πρόβλημα λυνόταν με την πρόβλεψη εξαιρέσεων στο θεσμικό και νομικό πλαίσιο ειδικά για τις Υπηρεσίες Ασφαλείας, εφόσον η ανάγκη άρσης του απορρήτου ήταν επαρκώς τεκμηριωμένη, στόχευε στο εθνικό ή/και στο κοινό καλό (καταπολέμηση τρομοκρατίας και εγκλήματος) και είχε την έγκριση δικαστικού λειτουργού (συνήθως εισαγγελέα) – και πάντα με την προϋπόθεση ότι οι υπηρεσίες αυτές δρουν με γνώμονα το κοινό καλό (που όμως κάποιοι την αμφισβητούν).

Όπως προαναφέρθηκε, προκειμένου οι χρήστες να προστατεύσουν τα ψηφιακά δεδομένα που στέλνουν και λαμβάνουν και γενικότερα τις επικοινωνίες τους από Hackers και υποκλοπείς, καταφεύγουν στην κρυπτογράφησή τους, η οποία πλέον προσφέρεται σαν βασική υπηρεσία από τους Παρόχους Υπηρεσιών Internet (ISP's – Internet Service Providers). Μάλιστα, σε κάποιες περιπτώσεις πολύ κρίσιμων

επικοινωνιών επιλέγουν υπηρεσίες ή αγοράζουν πακέτα ακόμα ισχυρότερης κρυπτογράφησης.

Επίσης οι τεχνικές κρυπτογράφησης εξελίσσονται διαρκώς και γίνονται όλο και πιο ισχυρές, αλλά και διαθέσιμες στο ευρύ κοινό. Αυτό όμως σημαίνει ότι δεν τις επιλέγουν μόνο οι νομοταγείς χρήστες που θέλουν να προστατευτούν από τους Hackers, αλλά και οι κακοποιοί. Ειδικότερα αυτοί που «ασχολούνται» με την παιδική πορνογραφία τις χρησιμοποιούν ευρύτατα προκειμένου να κρύψουν αφενός το πορνογραφικό υλικό και αφετέρου τα ψηφιακά ίχνη της διακίνησής του.

Από την άλλη, οι Αστυνομικές αρχές και οι Υπηρεσίες Ασφαλείας που είναι επιφορτισμένες με τον έλεγχο του τεράστιου όγκου δεδομένων που διακινείται και την ανίχνευση υλικού παιδικής πορνογραφίας «διαμαρτύρονται» προς τις Κυβερνήσεις τους ότι εξαιτίας της εκτεταμένης πλέον και ισχυρής κρυπτογράφησης, το έργο τους γίνεται όλο και δυσχερέστερο.

Οι λύσεις που προτείνουν οι Αρχές - και τις ενστερνίζονται σε μεγάλο βαθμό και οι Κυβερνήσεις – έχουν δύο κατευθύνσεις:

Η πρώτη, αφορά τη διάθεση στο ευρύ κοινό εκδόσεων λογισμικού κρυπτογράφησης με περιορισμένες δυνατότητες, ή με εσκεμμένα ενσωματωμένες «ευπάθειες» (γνωστές στις Αρχές) που θα καλύπτουν μεν τις βασικές ανάγκες του κοινού, αλλά οι Αρχές θα είναι σε θέση να τις εκμεταλλεύονται προκειμένου να «σπάνε» εύκολα και μαζικά τα κρυπτογραφημένα δεδομένα και να τα ερευνούν.

Η δεύτερη κατεύθυνση είναι ακόμα πιο παρεμβατική καθώς προτείνει ο κάθε κατασκευαστής κρυπτογραφικού λογισμικού, να έχει ενσωματωμένο και να θέτει σε γνώση μόνο των Αρχών, συγκεκριμένο τρόπο παράκαμψης όλων των δικλείδων ασφαλείας.

Στον αντίποδα, βρίσκονται άτομα, οργανισμοί και ιδρύματα που στοχεύουν στην υπεράσπιση των θεμελιωδών δικαιωμάτων των ανθρώπων από κάθε είδους κρατική ή άλλη παρέμβαση.

Η πλευρά αυτή υποστηρίζει ότι και οι δύο ανωτέρω προτάσεις είναι προβληματικές, γιατί αφενός θα κλονιστεί η εμπιστοσύνη που πρέπει να έχει το κοινό ότι οι πληροφορίες που διακινεί προστατεύονται από τα όσο το δυνατόν πιο ασφαλή (τη δεδομένη χρονική στιγμή) λογισμικά κρυπτογράφησης και αφετέρου γιατί οι «εσκεμμένες ευπάθειες» θα

εντοπιστούν χωρίς αμφιβολία και από τους κάθε λογής κακόβουλους, οι οποίοι στη συνέχεια θα αρχίσουν να τις εκμεταλλεύονται προς όφελός τους.

Η δε λύση της ενημέρωσης των Αρχών από τους κατασκευαστές για τους τρόπους παράκαμψης της ασφάλειας των λογισμικών κρυπτογράφησης ίσως παρέχει κάποιες εγγυήσεις σε δημοκρατικές κυβερνήσεις, αλλά σε περιπτώσεις αυταρχικών καθεστώτων, απλά θα τα βοηθήσει να γίνουν ακόμα αυταρχικότερα.

Γενικότερα, προκύπτει ο προβληματισμός ως προς το πώς θα διασφαλίζεται ότι η παρακολούθηση των επικοινωνιών θα γίνεται μόνο για αυτούς τους σκοπούς (εντοπισμός παράνομων συμπεριφορών) και όχι για άλλους που ενίοτε οι κυβερνήσεις επιθυμούν (π.χ. παρακολούθηση προσώπων για έκφραση πολιτικών πεποιθήσεων, παρακολούθηση whistleblowers κ.α.). Επίσης, πέραν αυτού, προκύπτει ο προβληματισμός ως προς το πώς θα είναι απόλυτα τεκμηριωμένη κάθε παρακολούθηση – για παράδειγμα, πώς ελέγχεται ότι μία αρχή, με «πρόφαση» το ότι κάποιος είναι ύποπτος για διακίνηση παράνομου υλικού, δεν θα παρακολουθεί τελικά αθώους πολίτες τους οποίους δεν θα έπρεπε να παρακολουθεί;

Ταυτόχρονα όμως, αναγνωρίζεται και η αδιαμφισβήτητη ανάγκη για αποτελεσματικό εντοπισμό υλικού παιδικής πορνογραφίας (καθώς και άλλου παράνομου υλικού) και προτείνονται ορισμένες μέθοδοι που υποστηρίζεται ότι το καταφέρνουν χωρίς να παραβιάζουν θεμελιώδη δικαιώματα.

4.2. Το αμφιλεγόμενο παράδειγμα της Αυστραλίας

Κάποιες χώρες ήδη ενστερνίστηκαν τις προτάσεις των αρχών και τις συμπεριέλαβαν στη νομοθεσία τους. Για παράδειγμα το κοινοβούλιο της Αυστραλίας ψήφισε ήδη από το 2018 νόμο που επιτρέπει στις Υπηρεσίες Πληροφοριών και Ασφαλείας της χώρας να απαιτούν πρόσβαση στις E2E κρυπτογραφημένες ψηφιακές επικοινωνίες και υπηρεσίες που προσφέρουν οι διάφορες εταιρείες. Αυτό σημαίνει ότι εταιρείες όπως η Meta και η Apple εξαναγκάζονται (επί ποινή μεγάλων προστίμων εφόσον δεν συμμορφωθούν), να ενσωματώσουν εσκεμμένα «κενά ασφαλείας» ή backdoors («κερκόπορτες») σε εφαρμογές ψηφιακής επικοινωνίας όπως η WhatsApp και η iMessage [13].

Μάλιστα, ο εν λόγω νόμος πηγαίνει ένα βήμα (ή και πολλά) παραπέρα: δίνει το δικαίωμα στις Αρχές Ασφαλείας, εάν το κρίνουν σκόπιμο, να παρακάμπτουν τις ίδιες τις εταιρείες

και την ιεραρχία τους και να απευθύνονται κατευθείαν σε μεμονωμένους υπαλλήλους (ή ομάδες υπαλλήλων) που κατέχουν κρίσιμα πόστα (π.χ. προγραμματιστές, υπεύθυνοι για τις ενημερώσεις λογισμικού), απαιτώντας (επί ποινή φυλάκισης εφόσον αρνηθούν) να εισάγουν (κρυφά) τα προαναφερθέντα εσκεμμένα κενά ασφαλείας στις εφαρμογές επικοινωνίας με κρυπτογράφηση [13].

Έτσι, με τον ένα ή τον άλλο τρόπο, οι Υπηρεσίες Ασφαλείας της Αυστραλίας για τις έρευνές τους, θα μπορούν να παρακάμπτουν εύκολα όλες τις δικλείδες ασφαλείας που υπάρχουν στις ψηφιακές επικοινωνίες.

Η εν λόγω ρύθμιση σε μορφή νομοσχεδίου, ήταν για αρκετούς μήνες σε διαβούλευση και αντιμετώπισε μεγάλη κριτική αλλά έγινε τελικά νόμος με τις ψήφους και της κυβέρνησης, αλλά και της αντιπολίτευσης. Το σκεπτικό με το οποίο ψηφίστηκε ήταν ότι θα παράσχει στις Αρχές τα πολύτιμα εργαλεία που δηλώνουν ότι χρειάζονται προκειμένου να είναι αποτελεσματικές στην καταπολέμηση του εγκλήματος και της τρομοκρατίας, οι οποίες διαρκώς εξελίσσονται και υιοθετούν πρόθυμα και γρήγορα κάθε νέα τεχνολογία που τους επιτρέπει να βρίσκονται μπροστά από τις αρχές και να ξεφεύγουν.

Αν και ο νόμος έχει σαφέστατα «άρωμα Μεγάλου Αδελφού», δεν μπορεί να αμφισβητήσει κανείς ότι το σκεπτικό του βασίζεται σε σοβαρά επιχειρήματα, ιδιαίτερα μάλιστα όταν το στοχοποιούμενο έγκλημα αφορά την παραγωγή και διακίνηση παιδικής πορνογραφίας (το οποίο πραγματεύεται η παρούσα διατριβή).

Ο αντίλογος και η κριτική για τον εν λόγω νόμο προέρχεται κυρίως από οργανισμούς και άτομα που μάχονται για την προάσπιση των θεμελιωδών δικαιωμάτων των ανθρώπων και της ιδιωτικότητάς τους, καθώς και από τους ίδιους τους κρυπτογράφους. Υποστηρίζουν ότι ο νόμος είναι πολύ γενικόλογος, ασαφής (π.χ. πόσο συχνά μπορούν να ζητούνται από τις εταιρείες στοιχεία;) και ευρύς (ενώ θα έπρεπε τουλάχιστον να είναι πολύ πιο συγκεκριμενοποιημένος), ενέχει πολλούς κινδύνους και θα λειτουργήσει ως ένα πολύ κακό μοντέλο και για άλλες χώρες, ιδιαίτερα για τις αγγλοσαξονικές Μ. Βρετανία, Ν. Ζηλανδία, Καναδά και Η.Π.Α. που έχουν παρόμοια κουλτούρα και στις οποίες υπάρχουν από καιρό ομάδες (lobbies) που υποστηρίζουν τέτοιου είδους παρεμβάσεις [13].

Η Βρετανία μάλιστα έχει ήδη από το 2016 περάσει τον νόμο “Investigatory Powers Act” που κατ’ ευφημισμό καλείται «Snoopers' Charter» και θέτει το πλαίσιο ώστε να αναγκάζονται οι εταιρείες να παρέχουν στις Αρχές πρόσβαση στις κρυπτογραφημένες

επικοινωνίες των χρηστών τους. Πάντως ο Βρετανικός νόμος δεν επιτρέπει την προσέγγιση ατόμων/υπαλλήλων των εταιρειών όπως αυτός της Αυστραλίας [13].

Επιπλέον, ο Αυστραλιανός νόμος φαίνεται περιέργως να αγνοεί το πραγματικό και αδιαμφησβήτητο γεγονός ότι η Τεχνολογία είναι παγκοσμιοποιημένη. Επομένως εάν μια εταιρεία υποχρεωθεί να εισάγει κάποια «κερκόπορτα» στο λογισμικό της κατόπιν εντολής των Αρχών Ασφαλείας της Αυστραλίας, θα πρέπει να το κάνει και σε παγκόσμιο επίπεδο. Έτσι ανοίγονται οι «ασκοί του Αιόλου» καθώς θα γίνει διαθέσιμο σε κάθε λογής hackers, εγκληματίες και αυταρχικά καθεστώτα άλλων χωρών που θα το εκμεταλλευτούν για τους δικούς τους σκοπούς.

Για να λειανθούν οι αντιρρήσεις χρησιμοποιούνται ευφημισμοί όπως «υπεύθυνη κρυπτογράφηση (responsible encryption)». Μάλιστα ο Αυστραλιανός νόμος έχει και μια παράγραφο με «Περιορισμούς (Limitations)» που αναφέρει ότι δεν πρέπει να ζητηθεί από τον Πάροχο της υπηρεσίας να ενσωματώσει ή να δημιουργήσει μια «συστημική αδυναμία ή ευπάθεια (systemic weakness or systemic vulnerability)» στο προϊόν ή την υπηρεσία, γεγονός που εκ πρώτης όψεως φαίνεται θετικό. Ως «Συστημική Ευπάθεια» νοείται για τον νόμο μια ευπάθεια που αφορά μια ολόκληρη τεχνολογική κατηγορία, αλλά δεν συμπεριλαμβάνει ευπάθειες που εισάγονται σε επιλεγμένες τεχνολογίες που αφορούν κάποιο συγκεκριμένο άτομο. Δηλαδή, ναι μεν δεν επιτρέπεται η εσκεμμένη εισαγωγή μιας συγκεκριμένης ευπάθειας σε όλες τις πλατφόρμες αποστολής και λήψης μηνυμάτων (messaging), αλλά επιτρέπεται να συμβεί σε μεμονωμένα προγράμματα messaging όπως τα WhatsApp ή iMessage [13].

Άλλη τεχνική των Αρχών που τη χρησιμοποιούν όλο και περισσότερο, είναι να πιέζουν τις εταιρείες να εντάσσουν κρυφά δικούς τους ανθρώπους (των Αρχών) σε κρυπτογραφημένες επικοινωνίες μεταξύ δύο ατόμων. Έτσι η επικοινωνία εξακολουθεί να είμαι κρυπτογραφημένη, αλλά συμμετέχει κρυφά και 3ο άτομο χωρίς να το γνωρίζουν οι άλλοι δύο [13].

Εκτός από τους υποστηρικτές της ιδιωτικότητας στις επικοινωνίες και οι ίδιοι οι κρυπτογράφοι υποστηρίζουν ότι οποιαδήποτε εσκεμμένη ευπάθεια κι αν εισαχθεί, θα γίνει γρήγορα αντιληπτή από Hackers και εγκληματίες που θα σπεύσουν να τη χρησιμοποιήσουν για τους δικούς τους σκοπούς, δημιουργώντας ένα τεράστιο θέμα ασφαλείας για όλους τους χρήστες και πιθανότατα και για τις ίδιες τις Αρχές που ζήτησαν την εισαγωγή της εσκεμμένης ευπάθειας .

Επί δεκαετίες οι κρυπτογράφοι αντιτίθονταν στις «κερκόπορτες» και το 2015 είχαν συνοψίσει τα επιχειρήματά τους σε ένα άρθρο με τίτλο «Keys Under Doormats (σε ελεύθερη μετάφραση: Κλειδιά κάτω από το χαλάκι της εξώπορτας)». Αλλά μετά τον Αυστραλιανό νόμο δημιουργήθηκε ένα νέο κύμα αντίθεσης. Ο οργανισμός IEEE αναφέρει σε ανακοίνωσή του ότι «*Οι μηχανισμοί κατ' εξαίρεσης πρόσβασης θα δημιουργήσουν κινδύνους … Οι προσπάθειες να περιοριστεί η ισχυρή κρυπτογράφηση ή να δημιουργηθούν σχήματα εγγύησης κλειδιών (key escrow schemes) σε εμπορικά προϊόντα μπορούν να έχουν μακροπρόθεσμες αρνητικές επιπτώσεις στην ιδιωτικότητα, ασφάλεια και πολιτικές ελευθερίες των πολιτών*» [08].

4.3. Η περίπτωση των Η.Π.Α. και ο νόμος EARN IT

Στην άλλη πλευρά του πλανήτη, στις Η.Π.Α., το Υπουργείο Δικαιοσύνης και το FBI είχαν για χρόνια ξεκινήσει μια καμπάνια προκειμένου να σταματήσουν οι εταιρείες να προσφέρουν στο ευρύ κοινό υπηρεσίες επικοινωνίας που ενσωματώνουν end-to-end κρυπτογράφηση (π.χ. iMessage, WhatsApp, Telegram, Signal). Η καμπάνια όμως αυτή δεν κέρδισε πολλούς υποστηρικτές, αφενός γιατί οι άνθρωποι (όπως είναι αναμενόμενο και λογικό), επιθυμούν να επικοινωνούν χωρίς να παραβιάζει κάποιος τρίτος την ιδιωτικότητα (privacy) της συνομιλίας τους και αφετέρου γιατί και οι ίδιες οι μεγάλες εταιρείες, Πάροχοι αυτών των υπηρεσιών (Microsoft, Apple, Google, Meta), δεν την υποστήριξαν, καθώς ήθελαν οι πελάτες τους να αισθάνονται και να είναι ασφαλείς [05].

Η επόμενη σκέψη της Αμερικανικής κυβέρνησης και των υπηρεσιών ασφαλείας ήταν να πιέσουν τους Παρόχους των εν λόγω υπηρεσιών να ενσωματώσουν σε αυτές «κερκόπορτες» (backdoors) που θα τους παρέχουν «κατ' εξαίρεση πρόσβαση» (exceptional access) στα δεδομένα χρηστών για τους οποίους υπάρχει υποψία τέλεσης σοβαρής εγκληματικής πράξης και φυσικά με την προϋπόθεση έκδοσης σχετικού εντάλματος έρευνας.

Αν και αυτή θα ήταν μια μέση λύση που ενδεχομένως θα ικανοποιούσε και τις δύο πλευρές, τελικά δεν ακολουθήθηκε. Αντ' αυτής η Κυβέρνηση και οι Αρχές, που φαίνεται πως είχαν στόχο την πλήρη κατάργηση της κρυπτογράφησης στις εμπορικές υπηρεσίες επικοινωνίας, αποφάσισαν να χρησιμοποιήσουν για τον σκοπό τους την εύλογη ανησυχία του κοινού για την διάδοση υλικού παιδικής πορνογραφίας, γνωστό με τα

αρχικά CSAM (Child Sexual Abuse Material). Η ύπαρξη και διακίνηση τέτοιου αισχρού υλικού είναι άκρως κατακριτέα και αποτελεί μεγάλο πρόβλημα για τους Παρόχους. Για να το αντιμετωπίσουν, εφαρμόζουν οικειοθελή έλεγχο για τέτοιο υλικό, συγκρίνοντάς τα video και τις εικόνες που διακινούνται μέσω υπηρεσιών Messaging και File Sharing με μια βάση δεδομένων από γνωστά φωτογραφικά «hashes" παιδικής πορνογραφίας, και εφόσον εντοπίσουν κάτι, στέλνουν αναφορά στο NCMEC (National Center for Missing & Exploited Children - «Εθνικό Κέντρο για αγνοούμενα παιδιά και παιδιά που έχουν υποστεί εκμετάλλευση») και αυτό με τη σειρά του ενημερώνει τις αρχές [05].

Η τεχνική "Photo Scanning", που στην συγκεκριμένη περίπτωση εφαρμόζεται αναμφισβήτητα για καλό σκοπό, προϋποθέτει μαζική έρευνα (scanning) μεγάλου όγκου εικόνων. Όμως η end-to-end κρυπτογράφηση έχει σχεδιαστεί ειδικά για να εμποδίζει τέτοιου είδους μαζικό scanning δεδομένων. Οπότε η συνύπαρξη και των δύο τεχνικών στην ίδια υπηρεσία επικοινωνίας αποτελεί πολύ μεγάλο τεχνικό πρόβλημα για τους Παρόχους, που ακόμα δεν έχει λυθεί αποτελεσματικά.

Την άνοιξη του 2020, μέλη και των δύο κομμάτων πέρασαν ένα νομοσχέδιο που ονομάστηκε EARN IT. Αυτοί που το κατακρίνουν ισχυρίζονται ότι ο πραγματικός στόχος του είναι να καταργήσει εξ' ολοκλήρου την end-to-end κρυπτογράφηση στις επικοινωνίες, χωρίς όμως αυτό να αναφέρεται ευθέως, αλλά με «πλάγιο» τρόπο επιχειρεί να καταστήσει την κρυπτογράφηση οικονομικά δυσβάστακτη για τους Παρόχους. Συγκεκριμένα, απαιτεί απ' αυτούς, είτε να λύσουν αποτελεσματικά το προαναφερθέν πρόβλημα της υλοποίησης μαζικού scanning σε κρυπτογραφημένα δεδομένα, είτε να πάψουν να εφαρμόζουν end-to-end κρυπτογράφηση. Και δεδομένου ότι οι ενδεχόμενες λύσεις για το συγκεκριμένο πρόβλημα βρίσκονται ακόμα σε ερευνητικό στάδιο, φαίνεται ότι απώτερος στόχος του νομοσχεδίου είναι να συμβεί το δεύτερο.

Σύμφωνα με τον EARN IT οι Πάροχοι των υπηρεσιών θεωρούνται υπεύθυνοι για τις όποιες παράνομες ενέργειες των χρηστών της υπηρεσίας τους, την οποία θα πρέπει να λειτουργούν με βάση κάποιες «καλές πρακτικές» (best practices). Όμως προς το παρόν και καθώς ο νόμος είναι σχετικά καινούργιος, δεν υπάρχουν ακόμα παγιωμένες «καλές πρακτικές» (εκτός βέβαια από την υποχρέωση για έρευνα για CSAM). Έτσι ο νόμος προβλέπει τη δημιουργία μιας επιτροπής με μέλη διορισμένα από την κυβέρνηση, η οποία θα λέει στους Παρόχους των υπηρεσιών ποιες τεχνικές θα πρέπει να ενσωματώσουν στις παρεχόμενες υπηρεσίες τους [05].

4.3.1. Οι αντιδράσεις στον EARN IT

Οι επικριτές του EARN IT τον θεωρούν έναν κρυφό «πολιορκητικό κριό» που έχει ως απώτερο στόχο να καταργήσει την E2E κρυπτογράφηση στις επικοινωνίες των χρηστών. Ισχυρίζονται ότι η φύση και η σύνθεση της επιτροπής, έτσι όπως περιγράφονται στον νόμο, δεν εγγυώνται την αμεροληψία και η επιτροπή μπορεί κάλλιστα να μην συμπεριλάβει ούτε έναν ειδικό στην κυβερνοασφάλεια. Θεωρούν δε σχεδόν σίγουρο ότι η E2E κρυπτογράφηση δεν θα θεωρηθεί καλή πρακτική.

Επιπλέον επισημαίνουν ότι ήδη οι εταιρείες, με δική τους πρωτοβουλία, δουλεύουν εντατικά και επενδύουν σημαντικά ποσά στην έρευνα και εξέλιξη αποτελεσματικότερων τεχνικών ανίχνευσης CSAM σε E2E κρυπτογραφημένα διακινούμενα δεδομένα (π.χ. η Google δουλεύει με τεχνικές Machine Learning). Αφενός κάνει καλό στην εικόνα τους καθώς δείχνουν εταιρική υπευθυνότητα σε ένα πολύ ευαίσθητο θέμα και αφετέρου και οι υπάλληλοί τους έχουν παιδιά! Φυσικά, ως εμπορικές εταιρείες λαμβάνουν υπόψη τους και το κόστος ενσωμάτωσης της οποιαδήποτε τεχνικής στα προϊόντα και τις υπηρεσίες που προσφέρουν. Όμως, υπό την απειλή του EARN IT και της επιτροπής των πολιτικών, είναι ιδιαίτερα αμφίβολο εάν θα συνεχίσουν να ερευνούν και στο μέλλον για πιο εξελιγμένες και αποτελεσματικότερες τεχνικές, καθώς θα είναι υποχρεωμένες να τις ενσωματώνουν στα προϊόντα τους, οποιοδήποτε κι αν είναι το κόστος. Πιθανότατα θα ακολουθήσουν την κατά πολύ οικονομικότερη λύση της κατάργησης της E2E κρυπτογράφησης [05].

Η σύγχρονη Κοινωνία, αυτή της Πληροφορίας έχει να επιδείξει μια πολύ κακή επίδοση στο να κρατάει τα υπολογιστικά της συστήματα ασφαλή. Αυτό έχει τεράστιο οικονομικό κόστος και υπονομεύει την ίδια τη εύρυθμη λειτουργία της. Η E2E κρυπτογράφηση είναι μια από τις λίγες τεχνικές που υπάρχουν για να προστατευτούν τα προσωπικά δεδομένα των χρηστών και οι πληροφορίες που διακινούν μέσω των ψηφιακών δικτύων επικοινωνιών από τους κάθε λογής επίδοξους εισβολείς (Hackers). Αποτελεί μάλιστα την πιο αποτελεσματική τεχνική.

Μένει να φανεί πως ο νόμος αυτός θα λειτουργήσει στην πράξη και εάν οι εταιρείες θα συμμορφωθούν ή θα αντισταθούν. Η Apple είχε ήδη εκδηλώσει την αντίθεσή της πριν ψηφιστεί ο νέος νόμος της Αυστραλίας καθώς και ο Βρετανικός «Investigatory Powers Act», ενώ το 2015 ήλθε σε σύγκρουση με το FBI στις Η.Π.Α, αρνούμενη να δημιουργήσει ένα εργαλείο για πρόσβαση στα κρυπτογραφημένα δεδομένα του iPhone ενός υπόπτου

για πυροβολισμούς. Είναι όμως άγνωστο εάν οι εταιρείες θα συνεχίσουν να αντιστέκονται, ιδιαίτερα εάν ο νόμος τις παρακάμπτει και στοχεύει κατευθείαν σε υπαλλήλους τους, όπως αυτός της Αυστραλίας. Επιπλέον, οι ποινές με τα πρόστιμα για τις εταιρείες και τις φυλακίσεις για τους υπαλλήλους είναι εξοντωτικές και σχεδιασμένες να κάμψουν κάθε αντίσταση. Κάποιοι «σκληροί» επικριτές των νόμων αυτών, φτάνουν στο σημείο να διατείνονται πως και οι πέντε Αγγλοσαξονικές χώρες, στον τομέα αυτόν βαδίζουν στα χνάρια αυταρχικών καθεστώτων που απαγορεύουν στους πολίτες τους την χρήση ψηφιακών προϊόντων που προσφέρουν ασφάλεια και προστατεύουν την ιδιωτικότητα των επικοινωνιών [05].

Κεφάλαιο 5

Η κατάσταση στην ΕΕ ως προς την ανίχνευση του περιεχομένου των επικοινωνιών

Καθώς η ανίχνευση παράνομου υλικού CSAM και Grooming είναι αδιαμφισβήτητα μια διεργασία με κομβική και ουσιώδη σημασία στη μάχη ενάντια στην παιδική πορνογραφία και στην εξάρθρωση των κυκλωμάτων που τη διακινούν, εδώ και κάποιο χρονικό διάστημα η Ευρωπαϊκή Ένωση έχει, όπως προαναφέρθηκε, αρχίσει να εισάγει νομοθετήματα που ρυθμίζουν το νομικό πλαίσιο, εντός του οποίου, αυτή θα πρέπει να διενεργείται. Ταυτόχρονα όμως εγείρονται διάφορα τεχνικά, νομικά και ηθικά ζητήματα, όπως για παράδειγμα ο τρόπος με τον οποίο οι Πάροχοι τηλεπικοινωνιακών υπηρεσιών όπως η Google, η Microsoft, η Meta, το Linkedin κτλ. θα ανιχνεύουν τέτοιο υλικό, χωρίς να παρεκκλίνουν από το νομικό πλαίσιο της ΕΕ για τα προσωπικά δεδομένα (που παρουσιάστηκε στο Κεφάλαιο 3);

Δύο είναι τα βασικά νομικά κείμενα της ΕΕ που διέπουν την ανίχνευση CSAM:

5.1. Ευρωπαϊκός Κανονισμός (EU Regulation) 2021/1232

Πρόκειται για έναν κανονισμό με προσωρινή ισχύ 3 ετών (μέχρι τον Αύγουστο του 2024), που ψηφίστηκε το 2021 από το Ευρωπαϊκό Κοινοβούλιο σε μια προσπάθεια να αντιμετωπιστεί με κάποιον τρόπο η μεγάλη αύξηση διακίνησης CSAM υλικού στο διαδίκτυο που παρατηρήθηκε κατά την περίοδο της πανδημίας Covid-19.

Επιτρέπει στους Παρόχους Διαδικτυακών Υπηρεσιών να παρεκκλίνουν από τις προϋποθέσεις των άρθρων 5 και 6 της e-Privacy Οδηγίας και να εξακολουθούν (σε

εθελοντική βάση) να εφαρμόζουν τις τεχνικές που έχουν ήδη αναπτύξει, προκειμένου να ανιχνεύουν παράνομο υλικό CSAM στο διαδίκτυο (και βέβαια στη συνέχεια να προβαίνουν στην αφαίρεσή του καθώς και σε σχετική αναφορά στις Αρχές). Χωρίς αυτόν τον Κανονισμό, πολλές τεχνικές ανίχνευσης δεν θα ήταν νόμιμες στην ΕΕ λόγω της e-Privacy Οδηγίας: ο Κανονισμός αυτός εισάγει μία εξαίρεση, με απώτερο σκοπό να εξασφαλίσει ότι πρακτικές που ήδη υλοποιούσαν Πάροχοι για την ανίχνευση του CSA είναι νόμιμες, ως κατ' εξαίρεση και υπό αυστηρές προϋποθέσεις «επέμβαση» στις επικοινωνίες παρά τις προβλέψεις της e- Privacy Οδηγίας [04, 20].

Ουσιαστικά, η εθελοντική χρήση αυτών των τεχνικών από τους Παρόχους «νομιμοποιείται» μέχρι τον Αύγουστο του 2024, ενώ κανονικά με βάση την e-Privacy οδηγία, δεν θα τους επιτρεπόταν να το κάνουν.

Παράλληλα προβλέπεται η στενότερη επιτήρηση των ενεργειών των Παρόχων από τις Εθνικές Αρχές Προστασίας Δεδομένων κάθε κράτους μέλους της ΕΕ, καθώς και η δυνατότητα υποβολής καταγγελίας (και δικαστικής διερεύνησής της) από άτομα που θεωρούν ότι τα θεμελιώδη δικαιώματά τους παραβιάστηκαν [04, 20].

Τέλος, κρίνεται σκόπιμο να τονιστεί εδώ, καθώς έχει ιδιαίτερη αξία για τη συνέχεια και τα συμπεράσματα της διατριβής, πως σε ένα από τα σκεπτικά αναγκαιότητας της οδηγίας αυτής (25), αναφέρεται ρητά ότι:

«Η διατερματική κρυπτογράφηση αποτελεί σημαντικό εργαλείο για τη διασφάλιση της προστασίας και του απορρήτου των επικοινωνιών των χρηστών, συμπεριλαμβανομένων των παιδιών. Τυχόν αποδυνάμωση της κρυπτογράφησης θα μπορούσε να αποτελέσει αντικείμενο κατάχρησης από κακόβουλους τρίτους. Καμία διάταξη του παρόντος κανονισμού δεν θα πρέπει, συνεπώς, να ερμηνεύεται ως απαγόρευση ή αποδυνάμωση της διατερματικής κρυπτογράφησης» [20].

Αυτό σημαίνει, ότι το Ευρωπαϊκό Κοινοβούλιο, παρά τη σαφή πρόθεσή του να ρυθμίσει το ζήτημα πρόσβασης σε περιεχόμενο επικοινωνιών με σκοπό την ανίχνευση CSAM αλλά και την αποπλάνηση ανηλίκων (grooming), αναγνωρίζει επίσημα την αξία της E2E κρυπτογράφησης και αντιτίθεται ξεκάθαρα στην απαγόρευση ή αποδυνάμωσή της με οποιονδήποτε τρόπο (αναφέροντας και το σχετικό σκεπτικό)!

5.2. Πρόταση νέου Κανονισμού της ΕΕ για ανίχνευση CSAM και Grooming

Επειδή ο Κανονισμός της ΕΕ 2021/1232 είναι όπως προαναφέρθηκε προσωρινός, τον Μάϊο του 2022 η Ευρωπαϊκή Επιτροπή έδωσε στην δημοσιότητα έναν νέο Κανονισμό [19] που φιλοδοξεί να διαδεχθεί τον ισχύοντα και βρίσκεται προς το παρόν στο στάδιο της «Πρότασης» (δηλ. δεν έχει ψηφιστεί και επομένως μπορεί να αλλάξει αρκετά).

Σκοπός του είναι να εγκαθιδρύσει ένα νέο νομικό πλαίσιο για την καλύτερη πρόληψη και αντιμετώπιση της σεξουαλικής κακοποίησης και εκμετάλλευσης των παιδιών (offline και online) και βασίζεται στην στρατηγική που έχει υιοθετήσει η ΕΕ για τα δικαιώματα του παιδιού [09].

Η Πρόταση Κανονισμού ενθαρρύνει μεν τους Παρόχους Υπηρεσιών Ψηφιακής Επικοινωνίας να εφαρμόζουν εθελοντικά τεχνικές ανίχνευσης CSAM και grooming στις πλατφόρμες τους, αλλά προβλέπει και νέες σχετικές υποχρεώσεις γι' αυτούς. Για παράδειγμα, θα πρέπει να διενεργούν «εκτίμηση κινδύνου» (risk assessment) για το κατά πόσο οι διαδικτυακές υπηρεσίες επικοινωνίας που προσφέρουν στους χρήστες τους δύνανται να χρησιμοποιηθούν από εγκληματίες για σεξουαλική κακοποίηση/εκμετάλλευση παιδιών και διακίνηση παιδικής πορνογραφίας. Εφόσον ο εκτιμώμενος κίνδυνος προκύπτει υψηλός, θα έχουν την υποχρέωση να εφαρμόζουν επιπλέον μέτρα εντοπισμού CSAM στις πλατφόρμες τους [09].

Μια τέτοια υποχρέωση δεν θα βασίζεται απλά στην «καλή θέληση» των Παρόχων, αλλά θα μπορεί να τους επιβληθεί και νομικά με την έκδοση Εντολής ανίχνευσης CSAM. Εάν κάτι τέτοιο συμβεί, υποχρεούνται να χρησιμοποιήσουν «αξιόπιστες τεχνολογίες εντοπισμού» (reliable detection technologies) για τον σκοπό αυτό. Μάλιστα, εφόσον εντοπιστεί CSAM, θα έχουν την υποχρέωση να το αναφέρουν στις Αρχές, να το μπλοκάρουν και να το αφαιρέσουν. Ακόμα κι αν οι Πάροχοι, προληπτικά (χωρίς σχετική εντολή), προβούν στην χρήση τεχνικών εντοπισμού CSAM στα δεδομένα που διακινούνται μέσω των προσφερόμενων υπηρεσιών τους, δεσμεύονται νομικά να αναφέρουν στις αρχές τα ευρήματά τους. Εφόσον δεν ανταποκριθούν στις ανωτέρω υποχρεώσεις τους, θα βρεθούν αντιμέτωποι με ποινές ύψους μέχρι 6% του ετήσιου εισοδήματός τους ή του παγκόσμιου τζίρου τους κατά το προηγούμενο οικονομικό έτος[09].

Προβλέπεται επίσης η ίδρυση ενός «Ευρωπαϊκού Κέντρου (EU Centre) για την πρόληψη και αντιμετώπιση της κακοποίησης παιδιών» που θα δημιουργήσει, συντηρεί και διαχειρίζεται Βάσεις Δεδομένων με «CSAM δείκτες (indicators)» που θα πρέπει να χρησιμοποιούν οι Πάροχοι και προφανώς θα δείχνει το βαθμό «συμμόρφωσής» τους με τις ανωτέρω υποχρεώσεις τους για εντοπισμό CSAM. Το Κέντρο θα έχει στη διάθεσή του εργαλεία εντοπισμού CSAM, τα οποία θα μπορεί να χορηγεί δωρεάν σε Παρόχους για τους οποίους έχει εκδοθεί νομική Εντολή, ώστε να μπορούν (εάν βέβαια θέλουν) να τα χρησιμοποιήσουν προκειμένου να εκπληρώσουν τις υποχρεώσεις τους που προκύπτουν από την Εντολή. Εδώ η Πρόταση τονίζει ότι το Κέντρο θα είναι «τεχνολογικά ουδέτερο» και επομένως η συμπερίληψη κάποιων συγκεκριμένων τεχνολογιών εντοπισμού CSAM στις διαθέσιμες στο «οπλοστάσιό» του, δεν θα πρέπει να εκληφθεί από τους Παρόχους ότι το Κέντρο παρέχει κίνητρα για την υιοθέτηση των συγκεκριμένων τεχνολογιών εκ μέρους τους και αντικίνητρα για την υιοθέτηση μιας εκ των υπολοίπων [09].

Ενώ δεν αμφισβητούνται οι καλοί σκοποί αυτής της Πρότασης Κανονισμού, η κριτική που της ασκείται επικεντρώνεται βασικά σε ένα, αλλά καίριο γεγονός που ανατρέπει τα πάντα, τουλάχιστον προς το παρόν και για το άμεσο μέλλον:

Η Πρόταση Κανονισμού διατείνεται ότι οι ρυθμίσεις που προβλέπει είναι συμβατές με την E2E κρυπτογράφηση, αλλά την τρέχουσα χρονική στιγμή δεν υπάρχει διαθέσιμη κάποια τεχνολογία που να επιτρέπει στους Παρόχους να την παρέχουν στους χρήστες τους και ταυτόχρονα να τηρούν τις υποχρεώσεις τους για εντοπισμό CSAM, όπως αυτές προκύπτουν από την Πρόταση.

Επομένως, οι επικριτές της Πρότασης αναφέρουν ότι η διατεινόμενη συμβατότητά της με την E2EE είναι «κενή ουσίας» και στην πραγματικότητα θα αναγκάσει τους Παρόχους (υπό την πίεση των προστίμων) είτε να καταργήσουν πλήρως την E2EE από τις υπηρεσίες τους, είτε να εφαρμόσουν μια εσκεμμένα μειωμένης ασφάλειας έκδοση κρυπτογράφησης, ώστε να συμμορφωθούν με τις προβλέψεις της.

Στο «ίδιο μήκος κύματος» κάποιοι νομοθέτες προτείνουν την προαναφερθείσα λύση της εσκεμμένης τοποθέτησης «backdoors» στις εφαρμοζόμενες τεχνικές κρυπτογράφησης που θα είναι διαθέσιμες προς χρήση από τις Αρχές, ενώ κάποιοι άλλοι προτείνουν την ανίχνευση CSAM από τη μεριά του χρήστη, ως την ενδεικνυόμενη εναλλακτική λύση (δηλαδή οι τεχνικές ανίχνευσης να εφαρμόζονται απευθείας στη συσκευή του χρήστη, πριν ξεκινήσει η επικοινωνία).

5.3 Η άποψη των EDPB και EDPS επί της Πρότασης Κανονισμού

Ο EDPS (European Data Protection Supervisor - «Ευρωπαίος Επόπτης Προστασίας Δεδομένων») από κοινού με την EDPB (European Data Protection Board - «Ευρωπαϊκή Επιτροπή Προστασίας Δεδομένων»), έχουν επισήμως εκφράσει την άποψή τους επί της εν λόγω Πρότασης [03]:

- Καταρχάς επισημαίνουν ότι το ίδιο το επεξηγηματικό σημείωμα (memo) της Πρότασης αναγνωρίζει ότι τα μέτρα που περιλαμβάνει αναμένεται να περιορίσουν θεμελιώδη δικαιώματα των χρηστών των υπηρεσιών που αφορά και τονίζουν ότι οι όποιοι τέτοιοι περιορισμοί θα πρέπει να συμμορφώνονται με τις απαιτήσεις του άρθρου 52 της Χάρτας Θεμελιωδών Δικαιωμάτων της ΕΕ που, μεταξύ άλλων, αναφέρει: «*Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον παρόντα Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων*» [24].

- Θεωρούν ότι προκύπτουν σημαντικές ανησυχίες για τα θεμελιώδη δικαιώματα της προστασίας της ιδιωτικότητας και των δεδομένων των χρηστών, από τις δυσανάλογα πολλές παρεμβάσεις και περιορισμούς που προτείνονται, ενώ οι όποιες ασφαλιστικές δικλείδες προβλέπονται για την προστασία τους είναι καθαρά διαδικαστικές και όχι ξεκάθαρες και ουσιώδεις. Επίσης, γεννά αρκετές (νομικές) αμφιβολίες, το κατά πόσον οι υπεύθυνοι για την εφαρμογή αυτών των δικλείδων προστασίας (ξεκινώντας από τους ιδιώτες Παρόχους και φτάνοντας στις κυβερνητικές ή/και δικαστικές αρχές) θα διαχειριστούν ξεχωριστά την κάθε περίπτωση που αφορά θεμελιώδη δικαιώματα.

- Θεωρούν επίσης ότι δεν ξεκαθαρίζονται επαρκώς κρίσιμα σημεία όπως η έννοια «σημαντικός κίνδυνος (significant risk)». Κανονικά, όταν ο νομοθέτης επιτρέπει σημαντικές παρεμβάσεις και περιορισμούς στα θεμελιώδη δικαιώματα, θα πρέπει να είναι απολύτως ξεκάθαρο νομικά το πότε και που θα επιτρέπονται. Φυσικά δεν είναι

εφικτό να καλύπτεται λεπτομερώς η κάθε περίπτωση και θα πρέπει να παρέχεται κάποια ευελιξία που θα βοηθά την εφαρμογή αυτών των περιορισμών στην πράξη. Όμως, οι EDPB & EDPS διατείνονται πως η συγκεκριμένη Πρόταση, λόγω της απουσίας ξεκάθαρων και ουσιωδών κανόνων, αφήνει πολλά περιθώρια διαφορετικών ερμηνειών και πιθανής καταστρατήγησης θεμελιωδών δικαιωμάτων με «μανδύα νομιμότητας». Εκφράζουν μάλιστα την ανησυχία τους ότι τα προτεινόμενα μέτρα εντοπισμού άγνωστου (νέου) υλικού CSAM ή/και εντοπισμού περιπτώσεων σεξουαλικής παρενόχλησης ανηλίκων (grooming), αν και έχουν καλό σκοπό, λόγω της επεμβατικής και πιθανολογικής φύσης τους και του υψηλού ποσοστού λαθών που παρουσιάζουν, θα παρεμβαίνουν στα δικαιώματα των ατόμων πολύ περισσότερο απ' όσο θα έπρεπε και απ' ότι είναι αναγκαίο!

- Στην Πρόταση προβλέπονται μέτρα που επιτρέπουν στις Αρχές να έχουν γενικά πρόσβαση στο περιεχόμενο ιδιωτικών συνομιλιών προκειμένου να εντοπίζουν περιπτώσεις σεξουαλικής παρενόχλησης ανηλίκων (grooming). Οι EDPB & EDPS διατείνονται ότι τα μέτρα αυτά πρόκειται να επηρεάσουν την ουσία των δικαιωμάτων που εγγυώνται τα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε. (*βλέπε ανωτέρω Ενότητα 3.1*) και θα πρέπει να αφαιρεθούν από την Πρόταση.

- Επίσης η Πρόταση δεν εξαιρεί την ερευνητική σάρωση επικοινωνιών Ήχου, γεγονός που είναι εξαιρετικά επεμβατικό και θα έπρεπε να βρίσκεται εκτός, τόσο για τα μηνύματα φωνής όσο και για τις ζωντανές επικοινωνίες.

- Αμφισβητούν την αποτελεσματικότητα των μέτρων αποκλεισμού (blocking), ενώ η απαίτηση από τους Παρόχους να αποκρυπτογραφούν τις online επικοινωνίες προκειμένου να μπλοκάρουν αυτές που αφορούν CSAM, θεωρείται υπερβολική και δυσανάλογη με το επιδιωκόμενο αποτέλεσμα. Επιπλέον επισημαίνουν ότι οι τεχνολογίες κρυπτογράφησης έχουν κεφαλαιώδη συνεισφορά στο σεβασμό της προσωπικής ζωής, στο απόρρητο των επικοινωνιών και στην ελευθερία της έκφρασης, καθώς και στην εν γένει ανάπτυξη της ψηφιακής οικονομίας που βασίζεται σε πολύ μεγάλο βαθμό στο υψηλό επίπεδο ασφάλειας και εμπιστοσύνης που αυτές προσφέρουν. Το δικαίωμα επιλογής τεχνολογίας εντοπισμού CSAM από τον Πάροχο, καθώς και των μέτρων προστασίας του απορρήτου των επικοινωνιών που θα εφαρμόζει, τίθενται υπό την αυστηρή υποχρέωση να συμβαδίζουν με τις απαιτήσεις

της Πρότασης, δηλαδή αφενός να υφίσταται εντοπισμός και αφετέρου να μην έχει ο Πάροχος το δικαίωμα άρνησης εφαρμογής της εντολής εντοπισμού επικαλούμενος αδυναμία για τεχνικούς λόγους.

- Θεωρούν ότι θα πρέπει να υπάρχει μια καλύτερη ισορροπία μεταξύ της διττής ανάγκης της κοινωνίας, αφενός να έχει ασφαλή κανάλια επικοινωνίας που προστατεύουν την ιδιωτικότητα και αφετέρου να καταπολεμά αποτελεσματικά τις περιπτώσεις εγκληματικής χρήσης αυτού του προνομίου. Θα πρέπει να αναφέρεται ξεκάθαρα στην πρόταση ότι τίποτα στον προτεινόμενο Κανονισμό δεν πρέπει να θεωρείται ως απαγόρευση ή αποδυνάμωση της κρυπτογράφησης.

- Ενώ καλωσορίζουν την αναφορά που περιέχεται στην Πρόταση ότι δεν επηρεάζονται οι εξουσίες και οι αρμοδιότητες που παρέχονται από τον GDPR στις Αρχές Προστασίας Δεδομένων, εκφράζουν την άποψη ότι η σχέση μεταξύ αυτών των αρχών και των Κανονιστικών αρχών που ορίζονται με την Πρόταση θα πρέπει να είναι καλύτερα ρυθμισμένες. Υπό το πρίσμα αυτό εκτιμούν μεν τον ρόλο που ανατίθεται στην EDPB ώστε να συμβάλλει στην εφαρμογή της Πρότασης στην πράξη (πιο συγκεκριμένα προβλέπεται για το Ευρωπαϊκό Κέντρο να συμβουλεύεται την άποψη του EDPB για τις τεχνολογίες που θα είναι διαθέσιμες στους Παρόχους προκειμένου να εκτελούν Εντολές), αλλά παράλληλα τονίζουν ότι θα πρέπει να διευκρινιστεί ξεκάθαρα ποιον σκοπό θα υπηρετούν οι απόψεις του EDPB και πώς αυτές θα επηρεάζουν τις ενέργειες του Ευρωπαϊκού Κέντρου. Επίσης η Πρόταση προβλέπει στενή συνεργασία του Κέντρου με την Europol που θα παρέχει και στα δύο μέρη την ευρύτερη δυνατή πρόσβαση στα πληροφοριακά συστήματα. Η EDPB και ο EDPS υποστηρίζουν κατ' αρχήν τη συνεργασία αυτή, αλλά καθώς το Ευρωπαϊκό Κέντρο δεν είναι αστυνομική αρχή, προτείνεται η βελτίωση κάποιων ζητημάτων, όπως ότι η μεταφορά προσωπικών δεδομένων μεταξύ τους θα γίνεται κατά περίπτωση, κατόπιν πλήρως τεκμηριωμένου αιτήματος και μέσω ενός ασφαλούς εργαλείου ανταλλαγής πληροφοριών.

Κεφάλαιο 6
Τεχνολογικές Προσεγγίσεις για Έλεγχο Επικοινωνιών

Στο παρόν Κεφάλαιο θα παρουσιαστούν κάποιες τεχνικές λύσεις που χρησιμοποιούν υφιστάμενες τεχνολογίες, ή έστω επερχόμενες στο άμεσο μέλλον (στο βαθμό που είναι γνωστά αρκετά στοιχεία γι' αυτές) και θα αξιολογηθούν κυρίως ως προς την αποτελεσματικότητά τους, αλλά και ως προς την προστασία της ιδιωτικότητας των χρηστών (καθώς και άλλα κριτήρια). Περιλαμβάνονται σε παράρτημα της Πρότασης Κανονισμού της ΕΕ [19, 10] (τα βασικά σημεία της οποίας παρουσιάστηκαν στο προηγούμενο Κεφάλαιο) και ενδεχομένως μπορούν να προσφέρουν λύση (ή έστω αποτελούν εξέλιξη προς τη σωστή κατεύθυνση), στο πρόβλημα της αποτελεσματικής ανίχνευσης CSAM και grooming στις E2EE επικοινωνίες.

Η αξιολόγηση των ανωτέρω τεχνικών βασίζεται σε 5 κριτήρια:

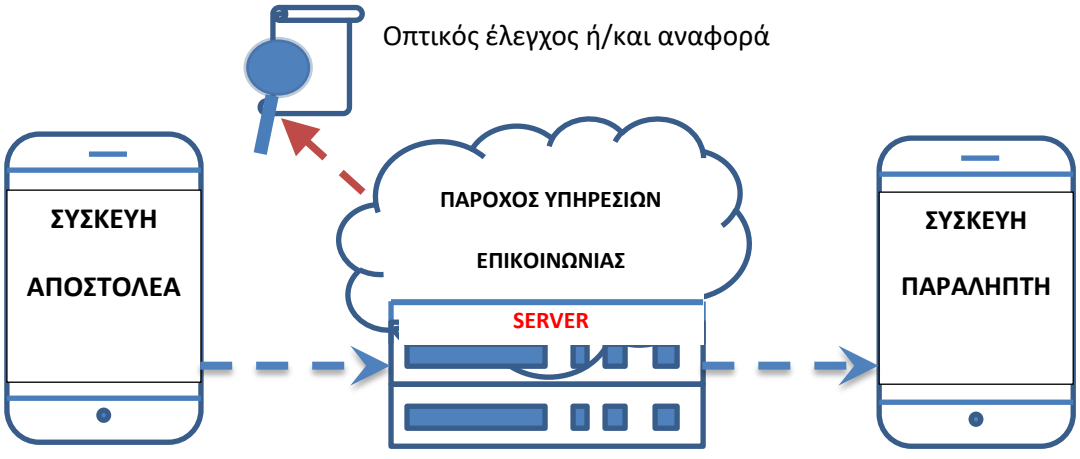
1) Αποτελεσματικότητα: Αξιολογείται το πόσο καλά η τεχνική εντοπίζει γνωστό αλλά και άγνωστο (δηλαδή νέο) υλικό CSA και grooming.
2) Εφαρμοσιμότητα: Αξιολογείται το πόσο «έτοιμη» είναι η τεχνική και πόσο εύκολα και γρήγορα μπορεί να εφαρμοστεί, με τι κόστος και σε τι κλίμακα;
3) Προστασία της Ιδιωτικότητας (Privacy): Αξιολογείται το επίπεδό της.
4) Ασφάλεια: Αξιολογείται το πόσο εύκολο είναι να χρησιμοποιηθεί η τεχνική από άτομα, εταιρείες, οργανισμούς και κυβερνήσεις για άλλους (αμφίβολους) σκοπούς που δεν έχουν σχέση με τον εντοπισμό CSAM και grooming.
5) Διαφάνεια: αξιολογείται το κατά πόσο η χρήση της τεχνικής μπορεί να τεκμηριωθεί και να δημοσιοποιηθεί στο ευρύ κοινό, έτσι ώστε να είναι εφικτή η εποπτεία της από τις αρμόδιες επιτροπές των κοινοβουλίων και από ανεξάρτητους οργανισμούς προστασίας των δικαιωμάτων των πολιτών και κατά συνέπεια, η απόδοση ευθυνών σε περίπτωση καταστρατήγησης του σκοπού και του πεδίου χρήσης της.

6.1. Σημείο Αναφοράς & Σύγκρισης: Μη κρυπτογραφημένες επικοινωνίες

Για να υπάρχει ένα σημείο αναφοράς και μέτρο σύγκρισης, θα εξεταστεί πρώτα η περίπτωση των μη κρυπτογραφημένων επικοινωνιών. Στην περίπτωση αυτή υπάρχουν διαθέσιμα εργαλεία, που μπορούν να εφαρμοστούν άμεσα από τον Πάροχο της επικοινωνίας προκειμένου να εντοπιστεί υλικό CSA (εικόνες, βίντεο) και grooming (κυρίως κείμενο):

α) Εργαλεία Hashing (σύγκρισης αλφαριθμητικών σειρών κατακερματισμού): Είναι κατάλληλα για εντοπισμό CSA φωτογραφιών και βίντεο. Μετατρέπουν το προς έλεγχο οπτικό υλικό σε μια μοναδική αλφαριθμητική σειρά κατακερματισμού (Hash), η οποία κατόπιν συγκρίνεται με μια Βάση Δεδομένων (ΒΔ) που περιέχει πλειάδα τέτοιων αλφαριθμητικών σειρών - Hashes που προέκυψαν από εξακριβωμένα γνωστό οπτικό υλικό CSA.

β) Εργαλεία Σύγκρισης «Λέξεων Κλειδιών»: Είναι κατάλληλα για εντοπισμό περιπτώσεων σεξουαλικής παρενόχλησης και εκβιασμού παιδιών (grooming – sextortion) όπου η επικοινωνία γίνεται μέσω μηνυμάτων (sexting). Τα εργαλεία αυτά ερευνούν το προς έλεγχο μήνυμα κειμένου προκειμένου να εντοπίσουν «λέξεις κλειδιά – (keywords)» ή/και ολόκληρες φράσεις που χρησιμοποιούνται συχνά σε τέτοιες περιπτώσεις.

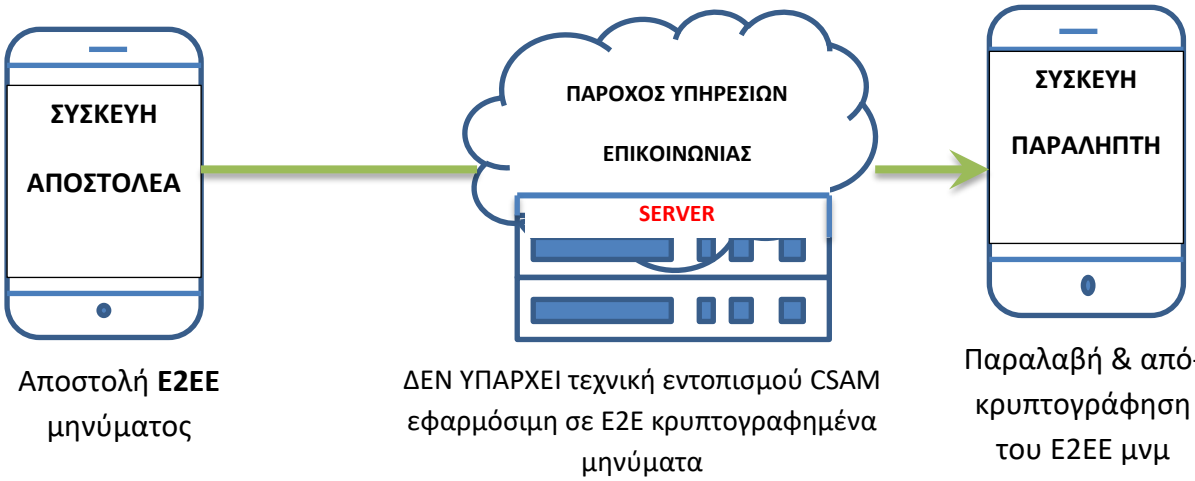


Σχήμα 2.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Υψηλή**, τόσο στον εντοπισμό CSAM όσο και στον εντοπισμό περιπτώσεων παρενόχλησης παιδιών με μηνύματα (grooming). Η επίδοση αυτή οφείλεται σε πολύ μεγάλο βαθμό στο ότι εδώ τα εργαλεία εφαρμόζονται σε μη κρυπτογραφημένες επικοινωνίες.
2) Εφαρμοσιμότητα: **Υψηλή**. Τα εργαλεία αυτά υπάρχουν εδώ και καιρό και χρησιμοποιούνται ευρέως, αποτελώντας μάλιστα την προεπιλεγμένη τεχνική λύση ανίχνευσης CSAM και grooming.
3) Προστασία της Ιδιωτικότητας: **Χαμηλή**. Ο Πάροχος μπορεί ανά πάσα στιγμή να έχει πρόσβαση στο περιεχόμενο των επικοινωνιών που διαχειρίζεται.
4) Ασφάλεια: **Μέτρια**. Εξαιτίας του (3) ανωτέρω. Πάντως μπορεί να επιτευχθεί μεγαλύτερος βαθμός ασφάλειας αναφορικά με την δυνατότητα πρόσβασης τρίτων, εφόσον εφαρμοστεί κάποιου άλλου είδους κρυπτογράφηση (π.χ. client-server).
5) Διαφάνεια: **Μέτρια**. Αν και η χρήση τεχνικών εντοπισμού CSAM και grooming μπορεί να γίνει (και γίνεται) γνωστή στο ευρύ κοινό (για λόγους διαφάνειας αλλά και αποτροπής διακίνησης CSAM), δεν είναι πάντα εφικτό να ελεγχθεί εάν γίνεται χρήση των ιδίων τεχνικών και για άλλους σκοπούς (νόμιμους ή μη), καθώς δεν υφίστανται πάντα αρμόδιοι εποπτικοί μηχανισμοί.

6.2. E2E Κρυπτογραφημένες Επικοινωνίες



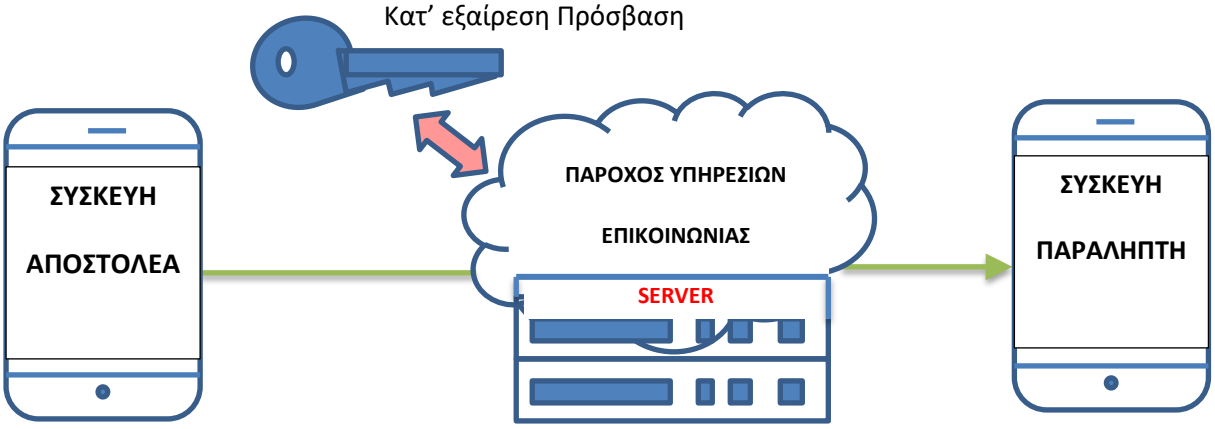
Σχήμα 3.

Στις E2EE επικοινωνίες χρησιμοποιείται ένα πρωτόκολλο δημοσίου κλειδιού (public key protocol) προκειμένου ο αποστολέας και ο παραλήπτης να συμφωνήσουν σ' ένα κρυφό κλειδί που θα τους επιτρέψει να διεξάγουν μια ασφαλή κρυπτογραφημένη επικοινωνία μεταξύ τους. Κανένας τρίτος δεν γνωρίζει (και δεν μπορεί να προσδιορίσει) το κλειδί αυτό, ούτε καν ο ίδιος ο Πάροχος και κατά συνέπεια δεν μπορεί να εφαρμόσει κανένα εργαλείο εντοπισμού CSAM και grooming, αφού ο server του δεν μπορεί να έχει καμία πρόσβαση στα δεδομένα.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Καμία**, καθώς δεν είναι εφικτό να εφαρμοστούν εργαλεία εντοπισμού CSAM και grooming.
2) Εφαρμοσιμότητα: **Μη αξιολογήσιμη**, καθώς δεν υπάρχει διαθέσιμη τεχνική λύση εντοπισμού CSAM και grooming, για να εφαρμοστεί.
3) Προστασία της Ιδιωτικότητας: **Υψηλή**. Μόνο ο αποστολέας και ο παραλήπτης μπορούν να έχουν πρόσβαση στο περιεχόμενο της επικοινωνίας.
4) Ασφάλεια: **Μη αξιολογήσιμη**, καθώς όπως προαναφέρθηκε, δεν υπάρχει κάποια τεχνική λύση εντοπισμού CSAM και grooming, για να πληγεί η ασφάλειά της.
5) Διαφάνεια: **Μη αξιολογήσιμη**, καθώς όπως προαναφέρθηκε, δεν υπάρχει κάποια τεχνική λύση εντοπισμού CSAM και grooming.

6.3. Κατ' εξαίρεση πρόσβαση σε E2EE επικοινωνίες



Αποστολή **E2EE** μηνύματος

ΔΕΝ ΥΠΑΡΧΕΙ τεχνική εντοπισμού CSAM & grooming, εφαρμόσιμη σε E2E κρυπτογραφημένα μηνύματα. Μπορεί όμως να το κάνει «**Κατ' Εξαίρεση**» σε ειδικές περιπτώσεις, αφού πρώτα αποκρυπτογραφήσει το μνμ

Παραλαβή & απο-κρυπτογράφηση του E2EE μνμ

Σχήμα 4.

Ουσιαστικά είναι ίδια με την παραπάνω κατηγορία, όμως με μια πολύ σημαντική διαφορά: Ο Πάροχος της επικοινωνίας καθώς και οι Αρχές έχουν δυνατότητα για κατ' εξαίρεση πρόσβαση στα κρυπτογραφημένα δεδομένα. Αυτό καθίσταται εφικτό με την εσκεμμένη ενσωμάτωση κάποιας «κερκόπορτας (backdoor)» στην E2E κρυπτογράφηση που «ανοίγει» με ειδικό κλειδί αποκρυπτογράφησης που έχει στη διάθεσή του ο Πάροχος για «εξαιρετικές περιπτώσεις». Δηλαδή η δυνατότητα αυτή δεν εφαρμόζεται σε μόνιμη ή/και προληπτική βάση, αλλά μόνο κατά περίπτωση και για εξαιρετικό λόγο (π.χ. να έχει εκδοθεί σχετικό ένταλμα έρευνας). Όταν συμβαίνει αυτό, τα διακινούμενα δεδομένα πρώτα αποκρυπτογραφούνται, και κατόπιν πραγματοποιείται εφαρμογή εργαλείων εντοπισμού CSAM και grooming, καθώς είναι πια εφικτό.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Χαμηλή**, καθώς όπως προαναφέρθηκε, δεν εφαρμόζεται σε προληπτική βάση, αλλά μόνο κατ' εξαίρεση σε συγκεκριμένες περιπτώσεις και υπό προϋποθέσεις.
2) Εφαρμοσιμότητα: **Μέτρια**. Η λύση είναι εφαρμόσιμη, άλλα στην πράξη το κόστος μπορεί να είναι υψηλό.
3) Προστασία της Ιδιωτικότητας: **Χαμηλή**. Θεωρητικά, ο Πάροχος μπορεί να έχει πρόσβαση σε όλο το περιεχόμενο των επικοινωνιών που διαχειρίζεται, οποιαδήποτε στιγμή, εάν αυτές κριθούν «εξαιρετικές περιπτώσεις».
4) Ασφάλεια: **Μέτρια → Χαμηλή**. Ανακύπτουν κάποια ζητήματα: Π.χ. τυπικό ζητούμενο μιας τέτοιας τεχνολογίας είναι να διασφαλίζει ότι την κατ' εξαίρεση πρόσβαση θα την εφαρμόσει ο εξουσιοδοτημένος φορέας και όχι κάποιος που «χάκαρε» τον φορέα ή τον παριστάνει. Επίσης, στην πράξη μπορεί να είναι δύσκολο να καθοριστεί ποιος θα μπορεί να λαμβάνει το δικαίωμα της κατ' εξαίρεση πρόσβασης και ποιος όχι.
5) Διαφάνεια: **Μέτρια**. Η λύση της εξουσιοδοτημένης κατ' εξαίρεση πρόσβασης μπορεί σχετικά εύκολα να τεκμηριωθεί και να δημοσιοποιηθεί στο ευρύ κοινό.

6.4. Τεχνικές Λύσεις που σχετίζονται με την Συσκευή

Σε αυτό το είδος λύσεων, κάποιες ή και όλες οι λειτουργίες που δεν είναι E2EE, δεν διεκπεραιώνονται από τον Server επικοινωνίας του Παρόχου, αλλά ανατίθενται στις Συσκευές, είτε του αποστολέα (καταλληλότερη για τον εντοπισμό διακίνησης CSAM), είτε

του χρήστη (καταλληλότερη για τον εντοπισμό περιπτώσεων σεξουαλικής παρενόχλησης ανηλίκων - grooming), είτε και των δύο, που είναι ακόμα πιο αποτελεσματική λύση.

6.4.1. Όλη η λειτουργία του εντοπισμού πραγματοποιείται στη συσκευή

Σε αυτή την λύση, όλες οι κύριες λειτουργίες εντοπισμού που θα γίνονταν από τον server (π.χ. κατακερματισμός/hashing και έλεγχος ταύτισης βίντεο, φωτογραφιών/εικόνων και κειμένου) ανατίθενται στην Συσκευή του αποστολέα και εφαρμόζονται πριν την κρυπτογράφηση του μηνύματος. Εάν, από τον έλεγχο δεν βρεθεί κάτι ύποπτο, το μήνυμα κρυπτογραφείται με E2EE και αποστέλλεται στον παραλήπτη.

Εφόσον όμως διαπιστωθεί υψηλού βαθμού ταύτιση με CSAM ή grooming, το μήνυμα επισημαίνεται ως ύποπτο και δεν προωθείται στον παραλήπτη αλλά αποστέλλεται για περαιτέρω (οπτικό) έλεγχο ή/και αναφορά στις Αρχές:

Έλεγχος εντοπισμού CSAM με Hashing εικόνων & σύγκριση με Hashes γνωστού CSAM για ΤΑΥΤΙΣΗ:
ΝΑΙ → Περαιτέρω οπτικός έλεγχος ή/& αναφορά
ΟΧΙ →**E2EE** του μνμ & αποστολή στον παραλήπτη

ΔΕΝ ΥΠΑΡΧΕΙ τεχνική εντοπισμού CSAM εφαρμόσιμη σε E2E κρυπτογραφημένα μηνύματα

Παραλαβή & απόκρυπτογράφηση του E2EE μνμ

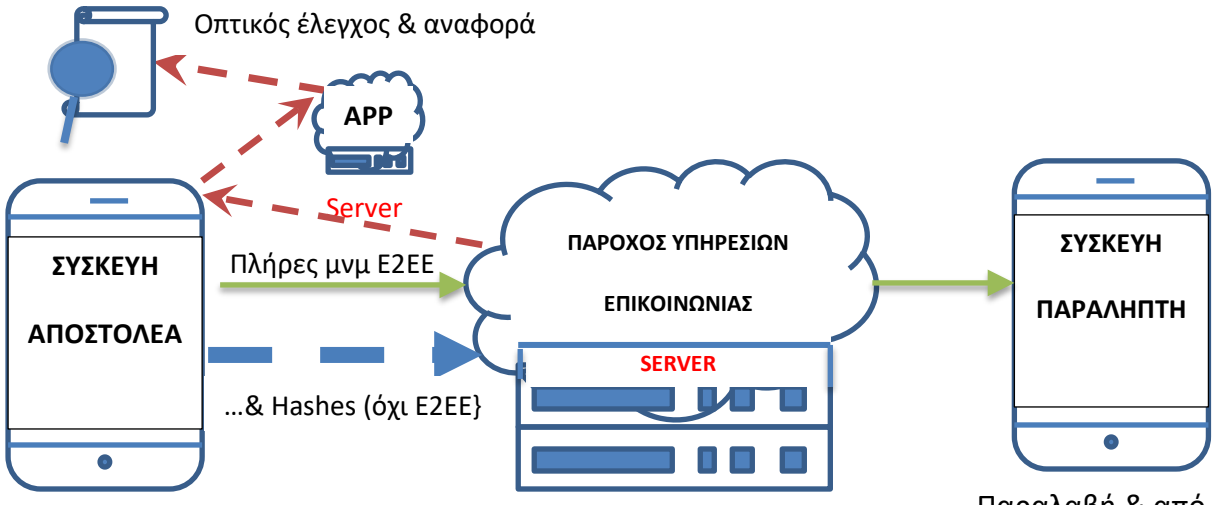
Σχήμα 5.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**, καθώς είναι κατάλληλη λύση για εντοπισμό γνωστού υλικού CSA. Όμως η αποτελεσματικότητά της μπορεί να περιορίζεται από τις τεχνικές προδιαγραφές της συσκευής (π.χ. ταχύτητα επεξεργασίας, μνήμη) σε σύγκριση με το εάν γινόταν από τον Server του Παρόχου.

2) Εφαρμοσιμότητα: **Μέτρια → Χαμηλή**. Είναι εύκολα εφαρμόσιμη λύση, άλλα απαιτεί σημαντική υπολογιστική ισχύ και μεγάλο αποθηκευτικό χώρο, που μια συσκευή μπορεί να μην διαθέτει - βλέπε και (1) ανωτέρω.
3) Προστασία της Ιδιωτικότητας: **Μέτρια**. Ο Πάροχος δεν αποκτά πρόσβαση σε μη κρυπτογραφημένα δεδομένα. Υφίστανται όμως θέματα ασφάλειας (βλέπε κατωτέρω) που μπορούν να επηρεάσουν σημαντικά την ιδιωτικότητα.
4) Ασφάλεια: **Χαμηλή**. Τα εργαλεία εντοπισμού που τρέχουν στη συσκευή μπορούν εύκολα να προσβληθούν ή/και να τροποποιηθούν από hackers ώστε να καταστούν ανενεργά (να μην λειτουργούν) ή αναποτελεσματικά (να μην εντοπίζουν CSAM/grooming), ή και να κατακλύζουν με ψευδείς εντοπισμούς (false positive) τα συστήματα των Οργανισμών αναφοράς ώστε να τα παραλύσουν. Επίσης, τυχόν διαρροή των εργαλείων εντοπισμού και των βασικών τους στοιχείων (π.χ. αλγόριθμος κατακερματισμού, λίστες hash και κλειδιών) μπορεί ουσιαστικά να επιφέρει την ακύρωσή τους και την παύση της χρήσης τους γενικότερα.
5) Διαφάνεια: **Μέτρια → Χαμηλή**. Τα προβλήματα ασφάλειας που αναφέρθηκαν ανωτέρω δύνανται να υπονομεύσουν την αξιοπιστία των ελέγχων που γίνονται, άρα και την οποιαδήποτε εποπτεία και δημόσια ενημέρωση του κοινού περί της ορθής και νόμιμης (ή μη) χρήσης της λύσης.

6.4.2. Συσκευή: Πλήρες Hashing – Server: Έλεγχος Ταύτισης με CSAM



α) Πριν κρυπτογραφήσει το μνμ, εξάγει Hashes από εικόνες/video.
β) Στέλνει το μνμ **E2EE**, καθώς και τα Hashes **C2SE**, στον Server

Σύγκριση των ληφθέντων Hashes, με Hashes γνωστού CSAM για ΤΑΥΤΙΣΗ:
ΟΧΙ →προωθεί το E2EE μνμ που έλαβε, στον παραλήπτη
ΝΑΙ → Μέσω της συσκευής ειδοποιείται ο APP Server να στείλει την (αυθεντική) εικόνα/video για οπτικό έλεγχο ή/& αναφορά

Παραλαβή & από-κρυπτογράφηση του E2EE μνμ

Σχήμα 6.

Σε αυτήν την λύση, πριν η Συσκευή του αποστολέα κρυπτογραφήσει το μήνυμα, εξάγει Hashes από τα βίντεο και τις φωτογραφίες/εικόνες που τυχόν περιέχει, Ακολούθως τα στέλνει στον Server με C2SE (client-to-server κρυπτογράφηση), όπως επίσης και το πλήρες μήνυμα (E2E κρυπτογραφημένο). Ο Server συγκρίνει τις ληφθείσες σειρές Hash με μια ΒΔ που περιέχει σειρές Hash επιβεβαιωμένου (γνωστού) υλικού CSA:
α) Εάν διαπιστωθεί υψηλού βαθμού ταύτιση το μήνυμα χαρακτηρίζεται ως ύποπτο και ζητείται από τον Application Server που έχει πρόσβαση στο «ύποπτο» βίντεο/εικόνα (στην αυθεντική του, μη κρυπτογραφημένη μορφή), να το στείλει για περαιτέρω για (οπτικό) έλεγχο. Εφόσον κι απ' αυτόν τον έλεγχο επιβεβαιωθεί ότι όντως πρόκειται για CSAM, γίνεται σχετική αναφορά στις Αρχές και ο Server «μπλοκάρει» το μήνυμα (δεν το προωθεί στον παραλήπτη).
β) Εάν δεν διαπιστωθεί ταύτιση (ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM από τον οπτικό έλεγχο), το πλήρες E2EE μήνυμα προωθείται από τον Server στον παραλήπτη, ο οποίος το αποκρυπτογραφεί προκειμένου να το διαβάσει.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**. Κατάλληλη λύση για εντοπισμό μόνο γνωστού υλικού CSA, αλλά ακατάλληλη για grooming (που αφορά κείμενα, όπου δεν είναι εφικτό να εφαρμοστεί τεχνική Hashing). Καθώς η λίστα με τις σειρές Hash βρίσκεται αποθηκευμένη στον Server, δεν υπάρχουν περιορισμοί για το μέγεθός της από τις τεχνικές δυνατότητες της συσκευής (όπως στην προηγούμενη κατηγορία).
2) Εφαρμοσιμότητα: **Υψηλή**. Είναι σχετικά εύκολα εφαρμόσιμη λύση, ενώ μπορεί να κατασκευαστεί και μια ανοικτού κώδικα έκδοσή της, για μικρότερους Παρόχους.
3) Προστασία της Ιδιωτικότητας: **Μέτρια**. Ο Πάροχος μπορεί να δει τις σειρές Hash των χρηστών. Και εδώ υφίστανται θέματα ασφάλειας (βλέπε κατωτέρω) που μπορούν να μετριάσουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας.
4) Ασφάλεια: **Μέτρια → Χαμηλή**. Ο αλγόριθμος Hashing στη συσκευή μπορεί εύκολα να προσβληθεί από hackers ώστε να καταστεί ανενεργός (να μην λειτουργεί) ή αναποτελεσματικός (να μην εντοπίζει CSAM), ή/και να τροποποιηθεί ώστε να κατακλύζει με ψευδείς εντοπισμούς (false positive) τα συστήματα των Οργανισμών αναφοράς προκειμένου να παραλύσουν. Είναι επίσης δυνατόν, να εισαχθούν δολίως στην ΒΔ του Server με τις λίστες Hash, σειρές Hash που δεν αφορούν CSA υλικό. Τυχόν διαρροή των εργαλείων εντοπισμού καθώς και των βασικών στοιχείων τους (π.χ.

αλγόριθμος κατακερματισμού, λίστες hash και κλειδιών) μπορεί ουσιαστικά να επιφέρει την ακύρωσή τους και την παύση της χρήσης τους γενικότερα.

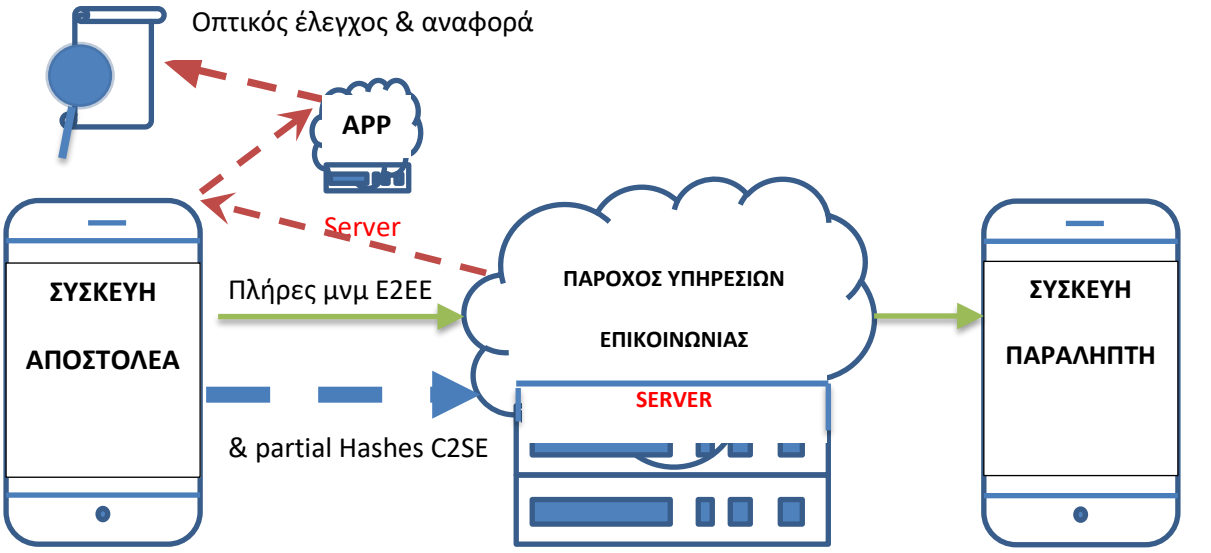
5) Διαφάνεια: **Μέτρια**. Τα προβλήματα ασφάλειας που αναφέρθηκαν ανωτέρω δύνανται να υπονομεύσουν την αξιοπιστία των ελέγχων που γίνονται, άρα και την οποιαδήποτε εποπτεία και δημόσια ενημέρωση του κοινού περί της ορθής και νόμιμης (ή μη) χρήσης της λύσης.

6.4.3. Συσκευή: Μερικό Hashing – Server: Απομένον Hashing & Έλεγχος Ταύτισης CSAM

Πρόκειται για μια υβριδική λύση, παρόμοια με την προηγούμενη, με την διαφορά ότι μόνο ένα μέρος του κατακερματισμού (Hashing) πραγματοποιείται στην Συσκευή, ενώ το υπόλοιπο πραγματοποιείται στον Server, όπου (όπως και προηγουμένως) πραγματοποιείται επίσης και ο έλεγχος ταύτισης CSAM. Με αυτόν τον τρόπο η διαδικασία γίνεται πιο «ελαφριά» (δεν επιβαρύνεται πολύ η Συσκευή) και πιο ασφαλής.

Πιο συγκεκριμένα και σε αυτήν την λύση, πριν η Συσκευή του αποστολέα κρυπτογραφήσει το μήνυμα, μετατρέπει τα βίντεο και τις φωτογραφίες/εικόνες που τυχόν περιέχει, σε μοναδικές μερικώς ολοκληρωμένες αλφαριθμητικές σειρές (partial Hashes). Ακολούθως τις στέλνει στον Server (με client-to-server κρυπτογράφηση), όπως επίσης και το (E2E κρυπτογραφημένο) πλήρες μήνυμα.

Ο Server από την πλευρά του ολοκληρώνει και καθιστά πλήρη τα ληφθέντα partial Hashes και κατόπιν τα συγκρίνει με μια ΒΔ που περιέχει Hashes επιβεβαιωμένου CSAM:
α) Εάν διαπιστωθεί υψηλού βαθμού ταύτιση το μήνυμα χαρακτηρίζεται ως ύποπτο και ζητείται από τον Application Server που έχει πρόσβαση στο «ύποπτο» βίντεο/εικόνα (στην αυθεντική του, μη κρυπτογραφημένη μορφή), να το στείλει για περαιτέρω για (οπτικό) έλεγχο. Εφόσον κι απ' αυτόν τον έλεγχο επιβεβαιωθεί ότι όντως πρόκειται για CSAM, γίνεται σχετική αναφορά στις Αρχές και ο Server «μπλοκάρει» το μήνυμα (δεν το προωθεί στον παραλήπτη).
β) Εάν δεν διαπιστωθεί ταύτιση (ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM από τον οπτικό έλεγχο), το πλήρες E2EE μήνυμα προωθείται από τον Server στον παραλήπτη, ο οποίος το αποκρυπτογραφεί προκειμένου να το διαβάσει.



α) Πριν κρυπτογραφήσει το μνμ, εξάγει **partial Hashes** από εικόνες /video.
β) Στέλνει το μνμ **E2EE**, καθώς και τα partial Hashes **C2SE**, στον Server

Μετατροπή των ληφθέντων partial Hashes σε πλήρη & Σύγκρισή τους με Hashes γνωστού CSAM για ΤΑΥΤΙΣΗ:
ΟΧΙ →προωθεί το E2EE μνμ που έλαβε, στον παραλήπτη
ΝΑΙ →Μέσω της συσκευής ειδοποιείται ο APP Server να στείλει την (αυθεντική) εικόνα/video για οπτικό έλεγχο ή/& αναφορά

Παραλαβή & από-κρυπτογράφηση του E2EE μνμ

Σχήμα 7.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**. Κατάλληλη λύση για εντοπισμό μόνο γνωστού υλικού CSA, αλλά ακατάλληλη για grooming (που αφορά κείμενα, όπου δεν είναι εφικτό να εφαρμοστεί τεχνική Hashing). Καθώς η λίστα με τις σειρές Hash βρίσκεται αποθηκευμένη στον Server, δεν υπάρχουν περιορισμοί για το μέγεθός της.
2) Εφαρμοσιμότητα: **Μέτρια**. Έχει αποδειχθεί στην θεωρία ότι η λύση αυτή είναι εφαρμόσιμη και μάλιστα τη στιγμή που γράφονται αυτές οι γραμμές, μπορεί να έχει ήδη εφαρμοστεί στην πράξη. Επειδή πρόκειται για σχετικά καινούργια λύση και οι λεπτομέρειες της πρακτικής εφαρμογής της είναι σημαντικές, (π.χ. για να επιτυγχάνεται η βέλτιστη ταχύτητα), κάποιες απ' αυτές θα πρέπει να αποσαφηνιστούν. Πάντως με τον επιμερισμό του κατακερματισμού μεταξύ Συσκευής και Server, η λύση αυτή αναμένεται να είναι πολύ πιο γρήγορη από την προηγούμενη καθώς η Συσκευή του αποστολέα απαλλάσσεται από σημαντικό όγκο επεξεργασίας.
3) Προστασία της Ιδιωτικότητας: **Μέτρια**. Ο Πάροχος μπορεί να δει τις σειρές Hash των χρηστών και επιπλέον, εξαιτίας του μερικού κατακερματισμού, μπορεί να δει και

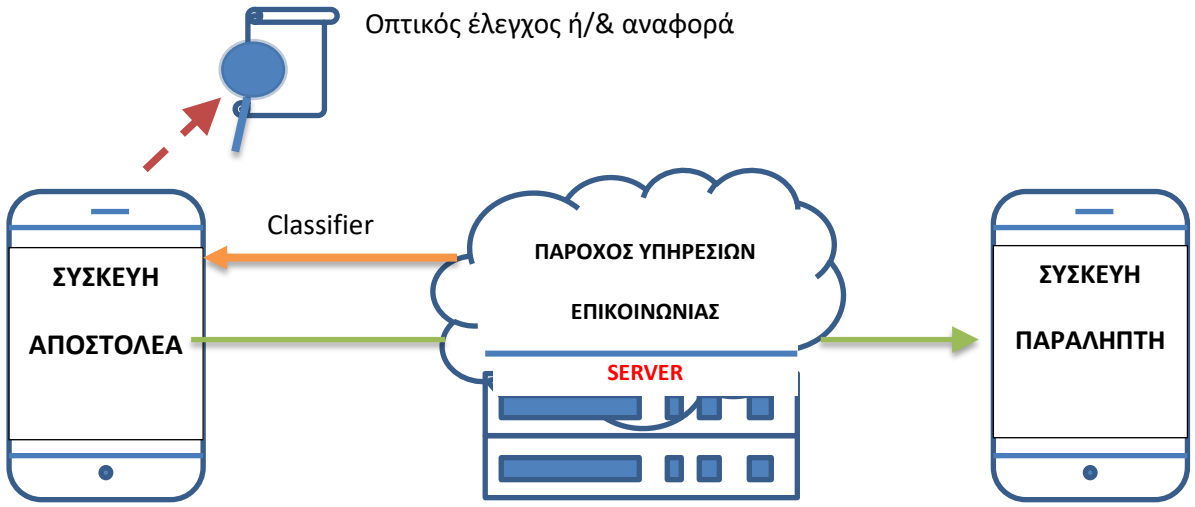
περισσότερες πληροφορίες για τις εικόνες. Παρόλο που γενικά βελτιώνεται η ασφάλεια εξαιτίας του μερικού κατακερματισμού, τα επιμέρους θέματα που αναφέρθηκαν και στην προηγούμενη λύση εξακολουθούν να υφίστανται (βλέπε κατωτέρω) και δύνανται να μετριάσουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας.

4) Ασφάλεια: **Μέτρια**. Η Συσκευή περιέχει μόνο ένα μέρος του αλγόριθμου Hashing, γεγονός που από μόνο του μειώνει τον κίνδυνο εφαρμογής τεχνικών αντίστροφης μηχανικής (reverse engineering) ή χειραγώγησης (manipulation) για την αποκάλυψή του, ενώ για περαιτέρω ασφάλεια μπορούν να εφαρμοστούν και τεχνικές «συσκότισης» που ανακατεύουν τα pixel της εικόνας και καθιστούν το Hash της μη αναστρέψιμο, χωρίς όμως να επηρεάζουν τη δημιουργία του.
5) Διαφάνεια: **Μέτρια**. Καθώς όμως το επίπεδο ασφαλείας της λύσης, παρά τις ανωτέρω βελτιώσεις, εξακολουθεί να παραμένει μέτριο, δύναται να υπονομεύσει την αξιοπιστία των ελέγχων που γίνονται, άρα και την οποιαδήποτε εποπτεία και δημόσια ενημέρωση του κοινού περί της ορθής και νόμιμης (ή μη) χρήσης της λύσης.

6.4.4. Χρήση Classifiers στην Συσκευή

Στόχος αυτής της λύσης είναι το λεγόμενο «Machine Learning», δηλαδή το να εκπαιδευτεί ο υπολογιστής που διενεργεί τον έλεγχο να αναγνωρίζει με μεγάλη βεβαιότητα υλικό CSA.

Ο Server του Παρόχου δημιουργεί τους λεγόμενους Classifiers (ταξινομητές) χρησιμοποιώντας μεγάλο αριθμό από δεδομένα (βίντεο, φωτογραφίες/εικόνες και/ή κείμενο) που έχουν επιβεβαιωμένα χαρακτηριστεί ως CSAM, και από άλλα δεδομένα που όμως δεν αποτελούν CSAM, προκειμένου να «εκπαιδευτεί» το σύστημα Machine Learning να ξεχωρίζει τα μεν από τα δε. Οι Classifiers είναι μια ομάδα χαρακτηριστικών που καθορίζει εάν το περιεχόμενο ενός μηνύματος σχετίζεται με CSAM. Ο Server «τοποθετεί» τους Classifiers στην Συσκευή του αποστολέα, η οποία τους χρησιμοποιεί (πριν την κρυπτογράφηση και αποστολή του μηνύματος) για να καθορίσει εάν το μήνυμα θα «ταξινομηθεί» ως ύποπτο για CSAM και θα προωθηθεί για οπτικό έλεγχο ή/και αναφορά. Εάν όμως οι Classifiers δεν το ταξινομήσουν ως ύποπτο (ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM κατά τον οπτικό έλεγχο), το μήνυμα κρυπτογραφείται με E2EE και αποστέλλεται στην συσκευή του παραλήπτη, η οποία το αποκρυπτογραφεί προκειμένου να διαβαστεί.



Πριν την κρυπτογράφηση του μνμ χρησιμοποιεί **Classifiers** για εντοπισμό CSAM. Εάν αυτός αποβεί:
ΘΕΤΙΚΟΣ → Περαιτέρω οπτι - κός έλεγχος ή/& αναφορά
ΑΡΝΗΤΙΚΟΣ →**E2EE** του μνμ & αποστολή στον παραλήπτη

1) «Εκπαιδεύει» τον **Machine Learning Αλγόριθμο**.
2) «Τοποθετεί» **Classifiers** στην Συσκευή του αποστολέα & τους κρατά ενημερωμένους

Παραλαβή & από- κρυπτογράφηση του E2EE μνμ

Σχήμα 8.

Επομένως ο ρόλος του Server του Παρόχου είναι να «εκπαιδεύει» τον «Machine Learning» αλγόριθμο, ώστε καθώς αντιμετωπίζει όλο και περισσότερες περιπτώσεις με CSAM, να γίνεται όλο και πιο «έξυπνος» και αποτελεσματικός. Φυσικά, προωθεί αυτήν την «επιπλέον γνώση» στους Classifiers που βρίσκονται στις συσκευές, με συχνές ενημερώσεις λογισμικού.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Χαμηλή**. Είναι ουσιαστικά η μόνη λύση που επιτρέπει τον απευθείας εντοπισμό άγνωστου υλικού CSA, καθώς φυσικά και γνωστού. Όμως, ο εντοπισμός βίντεο και φωτογραφιών/εικόνων με χρήση της τεχνικής «Machine Learning» δεν είναι ακόμα αρκετά εξελιγμένη τεχνική και παράγει σχετικά υψηλό αριθμό λαθών (σε σχέση με τις τεχνικές ελέγχου ταύτισης Hash).
   Οι αλγόριθμοι «Machine Learning» προϋποθέτουν:
   α) την ύπαρξη καλά «επισημασμένων» δεδομένων (ως CSAM ή μη) και μάλιστα σε συνεχή βάση, ώστε τα μοντέλα που εμπεριέχουν να είναι διαρκώς ενημερωμένα και να λειτουργούν αποτελεσματικά.
   β)…συνεχή ανατροφοδότηση για την ποιότητα της ταξινόμησης που διενεργούν (δηλαδή για τις επιτυχίες και τις αποτυχίες που έχουν), γεγονός που είναι ιδιαίτερα

δύσκολο να τους παρέχεται σε σταθερή βάση, όταν πρόκειται για εντοπισμό CSAM σε E2EE συστήματα.

Γενικά, η μη ενημέρωση των αλγορίθμων αυτών σε μόνιμη και σταθερή βάση μπορεί γρήγορα να τους καταστήσει «ξεπερασμένους».

Οι Classifiers φαίνεται να τα πηγαίνουν καλύτερα με τον εντοπισμό ύποπτων κειμένων (π.χ. περιπτώσεις grooming και sextortion) μέσω προτύπων συμπεριφοράς. Και εδώ όμως ισχύουν οι ανωτέρω προϋποθέσεις (α) και (β).

2) Εφαρμοσιμότητα: **Μέτρια→Χαμηλή**. «Classifiers Εικόνας» χρησιμοποιούνται ήδη από εταιρείες σε υπηρεσίες νέφους-cloud (π.χ. για να ανιχνεύουν συχνά εμφανιζόμενα πρόσωπα σε φωτογραφίες ή για αυτόματη ομαδοποίηση εικόνων), ενώ έχει ξεκινήσει και η χρήση τους για εντοπισμό CSAM. Απαιτείται όμως ακόμα πολύ δουλειά ιδιαίτερα στον τομέα του εντοπισμού βίντεο και εικόνων και στη δυνατότητα του να τρέχουν Classifiers στην συσκευή, δεδομένης της πολυπλοκότητας των μοντέλων και των απαιτήσεων που έχουν για συνεχείς ενημερώσεις. Όπως αναφέρθηκε και ανωτέρω, τα αποτελέσματα δείχνουν να είναι καλύτερα (και πιο εφαρμόσιμα) στον τομέα του εντοπισμού κειμένων (π.χ. grooming, sextortion).
3) Προστασία της Ιδιωτικότητας: **Μέτρια→Χαμηλή**. Οι πιθανοί κίνδυνοι ασφάλειας που υφίστανται (π.χ. προσβολή και χειραγώγηση των Classifiers), δύνανται να μετριάσουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας. Ειδικότερα για τους «Classifiers συμπεριφοράς» οι οποίοι ανιχνεύουν πιθανές περιπτώσεις CSAM με βάση τα «μεταδεδομένα» (metadata) του χρήστη, η διείσδυση στην ιδιωτικότητά του είναι σημαντικότερη απ' ότι με άλλα εργαλεία όπως το hashing. Επιπλέον, το σημαντικό ποσοστό λανθασμένων εντοπισμών CSAM μπορεί να επιφέρει την χωρίς λόγο αναφορά και περαιτέρω έρευνα δεδομένων χρηστών που όμως δεν εμπεριέχουν CSAM. Τέλος, είναι πιθανή η παράνομη χρήση Classifiers για άσχετες με CSA δραστηριότητες των χρηστών.
4) Ασφάλεια: **Μέτρια→Χαμηλή**. Οι Classifiers που βρίσκονται σε συσκευή είναι δυνατόν να προσβληθούν ή/και να χειραγωγηθούν ώστε να καταστούν ανενεργοί (να μην λειτουργούν) ή αναποτελεσματικοί (να μην εντοπίζουν CSAM), ή/και να κατακλύζουν με ψευδείς εντοπισμούς (false positive) τα συστήματα των Οργανισμών αναφοράς ώστε να τα παραλύσουν. Επίσης, το γεγονός ότι η τεχνική αυτή επιτρέπει τον εντοπισμό νέου άγνωστου υλικού CSA την καθιστά ευάλωτη σε adversarial attacks («ανάστροφες επιθέσεις») από παράνομους για τους ακριβώς αντίθετους

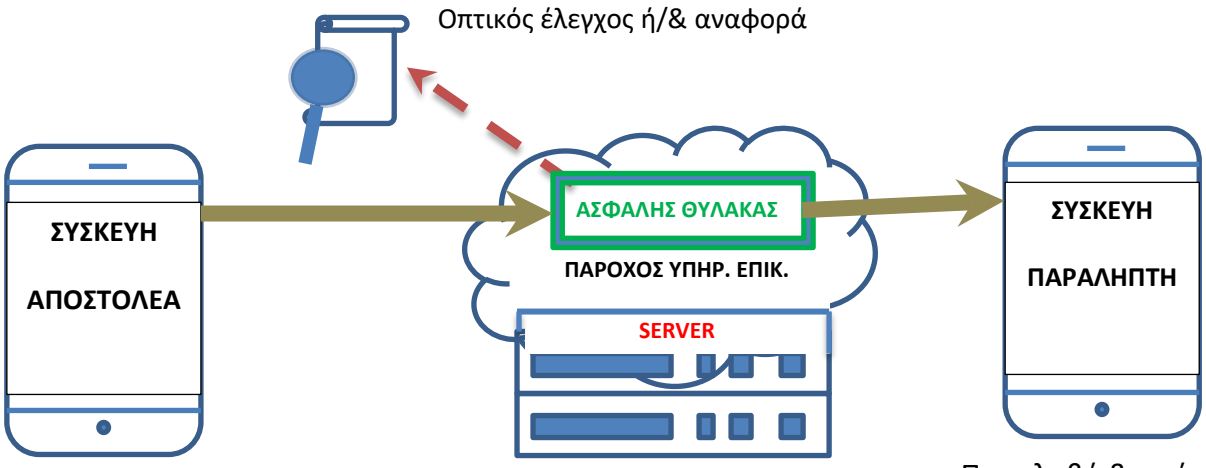
σκοπούς, δηλαδή για να εντοπίζουν νέο υλικό CSA για δικό τους όφελος. Αυτό μπορεί να επιτευχθεί με τη χρήση εξελιγμένων τεχνικών αντίστροφου Machine Learning, ικανών να υπερνικήσουν οποιονδήποτε Classifier.

5) Διαφάνεια: **Μέτρια**. Η χρήση της συγκεκριμένης λύσης μπορεί να τεκμηριωθεί σχετικά εύκολα και να δημοσιοποιηθεί στο ευρύ κοινό, αλλά το πώς ακριβώς δουλεύει ίσως είναι πιο δύσκολο να τεκμηριωθεί.

6.5. Τεχνικές Λύσεις που βασίζονται στον Server

Αυτό το είδος λύσεων βασίζεται στην μεταφορά σε ασφαλείς θύλακες μέσα στον Server του Παρόχου ή στους Servers τρίτων, κάποιων ή όλων των λειτουργιών που εκτελούνται από τον Server του Παρόχου σε μη E2EE επικοινωνίες (δηλαδή σε Client-to-Server κρυπτογραφημένες επικοινωνίες).

6.5.1. Ασφαλείς Θύλακες στον ESP Server



Στέλνει το κρυπτογραφημένο μήνυμα στον **Ασφαλή θύλακα** του Server του Παρόχου

Ο Ασφαλής θύλακας εντός του Server αποκρυπτογραφεί το μνμ & πραγμα-τοποιεί έλεγχο εντοπισμού CSAM. Εάν αυτός αποβεί:
ΘΕΤΙΚΟΣ → Περαιτέρω οπτικός έλεγχος ή/και αναφορά
ΑΡΝΗΤΙΚΟΣ → E2EE του μνμ & αποστολή στον παραλήπτη

Παραλαβή & από-κρυπτογράφηση του E2EE μνμ

Σχήμα 9.

Με αυτήν την λύση οι υπολογιστικά εντατικές λειτουργίες γίνονται σε έναν «ασφαλή θύλακα» που βρίσκεται στο «νέφος» (cloud) του Server του Παρόχου και προσφέρει ένα κλειστό και ασφαλές περιβάλλον για την εκτέλεσή τους. Εκεί αποκρυπτογραφούνται οι πληροφορίες του χρήστη και εκτελούνται οι ίδιες λειτουργίες και έλεγχοι που γίνονται σε μία μη E2EE επικοινωνία, με τη διαφορά ότι όλες οι ευαίσθητες πληροφορίες βρίσκονται προστατευμένες εντός του θύλακα.

Συγκεκριμένα η συσκευή του χρήστη στέλνει το κρυπτογραφημένο μήνυμα στον θύλακα του Server του Παρόχου. Εκεί το μήνυμα αποκρυπτογραφείται και ελέγχεται με εργαλεία εντοπισμού CSAM. Εάν βρεθεί κάτι ύποπτο, το μήνυμα προωθείται για οπτικό έλεγχο, που εφόσον επιβεβαιώσει ότι όντως πρόκειται για CSAM, γίνεται σχετική αναφορά στις Αρχές. Εάν όμως δεν βρεθεί κάτι ύποπτο, ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM κατά τον οπτικό έλεγχο, το μήνυμα αποστέλλεται με E2E κρυπτογράφηση στην συσκευή του παραλήπτη, η οποία το αποκρυπτογραφεί προκειμένου να διαβαστεί.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**. Μπορεί να εντοπίσει γνωστό και άγνωστο υλικό CSA και καθώς η λίστα με τις σειρές Hash βρίσκεται αποθηκευμένη στον Server, δεν υπάρχουν περιορισμοί για το μέγεθός της. Απαιτεί τεχνολογία που προς το παρόν βρίσκεται υπό εξέλιξη, υπόσχεται όμως πολλά για το μέλλον.
2) Εφαρμοσιμότητα: **Μέτρια→Χαμηλή**. Είναι μια λύση που απλοποιεί την διαδικασία εντοπισμού CSAM και ήδη κάποια συστήματα την ενσωματώνουν και την χρησιμοποιούν για άλλους σκοπούς. Όμως προς το παρόν λίγες μόνο εταιρείες έχουν πρόσβαση στο υλικό και το λογισμικό που απαιτείται λόγω της λειτουργικής πολυπλοκότητας της λύσης (αυτό όμως μπορεί να αλλάξει σε λίγα χρόνια, ιδίως εάν η λύση προσφέρεται σαν υπηρεσία από τους παρόχους νέφους-cloud). Επιπλέον, στον ίδιο της τον σχεδιασμό υπάρχουν ακόμα αρκετά θέματα συμβατότητας που θα πρέπει να αντιμετωπιστούν.
3) Προστασία της Ιδιωτικότητας: **Μέτρια → Υψηλή**. Τα δεδομένα των χρηστών (οι σειρές Hash και τα μηνύματά) δεν είναι ορατά στον Πάροχο. Το ίδιο ισχύει και για τις εφαρμοζόμενες λειτουργίες για τον εντοπισμό CSAM. Υπάρχουν όμως και εδώ θέματα ασφάλειας (π.χ. προσβολή των Server τρίτων από κυβερνητικές υπηρεσίες ή άλλους) που δύνανται να μετριάσουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας.
4) Ασφάλεια: **Μέτρια**. Η λύση αυτή βασίζεται στην πεποίθηση ότι ο ασφαλής θύλακας λειτουργεί όπως σχεδιάστηκε και δεν έχει προσβληθεί από κακόβουλους, καθώς

έχουν ήδη ανακαλυφθεί κάποιες ευπάθειες γι' αυτά τα συστήματα. Επίσης, η κατασκευάστρια εταιρεία του θύλακα θα γίνει αναπόφευκτα στόχος κακόβουλων, καθώς είναι η μόνη που κατέχει το κλειδί των εσωτερικών του λειτουργιών του και εάν καταφέρουν να αποκτήσουν πρόσβαση σε αυτόν, θα αποκτήσουν και τα κλειδιά αποκρυπτογράφησης των επικοινωνιών μεταξύ του Server και του παραλήπτη. Πάντως, ακόμα κι αν ο θύλακας έχει προσβληθεί στο παρελθόν, είναι εφικτό να πιστοποιηθεί ότι ο κώδικας που τρέχει επί του παρόντος στον εν λόγω θύλακα δεν έχει τροποποιηθεί από τότε που τοποθετήθηκε εκεί, καθώς και ότι ο χρήστης έχει συνδεθεί στον σωστό θύλακα και εκτελεί τις σωστές διαδικασίες.

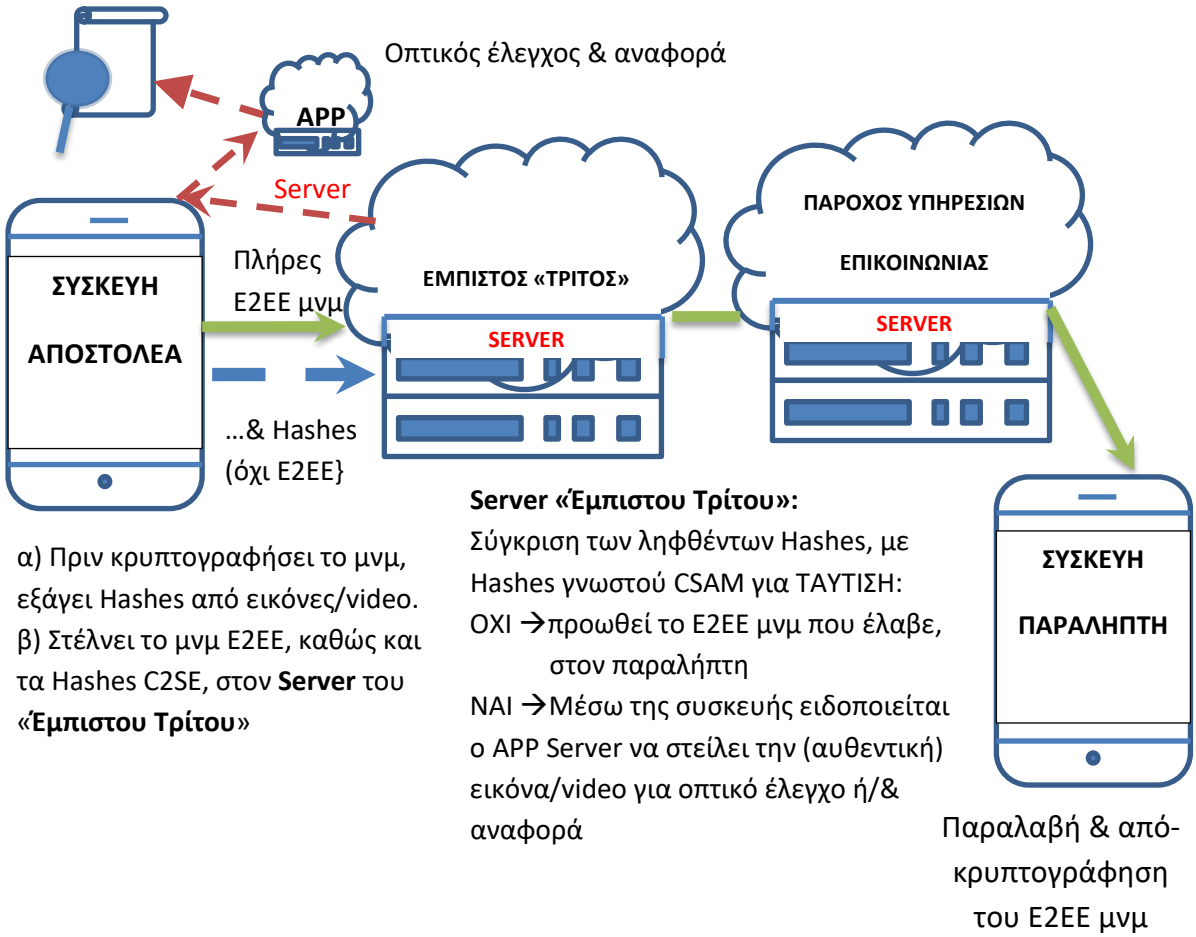
5) Διαφάνεια: **Χαμηλή.** Δεν είναι ξεκάθαρο το πώς ο ασφαλής θύλακας μπορεί να τεκμηριωθεί και να δημοσιοποιηθεί, έτσι ώστε μέσω της συνεχούς αξιολόγησης και της εποπτείας από τη βουλή και τους πολίτες, να διευκολυνθεί η απόδοση ευθύνης σε περίπτωση καταστρατήγησης της λύσης αυτής.

Μια πρόταση προκειμένου να μετριαστούν οι ανωτέρω ανησυχίες, κυρίως για την ασφάλεια και τη διαφάνεια, είναι τα Hash να αποστέλλονται χωρίς E2EE στον ασφαλή θύλακα και εκεί να γίνεται ο έλεγχος ταύτισης με CSAM. Αυτό θα εξαφάνιζε τον κίνδυνο να διαρρεύσουν τα ιδιωτικά κλειδιά E2EE, σε περίπτωση προσβολής του θύλακα. Έτσι η ανάγκη εμπιστοσύνης στον ασφαλή θύλακα θα περιοριστεί στην προστασία του αλγορίθμου Hashing και των παραμέτρων του.

6.5.2. Έλεγχος ταύτισης σε (μοναδικό) Server Τρίτου φορέα

Η λύση αυτή είναι σχεδόν όμοια με την αυτήν που παρουσιάστηκε στην ενότητα 6.4.2. (Συσκευή: Πλήρες Hashing - Server: Έλεγχος Ταύτισης με CSAM) με τη διαφορά ότι ο έλεγχος ταύτισης με CSAM δεν γίνεται στον Server του Παρόχου των υπηρεσιών επικοινωνίας, αλλά στον Server ενός «έμπιστου Τρίτου».

Πριν η συσκευή του αποστολέα κρυπτογραφήσει το μήνυμα, μετατρέπει τα βίντεο και τις φωτογραφίες/εικόνες που τυχόν περιέχει, σε σειρές Hash και στη συνέχεια τις στέλνει (με client-to-server κρυπτογράφηση) μαζί με το πλήρες μήνυμα (E2E κρυπτογραφημένο), στον Server ενός έμπιστου Τρίτου φορέα. Ο Server αυτός συγκρίνει τις ληφθείσες σειρές Hash με μια ΒΔ που περιέχει Hashes επιβεβαιωμένου CSAM:



Σχήμα 10.

α) Εάν διαπιστωθεί υψηλού βαθμού ταύτιση το μήνυμα χαρακτηρίζεται ως ύποπτο και ζητείται από τον Application Server που έχει πρόσβαση στο «ύποπτο» βίντεο/εικόνα (στην αυθεντική του, μη κρυπτογραφημένη μορφή), να το στείλει για περαιτέρω για (οπτικό) έλεγχο. Εφόσον κι απ' αυτόν τον έλεγχο επιβεβαιωθεί ότι όντως πρόκειται για CSAM, γίνεται σχετική αναφορά στις Αρχές και ο εν λόγω Server Τρίτου «μπλοκάρει» το μήνυμα (δεν το προωθεί στον παραλήπτη).

β) Εάν δεν διαπιστωθεί ταύτιση (ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM από τον οπτικό έλεγχο), το πλήρες E2EE μήνυμα προωθείται στην συσκευή του παραλήπτη όπου και αποκρυπτογραφείται προκειμένου να διαβαστεί.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**. Κατάλληλη λύση για εντοπισμό μόνο γνωστού υλικού CSA. Καθώς η λίστα με τις σειρές Hash βρίσκεται αποθηκευμένη στον Server του Τρίτου φορέα, δεν υπάρχουν περιορισμοί για το μέγεθός της.
2) Εφαρμοσιμότητα: **Χαμηλή**. Η λύση αυτή έχει θέματα επεκτασιμότητας, παρόλο που μπορεί κάλλιστα να προσφέρεται ως υπηρεσία από μικρότερους Παρόχους, που τη

λειτουργούν πάνω στην υποδομή νέφους μεγαλύτερων Παρόχων. Επίσης προϋποθέτει ένα συνδυασμό από κώδικα που τρέχει και στην συσκευή του αποστολέα και στον Server του Τρίτου φορέα, οπότε υφίστανται αλληλεξαρτήσεις.

3) Προστασία της Ιδιωτικότητας: **Μέτρια → Χαμηλή**. Ο Πάροχος δεν μπορεί να δει τις σειρές Hash των χρηστών και καμία λειτουργία εντοπισμού CSAM δεν λαμβάνει χώρα στον Server του. Υπάρχουν όμως και εδώ θέματα ασφάλειας (π.χ. προσβολή του Server του Τρίτου φορέα από κυβερνητικές υπηρεσίες ή άλλους) που μετριάζουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας. Επιπλέον, ο Τρίτος αυτός φορέας θα πρέπει να συνεργάζεται στενά με το τμήμα του Παρόχου που υλοποιεί την επικοινωνία (ή ακόμα και να αποτελεί μέρος του Παρόχου), γεγονός που γεννά αμφιβολίες σχετικά με την προάσπιση της ιδιωτικότητας. Η εξάρτηση του Τρίτου φορέα από τον Πάροχο μπορεί να είναι μικρότερη, εάν δεν λειτουργεί σε πραγματικό χρόνο και ελέγχει το μήνυμα για CSAM μετά την αποστολή του (και όχι πριν).
4) Ασφάλεια: **Μέτρια → Χαμηλή**. Επιπρόσθετα στα θέματα ασφαλείας που αναπτύχθηκαν στην περιγραφή της λύσης της ενότητας 6.4.2 (π.χ. κίνδυνος προσβολής και χειραγώγησης του αλγορίθμου Hashing), ο Server του Τρίτου φορέα μπορεί να δεχτεί επιθέσεις κρατικής προέλευσης ή από μεμονωμένα άτομα (hackers).
5) Διαφάνεια: **Μέτρια**. Τα προαναφερθέντα προβλήματα ασφάλειας δύνανται να υπονομεύσουν την αξιοπιστία των ελέγχων που γίνονται, άρα και την οποιαδήποτε εποπτεία και δημόσια ενημέρωση του κοινού περί της ορθής και νόμιμης (ή μη) χρήσης της λύσης.

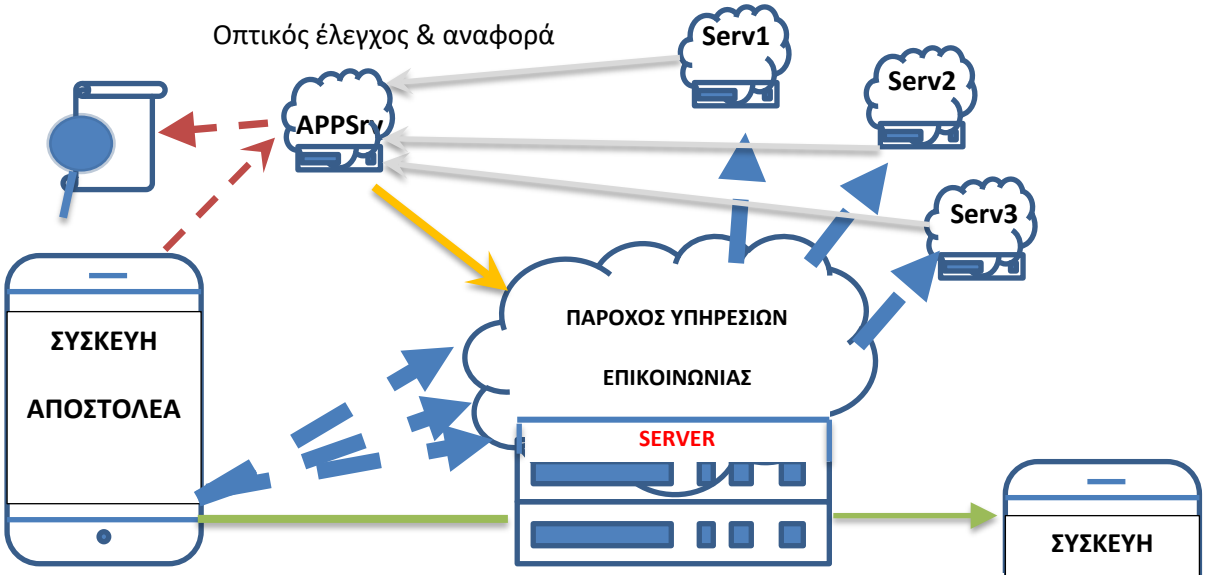
6.5.3. Έλεγχος ταύτισης σε πολλαπλούς Server Τρίτων φορέων

Στη λύση αυτή που βασίζεται σε «Πολυμερείς Υπολογισμούς» (Multi-Party Computation - MPC), η συσκευή του αποστολέα χωρίζει το υπό έλεγχο βίντεο ή εικόνα σε κομμάτια, τα οποία και κρυπτογραφεί με τα κλειδιά πολλαπλών έμπιστων Τρίτων φορέων και κατόπιν τα στέλνει στον Server του Παρόχου, ο οποίος στη συνέχεια τα προωθεί στους Servers των Τρίτων φορέων για να εκτελέσουν έλεγχο «μερικής ταύτισης». Ο Application Server συγκεντρώνει τα αποτελέσματα των πολλαπλών αυτών ελέγχων προκειμένου να διαπιστώσει εάν υπήρξε τελικά ταύτιση με CSAM.

α) Εάν διαπιστωθεί υψηλού βαθμού ταύτιση το μήνυμα χαρακτηρίζεται ως ύποπτο και το βίντεο/εικόνα που περιέχει, στέλνεται από τον Application Server (που έχει πρόσβαση στην αυθεντική του, μη κρυπτογραφημένη μορφή), για περαιτέρω για

(οπτικό) έλεγχο . Εφόσον κι απ' αυτόν τον έλεγχο επιβεβαιωθεί ότι όντως πρόκειται για CSAM, γίνεται σχετική αναφορά στις Αρχές και ο εν λόγω Server Τρίτου «μπλοκάρει» το μήνυμα (δεν το προωθεί στον παραλήπτη).

β) Εάν δεν διαπιστωθεί ταύτιση (ή δεν επιβεβαιωθεί ότι πρόκειται για CSAM από τον οπτικό έλεγχο), το πλήρες E2EE μήνυμα προωθείται στην συσκευή του παραλήπτη όπου και αποκρυπτογραφείται προκειμένου να διαβαστεί.



Πριν κρυπτογραφήσει το μνμ, χωρίζει τις εικόνες/video σε κομμάτια, εξάγει Hashes από αυτά, τα κρυπτογραφεί με κλειδιά «έμπιστων Τρίτων» & τα στέλνει μέσω του Server του Παρόχου στους Servers των «Τρίτων» για έλεγχο «μερικής» ταύτισης.
Εκεί στέλνει και το **E2EE** πλήρες μνμ

Servers «Τρίτων»: Εκτελούν έλεγχο «μερικής» ταύτισης των ληφθέντων Hashes.
APP Server: Συγκεντρώνει τα αποτελέσματα από τους "Τρίτους» και ελέγχει για ΤΑΥΤΙΣΕΙΣ;
ΝΑΙ → Στέλνει την εικόνα /video για οπτικό έλεγχο ή/και αναφορά
ΟΧΙ → Ζητά απ' τον Server να στείλει το E2EE μνμ στη Συσκευή Παραλήπτη

Παραλαβή & αποκρυπτογράφηση του E2EE μνμ

Σχήμα 11.

Αξιολόγηση:

1) Αποτελεσματικότητα: **Μέτρια → Υψηλή**. Κατάλληλη λύση για εντοπισμό μόνο γνωστού υλικού CSA. Καθώς η λίστα με τις σειρές Hash βρίσκεται αποθηκευμένη στους Servers Τρίτων φορέων, δεν υπάρχουν περιορισμοί για το μέγεθός της.
2) Εφαρμοσιμότητα: **Χαμηλή - Μέτρια → Χαμηλή**. Η λύση αυτή έχει θέματα καθυστερήσεων (ιδιαίτερα με αργές συνδέσεις), εξαιτίας των πολλαπλών ανταλλαγών δεδομένων μεταξύ της συσκευής του αποστολέα και των Servers των Τρίτων φορέων. Και εδώ απαιτείται ένας συνδυασμός από κώδικα που τρέχει και

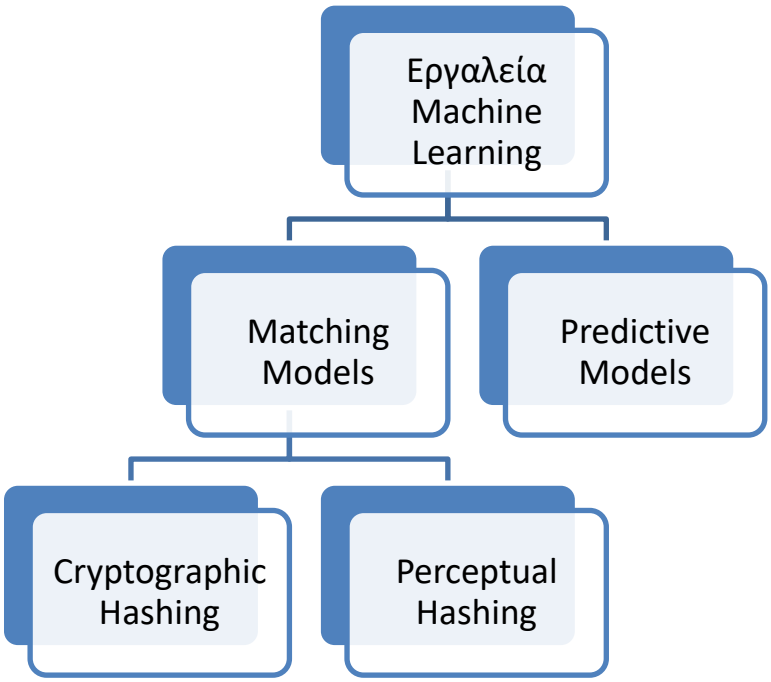
στην συσκευή του αποστολέα και στους Servers των Τρίτων φορέων, οπότε υφίστανται αλληλεξαρτήσεις. Μια παρόμοια τεχνολογία χρησιμοποιείται ήδη από την Google για διαδικτυακά καταστήματα, αλλά απαιτείται περαιτέρω έρευνα για να διαπιστωθεί πως μπορούν να αντιμετωπιστούν κάποια θέματα επεκτασιμότητας όταν εφαρμόζεται για εντοπισμό CSAM, καθώς και να διερευνηθεί ποια είναι τα σχετιζόμενα κόστη (οικονομικής αλλά και υπολογιστικής φύσης).

3) Προστασία της Ιδιωτικότητας: **Μέτρια**. Ο Πάροχος δεν μπορεί να δει τις σειρές Hash των χρηστών και καμία λειτουργία εντοπισμού CSAM δεν λαμβάνει χώρα στον Server του. Υπάρχουν όμως και εδώ θέματα ασφάλειας (π.χ. προσβολή του Server των Τρίτων φορέων από κυβερνητικές υπηρεσίες ή άλλους) που μετριάζουν σημαντικά τον βαθμό διασφάλισης της ιδιωτικότητας. Η λύση όμως αυτή με τους πολλαπλούς Τρίτους φορείς, μπορεί να διασφαλίσει την ιδιωτικότητα σε μεγαλύτερο βαθμό απ' ότι η προηγούμενη (με έναν και μοναδικό Τρίτο φορέα) καθώς εάν έστω κι ένας απ' αυτούς είναι έμπιστος, η σειρά hash θα παραμείνει ιδιωτική. Από την άλλη, είναι πιθανόν οι μεγάλες εταιρείες, που προσφέρουν κι αυτές υπηρεσίες ηλεκτρονικών επικοινωνιών, να απευθύνονται στους Τρίτους φορείς αυτής της λύσης για τις μικρότερες εταιρείες, γεγονός που μπορεί να δημιουργήσει κάποια θέματα ιδιωτικότητας.
4) Ασφάλεια: **Μέτρια**. Επιπρόσθετα στα θέματα ασφαλείας που αναπτύχθηκαν στην περιγραφή της λύσης της ενότητας 6.4.2 (π.χ. κίνδυνος προσβολής και χειραγώγησης του αλγορίθμου Hashing), οι Servers των Τρίτων φορέων μπορεί να δεχτούν επιθέσεις κρατικής προέλευσης ή από μεμονωμένα άτομα (hackers). Από την άλλη όμως, η λύση αυτή (με τους πολλαπλούς Τρίτους φορείς), παρέχει μεγαλύτερη ασφάλεια από την προηγούμενη (με τον έναν και μοναδικό Τρίτο φορέα), καθώς οι κάθε λογής κακόβουλοι θα πρέπει να προσβάλλουν πολλούς Servers αντί έναν.
5) Διαφάνεια: **Μέτρια**. Τα προαναφερθέντα προβλήματα ασφάλειας δύνανται να υπονομεύσουν την αξιοπιστία των ελέγχων που γίνονται, άρα και την οποιαδήποτε εποπτεία και δημόσια ενημέρωση του κοινού περί της ορθής και νόμιμης (ή μη) χρήσης της λύσης.

Μια άλλη πιθανή λύση που βασίζεται σε Server, είναι να χρησιμοποιηθούν Classifiers («ταξινομητές») που θα «τρέχουν» στον Server του Παρόχου και θα συλλέγουν metadata («μεταδεδομένα»). Αυτή φαίνεται να είναι η προσέγγιση που υιοθετεί η Meta στην υπηρεσία Messenger όπου θα χρησιμοποιεί E2EE, δεν είναι όμως γνωστές περισσότερες λεπτομέρειες.

Κεφάλαιο 7
Αποτίμηση Τεχνολογικών Λύσεων

Στο κεφάλαιο αυτό θα εμβαθύνουμε στα τεχνικά προβλήματα που αντιμετωπίζουν οι λύσεις που παρουσιάστηκαν στο προηγούμενο κεφάλαιο.



Σχήμα 12.

7.1. Perceptual Hashing σε E2E Κρυπτογράφηση

Υπάρχουν δύο κατηγορίες εργαλείων Machine Learning που θεωρούνται κατάλληλες για ανίχνευση συγκεκριμένου περιεχομένου σε E2E κρυπτογραφημένα μηνύματα: Η πρώτη κατηγορία χρησιμοποιεί μοντέλα Ταύτισης (Matching models) και η δεύτερη μοντέλα Πρόβλεψης (Predictive models) [02].

Τα μοντέλα Ταύτισης στοχεύουν στον εντοπισμό CSAM που ταυτίζεται ακριβώς ή σε πολύ μεγάλο βαθμό με ήδη γνωστό CSAM. Η τεχνική προϋποθέτει την ύπαρξη ενός «αλγορίθμου Hashing» και μιας ΒΔ που περιέχει hashes που προήλθαν από ήδη γνωστό

περιεχόμενο CSA. Ο Server του Παρόχου εκτελεί τον αλγόριθμο Hashing που συγκρίνει το υπό έλεγχο hash με όλα τα hashes της ΒΔ, αναζητώντας πλήρη ή μερική ταύτιση.

Υπάρχουν δύο τύποι των Μοντέλων Ταύτισης: Το «Κρυπτογραφικό Hashing» και το «Perceptual (αντιληπτικό) Hashing» [02].

Το πρώτο χρησιμοποιεί μια κρυπτογραφική Hashing συνάρτηση για τη δημιουργία ενός Hash που όπως έχει προαναφερθεί, είναι πολύ ευαίσθητο ακόμα και στην παραμικρή αλλαγή. Αυτή η προσέγγιση είναι κατάλληλη για τον εντοπισμό ήδη γνωστού υλικού CSA που δεν έχει υποστεί καμία τροποποίηση (βλέπε και Κεφάλαιο 2 - ενότητα 2.2).

Το Perceptual Hashing επιτρέπει στον Πάροχο να καθορίζει εκείνος τον βαθμό κατά τον οποίο δύο περιεχόμενα μπορούν να διαφέρουν μεταξύ τους και παρά το γεγονός αυτό, η τεχνική να τα θεωρεί ότι ταυτίζονται. Είναι κατάλληλη προσέγγιση για τον εντοπισμό CSA υλικού που έχει τροποποιηθεί ελάχιστα ώστε να αποφευχθεί ο εντοπισμός του. Επιπλέον, εφαρμόζεται επί απλών κειμένων, προκειμένου να ανιχνεύει αυτόματα περιεχόμενο, το οποίο ο Πάροχος έχει εκ των προτέρων ορίσει ως ανεπιθύμητο στο σύστημά του. Χρησιμοποιείται επίσης:
α) από Παρόχους υπηρεσιών όταν λαμβάνουν περιεχόμενο (Server-side scanning).
β) από εφαρμογές (π.χ. messaging) στη συσκευή του χρήστη πριν αποστείλει περιεχόμενο (Client-side scanning).
Και στις δύο ανωτέρω περιπτώσεις, εφόσον διαπιστωθεί ταύτιση με ανεπιθύμητο περιεχόμενο, το μήνυμα επισημαίνεται ως ύποπτο, «μπλοκάρεται», και δεν φτάνει στον παραλήπτη του [02].

Το πιο σημαντικό όμως για το Perceptual Hashing είναι ότι θεωρείται η πιο πολλά υποσχόμενη τεχνική που χρησιμοποιεί Hashing για την ανίχνευση ανεπιθύμητου περιεχομένου σε E2E κρυπτογράφηση και συγκεντρώνει το ενδιαφέρον των περισσότερων ερευνητών. Μάλιστα την χρησιμοποιεί και η Microsoft στην «PhotoDNA» [12].

Χρησιμοποιούνται και οι δύο εφικτές προσεγγίσεις της λύσης αυτής («Server-side» και «Client-side» scanning), αλλά αφενός δεν προσφέρουν τις αναμενόμενες (για κρυπτογραφημένες επικοινωνίες) εγγυήσεις προστασίας της ιδιωτικότητας των χρηστών και αφετέρου εισάγουν «ευπάθειες» ασφαλείας που τις υπονομεύουν. Πιο συγκεκριμένα, στην «Server-side scanning» προσέγγιση θα εξαχθούν hashes από το περιεχόμενο πριν αυτό κρυπτογραφηθεί, τα οποία θα σταλούν στον Server του Παρόχου

για να ελεγχθούν. Αυτό όμως αποτελεί παραβίαση της ιδιωτικότητας του αποστολέα καθώς τα hashes μπορούν να αποκαλύψουν στοιχεία για το περιεχόμενο [02].

Για να αντιμετωπιστούν τέτοιου είδους θέματα παραβίασης της ιδιωτικότητας, οι Kulshrestha & Mayer σε δημοσίευση εργασίας τους το 2021, πρότειναν μια προσέγγιση που χρησιμοποιεί μεν την τεχνική Perceptual Hashing, αλλά όπως διατείνονται, προστατεύει παράλληλα και την ιδιωτικότητα των χρηστών και μπορεί να εφαρμοστεί σε E2E κρυπτογραφημένα μηνύματα προκειμένου να εντοπίζεται εάν υπάρχει κακόβουλο περιεχόμενο σε αυτά (π.χ. CSAM). Ο Server του Παρόχου δύναται να ελέγξει εάν το περιεχόμενο του E2EE μηνύματος ταυτίζεται με κάποιο ήδη γνωστό ανεπιθύμητο περιεχόμενο, χωρίς όμως να μαθαίνει κάτι άλλο για το μήνυμα ή το hash. Επίσης, και ο χρήστης δεν θα μαθαίνει τίποτα για το περιεχόμενο της ΒΔ με τα hashes, καθώς η προσέγγιση είναι του τύπου «Server-side scanning» και η ΒΔ με τα ανεπιθύμητα hashes θα φυλάσσεται μόνο στον Server του Παρόχου και δεν θα διανέμεται στις συσκευές των χρηστών. Οι ανωτέρω ερευνητές χρησιμοποιούν μια κρυπτογραφική τεχνική που ονομάζεται «Private Information Retrieval» (Ανάκτηση Ιδιωτικών Πληροφοριών) που επιτρέπει σε ένα στοιχείο να εξαχθεί από μια ΒΔ, χωρίς όμως η ΒΔ να γνωρίζει ποιο ήταν το στοιχείο αυτό ([02] σελ. 23,32).
Ενώ η τεχνική αυτή μετριάζει τον κίνδυνο αποκάλυψης των hashes στον Server, οι κίνδυνοι που σχετίζονται με οποιουδήποτε είδους «παρακολούθηση» υφίστανται. Ακόμα κι ένα πρωτόκολλο που δεν αποκαλύπτει απολύτως καμία πληροφορία για το ίδιο το μήνυμα, μπορεί να προσβληθεί από πλατφόρμες που έχουν σαν στόχο να διενεργούν παρακολούθηση πάνω σε περιβάλλον E2E κρυπτογράφησης. Αντί ένας Πάροχος να ανιχνεύει μόνο ταυτίσεις με αδιαμφισβήτητα κακόβουλο περιεχόμενο, μπορεί κρυφά να τοποθετεί άλλου είδους περιεχόμενο που μπορεί να είναι ανεπιθύμητο για τον ίδιο ή για το εκάστοτε καθεστώς. Δηλαδή η ανάπτυξη, διάδοση και εφαρμογή αυτών των πρωτοκόλλων σε χώρες με δημοκρατικές κυβερνήσεις για καλούς σκοπούς (π.χ. εντοπισμός CSAM), πιθανότατα θα δώσει τη δυνατότητα και σε αυταρχικά καθεστώτα να χρησιμοποιήσουν τα ίδια εργαλεία για κακούς σκοπούς, όπως περιορισμό της ελευθερίας του λόγου και παρακολούθηση των πολιτών τους [02].

Αν και οι ανωτέρω λύσεις προσπαθούν να περιορίσουν όσο το δυνατόν περισσότερο, την αποκάλυψη πληροφοριών στον Server του Παρόχου, η ίδια η απλή πληροφορία ότι το περιεχόμενο ενός κρυπτογραφημένου μηνύματος ταυτίζεται (ή δεν ταυτίζεται) με

ανεπιθύμητο περιεχόμενο, αποτελεί ένα είδος πληροφόρησης, άρα εξακολουθεί να παραβιάζει σ' ένα βαθμό την ιδιωτικότητα, καθώς αποκαλύπτει κάτι γι' αυτήν την επικοινωνία, που μάλιστα είναι και κρυπτογραφημένη. Επιπλέον, οι λύσεις αυτές παρουσιάζουν αρκετά υψηλά νούμερα λανθασμένων ανιχνεύσεων («false matches»). Εάν δεν υπάρξει αποτελεσματικός τρόπος εύρεσης, αγνόησης και ακύρωσης των «false matches», πιθανότατα θα ερμηνευτούν από τον Πάροχο ότι ο αποστολέας των μηνυμάτων που επισημάνθηκαν λανθασμένα, εμπλέκεται σε διακίνηση παράνομου περιεχομένου (π.χ. CSAM).

Αντίθετα, στο Client-side scanning, τα ανεπιθύμητα hashes αποθηκεύονται στην συσκευή του χρήστη και ο έλεγχος ταύτισης γίνεται εκεί. Εάν τα αποτελέσματά του παραμείνουν γνωστά μόνο στον χρήστη δεν υπάρχει πρόβλημα, αλλά εάν διαμοιράζονται και με τον Server, οι εγγυήσεις προστασίας της ιδιωτικότητας σε περιβάλλοντα E2EE επικοινωνίας παραβιάζονται. Εγείρονται επίσης σοβαροί προβληματισμοί για το Perceptual Hashing όταν εφαρμόζεται σε απλό κείμενο για εντοπισμό περιπτώσεων grooming, διότι η τεχνική είναι αποτελεσματική μόνο όταν το παράνομο περιεχόμενο έχει διαμοιραστεί πάνω από μία (1) φορά. Σύμφωνα όμως με μελέτη που έγινε στις Η.Π.Α, από τις περιπτώσεις διακίνησης CSAM για τις οποίες έχει γίνει αναφορά, περίπου το 85% έχουν αναφερθεί μόνο 1 φορά. Αυτό σημαίνει ότι ο μεγαλύτερος όγκος του παράνομου περιεχομένου είναι πρωτοεμφανιζόμενο, άρα η τεχνική δεν μπορεί να το ανιχνεύσει.
Επιπλέον, ο έλεγχος ταύτισης με hashes, ιδιαίτερα όταν ο Hashing αλγόριθμος είναι γνωστός στο κοινό, είναι ευάλωτος σε επιθέσεις «δηλητηρίασης» (poisoning attacks) με εσκεμμένες προσθήκες hashes στη ΒΔ προκειμένου να δημιουργούνται λανθασμένες ανιχνεύσεις. Η μέθοδος αυτή χρησιμοποιείται και για λογοκρισία με την εισαγωγή hashes από ευαίσθητο πολιτικό περιεχόμενο (και ανεπιθύμητο για το εκάστοτε καθεστώς) στη ΒΔ των hashes. Δηλαδή, αν και οι λόγοι για τους οποίους δημιουργήθηκε η τεχνική είναι θεμιτοί, στα χέρια αυταρχικών καθεστώτων μπορεί να καταλήξει να είναι εργαλείο καταπίεσης.

Η πρακτική εφαρμογή του Client-side scanning σε E2EE επικοινωνίες μεταφέρει τις ανωτέρω ευπάθειες σε όλο το σύστημα, καθώς η διανομή της ΒΔ με τα ανεπιθύμητα hashes στις συσκευές των χρηστών, μπορεί να οδηγήσει στην «χειραγώγησή» της από κακόβουλους.

Μια άλλη πρόταση έγινε το 2020 από τον Reis και άλλους ερευνητές [14], και ασχολείται με την δυνατότητα να χρησιμοποιηθεί η μέθοδος Perceptual Hashing για την ανίχνευση παραπληροφόρησης στην εφαρμογή WhatsApp και κατ' επέκταση και σε άλλες E2EE υπηρεσίες χρησιμοποιώντας ένα μοντέλο Client-side scanning. Ο αρχικός στόχος της ερευνητικής ομάδας ήταν η κατανόηση των sharing patterns (μοτίβων διαμοιρασμού) στην εφαρμογή WhatsApp, αλλά κατά τη διάρκεια της εξέλιξής της προτάθηκε μία αρχιτεκτονική που θα μπορούσε να ενσωματωθεί στην εφαρμογή WhatsApp, προκειμένου να εντοπίζει και να επισημαίνει στις συσκευές των χρηστών, περιπτώσεις παραπληροφόρησης. Σύμφωνα με την πρότασή των ερευνητών, το Facebook θα διατηρεί ένα σετ από Perceptual hashes για εικόνες που ελέγχθηκαν και βρέθηκαν να αποτελούν προϊόντα παραπληροφόρησης (π.χ. εικόνες που ενώ ήταν άσχετες με κάποια συγκεκριμένη επικοινωνία, διαμοιράστηκαν κατά τη διάρκειά της και άρα κρίθηκαν ύποπτες, ή εικόνες που τροποποιήθηκαν/χειραγωγήθηκαν με απλές τεχνικές προκειμένου να δημιουργηθούν τα λεγόμενα «cheap fakes"). Αυτά τα hashes θα αποθηκεύονται κατόπιν στη συσκευή του χρήστη και θα ενημερώνονται περιοδικά. Κατά τη αποστολή (ή και λήψη) μιας εικόνας, το hash της θα συγκριθεί με τα προαναφερθέντα hashes και εφόσον χαρακτηριστεί ως παραπληροφόρηση, θα σταλούν σχετικές προειδοποιήσεις στους χρήστες (αποστολέα ή/και παραλήπτη). Η πρόταση δεν προβλέπει την επισήμανση των χρηστών από την πλατφόρμα, ως διακινητές παραπληροφόρησης. Οι παραλήπτες έχουν φυσικά τη δυνατότητα να υποβάλουν σχετική αναφορά, αλλά δεν υφίσταται κάποια αυτοματοποιημένη διαδικασία απόδοσης ευθύνης για αποστολή ή λήψη μηνυμάτων παραπληροφόρησης.

Όπως προαναφέρθηκε, στην «Client-side scanning» προσέγγιση, το πλήρες σετ από hashes ανεπιθύμητου περιεχομένου είναι αποθηκευμένο στην συσκευή του χρήστη και εκεί πραγματοποιείται ο έλεγχος και ο τυχόν εντοπισμός. Το γεγονός αυτό, από τη μία προστατεύει την ιδιωτικότητα του χρήστη (όλα γίνονται στην συσκευή του και δεν εμπλέκονται άλλα μέρη), αλλά από την άλλη σημαίνει ότι κάποιος κακόβουλος μπορεί να ανακαλύψει το σετ αυτό και έτσι θα γνωρίζει ποιες εικόνες περιλαμβάνονται στην ΒΔ. Έτσι θα έχει τη δυνατότητα αφενός να ελέγξει εάν οι παράνομες εικόνες που επιθυμεί να διακινήσει περιλαμβάνονται στη ΒΔ (ή όχι – επομένως δεν θα «κινδυνέψει» να εντοπιστούν) και αφετέρου να αναπτύξει μεθόδους «χειραγώγησης» της ΒΔ και τροποποίησης των hashes σε αυτήν, ώστε να αποφεύγεται ο εντοπισμός των δικών του hashes [02].

Η ανωτέρω ευπάθεια υπονομεύει γενικότερα την χρησιμότητά της «Client-side scanning» προσέγγισης. Μάλιστα η χρήση της για εντοπισμό διακίνησης CSAM αποδεικνύεται ιδιαίτερα προβληματική, καθώς πολλοί κακόβουλοι έχουν «ιδιαίτερα» κίνητρα να αναπτύξουν μεθόδους καταστρατήγησής της. Αυτό εν μέρει εξηγεί και το γιατί οι αλγόριθμοι για πολύ γνωστές μεθόδους όπως το PhotoDNA δεν δημοσιοποιούνται στο ευρύ κοινό, καθώς είναι ευάλωτοι σε επιθέσεις.

Πέραν των ανωτέρω, υφίστανται κι άλλοι παράγοντες που δύναται να περιορίζουν την ευρεία εφαρμογή της λύσης, όπως η υπολογιστική ισχύς, ο διαθέσιμος χώρος αποθήκευσης, το είδος της σύνδεσης με το Διαδίκτυο και η κατανάλωση των μπαταριών (π.χ. για κινητά, όπου παρατηρούνται σημαντικές διαφορές μεταξύ του αναπτυσσόμενου και του αναπτυγμένου κόσμου ως προς τα μοντέλα που προτιμώνται και τις δυνατότητές τους).

Συνοψίζοντας, και οι δύο προσεγγίσεις («Server-side» και «Client-side» scanning) είναι τεχνικές ταύτισης hash που μπορούν να χρησιμοποιηθούν σε E2E κρυπτογραφημένες επικοινωνίες, αλλά παρέχουν πρόσβαση στο μήνυμα σε τρίτους ή εισάγουν σημαντικές ευπάθειες στο σύστημα, ή και τα δύο. Ακόμα και στην «Client-side scanning» προσέγγιση όπου δεν εμπλέκεται τρίτος, (μόνο ο αποστολέας και ο παραλήπτης ενημερώνονται εάν εντοπιστεί ανεπιθύμητο υλικό) εμπεριέχεται ο κίνδυνος χειραγώγησης της ΒΔ των Hashes από κακόβουλους. Επομένως, όπως αναφέρθηκε και αρχικά, δεν παρέχουν τα αναμενόμενα για την E2E κρυπτογράφηση εχέγγυα ασφάλειας και ιδιωτικότητας [02].

7.2. Μοντέλα Πρόβλεψης (Predictive Models) για εντοπισμό περιεχομένου σε E2EE επικοινωνίες.

Η 2η κατηγορία εργαλείων Machine Learning για τον εντοπισμό συγκεκριμένου περιεχομένου χρησιμοποιεί μοντέλα Πρόβλεψης (Predictive models) που στοχεύουν να αναγνωρίσουν χαρακτηριστικά βασιζόμενα στην πρότερη «εμπειρία μάθησης» της μηχανής. Η προσέγγιση αυτή χρησιμοποιείται συχνά για τον εντοπισμό καινούργιου ή αγνώστου μέχρι στιγμής περιεχομένου CSA και συνήθως απαιτείται μεγάλος όγκος δεδομένων προκειμένου να εκπαιδευτεί το μοντέλο να προβλέπει εάν κάποιο συγκεκριμένο κομμάτι δεδομένων έχει κάποια χαρακτηριστικά. Περιλαμβάνουν μοντέλα Computer Vision που εκτελούν ανάλυση σχημάτων, χρωμάτων, υφής κ.α. και μοντέλα

Computer Audition που αναλύουν ήχους. Κλασσικό παράδειγμα του πρώτου είναι ένας «Image Classifier» (ταξινομητής εικόνας) που προσπαθεί να καταλάβει εάν η εικόνα που ανέβασε ένας χρήστης είναι ενός σκύλου ή μιας γάτας.

Τα Machine Learning εργαλεία ελέγχου και εντοπισμού περιεχομένου μπορούν να λειτουργήσουν και σε κείμενα (Duarte et al., 2017) και σε πολυμέσα (βίντεο, εικόνα και ήχο). (Shenkman et al., 2021).

Αξιοποιώντας την καλή βάση που προσφέρουν οι ανωτέρω τεχνικές, ο Mayer σε δημοσίευσή του το 2019 παρέχει χρήσιμες ιδέες και οδηγίες που μπορούν να χρησιμοποιήσουν οι ερευνητές προκειμένου να αναπτύξουν ένα μοντέλο που θα προβλέπει αποτελεσματικά την ύπαρξη παράνομου περιεχομένου σε E2EE περιβάλλον. Ένας τρόπος να επιτευχθεί αυτό είναι με Machine Learning αλγόριθμους που αποσκοπούν στον εντοπισμό προβληματικών μηνυμάτων απλού κειμένου (π.χ. spam) κάνοντας χρήση προ-εκπαιδευμένων Classifiers ενσωματωμένων στην messaging (ή άλλη) εφαρμογή που βρίσκεται εγκατεστημένη στη συσκευή του χρήστη. Μόλις αυτή αποκρυπτογραφήσει ένα μήνυμα, ο Classifier θα έχει τη δυνατότητα να το ταξινομήσει/επισημάνει ως πιθανό μήνυμα spam.

Φυσικά και γι' αυτήν την προσέγγιση υφίστανται πρακτικοί περιορισμοί, όπως η επεξεργαστική ισχύς και η εκάστοτε επάρκεια της μπαταρίας της συσκευής. Πάντως, εφόσον η όλη επεξεργασία λαμβάνει χώρα στη συσκευή του χρήστη και δεν αποκαλύπτεται καμία πληροφορία σε τρίτους, τα εχέγγυα μη παραβίασης της ιδιωτικότητας της E2EE δεν παραβιάζονται. Επομένως είναι μια πολλά υποσχόμενη προσέγγιση, αλλά απαιτείται ακόμα σημαντικός όγκος έρευνας για να καταστεί αποτελεσματική και βιώσιμη.

7.3. Οι κίνδυνοι του Client-side scanning.

Το Client-side scanning (CSS) επιτρέπει την ανάλυση των μηνυμάτων για εντοπισμό παράνομου περιεχομένου (π.χ. CSAM) σε επίπεδο συσκευής. Σε περίπτωση που υπάρξει εντοπισμός, γίνεται αναφορά της παρουσίας του, καθώς και της πηγής του, στις αρχές. Σε αντίθετη περίπτωση, το μήνυμα αποστέλλεται στον παραλήπτη του και καμιά άλλη πληροφορία σχετικά με αυτό δεν αποκαλύπτεται. Οι υποστηρικτές του CSS διατείνονται ότι αποτελεί τη λύση στο ερώτημα που έχει γίνει πια διαχρονικό «κρυπτογραφία ή

δημόσια ασφάλεια» καθώς προστατεύει την ιδιωτικότητα των χρηστών με ισχυρή E2E κρυπτογράφηση και ταυτόχρονα επιτρέπει την διερεύνηση σοβαρών εγκλημάτων, όπως η διακίνηση CSAM [01].

Υπάρχει όμως και αντίλογος από ερευνητές που ισχυρίζονται ότι η CSS προσέγγιση από τη φύση της, αφενός ενέχει σοβαρούς κινδύνους για την ασφάλεια και την ιδιωτικότητα των πολιτών/χρηστών καθώς δεν αποτρέπει την παρακολούθηση και αφετέρου η βοήθεια που προσφέρει στις Αρχές για την πρόληψη και για την καταπολέμηση των σοβαρών εγκλημάτων δεν είναι σημαντική και αποτελεσματική, αλλά προβληματική[01].

Υπάρχουν διάφοροι τρόποι με τους οποίους η CSS μπορεί να αποτύχει, να παρακαμφθεί ή και να χρησιμοποιηθεί για κακόβουλους σκοπούς. Οι υποστηρικτές της επιθυμούν την καθολική ανάπτυξη της CSS σε όλες τις συσκευές των πολιτών, αλλά εφόσον αυτό συμβεί, θα επηρεαστεί αρνητικά η ασφάλεια όλων αδιακρίτως, δηλαδή και των παρανόμων, αλλά και των νομοταγών πολιτών [01].

Ενώ θα μπορούσε κάλλιστα να εγκατασταθεί κρυφά (με εισαγγελική εντολή) μόνο στις συσκευές των υπόπτων, ή με δικαστική διαταγή στις συσκευές αυτών που προέβησαν σε σοβαρά εγκλήματα στο παρελθόν. Άλλωστε η ύπαρξη «δεσμεύσεων» ή «περιορισμών» για πρώην καταδίκους μετά από την αποφυλάκισή τους, δεν είναι κάτι καινούργιο. Υφίσταται εδώ και χρόνια στις Η.Π.Α., όπου στοιχεία όπως το ονοματεπώνυμο και η διαμονή των ατόμων που έχουν καταδικαστεί στο παρελθόν για σεξουαλικά εγκλήματα (π.χ. βιασμούς, σεξουαλική παρενόχληση ανηλίκων κτλ.) παραμένουν (μετά την αποφυλάκισή τους) σε λίστα με «Sex Offenders» στην οποία μπορεί να έχει πρόσβαση ο καθένας.

Από τεχνικής απόψεως, το πλεονέκτημα της CSS έναντι άλλων μεθόδων είναι ότι επιτρέπει την E2E κρυπτογράφηση (αλλά αυτό είναι συζητήσιμο εάν το μήνυμα έχει ήδη ελεγχθεί για παράνομο περιεχόμενο, όπως CSAM). Πρέπει να θεωρείται μια αυτοματοποιημένη «μαζική» και χωρίς διάκριση «παρέμβαση/έλεγχος - bulk intercept», αν και κατανεμημένη (στις συσκευές των χρηστών). Μάλιστα, αφού επιτρέπει στις Αρχές να έχουν πρόσβαση σε ιδιωτικό περιεχόμενο, πολλοί την χαρακτηρίζουν ως μέθοδο «Υποκλοπής» και τονίζουν ότι σε περιοχές που απαγορεύεται το «bulk intercept» θα πρέπει να απαγορεύεται και το «bulk CSS» [01].

Παρόλο που η CSS παρουσιάζεται ότι προστατεύει αποτελεσματικά την ασφάλεια των επικοινωνιών, η τεχνολογία της μπορεί να αναπροσαρμοστεί για να αποτελέσει ένα εργαλείο μαζικής παρακολούθησης.

Το γεγονός ότι το κύριο μέρος της λειτουργίας της πραγματοποιείται στην συσκευή του χρήστη παρουσιάζεται ως πλεονέκτημα που προάγει την ασφάλεια. Αρκετοί όμως υποστηρίζουν το αντίθετο, με το σκεπτικό ότι καθώς οι περισσότερες συσκευές παρουσιάζουν ευπάθειες, οι δυνατότητες ελέγχου και παρακολούθησης της CSS δύνανται να χρησιμοποιηθούν κακόβουλα από πιθανούς «αντιπάλους» που ποικίλουν από κατασκόπους άλλων κρατών σε εγκληματίες ή/και εκβιαστές και από επαγγελματικούς ανταγωνιστές σε συζύγους/συντρόφους [01].

Επιπλέον, η αδιαφάνεια που διακρίνει τα Λειτουργικά Συστήματα των κινητών τηλεφώνων δυσκολεύει σημαντικά την επιβεβαίωση «πέραν πάσης αμφιβολίας» ότι η CSS στοχεύει αποκλειστικά και μόνο στον εντοπισμό παράνομου υλικού.

Οι επικριτές της CSS ισχυρίζονται ότι παραβιάζει πολύ περισσότερο την ιδιωτικότητα των χρηστών απ’ ότι η λύση της διάθεσης «εργαλείων μειωμένης κρυπτογραφικής ισχύος» για το ευρύ κοινό, που υποστηρίζεται από άλλες προτάσεις. Διατείνονται ότι η δεύτερη «διαβάζει» μόνο το περιεχόμενο κρυπτογραφημένων επικοινωνιών, ενώ η CSS δίνει στις αρχές τη δυνατότητα της απομακρυσμένης έρευνας όχι μόνο των επικοινωνιών αλλά και των υπολοίπων πληροφοριών που βρίσκονται αποθηκευμένες στις συσκευές των χρηστών.

Επίσης διατείνονται ότι η γενικευμένη ενσωμάτωση ισχυρότατων τεχνολογιών έρευνας και εντοπισμού πληροφοριών στις συσκευές όλων των χρηστών, άκριτα (χωρίς να καταλαβαίνουμε πλήρως τις ευπάθειές τους ή να αναλογιζόμαστε επαρκώς τις τεχνικές και κοινωνικές επιπτώσεις τους), θα είναι ένα πολύ επικίνδυνο κοινωνικό πείραμα. Μάλιστα, με δεδομένη την πρόσφατη εμπειρία από διάφορες χώρες και της πιθανολογούμενης παρέμβασης αντιπάλων κρατών στις εθνικές εκλογές και τα δημοψηφίσματα τους, θεωρούν πως θα πρέπει να αποτελεί προτεραιότητα εθνικής ασφάλειας η αποτροπή της κάθε λογής απόπειρας κατασκοπείας των νομοταγών πολιτών και επηρεασμού της κοινής γνώμης [01].

Εν κατακλείδι, θεωρούν την CSS μια επικίνδυνη τεχνολογία που κάνει τους νομοταγείς πολίτες πολύ πιο ευάλωτους σε παραβιάσεις της ιδιωτικότητάς τους και των προσωπικών τους δεδομένων. Ακόμα κι αν αναπτυχθεί αρχικά για τον θεμιτό σκοπό της

έρευνας για τον εντοπισμό περιεχομένου CSA, θεωρείται σχεδόν σίγουρο ότι θα υπάρξει στη συνέχεια τεράστια πίεση να επεκταθεί το πεδίο εφαρμογής της και θα είναι πολύ δύσκολο τότε για τους πολίτες να αντιταχθούν σε αυτήν την επέκταση ή να ελέγξουν την όποια (πιθανή) καταστρατήγηση των θεμιτών στόχων της μεθόδου. Η δυνατότητα που έχουν σήμερα οι πολίτες των Δημοκρατικών χωρών να χρησιμοποιούν ψηφιακές συσκευές, να δημιουργούν και να αποθηκεύουν περιεχόμενο και να επικοινωνούν μεταξύ τους, βασίζεται στην ασφάλεια που νιώθουν να τα κάνουν όλα αυτά. Η εισαγωγή τεχνολογιών ελέγχου των συσκευών και των δεδομένων που αυτές διακινούν ή αποθηκεύουν, θα πλήξει σοβαρά αυτό το αίσθημα ασφάλειας και θα κλονίσει την εμπιστοσύνη τους στην ύπαρξη πραγματικής ελευθερίας και Δημοκρατίας [01].

Το NCMEC ανακοίνωσε ότι το έτος 2020 έλαβε πάνω από 21 εκατομμύρια αναφορές δικτυακών (online) περιπτώσεων σεξουαλικής εκμετάλλευσης παιδιών, που αντιστοιχεί σε αύξηση 28% (!) σε σχέση με το 2019. Πιθανότατα αυτή η πολύ μεγάλη αύξηση, οφείλεται κατά ένα μέρος στο γεγονός ότι το έτος αυτό ήταν η πρώτη χρονιά της πανδημίας Covid-19 και των αυστηρών lockdown, οπότε ο κόσμος πέρναγε πολλές ώρες μπροστά σε έναν Η/Υ, tablet ή κινητό. Σημαίνει όμως επίσης ότι η διακίνηση CSAM δεν αποτελεί πλέον μια περιορισμένη μορφή εγκληματικότητας όπως στο παρελθόν (πριν την αλματώδη διάδοση του Διαδικτύου και των επικοινωνιών), που ασκούνταν με έντυπο, φωτογραφικό κυρίως υλικό από περιθωριακά άτομα. Αποτελεί μια ραγδαία αναπτυσσόμενη μορφή επικερδούς εγκληματικότητας που εκμεταλλεύθηκε στο μέγιστο τα νέα εργαλεία την ψηφιακής εποχής και στην οποία εμπλέκονται πάρα πολλά άτομα «πέραν πάσης υποψίας», είτε ως διακινητές, είτε (οι περισσότεροι) ως «πελάτες». Είναι λοιπόν αδήριτη η ανάγκη, αυτή η μορφή εγκληματικότητας, να αντιμετωπιστεί σοβαρά και με αποτελεσματικό τρόπο και στον τομέα της πρόληψης και στον τομέα της καταστολής [16].

Όμως, το έργο αυτό καθίσταται για τις Αρχές μη διαχειρίσιμο, εξαιτίας του τεράστιου όγκου δεδομένων που διακινείται και που αυξάνει καθημερινά, καθώς εκατομμύρια χρήστες παγκοσμίως «ανεβάζουν» σε πλατφόρμες όλο και περισσότερα δεδομένα σε όλες τις μορφές πολυμέσων (εικόνες, βίντεο, μουσική, κείμενο).

Μια προσέγγιση για την ανάλυση αυτού του τεράστιου και διαρκώς αυξανόμενου όγκου δεδομένων είναι η μετατροπή, για παράδειγμα των εικόνων, σε μια μορφή που περιέχει μόνο κάποια συγκεκριμένα και στενά συνδεδεμένα με την εικόνα χαρακτηριστικά, έτσι ώστε να καταλαμβάνει πολύ λιγότερο χώρο. Αυτές οι «συμπαγείς» αναπαραστάσεις

πολυμέσων (εικόνων, βίντεο, κτλ.) επιτρέπουν μια πολύ πιο γρήγορη και αποτελεσματική διερεύνησή τους από τεχνικές εντοπισμού CSAM όπως η τεχνική Perceptual Hashing. Μάλιστα οι πιο πρόσφατοι αλγόριθμοι, χρησιμοποιούν Νευρωνικά δίκτυα για την εξαγωγή χαρακτηριστικών [16].

Τον Αύγουστο του 2021 η Apple ανακοίνωσε ότι σχεδίασε μια καινούργια τεχνική εντοπισμού CSAM με γνώμονα την προστασία της ιδιωτικότητάς τους (Privacy Enhancing Cryptography – PEC) που χρησιμοποιεί Νευρωνικά δίκτυα και εφαρμόζεται στις συσκευές των χρηστών (Client-side scanning), μόνο σε εικόνες. Η τεχνική ονομάζεται «NeuralHash» και ενεργοποιείται όταν οι χρήστες επιθυμούν να ανεβάσουν στο iCloud, εικόνες που είναι αποθηκευμένες στις συσκευές τους. Χρησιμοποιεί έναν Perceptual Hashing αλγόριθμο που εκτελεί PSI (Private Set Intersection – «Ασφαλή εύρεση κοινών τιμών από δύο σύνολα») προκειμένου να συγκρίνει hashes από τις εν λόγω εικόνες, με hashes από εικόνες γνωστού CSA περιεχομένου, αποθηκευμένων σε ΒΔ που θα παρέχεται στην Apple από το NCMEC και θα αποθηκεύεται για τον σκοπό αυτό σε κρυπτογραφημένη μορφή, στις συσκευές των χρηστών [11, 16].

Η Apple διατείνεται ότι η PSI διασφαλίζει ότι η εταιρεία θα πληροφορείται μόνο για την ύπαρξη παράνομου περιεχόμενου (εάν υπάρχει) και για τίποτα παραπάνω. Δηλαδή, δεν θα έχει πρόσβαση σε καμία από τις υπόλοιπες ιδιωτικές πληροφορίες που είναι αποθηκευμένες στις συσκευές των χρηστών. Παράλληλα, παρείχε διαβεβαιώσεις και για την αξιοπιστία της τεχνικής, αναφέροντας ότι ο κίνδυνος να υπάρξουν λανθασμένοι εντοπισμοί CSAM είναι πολύ μικρός. Όσον αφορά την ασφάλεια του συστήματος, η Apple επικαλέστηκε τις (θετικές) απόψεις ειδικών και ανεξάρτητων ερευνητών.

Παρόλα αυτά, το NeuralHash αντιμετώπισε αρκετά μεγάλη δημόσια κριτική, όχι μόνο για πιθανές παραβιάσεις της ιδιωτικότητας, αλλά και για την αξιοπιστία της. Σχετικά με την τελευταία, δεν έχουν μέχρι στιγμής δημοσιευτεί αναλύσεις που να διερευνούν λεπτομερώς τον πυρήνα της λύσης, δηλαδή αυτόν καθ' αυτόν τον υπολογισμό του hash, ώστε να εξαχθούν πιο βάσιμα συμπεράσματα.

Στους κύκλους των ερευνητών είναι αρκετά γνωστό και αποδεκτό, τουλάχιστον στην θεωρία, ότι τα Νευρωνικά δίκτυα είναι ευάλωτα σε διάφορα είδη επιθέσεων. Αυτό όμως που ενδιαφέρει τελικά είναι όταν κάποια λύση εφαρμοστεί στην πράξη, πώς θα επηρεάσει τα εκατομμύρια συστήματα που χρησιμοποιούνται σε όλον τον κόσμο και τους χρήστες τους, οι οποίοι πιθανότατα δεν γνωρίζουν την ύπαρξη αυτών των

κινδύνων. Μάλιστα πιθανολογείται ότι η χρήση Νευρωνικών δικτύων που έχουν τη δυνατότητα να υπολογίζουν gradients (κλίσεις), κάνει το έργο αυτών που θέλουν να εξαπολύσουν επιθέσεις εναντίον τους ακόμα ευκολότερο καθώς αφήνει πολλά «εκμεταλλεύσιμα» κενά για επιθέσεις [16].

Εκ πρώτης άποψης, η PSI φαίνεται να αποτελεί μια καλή προσέγγιση όσον αφορά την διασφάλιση της ιδιωτικότητας των χρηστών και η τεχνική NeuralHash που την υιοθετεί και χρησιμοποιεί τη μέθοδο Perceptual Hashing, αποτελεί αυτήν την στιγμή την πιο αντιπροσωπευτική περίπτωση της μεταστροφής των τεχνολογιών εντοπισμού περιεχομένου από Server-side scanning σε Client-side scanning. Όπως όμως αναφέρθηκε ανωτέρω, η μέθοδος Perceptual Hashing δεν χρησιμοποιεί τους παραδοσιακούς αλγορίθμους κρυπτογραφικού Hashing που παράγουν πολύ διαφορετικά Hash ακόμα και για εισερχόμενα δεδομένα με πολύ μικρές διαφορές. Αντίθετα χρησιμοποιεί τους Perceptual Hashing αλγόριθμους που (όπως και οι κρυπτογραφικοί) από μια εικόνα παράγουν ένα hash μοναδικό για την συγκεκριμένη εικόνα, αλλά και από μια περίπου ίδια εικόνα (με μικρές διαφορές στο μέγεθος και την ποιότητα) παράγουν το ίδιο hash. Οπότε υφίσταται τελικά υψηλός κίνδυνος λανθασμένων εντοπισμών, δηλαδή ο αλγόριθμος θα ανιχνεύει ταύτιση μεταξύ δύο εικόνων, χωρίς όμως να διασφαλίζει ότι αυτή όντως ισχύει στην πραγματικότητα. Επιπλέον, καθώς η τεχνική εφαρμόζει όπως προαναφέρθηκε Client-side scanning για τον εντοπισμό CSAM μόνο σε εικόνες πριν αυτές ανέβουν στο iCloud, είναι λογικό να υποθέσει κανείς ότι οι Κυβερνήσεις θα πιέσουν την Apple να τροποποιήσει τη μέθοδό της ώστε να περιλαμβάνει και άλλους τύπους περιεχομένων ή να μπλοκάρει άλλα είδη αρχείων (π.χ. με πολιτικά μηνύματα) [11].

Αμέσως μετά την ανακοίνωσή της, η Apple δέχτηκε σφοδρή κριτική σε παγκόσμιο επίπεδο, ότι οι συσκευές της θα μετατραπούν σε μηχανές διαρκούς ελέγχου όλων των φωτογραφιών και μηνυμάτων που περνάνε απ' αυτές.

Το ίδρυμα EFF (Electronic Frontier Foundation) αμφισβήτησε ότι ένα σύστημα Client-side scanning που σχεδιάστηκε για τον εντοπισμό διακίνησης CSAM, θα χρησιμοποιηθεί αποκλειστικά και μόνο για τον σκοπό αυτό, όσο καλές κι αν είναι οι αρχικές προθέσεις και διαβεβαιώσεις. Το EFF θεωρεί σχεδόν σίγουρο ότι θα ασκηθούν τεράστιες πιέσεις από διάφορους φορείς (κυρίως Κυβερνητικούς και Αστυνομικούς) και ότι τελικά οι διαβεβαιώσεις αυτές θα καταστρατηγηθούν και το σύστημα θα χρησιμοποιηθεί και για άλλους σκοπούς που έχουν σχέση με την καταπάτηση θεμελιωδών δικαιωμάτων των ατόμων, σε παγκόσμια κλίμακα [11].

Μάλιστα, προς επίρρωση των ανωτέρω, το EFF φέρνει παραδείγματα διαφόρων χωρών (συνήθως με αυταρχικά καθεστώτα) που ήδη πέρασαν νόμους που υποχρεώνουν τους Παρόχους να ενημερώνουν τις Αρχές ή/και να προβαίνουν σε διάφορες ενέργειες. Κάνει μάλιστα ιδιαίτερη αναφορά στην Ινδία (μια Δημοκρατική χώρα) της οποίας το κοινοβούλιο πέρασε νόμο που απαιτεί από τις πλατφόρμες να καταδεικνύουν την προέλευση των μηνυμάτων και να ελέγχουν προληπτικά όλο το περιεχόμενό τους, καθώς και σε νόμο της Αιθιοπίας (που μπορεί κάλλιστα να εφαρμοστεί και στη διακίνηση μηνυμάτων) που απαιτεί οτιδήποτε θεωρείται από την κυβέρνηση «παραπληροφόρηση» να «κατεβαίνει» εντός 24 ωρών. Επίσης, γίνεται αναφορά και σε πιθανές περιπτώσεις:

α) καταπίεσης διαφόρων κοινωνικών ομάδων («ανεπιθύμητων» σε αυταρχικά καθεστώτα), όπως μειονοτήτων ή της LGBTQ+ κοινότητας με απαγόρευση περιεχομένου σχετιζόμενου με αυτές τις ομάδες,

β) καταπίεσης και «ηλεκτρονικής φίμωσης» όσων εκφράζουν αντικυβερνητικές απόψεις σε αυταρχικά καθεστώτα, με απαγόρευση της έκφρασης των θέσεών τους στα ψηφιακά μέσα, και της ενημέρωσης των πολιτών γι' αυτές, καθώς και για τις δράσεις τους (π.χ. εκκλήσεις για αντικυβερνητικές συγκεντρώσεις) [11].

Ένα περίπου μήνα μετά την αρχική της ανακοίνωση (Σεπτέμβριος 2021) και κατόπιν όλης αυτής της κριτικής, η Apple επανήλθε με νέα ανακοίνωση που ανέφερε ότι (σε ελεύθερη μετάφραση): «*κατόπιν την ανατροφοδότησης που έλαβε από πελάτες, ερευνητές, ομάδες υποστήριξης των ανθρωπίνων δικαιωμάτων και άλλους, αποφασίστηκε ότι απαιτείται περισσότερος χρόνος για να συλλεχθούν πληροφορίες και να γίνουν βελτιώσεις πριν γίνουν εμπορικά διαθέσιμα αυτά τα κρίσιμα και σημαντικά εργαλεία που προάγουν την ασφάλεια των παιδιών*» [11].

Η τελική εκτίμηση για τη NeuralHash είναι αφενός ότι όταν εφαρμόζεται στην πράξη και σε μεγάλη κλίμακα για τον εντοπισμό CSAM σε εικόνες, παρουσιάζει αρκετούς κινδύνους και μειονεκτήματα και αφετέρου ότι δημιουργεί επιπλέον θέματα ασφάλειας και παραβίασης της ιδιωτικότητας, όπως αναίτια αλγοριθμική παρακολούθηση των χρηστών. Αποτελεί μεν την «τρέχουσα» λύση, αλλά απέχει αρκετά από το να είναι «ιδανική» (τηρουμένων πάντα των συμβιβασμών που συνήθως απαιτούνται να γίνονται κατά την πρακτική εφαρμογή μιας λύσης). Απαιτείται επομένως περαιτέρω έρευνα για την εξέλιξη πιο ολοκληρωμένων, εύρωστων και ασφαλών συστημάτων που θα περιορίζουν στο μέγιστο τα ανωτέρω μειονεκτήματα και θα είναι λιγότερο διεισδυτικά στην ιδιωτικότητα των ατόμων/χρηστών.

Κεφάλαιο 8
Συμπεράσματα

Από εγκληματολογικές στατιστικές έρευνες σε διάφορες χώρες, είναι δυστυχώς προφανές, ότι η σεξουαλική κακοποίηση και εκμετάλλευση παιδιών με σκοπό το κέρδος - και κατά συνέπεια και η διακίνηση παιδο-πορνογραφικού υλικού - είναι ειδεχθή εγκλήματα που όμως απαντώνται σε παγκόσμιο επίπεδο και σε διαρκώς αυξανόμενο βαθμό, εκμεταλλευόμενα στο έπακρο τις εκάστοτε τεχνολογικές εξελίξεις, ιδίως στις τηλεπικοινωνίες. Ειδικότερα, μέσα από τηλεπικοινωνιακές υπηρεσίες και εφαρμογές του Διαδικτύου διακινείται παράνομο υλικό ή/και προσεγγίζονται ανήλικοι με σκοπό την αποπλάνησή τους. Σε αυτό το πλαίσιο, πολλοί εξ αυτών προσπαθούν να καλύπτουν τα «ίχνη» τους για να μην εντοπιστούν, εκμεταλλευόμενοι διάφορες υπηρεσίες ασφαλείας που ενυπάρχουν, όπως η κρυπτογράφηση.

Προκύπτει λοιπόν η αδιαμφισβήτητη ανάγκη, αυτό το είδος εγκλήματος να καταπολεμηθεί παγκοσμίως με όσο το δυνατόν πιο αποτελεσματικό τρόπο.

Απ' όσα εκτέθηκαν ανωτέρω στα πλαίσια της παρούσας μεταπτυχιακής διατριβής, προέκυψαν δύο, επίσης αδιαμφισβήτητα, στοιχεία:

1) Απ' όλες τις μεθόδους κρυπτογράφησης των επικοινωνιών, η πιο ασφαλής και «φιλική» προς την ιδιωτικότητα των χρηστών είναι η End-to-End («Διατερματική») κρυπτογράφηση, καθώς μέχρι σήμερα δεν υπάρχει μέθοδος που να την προσβάλει (ούτε καν ο Πάροχος της υπηρεσίας μπορεί να διαβάσει το περιεχόμενο μιας επικοινωνίας).

- Και καθώς προς το παρόν εξακολουθεί να είναι διαθέσιμη στο ευρύ κοινό, προσφέρει στους νομοταγείς πολίτες το πολύ σημαντικό πλεονέκτημα της «Απόλυτης Ασφάλειας» στις μεταξύ τους επικοινωνίες.

Ταυτόχρονα όμως, η E2E κρυπτογράφηση εγείρει και ένα πολύ σημαντικό ζήτημα (ή μειονέκτημα, όπως θα μπορούσε να ισχυριστεί κανείς):

- Οι κάθε λογής παράνομοι (μεταξύ των οποίων και οι δράστες σεξουαλικής κακοποίησης παιδιών, καθώς και οι διακινητές παιδικής πορνογραφίας, που αφορούν την παρούσα διατριβή) δύνανται να επιλέγουν επίσης την E2E κρυπτογράφηση προκειμένου να επικοινωνούν, να διακινούν υλικό CSA και να καλύπτουν τα ψηφιακά τους ίχνη, με απόλυτη ασφάλεια.

2) Από τα ανωτέρω προκύπτει μία «σύγκρουση» θεμελιωδών δικαιωμάτων – από τη μία πλευρά η προστασία των παιδιών και από την άλλη πλευρά η προστασία της ιδιωτικότητας, των προσωπικών δεδομένων και της ελευθερίας του λόγου. Ως εκ τούτου, αναπόφευκτα, επικρατούν δύο απόψεις (μεταξύ των νομοταγών πολιτών) για το πώς μπορεί να επιτευχθεί αποτελεσματική αντιμετώπιση αυτών των εγκλημάτων:

Η πρώτη συγκεντρώνει εκείνους που διατίθενται να θυσιάσουν το πλεονέκτημα της απόλυτα ασφαλούς επικοινωνίας και κατά συνέπεια και την ιδιωτικότητά τους, προκειμένου να καταπολεμηθεί αυτού του είδους το έγκλημα, καθώς και άλλα (π.χ. τρομοκρατία). Φυσικά υπάρχουν παραλλαγές της άποψης που ποικίλουν από την ενσωμάτωση «κερκόπορτας-backdoor» στην E2E κρυπτογράφηση για χρήση από τις Αρχές, έως και την πλήρη κατάργηση της E2E κρυπτογράφησης για υπηρεσίες επικοινωνίας διαθέσιμες στο κοινό.
Υπέρ της άποψης αυτής τάσσονται φυσικά οι διάφορες υπηρεσίες επιβολής του νόμου (καθώς διευκολύνεται σημαντικά το έργο τους), πολλές (δημοκρατικές) κυβερνήσεις, καθώς και απλοί πολίτες.

Άποψη του γράφοντα είναι αφενός ότι η πλειοψηφία των ανωτέρω (ιδιαίτερα στις δημοκρατικές χώρες) αποτελείται από απλούς νομοταγείς πολίτες, αστυνομικούς, στρατιωτικούς, πολιτικούς κλπ. που υποστηρίζουν ένθερμα αυτήν την άποψη, διακατεχόμενοι από ειλικρινή πρόθεση να βοηθήσουν στην καταπολέμηση αυτού του είδους των εγκλημάτων κατά των παιδιών. Αφετέρου όμως θα πρέπει να ληφθεί υπόψη, πως στις τάξεις των υποστηρικτών αυτής της άποψης, παρεισφρέει και ένας σημαντικός αριθμός ατόμων με ακραίες και αυταρχικές απόψεις, τάσεις «μεγάλου αδελφού» και παρακολούθησης των άλλων, καθώς και εξάλειψης με κάθε τρόπο - νόμιμο ή μη - της όποιας αντίθετης με τη δικιά τους, άποψης. Τα άτομα αυτά, σε δημοκρατικές χώρες, μπορεί να είναι επίσης απλοί πολίτες, αστυνομικοί, στρατιωτικοί και πολιτικοί ακραίων κομμάτων, ενώ σε χώρες με αυταρχικά καθεστώτα μπορεί να συμμετέχει ολόκληρο το κυβερνών πολιτικο-στρατιωτικό/αστυνομικό κατεστημένο, καθώς τέτοιες πρακτικές

παρακολούθησης εξασφαλίζουν την φίμωση των αντιπάλων και την παραμονή του στην εξουσία.

Η δεύτερη άποψη συγκεντρώνει εκείνους που ναι μεν αναγνωρίζουν το πρόβλημα της διακίνησης CSAM και την ανάγκη αντιμετώπισής του, αλλά δεν διατίθενται σε καμία περίπτωση να θυσιάσουν τα θεμελιώδη δικαιώματα της Ιδιωτικότητάς τους και του Απορρήτου των Επικοινωνιών τους, που τους προσφέρει η E2E κρυπτογράφηση. Προτείνουν δε διάφορες τεχνικές λύσεις που διατείνονται ότι λειτουργούν αποτελεσματικά για την ανίχνευση CSA και Grooming περιεχομένου επί E2E κρυπτογραφημένων επικοινωνιών.
Υπέρ της άποψης αυτής τάσσονται ιδρύματα προστασίας των θεμελιωδών ανθρωπίνων δικαιωμάτων, ακτιβιστές και πάρα πολλοί απλοί πολίτες.

Και εδώ η άποψη του γράφοντα είναι αφενός ότι η πλειοψηφία των υποστηρικτών αυτής της άποψης αποτελείται επίσης από απλούς και νομοταγείς πολίτες που διακατέχονται από ειλικρινή κίνητρα να προστατέψουν πάση θυσία τα προαναφερθέντα θεμελιώδη δικαιώματα από κάθε προσπάθεια παραβίασής τους (έστω και για θεμιτό σκοπό), καθώς διακρίνουν πιθανή επέκταση της παραβίασης αυτής και για αθέμιτους σκοπούς. Αφετέρου όμως πρέπει επίσης να συνυπολογιστεί ότι στις τάξεις των υποστηρικτών και αυτής της άποψης, παρεισφρέει ένας σημαντικός αριθμός ατόμων με ιδιοτελή και αμφιβόλου νομιμότητας κίνητρα, που επικαλούμενοι τα θεμελιώδη ανθρώπινα δικαιώματα, επιθυμούν να αποκρύψουν τις τυχόν παράνομες δραστηριότητές τους.

Διαπιστώθηκε επίσης στη διατριβή, μετά από την εξέταση των τεκταινόμενων παγκοσμίως στο νομοθετικό επίπεδο, πως οι υποστηρικτές και των δύο απόψεων προσπαθούν να τις προωθήσουν και να τις καταστήσουν νόμο του εκάστοτε κράτους, άλλες φορές με επιτυχία και άλλες όχι. Μάλιστα, επί του παρόντος, διακρίνεται μια ισχυρότερη τάση υιοθέτησης της πρώτης άποψης, στις νομοθετικές ρυθμίσεις.

Η αλήθεια είναι ότι και οι δύο απόψεις στηρίζονται σε βάσιμα επιχειρήματα. Δηλαδή δεν πρόκειται για κάποια περίπτωση που η μία άποψη υπερισχύει καταφανώς σε επιχειρήματα έναντι της άλλης. Η άποψη του γράφοντα επ' αυτού (χωρίς καμία διάθεση αποστασιοποίησης από το ζήτημα) είναι ότι είναι θέμα της Δημοκρατίας να το λύσει. Οι υποστηρικτές και των δύο απόψεων θα πρέπει να παρουσιάσουν στο ευρύ κοινό τα (βάσιμα όπως προαναφέρθηκε) επιχειρήματά τους και εκείνη η άποψη που θα κερδίσει

την πλειοψηφία θα επικρατήσει. Έτσι λειτουργεί και έτσι πρέπει να λειτουργεί η Δημοκρατία.

Στο ανωτέρω δίλημμα μπορεί να φανεί χρήσιμη η παρούσα μεταπτυχιακή διατριβή, ως πηγή αμερόληπτης πληροφόρησης, αφενός για τα ισχύοντα παγκοσμίως σχετικά νομοθετικά πλαίσια (ή τα προτεινόμενα και πιθανώς αναμενόμενα να ισχύσουν) και αφετέρου για την αποτελεσματικότητα, εφαρμοσιμότητα, ασφάλεια κλπ., των τεχνικών λύσεων που προτείνονται ως εναλλακτική λύση από τους υποστηρικτές της δεύτερης άποψης.

Θα ήταν παράλειψη να μην αναφερθεί στο σημείο αυτό ότι υφίσταται και ο κίνδυνος, μια χώρα που δεν έχει καν αποφανθεί επί του ανωτέρω ζητήματος (πόσο μάλλον να μην έχει ψηφίσει σχετικό νόμο), να επηρεαστεί από γεγονότα που συνέβησαν ή νομοθετήματα που ψηφίστηκαν σε κάποια άλλη (ή άλλες), ιδιαίτερα εάν αυτή είναι μεγάλη και ισχυρή. Κάτι τέτοιο μπορεί να συμβεί εξαιτίας της παγκοσμιοποιημένης αγοράς και είναι ακριβώς αυτό που φοβούνται οι επικριτές του νόμου που ψηφίστηκε στην Αυστραλία. Για παράδειγμα, εάν μια πολυεθνική εταιρεία υπηρεσιών ή λογισμικού αναγκαστεί να καταργήσει κάποια λειτουργία από το προϊόν της εξαιτίας ενός νόμου που ψηφίστηκε σε μια μεγάλη χώρα (π.χ. Η.Π.Α.), πιθανότατα θα το καταργήσει και σε παγκόσμιο επίπεδο.

Καθόσον αφορά λοιπόν τις τεχνικές λύσεις που παρουσιάστηκαν και αξιολογήθηκαν στα Κεφάλαια 6 και 7, διαφαίνεται δυστυχώς ότι ακόμα δεν υπάρχει ώριμη τεχνολογία που να επιτυγχάνει τη «χρυσή τομή». Η Ευρωπαϊκή Επιτροπή φαίνεται να προσπαθεί να εγγυηθεί ότι δεν παραβιάζεται η E2E κρυπτογράφηση με το να προτείνει λύσεις που «ενσωματώνουν» πολλές λειτουργίες στη συσκευή του χρήστη. Ωστόσο, έγκριτοι ειδικοί στο χώρο της κρυπτογραφίας και της ασφάλειας επικοινωνιών καταθέτουν επιχειρήματα [01] (που συμπεριλήφθηκαν στην παρούσα διατριβή), ότι κάτι τέτοιο επί της ουσίας δεν λύνει κανένα πρόβλημα – τουναντίον, γεννά καινούργια, λαμβάνοντας υπόψη πόσο «ευπαθείς» είναι οι συσκευές των χρηστών στο να παρεισφρέουν κακόβουλα λογισμικά ή αρχεία και να επηρεάζουν τη λειτουργία τους. Μάλιστα, οι ίδιοι οι ερευνητές κάνουν ειδική αναφορά στην περίπτωση της Apple (όπως περιγράφηκε ανωτέρω), η οποία φαίνεται ότι προσπάθησε πράγματι να υλοποιήσει μία λύση που να ενσωματώνει τεχνολογίες φιλικές προς την ιδιωτικότητα, αλλά τελικά η ίδια η εταιρεία την απέσυρε πριν καν την υλοποιήσει. Σημειώνεται πως στο ίδιο πνεύμα κινούνται και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων-EDPS και η Ευρωπαϊκή Επιτροπή

Προστασίας Δεδομένων-EDPB, στην επίσημα δημοσιευμένη κοινή τους άποψη επί της Πρότασης νέου Κανονισμού της ΕΕ για την ανίχνευση CSAM και Grooming [03].

Από την πλευρά του γράφοντα, προκύπτει ως συμπέρασμα ότι χρειάζεται περαιτέρω έρευνα προκειμένου να προκύψουν νέες τεχνολογίες που θα μπορέσουν να αντιμετωπίσουν αποτελεσματικά τα ζητήματα. Δεν θα πρέπει να οδηγηθούμε σε μία άνευ όρων κατάργηση της E2E κρυπτογράφησης – η οποία, πέραν των σημαντικών προβλημάτων που θα επιφέρει για τους λόγους που εκτέθηκαν αναλυτικά στην παρούσα διατριβή - εν τέλει θα πλήξει και την προστασία των ίδιων των παιδιών και ανηλίκων, αφού οι εγκληματίες θα διευκολύνονται να παρακολουθούν, π.χ. συνομιλίες εφήβων ή φωτογραφίες παιδιών που ανταλλάζουν πολλές φορές οι γονείς τους. Αντίστοιχα, οι υπάρχουσες προτεινόμενες τεχνικές που διατείνονται ότι δεν πλήττουν την E2E κρυπτογράφηση, είναι αμφίβολο ότι όντως το επιτυγχάνουν, αφού εν τέλει υφίσταται επεξεργασία των δεδομένων των χρηστών που βρίσκονται αποθηκευμένα στις συσκευές τους σε μη κρυπτογραφημένη μορφή. Κι αυτό είναι κάτι που οποιοσδήποτε χρήστης που αισθάνεται ασφαλής χρησιμοποιώντας μία E2E εφαρμογή, δεν θα περίμενε να συμβαίνει. Συνεπώς, οι νέες τεχνικές (αρκετές εκ των οποίων είναι σε κάποια αρχικά στάδια), θα πρέπει να μελετηθούν και να υλοποιηθούν κατάλληλα με τη δέουσα προσοχή - ειδικότερα οι ακόλουθες:

1) Κρυπτογράφηση βάσει αναζήτησης (searchable encryption): Πρόκειται για προηγμένες κρυπτογραφικές τεχνικές που επιτρέπουν σε μία οντότητα να αναζητά εντός ενός κρυπτογραφημένου κειμένου, το οποίο όμως δεν μπορεί να αποκρυπτογραφήσει, αν υπάρχουν κάποιες συγκεκριμένες λέξεις. Κατά αυτόν τον τρόπο, ο Πάροχος μίας τηλεπικοινωνιακής υπηρεσίας ενδεχομένως να μπορεί να «επισημαίνει» και να διακόπτει κάποιες επικοινωνίες ως «ύποπτες», χωρίς όμως να έχει μάθει οτιδήποτε άλλο από το περιεχόμενο της επικοινωνίας.

2) Ομομορφική κρυπτογράφηση (Homomorphic encryption): Πρόκειται για προηγμένες κρυπτογραφικές τεχνικές που επιτρέπουν σε έναν φορέα να κάνει κάποιους υπολογισμούς επί κρυπτογραφημένων δεδομένων, χωρίς να μπορεί να ανακτήσει το περιεχόμενο των αρχικών δεδομένων. Η ιδιότητα αυτή ενδεχομένως να μπορούσε να ενσωματωθεί κατάλληλα σε μία τεχνολογική λύση για την επίτευξη του επιδιωκόμενου σκοπού. Αντίστοιχα θα πρέπει να ληφθούν υπόψη και διάφορες τεχνικές ασφαλών

υπολογισμών πολλών μελών (MPC) – εξάλλου, η ομομορφική κρυπτογράφηση αποτελεί μία (εκ πολλών πιθανών) μεθόδων για την υλοποίηση MPC.

3) Η μέθοδος «message franking»: Με βάση βιβλιογραφικές αναφορές [02, 06], αυτή η μέθοδος έχει ήδη αρχίσει να υλοποιείται. Εφαρμόζεται σε E2EE επικοινωνίες και έχει την εξής ιδιότητα: αν ένας χρήστης Β έλαβε αίτημα E2EE επικοινωνίας από έναν χρήστη Α και αυτή υλοποιηθεί, μπορεί αν θέλει να αποδείξει σε κάποιον τρίτο (π.χ. στις Αρχές επιβολής του νόμου) ότι ο Α ξεκίνησε τη συγκεκριμένη επικοινωνία μαζί του με το συγκεκριμένο περιεχόμενο, χωρίς να μπορεί ο Α να την αμφισβητήσει. Με άλλα λόγια, αυτή η τεχνική βασίζεται σε αναφορές χρηστών για παράνομο υλικό ή επικοινωνία που λαμβάνουν. Αν υλοποιηθεί σωστά και με εγγυήσεις ασφάλειας, δεν πλήττεται η E2E λογική, και παρέχεται η δυνατότητα της υπόδειξης κάποιου εγκληματία, από άλλον χρήστη, με αποδείξεις που δεν επιδέχονται αμφισβήτησης.

4) Αναγνώριση «ύποπτων» συμπεριφορών από τα μεταδεδομένα (metadata) της επικοινωνίας. Για παράδειγμα:
- μήπως κάποιος χρήστης επικοινωνεί συχνά με ανήλικους;
- μήπως χρησιμοποιείται κάποια ύποπτη IP διεύθυνση;
- μήπως αποστέλλονται πολύ συχνά μεγάλα αρχεία που μπορούν να παραπέμπουν σε βίντεο και, εάν ναι, μήπως οι παραλήπτες είναι αντίστοιχα «ύποπτοι» λόγω τέτοιων διαδικτυακών συμπεριφορών;
Εδώ, οι τεχνικές μηχανικής μάθησης μπορούν να δώσουν λύσεις (ήδη τέτοιες τεχνικές χρησιμοποιούνται για ανίχνευση spam) [02]. Σαφέστατα μία τέτοια λύση οδηγεί στην αναγνώριση ύποπτων συμπεριφορών και όχι στην απόδειξη παράνομης συμπεριφοράς, αλλά μπορούν πιθανώς να οδηγήσουν σε προληπτικό περιορισμό της επικοινωνίας του χρήστη, ώστε να αποφευχθεί η οποιαδήποτε έκνομη συμπεριφορά ή και κάποιο έγκλημα.

Φυσικά, οι ανωτέρω λύσεις δεν μπορούν να θεωρηθούν εκ των προτέρων πανάκεια, αλλά τομείς για τους οποίους απαιτείται περαιτέρω έρευνα και φυσικά χρόνος. Προκειμένου λοιπόν να δοθεί στους ερευνητές ο απαραίτητος αυτός χρόνος για να εξελίξουν πιο λειτουργικές και αξιόπιστες τεχνικές, καλό θα ήταν να υπάρξει σε παγκόσμιο επίπεδο ένα moratorium μεταξύ των δύο κυρίαρχων απόψεων και αποφυγή ενεργειών επιβολής της μιας στην άλλη με νόμους), καθώς έτσι δημιουργούνται de facto καταστάσεις και ο κίνδυνος να σταματήσει κάθε είδους έρευνα για την εξέλιξη τεχνικών που εκ προοιμίου θα έχουν κριθεί μη νόμιμες.

Κεφάλαιο 9
Επίλογος

Η παρούσα μεταπτυχιακή διατριβή εστίασε σε ένα πολύ σημαντικό ζήτημα, το οποίο ενέχει τη «σύγκρουση» θεμελιωδών ατομικών δικαιωμάτων: εκ πρώτης όψεως θα έλεγε κανείς ότι τα δικαιώματα αυτά είναι αντίρροπα, αν και δεν είναι ακριβώς έτσι (για παράδειγμα, η υποβάθμιση της ασφάλειας και της προστασίας των προσωπικών δεδομένων επηρεάζει άμεσα την ασφάλεια και των παιδιών). Ως εκ τούτου, η αντιμετώπισή του απαιτεί τη μέγιστη δυνατή προσοχή και την ενεργή συμμετοχή της κοινότητας με κατάθεση απόψεων και επιχειρημάτων (από τις αρχές επιβολής του νόμου, τις αρχές προστασίας δικαιωμάτων κ.α.). Παράλληλα, όπως είδαμε και στο προηγούμενο κεφάλαιο, κρίνεται σκόπιμο να ενταθεί η προσπάθεια της ερευνητικής κοινότητας στην ανάπτυξη λύσεων που θα αντιμετωπίζουν, στον καλύτερο δυνατό βαθμό, τα ζητήματα που ανακύπτουν, αφού διαφαίνεται ότι οι υπάρχουσες τεχνικές δεν καταφέρνουν να επιτύχουν τη βέλτιστη στάθμιση μεταξύ των δικαιωμάτων.

Θα πρέπει επίσης να αναφερθεί ότι κάθε νομοθετική πρωτοβουλία η οποία προκειμένου να αντιμετωπίσει ένα πολύ σοβαρό ζήτημα οδηγεί σε περιορισμό άλλων δικαιωμάτων, πρέπει να είναι απόλυτα τεκμηριωμένη ως προς την αποτελεσματικότητα και την αναλογικότητά της. Στη συγκεκριμένη περίπτωση, εφόσον υπάρχουν αναφορές ότι γνωστές τηλεπικοινωνιακές υπηρεσίες χρησιμοποιούνται από εγκληματίες για τα ειδεχθή εγκλήματα που αναφέρθηκαν ανωτέρω, θα πρέπει να υπάρχει λεπτομερής τεκμηρίωση ως προς το γιατί οι τεχνικές που προτείνονται από το νομοθέτη (και οι οποίες εκ των πραγμάτων περιορίζουν άλλα δικαιώματα) θα είναι πράγματι αποτελεσματικές; Όμως, μια τέτοια τεκμηρίωση που να πείθει όλους τους αρμόδιους φορείς (συμπεριλαμβανομένων και των οργάνων της ΕΕ), δεν φαίνεται να υπάρχει ακόμα, παρόλο που οι περιορισμοί αυτοί θα ισχύουν για όλους ανεξαιρέτως.

Έτσι εξακολουθούν να μένουν αναπάντητα διάφορα κρίσιμα ερωτήματα, όπως για παράδειγμα: πώς θεωρείται δεδομένο ότι οι εγκληματίες, γνωρίζοντας πλέον ότι υπάρχουν τεχνικές ανίχνευσης, θα συνεχίσουν να χρησιμοποιούν τις εν λόγω υπηρεσίες και δεν θα βρουν άλλους τρόπους, όπως, π.χ. το «σκοτεινό Διαδίκτυο» (dark web), για το

οποίο, αν και είναι γνωστό ότι αποτελεί, μεταξύ άλλων, και πεδίο επικοινωνίας εγκληματιών, δεν καταβάλλεται καμία ουσιαστική προσπάθεια από τους ανά την υφήλιο νομοθέτες για την ρύθμισή του; Πώς επίσης διασφαλίζεται ότι οι εγκληματίες δεν θα προσπαθήσουν απλά να «κρύψουν» τα ψηφιακά ίχνη τους – π.χ. κρυπτογραφώντας με δικά τους λογισμικά την επικοινωνία τους;

Στο πλαίσιο αποτίμησης της αναλογικότητας και αποτελεσματικότητας του μέτρου, χρήσιμο είναι να αναφέρουμε ότι, σε πρόσφατη εργασία [07], καταδείχτηκε ότι, με βάση το υφιστάμενο νομικό πλαίσιο ευρωπαϊκής χώρας (συγκεκριμένα της Ολλανδίας), η ύπαρξη E2E κρυπτογράφησης τελικά δεν εμπόδισε τον εντοπισμό εγκληματιών. Μάλιστα, η εργασία αυτή εξέτασε σωρεία περιπτώσεων που έκρινε το οικείο σύστημα απονομής δικαιοσύνης της χώρας. Παρόλο που αφορά μόνο μία χώρα, η εν λόγω εργασία καταδεικνύει περαιτέρω τον ανωτέρω συλλογισμό, ως προς το πόσο σημαντικό είναι να τεκμηριωθεί επί πραγματικών δεδομένων, η αναγκαιότητα υποβάθμισης ή κατάργησης της E2E κρυπτογράφησης.

Εν κατακλείδι, θα πρέπει να ειπωθεί ότι, όπως αναφέρεται και στην αναφορά του CDT «Outside Looking In Approaches to Content Moderation in End-to-End Encrypted Systems» [02], καμία τεχνολογική λύση από μόνη της δεν μπορεί να αποδώσει καθολική λύση στο τεράστιας κρισιμότητας αυτό ζήτημα. Οι κοινωνίες θα πρέπει να εστιάσουν βαθύτερα στις αιτίες (κοινωνικές, πολιτικές κτλ.) που προκαλούν αυτές τις εγκληματικές πράξεις κατά παιδιών, καθώς και στους μηχανισμούς και τις δομές που θα πρέπει να λειτουργούν εντός τους για την πρόληψη και αποτροπή τους. Θα πρέπει δηλαδή να εστιάσουν στον πυρήνα του προβλήματος, και να μην περιορίζονται στον εντοπισμό του υλικού και των υπαιτίων κατόπιν της τέλεσης των πράξεων αυτών.

Βιβλιογραφία

[01] Abelson H. et al, “Bugs in our Pockets: The Risks of Client-Side Scanning”, (2021).

[02] CDT - Center for Democracy and Technology “Outside Looking In Approaches to Content Moderation in End-to-End Encrypted Systems” σελ. 22-26, 32 (2021).

[03] European Data Protection Board, “EDPB-EDPS Joint Opinion 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) - διαθέσιμη στο Διαδίκτυο: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

[04] European Parliament, “Parliament adopts temporary rules to detect child sexual abuse online”, (2021) - άρθρο διαθέσιμο στο Διαδίκτυο: https://www.europarl.europa.eu/news/en/press-room/20210701IPR07503/parliament-adopts-temporary-rules-to-detect-child-sexual-abuse-online

[05] Green M. - Cryptography Engineering Blog: “EARN IT is a direct attack on end-to-end encryption”, (2020) - διαθέσιμο στο Διαδίκτυο: https://blog.cryptographyengineering.com/2020/03/06/earn-it-is-an-attack-on-encryption/

[06] Grubbs, P., Lu, J., Ristenpart T., “Message Franking via Committing Authenticated Encryption”. In: Katz, J., Shacham, H. (eds) Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science(), vol 10403. Springer, Cham

[07] Hartel, P., Van Wegberg R., “Going dark? Analyzing the Impact of End-to-End Encryption on the Outcome of Dutch Criminal Court Cases”, (2021) - Διαθέσιμο στο Διαδίκτυο: https://arxiv.org/abs/2104.06444

[08] IEEE, Position Statement: “In Support of Strong Encryption”, (2018).

[09] Internet Society, “Internet Impact Brief: European Commission Proposal to Prevent and Combat Child Sexual Abuse”, (2022) – Ιστοσελίδα διαθέσιμη στο Διαδίκτυο: https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-eu-proposal-to-prevent-and-combat-child-sexual-abuse/

[10] “Leaked Commission Documents on CSAM”

[11] Limniotis K., MDPI “Cryptography as the Means to Protect Fundamental Human Rights” (2021)

[12] Microsoft, “PhotoDNA” - Διαθέσιμο στο Διαδίκτυο: https://www.microsoft.com/en-us/photodna

[13] Newman L.H., “Australia's Encryption-Busting Law Could Impact Global Privacy” - Ιστοσελίδα “Wired”, (2018) – άρθρο διαθέσιμο στο Διαδίκτυο: https://www.wired.com/story/australia-encryption-law-global-impact/

[14] Reis J., Melo P. et Al “Detecting Misinformation on WhatsApp without Breaking Encryption”, (2020) - Association for the Advancement of AI (www.aaai.org).

[15] Stallings W. “Cryptography and network security”, (2011) - ελληνική έκδοση, Ίων.

[16] Struppek L. et Al. “Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash”, (2022) - Seoul, Republic of Korea

[17] Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων: e-Privacy «Οδηγία 2002/58/ΕΚ» - διαθέσιμη στο Διαδίκτυο: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_el.pdf

[18] Ευρωπαϊκή Επιτροπή, «Κανονισμός 2016/679/ΕΕ - Γενικός Κανονισμός για την Προστασία Δεδομένων», - διαθέσιμος στο Διαδίκτυο: https://www.privacy-regulation.eu/el/index.htm

[19] Ευρωπαϊκή Επιτροπή: Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη «Θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών», (2022) - διαθέσιμη στο Διαδίκτυο: https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0014.02/DOC_1&format=PDF

[20] Ευρωπαϊκό Κοινοβούλιο, «Κανονισμός (ΕΕ) 2021/1232 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου» - διαθέσιμος στο Διαδίκτυο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021R1232&from=EN

[21] Ευρωπαϊκό Συμβούλιο – Συμβούλιο της Ευρωπαϊκής Ένωσης «Η προστασία δεδομένων στην ΕΕ», - διαθέσιμο στο Διαδίκτυο: https://www.consilium.europa.eu/el/policies/data-protection/

[22] Ευρωπαϊκό Συμβούλιο – Συμβούλιο της Ευρωπαϊκής Ένωσης.
«Ο γενικός κανονισμός για την προστασία των δεδομένων – Ενημερωτικό Γράφημα» - διαθέσιμο στο Διαδίκτυο:
https://www.consilium.europa.eu/el/infographics/data-protection-regulation-infographics/

[23] Λιμνιώτης Κ., Σημειώσεις μαθήματος ΑΠΚΥ «ΑΥΔ621-Κρυπτογραφία», (2018).

[24] Χάρτα Θεμελιωδών Δικαιωμάτων της ΕΕ. Διαθέσιμη στο διαδίκτυο:
https://fra.europa.eu/en/eu-charter