

Βελτιώνοντας την Αντιτρομοκρατική Ανταπόκριση

Οδηγός Έξι Βημάτων για την Τήρηση του Κανονισμού ΤΠΔ της ΕΕ

Sophia Rothut, Heidi Schulze, Diana Rieger, Catherine Bouko & Brigitte Naderer
Μετάφραση από τους Μαρκάρ Σανγκογιάν και Σταύρο Δελαβίνια



Tech Against Terrorism Europe (TATE)

Ο παρών οδηγός είναι τμήμα του Tech Against Terrorism Europe (TATE). Το πρόγραμμα TATE χρηματοδοτείται από την Ευρωπαϊκή Ένωση (ISF-2021-AG-TCO-101080101). Το πρόγραμμα υποστηρίζει τους μικρότερους Παρόχους Υπηρεσιών Φιλοξενίας (HSPs) στη δημιουργία των αντιτρομοκρατικών τους πλαισίων και στην υποβολή εκθέσεων διαφάνειας, όπως απαιτείται από τον Κανονισμό σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο (ΤΠΔ) και την Οδηγία 2017/541 της Ε.Ε.

tate.techagainstterrorism.org

Funded by the
European Union



Ομάδα Σύνταξης

Η **Sophia Rothut** είναι επιστημονική συνεργάτιδα στο εργαστήριο του καθηγητή Rieger (LMU Munich). Στο πλαίσιο του ευρωπαϊκού προγράμματος TATE, εργάζεται πάνω στις απαιτήσεις για την αντιμετώπιση του τρομοκρατικού περιεχομένου στο διαδίκτυο. Η έρευνά της επικεντρώνεται στη διαδικτυακή ριζοσπαστικοποίηση, την ενσωμάτωση των ριζοσπαστικών ιδεών και τους πολιτικούς/ακροδεξιούς παράγοντες επιρροής.

Η **Heidi Schulze** είναι επιστημονική συνεργάτιδα στο Τμήμα Μέσων Μαζικής Ενημέρωσης και Επικοινωνίας του LMU του Μονάχου. Στο LMU, είναι μέλος του ερευνητικού εργαστηρίου του καθηγητή Rieger και μελετά τη δυναμική της ριζοσπαστικοποίησης στο διαδίκτυο στο πλαίσιο του μεγάλης κλίμακας ερευνητικού έργου MOTRA - Monitoring System and Transfer Platform Radicalisation. Στην έρευνά της εστιάζει στη ριζοσπαστική/εξτρεμιστική (ομαδική) επικοινωνία σε εναλλακτικές κοινωνικές πλατφόρμες και περιθωριακές κοινότητες, καθώς και στα χαρακτηριστικά και το κοινό των υπερκομματικών ειδησεογραφικών ιστότοπων.

Η **Diana Rieger** είναι Καθηγήτρια στο Τμήμα Μέσων Μαζικής Ενημέρωσης και Επικοινωνίας του LMU του Μονάχου. Διεξάγει έρευνα σχετικά με τη διαδικτυακή ριζοσπαστικοποίηση, τη ρητορική μίσους και τις επιπτώσεις του ψυχαγωγικού περιεχομένου. Έχει επίσης δημοσιεύσει σχετικά με την ανάπτυξη και την αξιολόγηση αντιμέτρων κατά της ριζοσπαστικοποίησης.

Η **Catherine Bouko** είναι αναπληρώτρια καθηγήτρια Επικοινωνίας και Γαλλικών στο Πανεπιστήμιο της Γάνδης (Βέλγιο). Η κύρια έρευνά της αφορά την πολιτική επικοινωνία, τον εξτρεμισμό και την ιδιότητα του πολίτη στα μέσα κοινωνικής δικτύωσης, με ιδιαίτερη έμφαση στην επικοινωνία με βάση την εικόνα. Μεθοδολογικά, χρησιμοποιεί (πολυτροπική) ανάλυση λόγου, ποσοτική ανάλυση περιεχομένου, σημειωτική και εθνογραφία.

Η **Brigitte Naderer** είναι μεταδιδακτορική ερευνήτρια στο Κέντρο Δημόσιας Υγείας, Τμήμα Κοινωνικής και Προληπτικής Ιατρικής, Μονάδα Έρευνας Αυτοκτονιών και Προαγωγής Ψυχικής Υγείας στο Ιατρικό Πανεπιστήμιο της Βιέννης. Προηγουμένως έχει εργαστεί στο Τμήμα Μέσων Μαζικής Ενημέρωσης και Επικοινωνίας του LMU του Μονάχου μέχρι τον Μάρτιο του 2023. Η έρευνά της επικεντρώνεται στην παιδεία στα μέσα ενημέρωσης, τη διαδικτυακή ριζοσπαστικοποίηση και την επίδραση των μέσων ενημέρωσης σε παιδιά και εφήβους.



Ευχαριστίες: Ευχαριστούμε πολύ τους Tech Against Terrorism για τη συμβολή και τα σχόλιά τους επί του παρόντος οδηγού. Επίσης, θέλουμε να ευχαριστήσουμε την Καθηγήτρια Maura Conway για τα πολύτιμα σχόλιά της.

Τη μετάφραση για την ελληνική έκδοση ανέλαβαν οι Μαρκάρ Σανγκογιάν και Σταύρος Δελαβίνιας.

Πίνακας Περιεχομένων

A. Εισαγωγή.....	5
B. Βασικές Υποχρεώσεις και Συστάσεις σε Σχέση με τον Κανονισμό ΤΠΔ.....	9
Κεφάλαιο 1	
Σύνταξη και Εφαρμογή Όρων Παροχής Υπηρεσιών για την Απαγόρευση Τρομοκρατικού Περιεχομένου.....	11
1. Τι είναι οι Όροι Παροχής Υπηρεσιών (ΟΠΥ);	12
2. Γιατί είναι απαραίτητο να υπάρχουν σαφείς και αξιόπιστοι ΟΠΥ;.....	12
3. Πρακτικές συμβουλές και οδηγίες: Ποια είναι τα στοιχεία των αξιόπιστων ΟΠΥ;	13
Κεφάλαιο 2	
Ειδικά μέτρα για τον Εντοπισμό και την Αφαίρεση (Τρομοκρατικού) Περιεχομένου.....	16
1. Καθιέρωση διαδικασιών αναγνώρισης παράνομου και επιβλαβούς περιεχομένου	17
2. Διαδικασία εντοπισμού τρομοκρατικού περιεχομένου	17
3. Πρακτικές συμβουλές και οδηγίες: Τι βοηθά στην αξιολόγηση του κατά πόσον το περιεχόμενο είναι παράνομο;.....	19
4. Τι πρέπει να κάνω αν κρίνω διαφορετικά; Πώς να αμφισβητήσετε μια ληφθείσα εντολή αφαίρεσης	22
Κεφάλαιο 3	
Καθιέρωση Αποτελεσματικών Μηχανισμών Εποπτείας Τρομοκρατικού Περιεχομένου στο Διαδίκτυο	24
1. Τι είναι η εποπτεία περιεχομένου και για ποιό λόγο είναι απαραίτητη σε ορισμένες περιπτώσεις;.....	24
2. Πρακτικές συμβουλές και οδηγίες: Πώς πρέπει να εφαρμόζεται η εποπτεία περιεχομένου;	27
3. Εναλλακτικές μέθοδοι εποπτείας	29
Κεφάλαιο 4	
Καθορισμός Σημείων Επαφής και Νόμιμων Εκπροσώπων.....	32
1. Τι είναι τα σημεία επαφής και οι νόμιμοι εκπρόσωποι;	32
2. Για ποιο λόγο είναι απαραίτητο να υπάρχει σημείο επαφής ή νόμιμος εκπρόσωπος;	33
3. Ποια είναι η αρμόδια αρχή ενός κράτους μέλους της ΕΕ και πώς μπορώ να επικοινωνήσω μαζί της;.....	34
Κεφάλαιο 5	
Καθορισμός Συστήματος Ειδοποίησης Χρηστών και Υποβολής Καταγγελιών για Αφαιρεθέν Περιεχόμενο.....	35
1. Για ποιο λόγο είναι απαραίτητη η δημιουργία ενός διαφανούς μηχανισμού υποβολής καταγγελιών;.....	35
2. Ποιες είναι οι απαιτήσεις για ένα σύστημα υποβολής καταγγελιών;.....	36
3. Πώς πρέπει να διαχειρίζονται οι καταγγελίες και ποια είναι τα πιθανά αποτελέσματα;.....	37
4. Πρακτικές συμβουλές και οδηγίες: Ποια στοιχεία είναι χρήσιμα κατά την δημιουργία ενός συστήματος υποβολής καταγγελιών;.....	37
Κεφάλαιο 6	
Πρακτικές Επισημάνσεις και Συμβουλές Σχετικά με την Υποβολή Εκθέσεων Διαφάνειας	40
1. Τι είναι οι εκθέσεις διαφάνειας;.....	40
2. Γιατί είναι απαραίτητες οι εκθέσεις διαφάνειας;	41
3. Διαδικασία προετοιμασίας των εκθέσεων διαφάνειας	42
4. Ποιες πληροφορίες και μετρήσεις πρέπει να περιλαμβάνονται στην έκθεση διαφάνειας;	44
Γ. Ευχαριστούμε για τη Συνδρομή σας στην Αντιμετώπιση της Τρομοκρατικής Απειλής!.....	45
Δ. Γλωσσάρι	46

A. Εισαγωγή

Τι πραγματεύεται ο οδηγός και γιατί αξίζει να τον διαβάσετε...

Ο παρών οδηγός ασχολείται με τις **υποχρεώσεις των Παρόχων Υπηρεσιών Φιλοξενίας (ΠΥΦ) από τον Ευρωπαϊκό Κανονισμό για το τρομοκρατικό περιεχόμενο στο διαδίκτυο (ΤΠΔ)** που εγκρίθηκε τον Απρίλιο του 2021. Ασχολείται με το τι πρέπει να λάβουν υπόψη οι ΠΥΦ για να αντιμετωπίσουν τη διάδοση τρομοκρατικού περιεχομένου στο διαδίκτυο και παρέχει πρακτικές συμβουλές σχετικά με τον τρόπο εφαρμογής διαφόρων μέτρων για το σκοπό αυτό.

Ο οδηγός επικεντρώνεται κατ' αρχάς στις **ελάχιστες απαιτήσεις που πρέπει να πληρούν οι ΠΥΦ ώστε να συμμορφωθούν με τον Κανονισμό ΤΠΔ**. Κατά δεύτερον, παρέχει **συμβουλές και πρακτικές συμβουλές σχετικά με τα κατάλληλα (προ-)ενεργητικά μέτρα που πρέπει οι ΠΥΦ να υιοθετήσουν** για να περιηγηθούν επιτυχώς στην πολυπλοκότητα της εφαρμογής των ρυθμιστικών διατάξεων (πχ τι να κάνετε όταν εμφανίζεται στο γραμματοκιβώτιό σας μια εντολή απομάκρυνσης) και προετοιμάζει τους ΠΥΦ για την αντιμετώπιση της εκμετάλλευσης των πλατφορμών τους από τρομοκρατικούς δρώντες.

Ο παρών οδηγός αποτελεί μέρος του προγράμματος Tech Against Terrorism Europe (TATE), που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή. Η κοινοπραξία του TATE αποτελείται από 7 φορείς: Dublin City University, Ghent University, JOS Project, LMU Munich, Saher Europe, Swansea University και Tech Against Terrorism. Στόχος του TATE είναι η ενημέρωση σχετικά με τον Κανονισμό ΤΠΔ της ΕΕ και η υποστήριξη μικρών και πολύ μικρών εταιρειών τεχνολογίας προς λήψη μέτρων για τη στήριξη του Κανονισμού. Από κοινού με άλλους πόρους, το πρόγραμμα TATE έχει δημιουργήσει αυτό τον οδηγό για να καταστήσει τις νομικές και πρακτικές προσδοκίες όσο το δυνατόν πιο κατανοητές για τους ΠΥΦ.

Σε ποιους απευθύνεται αυτός ο οδηγός;

Ο οδηγός απευθύνεται σε παρόχους υπηρεσιών φιλοξενίας (ΠΥΦ) και το ανθρώπινο δυναμικό τους, καθώς και σε επαγγελματίες Τεχνολογιών Πληροφοριών (IT) που επιθυμούν να εφαρμόσουν τεχνικά χαρακτηριστικά για την αντιμετώπιση τρομοκρατικού περιεχομένου σε πλατφόρμες. Σκοπός του είναι να παράσχει πληροφορίες σχετικά με τις ελάχιστες προϋποθέσεις που πρέπει να πληρούνται για τη συμμόρφωση με τον Κανονισμό ΤΠΔ της ΕΕ.

Δημιουργήσαμε αυτό τον οδηγό και άλλους πόρους στο πλαίσιο του TATE για την υποστήριξη μικρών και πολύ μικρών ΠΥΦ. Αναγνωρίζουμε πως οι μικροί και οι πολύ μικροί ΠΥΦ συχνά διαθέτουν περιορισμένους πόρους για την αντιμετώπιση του τρομοκρατικού περιεχομένου στις πλατφόρμες τους. **Ωστόσο, είναι εξαιρετικά σημαντικό οι μικροί και οι πολύ μικροί ΠΥΦ να μην παραμελούν την απειλή, καθώς οι μικρότερες πλατφόρμες είναι πιο πιθανό να αξιοποιηθούν από τρομοκρατικούς δρώντες.** (για πληροφορίες, δείτε αυτή την έκθεση του Tech Against Terrorism).

Ποια είναι τα βασικά στοιχεία του Κανονισμού της ΕΕ για το Τρομοκρατικό Περιεχόμενο στο Διαδίκτυο (ΤΠΔ);

Ο Ευρωπαϊκός Κανονισμός για το Τρομοκρατικό Περιεχόμενο στο Διαδίκτυο (ΤΠΔ) εισήλθε σε ισχύ τον Ιούνιο 2022 και **υποχρεώνει τους ΠΥΦ να απομακρύνουν περιεχόμενο ή να διακόπτουν την πρόσβαση σε αυτό εντός μίας ώρας από τη λήψη μιας εντολής αφαίρεσης από μια αρμόδια αρχή.**

Οι ΠΥΦ οφείλουν να συνεργάζονται με τις αρχές επιβολής του νόμου, όπως η Europol, καθώς και με άλλες αρμόδιες αρχές, για τον εντοπισμό και την απομάκρυνση τρομοκρατικού περιεχομένου που μπορεί να υπάρχει στις πλατφόρμες τους. Για να συμμορφωθούν με τον κανονισμό ΤΠΔ, **οι ΠΥΦ πρέπει επίσης να εφαρμόζουν αποτελεσματικά και ανάλογα μέτρα για να αποτρέπουν την εκ νέου ανάρτηση τρομοκρατικού περιεχομένου** και υπόκεινται σε περαιτέρω υποχρεώσεις για τις οποίες θα ενημερωθείτε στον παρών οδηγό

Πώς δομείται ο παρών οδηγός;

Ο Κανονισμός ΤΠΔ απαιτεί επί του παρόντος από τους ΠΥΦ να:

- 1) Συντάσσουν κατάλληλους Όρους Παροχής Υπηρεσιών (► [κεφάλαιο 1](#)),
- 2) Λάβουν ειδικά μέτρα για τον εντοπισμό και την αφαίρεση τρομοκρατικού περιεχομένου (► [κεφάλαιο 2](#)),
- 3) Καθιερώσουν αποτελεσματικούς μηχανισμούς εποπτείας και ελέγχου (► [κεφάλαιο 3](#)),
- 4) Καθορίσουν σημεία επαφής και νομικούς εκπροσώπους (► [κεφάλαιο 4](#)),
- 5) Ρυθμίσουν μηχανισμούς ειδοποίησης χρηστών και καταγγελιών (► [κεφάλαιο 5](#)),
- 6) Δημοσιεύουν εκθέσεις διαφάνειας (► [κεφάλαιο 6](#)).

Διαρθρώσαμε τις επεξηγήσεις και τις συστάσεις που παρέχονται στον παρόντα οδηγό σύμφωνα με αυτές τις έξι κύριες απαιτήσεις. Στην αρχή κάθε κεφαλαίου, θα βρείτε μια σύντομη περίληψη του περιεχομένου του κεφαλαίου και των κύριων σημείων του. Στη συνέχεια, θα σας δοθούν λεπτομερείς πληροφορίες σχετικά με το τι απαιτεί ή παροτρύνει ο Κανονισμός ΤΠΔ ώστε να εφαρμόσουν οι ΠΥΦ, καθώς και περαιτέρω πρακτικές συμβουλές για την προστασία της πλατφόρμας σας από τρομοκρατικό (και άλλο επιβλαβές) περιεχόμενο.

Ποιες πλατφόρμες επηρεάζονται από τον Κανονισμό ΤΠΔ;

Ο Κανονισμός ΤΠΔ επηρεάζει τους Παρόχους Υπηρεσιών Φιλοξενίας, που περιλαμβάνει οποιαδήποτε πλατφόρμα επιτρέπει στους χρήστες να διανέμουν πληροφορίες στο κοινό μέσω των υπηρεσιών της.

Ο Κανονισμός ΤΠΔ ισχύει **για όλους τους ΠΥΦ όλων των μεγεθών και για κάθε ΠΥΦ που προσφέρει τις υπηρεσίες του στην Ε.Ε.** Ισχύει, επίσης, για ΠΥΦ που βρίσκονται εκτός της ΕΕ όταν ένας ΠΥΦ (1) έχει σημαντικό αριθμό χρηστών σε ένα ή περισσότερα κράτη-μέλη της Ε.Ε. ή (2) απευθύνει τις δραστηριότητες του σε ένα ή περισσότερα κράτη-μέλη της Ε.Ε.

Πότε θεωρείται πως ένας ΠΥΦ «εκτίθεται σε τρομοκρατικό περιεχόμενο»;

Ο Κανονισμός ΤΠΔ επιβάλλει συγκεκριμένες υποχρεώσεις στους ΠΥΦ που «εκτίθενται σε τρομοκρατικό περιεχόμενο». Σύμφωνα με το [Άρθρο 5.4](#), η έκθεση αυτή συμβαίνει όταν ένας ΠΥΦ έχει ενημερωθεί κι έχει λάβει δύο ή περισσότερες οριστικές εντολές αφαίρεσης κατά τη διάρκεια των προηγούμενων 12 μηνών από την αρμόδια αρχή του κράτους-μέλους στο οποίο ο ΠΥΦ έχει την κύρια εγκατάσταση του ή το νόμιμο εκπρόσωπό του στην Ε.Ε.

Τι καθιστά τρομοκρατικό περιεχόμενο;

Δεδομένου ότι ο Κανονισμός ΤΠΔ αφορά το τρομοκρατικό περιεχόμενο που διαδίδεται μέσω διαδικτύου, είναι σημαντικό να δοθεί ένας ορισμός. Η [Οδηγία 2017/541 της Ε.Ε.](#) θέτει τη βάση για τον Κανονισμό ΤΠΔ καθορίζοντας τι νοείται ως τρομοκρατικό περιεχόμενο.



Το περιεχόμενο θεωρείται τρομοκρατικό όταν υποκινεί στη διάπραξη πράξεων ή προωθεί προθέσεις υπέρ τρομοκρατικού σκοπού, συμβάλλοντας με αυτόν τον τρόπο άμεσα ή έμμεσα στην απειλή τρομοκρατικών εγκλημάτων.

Η απειλή διάπραξης τρομοκρατικού εγκλήματος λογίζεται επίσης ως τρομοκρατικό περιεχόμενο, όπως και η παροχή πληροφοριών, υποστήριξης ή χρηματοδότησης για τις πράξεις αυτές.

Τύποι τρομοκρατικών εγκλημάτων

Τα τρομοκρατικά εγκλήματα μπορεί να περιλαμβάνουν τα εξής ([Οδηγία 2017/541 της Ε.Ε., άρθρο 3.1](#)):

- Επιθέσεις κατά της ζωής ή της σωματικής ακεραιότητας ενός ατόμου
- Απαγωγή ή ομηρία
- Πρόκληση εκτεταμένων καταστροφών σε συγκεκριμένες εγκαταστάσεις και υποδομές (π.χ. κυβερνητικές/δημόσιες εγκαταστάσεις, συστήματα μεταφορών και πληροφοριών) που ενδέχεται να θέσουν σε κίνδυνο ανθρώπινες ζωές ή να οδηγήσουν σε μεγάλες οικονομικές απώλειες
- Κατάσχεση αεροσκαφών, πλοίων ή άλλων μέσων δημόσιας ή εμπορευματικής μεταφοράς
- Κατασκευή, κατοχή, απόκτηση, μεταφορά, προμήθεια ή χρήση εκρηκτικών υλών ή όπλων και έρευνα και ανάπτυξη χημικών, βιολογικών, ραδιολογικών ή πυρηνικών όπλων.
- Απελευθέρωση επικίνδυνων ουσιών ή πρόκληση πυρκαγιών, πλημμυρών ή εκρήξεων και διακοπή βασικών πόρων (π.χ. νερό, ηλεκτρική ενέργεια) από την οποία κινδυνεύει η ανθρώπινη ζωή.

- Παρεμπόδιση ή διακοπή της παροχής νερού, ηλεκτρικής ενέργειας ή οποιουδήποτε άλλου θεμελιώδους φυσικού πόρου, από τον οποίο κινδυνεύει η ανθρώπινη ζωή.

Η καθοδήγηση τρομοκρατικής ομάδας ή η σκόπιμη συμμετοχή στις δραστηριότητές της θεωρείται επίσης ποινικό αδίκημα ([Οδηγία 2017/541 της Ε.Ε., Άρθρο 4](#)). Αυτό περιλαμβάνει την παροχή (πληροφοριακών) πόρων (π.χ. οδηγίες ή υλικά για την κατασκευή όπλων) για τρομοκρατικούς σκοπούς ή τη χρηματοδότηση τέτοιων δραστηριοτήτων.

Με τα αδικήματα αυτά, οι τρομοκρατικοί δρώντες αποσκοπούν α) στο σοβαρό εκφοβισμό του κοινού, β) στον αδικαιολόγητο εξαναγκασμό μιας κυβέρνησης ή ενός διεθνούς οργανισμού να εκτελέσει (να απόσχει) μια συγκεκριμένη πράξη, ή γ) στη σοβαρή αποσταθεροποίηση ή καταστροφή των θεμελιωδών πολιτικών, συνταγματικών, οικονομικών ή κοινωνικών δομών μιας χώρας ή ενός διεθνούς οργανισμού. ([Οδηγία 2017/541 της Ε.Ε., Άρθρο 3.2](#)).

Συνοψίζοντας, το περιεχόμενο θεωρείται τρομοκρατικό περιεχόμενο όταν επιτρέπει, υποστηρίζει ή διευκολύνει ένα τρομοκρατικό έγκλημα ή όταν περιλαμβάνει απειλή διάπραξης τρομοκρατικού εγκλήματος.

B. Βασικές Υποχρεώσεις και Συστάσεις σε Σχέση με τον Κανονισμό ΤΠΔ

Στα επόμενα κεφάλαια θα βρείτε πληροφορίες σχετικά με έξι βασικά στοιχεία του κανονισμού ΤΠΔ και βήματα για να θωρακίσετε την πλατφόρμα σας απέναντι στην τρομοκρατική απειλή. Αυτές περιλαμβάνουν τους ακόλουθους βασικούς τομείς και ερωτήσεις.

Κεφάλαιο 1: Σύνταξη και Εφαρμογή Όρων Παροχής Υπηρεσιών για την Απαγόρευση Τρομοκρατικού Περιεχομένου

1. Τι είναι οι Όροι Παροχής Υπηρεσιών (ΟΠΥ);
2. Γιατί είναι απαραίτητο να υπάρχουν σαφείς και αξιόπιστοι ΟΠΥ;
3. Πρακτικές συμβουλές και οδηγίες: Ποια είναι τα στοιχεία των αξιόπιστων ΟΠΥ;

Κεφάλαιο 2: Ειδικά Μέτρα για τον Εντοπισμό και την Αφαίρεση (Τρομοκρατικού) Περιεχομένου

1. Γιατί είναι απαραίτητη η καθιέρωση διαδικασιών αναγνώρισης παράνομου και επιβλαβούς περιεχομένου;
2. Διαδικασία εντοπισμού τρομοκρατικού περιεχομένου
3. Πρακτικές συμβουλές και οδηγίες: Τι βοηθά στην αξιολόγηση του κατά πόσον το περιεχόμενο είναι παράνομο;
4. Τι πρέπει να κάνω αν κρίνω διαφορετικά; Πώς να αμφισβητήσετε μια ληφθείσα εντολή αφαίρεσης;

Κεφάλαιο 3: Καθιέρωση Αποτελεσματικών Μηχανισμών Εποπτείας του Τρομοκρατικού Περιεχομένου στο Διαδίκτυο

1. Τι είναι η εποπτεία περιεχομένου και για ποιο λόγο είναι απαραίτητη σε ορισμένες περιπτώσεις;
2. Πρακτικές συμβουλές και οδηγίες: Πώς πρέπει να εφαρμόζεται η εποπτεία περιεχομένου;
3. Εναλλακτικές μέθοδοι εποπτείας

Κεφάλαιο 4: Καθορισμός Σημείων Επαφής και Νόμιμων Εκπροσώπων

1. Τι είναι τα σημεία επαφής και οι νόμιμοι εκπρόσωποι;
2. Για ποιο λόγο είναι απαραίτητο να υπάρχει σημείο επαφής ή νόμιμος εκπρόσωπος;
3. Ποια είναι η αρμόδια αρχή ενός κράτους-μέλους της Ε.Ε. και πώς μπορώ να επικοινωνήσω μαζί της;

Κεφάλαιο 5: Καθορισμός Συστήματος Ειδοποίησης Χρηστών και Υποβολής Καταγγελιών για Αφαιρεθέν Περιεχόμενο

1. Για ποιο λόγο είναι απαραίτητη η δημιουργία ενός διαφανούς μηχανισμού υποβολής καταγγελιών;
2. Ποιες είναι οι απαιτήσεις για ένα σύστημα υποβολής καταγγελιών;

3. Πώς πρέπει να διαχειρίζονται οι καταγγελίες και ποια είναι τα πιθανά αποτελέσματα;
4. Πρακτικές συμβουλές και οδηγίες: Ποια στοιχεία είναι χρήσιμα κατά τη δημιουργία ενός συστήματος υποβολής καταγγελιών;

Κεφάλαιο 6: Πρακτικές Επισημάνσεις και Συμβουλές Σχετικά με την Υποβολή Εκθέσεων Διαφάνειας

1. Τι είναι οι εκθέσεις διαφάνειας;
2. Γιατί είναι απαραίτητες οι εκθέσεις διαφάνειας;
3. Διαδικασία προετοιμασίας των εκθέσεων διαφάνειας
4. Ποιες πληροφορίες και μετρήσεις πρέπει να περιλαμβάνονται στην έκθεση διαφάνειας;

Ο οδηγός εξηγεί τις **πτυχές του Κανονισμού ΤΠΔ, που είναι πιο σημαντικές για τις πλατφόρμες, ενώ παρέχει επίσης πρακτικές συμβουλές σχετικά με τα προληπτικά μέτρα που μπορούν να ληφθούν για την αντιμετώπιση της διάδοσης επιβλαβούς περιεχομένου στο διαδίκτυο**. Τέτοια μέτρα είναι απαραίτητα για την προετοιμασία των πλατφορμών ενάντια στην τρομοκρατική εκμετάλλευση των υπηρεσιών τους - ή στη γλώσσα του Κανονισμού ΤΠΔ: για να είστε σε θέση να χειριστείτε την κατάσταση όταν η πρώτη και κάθε επόμενη εντολή αφαίρεσης φτάσει στο γραμματοκιβώτιό σας.

Κεφάλαιο 1

Σύνταξη και Εφαρμογή Όρων Παροχής Υπηρεσιών για την Απαγόρευση Τρομοκρατικού Περιεχομένου



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Οι Όροι Παροχής Υπηρεσιών (ΟΠΥ) είναι ένα **δεσμευτικό συμφωνητικό** μεταξύ του χρήστη και του Παρόχου Υπηρεσιών Φιλοξενίας (ΠΥΦ), το οποίο καθορίζει την κατάλληλη και επιτρεπόμενη χρήση της πλατφόρμας.
- Οι ΠΥΦ (1) καθορίζουν στους ΟΠΥ τους **τη στρατηγική τους για την αντιμετώπιση της διάδοσης τρομοκρατικού περιεχομένου** και (2) **απαγορεύουν** τη διάδοση **τρομοκρατικού περιεχομένου**.
- Επιπλέον, και υπερβαίνοντας το πεδίο εφαρμογής του Κανονισμού ΤΠΔ, οι ΠΥΦ δύναται και οφείλουν να εξετάζουν το ενδεχόμενο απαγόρευσης άλλων μορφών επιβλαβούς περιεχομένου (π.χ. εξτρεμιστικό περιεχόμενο, ρητορική μίσους).
- Οι ΟΠΥ αποτελούν μια **νομική υποχρέωση** υπό τον Κανονισμό ΤΠΔ και δύναται επίσης να ενσωματώσουν **χρήσιμες προστατευτικές διατάξεις για μια πλατφόρμα**.
- Απαιτούνται διάφορα στοιχεία προκειμένου να καταστούν οι ΟΠΥ σας όσο το δυνατόν πιο ανθεκτικοί, συμπεριλαμβανομένου του ορισμού του τρομοκρατικού περιεχομένου και της γνωστοποίησης της στρατηγικής του ΠΥΦ για την καταπολέμηση του τρομοκρατικού περιεχομένου στην πλατφόρμα της.

Οι κατάλληλοι Όροι Παροχής Υπηρεσιών (ΟΠΥ) αποτελούν τη βάση για την απαγόρευση και, κατά συνέπεια, το χειρισμό του τρομοκρατικού περιεχομένου. Ο Κανονισμός ΤΠΔ προτρέπει ρητά τους ΠΥΦ να καθορίζουν «την πολιτική τους για την αντιμετώπιση της διάδοσης τρομοκρατικού περιεχομένου και συμπεριλαμβάνουν, κατά περίπτωση, εύληπτη εξήγηση της λειτουργίας των ειδικών μέτρων, καθώς και της χρήσης, όπου ενδείκνυται, αυτοματοποιημένων εργαλείων». ([Κανονισμός ΤΠΔ, άρθρο 7.1](#)).

Επιπλέον, και υπερβαίνοντας το πεδίο εφαρμογής του Κανονισμού ΤΠΔ, οι ΠΥΦ δύναται και οφείλουν να **εξετάζουν το ενδεχόμενο απαγόρευσης άλλων μορφών επιβλαβούς περιεχομένου** (π.χ. εξτρεμιστικό περιεχόμενο, ρητορική μίσους, προτροπή στη βία) εντός των ΟΠΥ τους. Με αυτό τον τρόπο, οι ΟΠΥ δύναται να συμβάλουν στη δημιουργία ενός πλαισίου για μια ψηφιακή κουλτούρα των πολιτών.

1. Τι είναι οι Όροι Παροχής Υπηρεσιών (ΟΠΥ);

Οι ΟΠΥ είναι κανόνες που καθορίζονται από και για συγκεκριμένες πλατφόρμες και καθορίζουν (1) τις ευθύνες των ΠΥΦ έναντι των χρηστών τους και (2) την κατάλληλη και επιτρεπόμενη, αλλά και απαγορευμένη συμπεριφορά και περιεχόμενη στην εν λόγω πλατφόρμα. Οι χρήστες οφείλουν να αποδέχονται αυτούς τους όρους αν επιθυμούν να κάνουν χρήση των υπηρεσιών των ΠΥΦ.

Τα συνώνυμα που χρησιμοποιούνται για τους ΟΠΥ είναι, για παράδειγμα, όροι χρήσης, όροι και προϋποθέσεις ή πρότυπα της κοινότητας. Ο Κανονισμός ΤΠΔ χρησιμοποιεί τη φράση «όροι και προϋποθέσεις» και την ορίζει ως «όλους τους όρους, τις προϋποθέσεις και τις ρήτρες, ανεξαρτήτως ονομασίας ή μορφής, που διέπουν τη συμβατική σχέση μεταξύ ενός παρόχου υπηρεσιών φιλοξενίας και των χρηστών του.» ([Κανονισμός ΤΠΔ, άρθρο 2.8](#)).

2. Γιατί είναι απαραίτητο να υπάρχουν σαφείς και αξιόπιστοι ΟΠΥ;

Για μια βαθύτερη ματιά στο γιατί είναι απαραίτητο να υπάρχουν σαφείς και αξιόπιστοι ΟΠΥ, παρουσιάζουμε δύο διαφορετικές οπτικές γωνίες: τη νομική και την εταιρική/επιχειρησιακή.

α) Νομική Οπτική Γωνία

Συμμόρφωση με το δίκαιο (της Ε.Ε.)

Οι ΟΠΥ απαιτείται να συμμορφώνονται με την ισχύουσα (ευρωπαϊκή) νομοθεσία, συμπεριλαμβανομένου του Κανονισμού ΤΠΔ, αλλά και της [Οδηγίας 2017/541 της Ε.Ε.](#), που ενισχύει τον ευρωπαϊκό χειρισμό του τρομοκρατικού περιεχομένου με (1) την παροχή ορισμού του τρομοκρατικού περιεχομένου, (2) τον καθορισμό κυρώσεων γι' αυτό ([Άρθρο 15](#)), (3) την ενίσχυση των δικαιωμάτων και της υποστήριξης των θυμάτων και (4) την αναγνώριση της τρομοκρατίας ως διεθνικής, διασυνοριακής απειλής. Τόσο ο Κανονισμός ΤΠΔ όσο και η Οδηγία προωθούν την ενωσιακή και διεθνή συνεργασία. Οι ΟΠΥ είναι ένα πεδίο όπου οι ΠΥΦ μπορούν να τονίσουν τη δέσμευσή τους για την αντιμετώπιση της τρομοκρατικής δραστηριότητας.

Προστασία του ΠΥΦ από νομική ευθύνη

Οι ΟΠΥ έχουν ως στόχο να προστατεύσουν έναν ΠΥΦ από την ευθύνη (εφόσον οι ΟΠΥ συμμορφώνονται με την ισχύουσα νομοθεσία). Δεδομένου ότι πρόκειται για μια σύμβαση μεταξύ του ΠΥΦ και των χρηστών του, οι ΟΠΥ αποτελούν νομικά δεσμευτική συμφωνία μεταξύ των δύο μερών. Οι ΟΠΥ επιτρέπουν στον ΠΥΦ να θέτει κανόνες για τη (μη) αποδεκτή χρήση σύμφωνα με τις αξίες του ΠΥΦ.

Αιτιολόγηση της (προληπτικής) αφαίρεσης περιεχομένου

Επιπρόσθετα, οι σαφείς ΟΠΥ είναι σημαντικές όταν αντιμετωπίζετε και ελέγχετε προβληματικό περιεχόμενο. Οι ΠΥΦ μπορούν να ανατρέξουν στους ΟΠΥ τους ώστε να δικαιολογήσουν τον έλεγχο του περιεχομένου, εάν περιλαμβάνουν λεπτομερείς

πληροφορίες σχετικά με τις απαγορευμένες πρακτικές περιεχομένου, συμπεριλαμβανομένης της απαγόρευσης της τρομοκρατίας.

β) Εταιρική Οπτική Γωνία

Διατήρηση της επιχειρησιακής δραστηριότητας

Πρώτον, η συμμόρφωση με τη νομοθεσία αποτελεί κεντρικό στοιχείο της επιχειρησιακής δραστηριότητας των ΠΥΦ και, ως εκ τούτου, της επιτυχίας της εταιρείας. Οι ΠΥΦ έχουν ορισμένη ευθύνη έναντι των μετόχων του, οι οποίοι αναμένουν τη συμμόρφωση. Επιπλέον, ενδέχεται να προκύψει οικονομική ευθύνη και κυρώσεις ή βλάβη της φήμης είναι περαιτέρω πιθανές συνέπειες της μη συμμόρφωσης.

Επίδειξη της πολιτικής ευθύνης των ΠΥΦ

Δεύτερον, ως εξέχουσες κοινωνικές οντότητες, οι ΠΥΦ έχουν ευθύνες απέναντι στο κοινό, τόσο συλλογικά όσο και ατομικά. Η ευθύνη απέναντι στο ευρύ κοινό περιλαμβάνει την αντιμετώπιση παράνομων δραστηριοτήτων όπως η τρομοκρατία και τον εντοπισμό και την πρόληψη τρομοκρατικού περιεχομένου πριν αυτό διαδοθεί ευρέως. Δηλώνοντας στους ΟΠΥ πως απαγορεύονται οι παράνομες δραστηριότητες, οι ΠΥΦ θέτουν τα θεμέλια για μια ασφαλέστερη διαδικτυακή σφαίρα και μπορούν να βασίζονται σε αυτά κατά την αντιμετώπιση παράνομου περιεχομένου. Οι σαφείς ΟΠΥ βοηθούν επιπλέον τις εταιρείες να επιδείξουν την ευθύνη τους προς τα μεμονωμένα μέλη του κοινού, οικοδομώντας εμπιστοσύνη μέσω της διαφάνειας. Από την άποψη αυτή, οι ΠΥΦ αποδεικνύουν στους μεμονωμένους χρήστες ότι θα προστατεύονται από επιβλαβές περιεχόμενο στην πλατφόρμα, όταν το περιεχόμενο αυτό απαγορεύεται ρητά και αποτελεσματικά στους ΟΠΥ τους.

3. Πρακτικές συμβουλές και οδηγίες: Ποια είναι τα στοιχεία των αξιόπιστων ΟΠΥ;

Οι ακόλουθες ενότητες παρέχουν καθοδήγηση σχετικά με τα στοιχεία που θα πρέπει να λάβετε υπόψη σας, ως ΠΥΦ, κατά τη σύνταξη των ΟΠΥ στο πλαίσιο του Κανονισμού ΤΠΔ.

Είναι σημαντικό να τονιστεί πως η ανάπτυξη ΟΠΥ είναι μια επαναληπτική διαδικασία: Οι ΟΠΥ μπορεί και πρέπει να προσαρμόζονται εάν είναι απαραίτητο, για παράδειγμα, ως απάντηση στις υποδείξεις των χρηστών και συμβαδίζοντας με τις εθνικές ή διεθνείς νομοθετικές εξελίξεις. Ο Κανονισμός ΤΠΔ απαιτεί αυτό το βαθμό προσαρμοστικότητας: οι ΠΥΦ, αν εκτεθούν σε τρομοκρατικό περιεχόμενο, υποχρεούνται να τροποποιούν τους ΟΠΥ τους, ώστε να το δηλώνουν, καθώς και να **περιγράφουν τα μέτρα που θα ληφθούν για την αντιμετώπιση της κακόβουλης χρήσης της πλατφόρμας για τρομοκρατικούς σκοπούς** ([Κανονισμός ΤΠΔ, άρθρο 5.1](#)).

Συγκεκριμένα, συνιστούμε να δώσετε προσοχή στη **σαφήνεια** και τη **δομή** των ΟΠΥ. Μελέτες δείχνουν ότι οι χρήστες αφιερώνουν ελάχιστο χρόνο στην ανάγνωση των ΟΠΥ και δε δίνουν αρκετή προσοχή στις πληροφορίες που παρουσιάζονται· οι ΟΠΥ λειτουργούν κυρίως ως

υπενθύμηση της γενικής αντίληψης των χρηστών για το τι επιτρέπεται και τι όχι^{1,2}. Για να διευκολυνθεί η πλοήγηση και η κατανόηση των ΟΠΥ, συνιστάται να επενδύσετε χρόνο στον οπτικό σχεδιασμό των ΟΠΥ και να εργαστείτε με σαφείς επικεφαλίδες ή λίστες με κουκκίδες (bullet points). Ενδεχομένως να είναι χρήσιμο να υπενθυμίζετε στους χρήστες κατά διαστήματα τις πτυχές των ΟΠΥ και, εάν έχει εντοπιστεί ύποπτη συμπεριφορά, να προειδοποιείτε για τις πιθανές συνέπειες (πχ μέσω ενός αναδυόμενου παραθύρου)².

Κατά τη σύνταξη και αναθεώρηση των ΟΠΥ, **η ακόλουθη λίστα μπορεί να χρησιμεύσει ως οδηγός για τη βελτιστοποίηση της συμμόρφωσης με τον Κανονισμό ΤΠΔ.**



Δώστε ορισμό του τρομοκρατικού περιεχομένου

Η ύπαρξη λειτουργικών ορισμών της τρομοκρατίας και του τρομοκρατικού περιεχομένου είναι σημαντική για τη λήψη μέτρων κατά του περιεχομένου και της συμπεριφοράς. Οι ορισμοί θα πρέπει να εμφανίζονται στους ΟΠΥ και να αναφέρονται κατά την αξιολόγηση του περιεχομένου. Οι υπάρχοντες ορισμοί που έχουν ήδη παρουσιαστεί και συζητηθεί στον παρών οδηγό (► [βλ. ορισμό εδώ](#)), ιδίως εκείνοι που βασίζονται στην [Οδηγία 2017/541 της Ε.Ε.](#), μπορούν να παράσχουν χρήσιμη καθοδήγηση από αυτή την άποψη.



Γνωστοποιήστε τη στρατηγική σας για την καταπολέμηση του τρομοκρατικού περιεχομένου

Ο κανονισμός ΤΠΔ υποχρεώνει τους ΠΥΦ που εκτίθενται σε τρομοκρατικό περιεχόμενο να εξηγούν στους ΟΠΥ τους τόσο τη στρατηγική τους για την καταπολέμηση της διάδοσης τέτοιου περιεχομένου όσο και κάθε αυτοματοποιημένο μέσο που χρησιμοποιούν (π.χ. στην αναγνώριση απαγορευμένου περιεχομένου· [κεφάλαιο 2](#)). Ο Κανονισμός ΤΠΔ απαιτεί επίσης από τους ΠΥΦ να εφαρμόζουν ειδικά μέτρα μόλις εκτεθούν σε τρομοκρατικό περιεχόμενο (π.χ. συστήματα αναφοράς επιβλαβούς περιεχομένου από τους χρήστες, συστήματα καταγγελιών για την αφαίρεση περιεχομένου· ► [κεφάλαιο 4](#)) ([Κανονισμός ΤΠΔ, άρθρο 7.1](#)).



Χρησιμοποιήστε καταλόγους προσδιορισμού και εξετάστε το ενδεχόμενο σαφούς απαγόρευσης άλλων κατηγοριών επιβλαβών μορφών περιεχομένου

Μια ποικιλία τύπων περιεχομένου μπορεί να είναι επιβλαβής για τους χρήστες, την κοινωνία και την ίδια την πλατφόρμα. Συνεπώς, οι ΠΥΦ θα πρέπει να εξετάζουν τις ακόλουθες πρόσθετες απαγορεύσεις, οι οποίες αντιμετωπίζονται και από άλλα νομικά πλαίσια, όπως ο νόμος περί ψηφιακών υπηρεσιών, και, ως εκ τούτου, να απαγορεύουν περιεχόμενο που περιέχει, για παράδειγμα, ρητορική μίσους ή υποκίνηση σε βία. Σε επίπεδο φορέα, οι τρομοκρατικές ομάδες μπορούν να αποκλείονται από τη χρήση της πλατφόρμας. Οι [κατάλογοι προσδιορισμού](#) (δηλαδή οι επίσημοι κατάλογοι τρομοκρατικών ομάδων που δημοσιεύονται από τα δημοκρατικά κράτη) αποτελούν μια

¹ Obar, J. A., & Oeldorf-Hirsch, A. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*, 23(1), 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>

² Robinson, E. P., & Zhu, Y. (2020). Beyond “I Agree”: Users’ Understanding of Web Site Terms of Service. *Social Media + Society*, 6(1), 1–13. <https://doi.org/10.1177/2056305119897321>

καλή πηγή για τέτοιες απαγορεύσεις. Επιπλέον, οι αρμόδιες αρχές μπορούν να ειδοποιήσουν τους ΠΥΦ για περιεχόμενο που δεν μπορεί να χαρακτηριστεί τρομοκρατικό, αλλά είναι ωστόσο επιβλαβές· η αξιολόγηση του περιεχομένου με βάση τους ΟΠΥ και ο ενδεχόμενος χειρισμός του επιβλαβούς περιεχομένου είναι ευθύνη των ΠΥΦ ([Κανονισμός ΤΠΔ, 40](#)).



Κοινοποιήστε την αποδεκτή χρήση

Οι ΟΠΥ θα πρέπει επίσης να περιγράφουν, με αναφορά στις αξίες και τους σκοπούς των πλατφορμών, ποιες συμπεριφορές χρήσης είναι όχι απλώς αποδεκτές αλλά και ευπρόσδεκτες και ενθαρρυμένες από τους ΠΥΦ. Δεν υπάρχει ένα καθολικό πρότυπο για αυτό – ποικίλλει σε μεγάλο βαθμό ανάλογα με τις λειτουργίες και τις αρχές της πλατφόρμας. Τούτου λεχθέντος, η περιγραφή της αποδεκτής χρήσης δεν απαιτείται ρητά για την εκπλήρωση των υποχρεώσεων του Κανονισμού ΤΠΔ.



Παρέχετε πληροφορίες σχετικά με τον τρόπο αναφοράς απαγορευμένου περιεχομένου

Ένας τρόπος για την αποκάλυψη παράνομου περιεχομένου και περιεχομένου που παραβιάζει τους ΟΠΥ είναι τα συστήματα αναφοράς χρηστών. Ως εκ τούτου, οι ΠΥΦ θα πρέπει να συμπεριλάβουν ένα τμήμα στους ΟΠΥ τους που να εξηγεί τις διαδικασίες για την αναφορά περιεχομένου για το οποίο υπάρχουν υποψίες ότι παραβιάζει τους ΟΠΥ.



Καθορίστε τις συνέπειες παραβίασης των ΟΠΥ

Για να διασφαλιστεί η διαφανής αντιμετώπιση των παραβιάσεων των ΟΠΥ και για να παραμείνουν υπόλογοι απέναντι στο κοινό, οι ΠΥΦ θα πρέπει να ορίζουν σαφώς στους ΟΠΥ τους τις ενέργειες που θα λαμβάνονται κατά των χρηστών ή/και του περιεχομένου για παραβιάσεις των ΟΠΥ. Ωστόσο, σύμφωνα με τον Κανονισμό ΤΠΔ, η εντολή αφαίρεσης από αρμόδια αρχή πρέπει να οδηγεί σε αφαίρεση του περιεχομένου εντός μίας ώρας από την επισήμανσή του. Οι εντολές αφαίρεσης μπορούν επίσης να υλοποιηθούν με αποκλεισμό του περιεχομένου ή γεωγραφικό αποκλεισμό του στην ΕΕ.



Δημοσιεύστε ετήσιες εκθέσεις διαφάνειας

Κατά την προετοιμασία και αναθεώρηση των ΟΠΥ, οι ΠΥΦ θα πρέπει να δεσμεύονται δημόσια για την τακτική δημοσίευση εκθέσεων διαφάνειας. Πρακτικές συμβουλές και ρυθμιστικές απαιτήσεις του Κανονισμού ΤΠΔ για τη δημιουργία εκθέσεων διαφάνειας ακολουθούν στο ► [κεφάλαιο 6](#).

Κεφάλαιο 2

Ειδικά μέτρα για τον Εντοπισμό και την Αφαίρεση (Τρομοκρατικού) Περιεχομένου



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Η ικανότητα των ΠΥΦ να αναγνωρίζουν το περιεχόμενο ως τρομοκρατικό είναι θεμελιώδους σημασίας για την εφαρμογή του κανονισμού ΤΠΔ και πέραν αυτού.
- Σε πολλές περιπτώσεις, οι αποφάσεις που πρέπει να ληφθούν δεν είναι εύκολες και μπορεί να είναι **πολύ συγκυριακές και ευαίσθητες**.
- Τα **θεμελιώδη δικαιώματα**, όπως η ελευθερία της έκφρασης, πρέπει να λαμβάνονται προσεκτικά υπόψη.
- Σε ό,τι αφορά τον κανονισμό ΤΠΔ, οι ΠΥΦ δε χρειάζεται να αξιολογούν τη νομιμότητα του περιεχομένου που επισημαίνεται από μια αρμόδια αρχή. Ωστόσο, από τη στιγμή που έχει εκδοθεί εντολή αφαίρεσης, **τόσο οι ΠΥΦ όσο και οι πάροχοι περιεχομένου (δηλαδή οι χρήστες) έχουν το δικαίωμα να την αμφισβητήσουν**.
- Συνιστάται να δημιουργηθεί μια διαδικασία που ακολουθείται κατά τον εντοπισμό τρομοκρατικού περιεχομένου. Μια τέτοια διαδικασία θα περιλαμβάνει πολλαπλά βήματα.
- Στην αξιολόγηση του περιεχομένου υπεισέρχονται διάφορα πρακτικά ζητήματα, όπως η χρήση καταλόγων ονομασίας ή βάσεων δεδομένων συμβόλων και οι μέθοδοι διεξαγωγής των απαιτούμενων ασκήσεων εξισορρόπησης.
- Επιπλέον, οι διαδικασίες επανεξέτασης διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην ειδική περίπτωση των **διασυνοριακών εντολών αφαίρεσης**, όπου ένας ΠΥΦ δε λαμβάνει την εντολή αφαίρεσης από την αρμόδια αρχή στην οποία έχει την κύρια εγκατάστασή του ή τον νόμιμο εκπρόσωπό του. Στις περιπτώσεις αυτές **εφαρμόζονται ειδικές διαδικασίες**.

Είναι θεμελιώδους σημασίας οι ΠΥΦ να είναι σε θέση να αξιολογούν αν το περιεχόμενο είναι παράνομο ή τρομοκρατικό, προκειμένου να εντοπίζουν προληπτικά τρομοκρατικό περιεχόμενο, καθώς και να αμφισβητούν νομικά τις εντολές αφαίρεσης όταν οι ΠΥΦ πιστεύουν ότι έχουν εκδοθεί εσφαλμένα. Ο σωστός προσδιορισμός του περιεχομένου ως παράνομου και τρομοκρατικού είναι σημαντικός για τη διατήρηση του κατά τα άλλα νόμιμου και μη τρομοκρατικού περιεχομένου στο διαδίκτυο. Τέτοιες αποφάσεις είναι συχνά δύσκολες, και είναι **πάντα απαραίτητο να σταθμίζεται η βλάβη του περιεχομένου έναντι της βλάβης από την παραβίαση του θεμελιώδους δικαιώματος της ελευθερίας της έκφρασης**.

1. Καθιέρωση διαδικασιών αναγνώρισης παράνομου και επιβλαβούς περιεχομένου

Οι διαδικασίες αναγνώρισης περιλαμβάνουν μια καθορισμένη σειρά βημάτων που λαμβάνουν οι εταιρείες ή οι πλατφόρμες για να προσδιορίσουν εάν το περιεχόμενο παραβιάζει τον Κανονισμό ΤΠΔ ή στοιχεία των ΟΠΥ των πλατφορμών. Τα βήματα αυτά θα πρέπει να καθοδηγούν μια μεθοδική αξιολόγηση και να επιτρέπουν την εξαγωγή αιτιολογημένου συμπεράσματος σχετικά με την παρανομία του περιεχομένου.

Τέτοιες αποφάσεις εξισορρόπησης είναι **απαραίτητες για:** α) τη **λήψη προληπτικών μέτρων** κατά του τρομοκρατικού ή/και άλλως επιβλαβούς περιεχομένου και β) την **αμφισβήτηση αμφιλεγόμενων περιπτώσεων εντολών αφαίρεσης** που εκδίδονται από την αρμόδια αρχή βάσει του κανονισμού για την ΤΠΔ (περισσότερες πληροφορίες σχετικά με τη διαδικασία ένδικων μέσων θα ακολουθήσουν στο παρόν κεφάλαιο στην ενότητα ► [υπο-κεφάλαιο 4](#)).

Συνιστάται η λήψη προληπτικών μέτρων κατά του τρομοκρατικού και άλλου επιβλαβούς περιεχομένου για διάφορους λόγους.

1. Με την εφαρμογή τέτοιων μέτρων οι ΠΥΦ επιδεικνύουν αξιοπιστία και καλή θέληση έναντι των πολιτικών φορέων λήψης αποφάσεων, των αρμόδιων αρχών και άλλων σχετικών ενδιαφερομένων μερών.
2. Τα προληπτικά μέτρα οικοδομούν εμπιστοσύνη με τα ενδιαφερόμενα μέρη, επειδή περιορίζουν θετικά τη νομική ευθύνη ή τη ζημία στη φήμη που μπορεί να προκύψει από την τρομοκρατική εκμετάλλευση των πλατφορμών.
3. Η ελλιπής ή ανεπαρκής δράση κατά του τρομοκρατικού, εξτρεμιστικού ή άλλως επιβλαβούς περιεχομένου μπορεί να έχει ως αποτέλεσμα η πλατφόρμα να προσελκύει χρήστες που σκοπεύουν να διανείμουν ακριβώς τέτοιο περιεχόμενο. Συνέπεια αυτού θα ήταν η αυξημένη επικράτηση απαγορευμένου περιεχομένου που, με τη σειρά του, απαιτεί μεγαλύτερες επενδύσεις χρόνου, προσπάθειας και οικονομικών πόρων εκ μέρους των ΠΥΦ για την καταπολέμησή του.

2. Διαδικασία εντοπισμού τρομοκρατικού περιεχομένου

1) Ορισμός τρομοκρατικού περιεχομένου

Κάθε ταξινόμηση του περιεχομένου γίνεται με αναφορά σε έναν ορισμό. Όσον αφορά τον Κανονισμό ΤΠΔ, ο ορισμός του τρομοκρατικού περιεχομένου είναι αυτός που περιέχεται στην [Οδηγία 2017/541 της Ε.Ε.](#), όπως αναφέρεται στην ► [εισαγωγή](#). Ορίζει το τρομοκρατικό περιεχόμενο ως περιεχόμενο κειμένου, οπτικό ή ακουστικό

«υλικό που υποκινεί ή καλεί στην τέλεση ή τη συμβολή στην τέλεση τρομοκρατικών εγκλημάτων, ή που καλεί στη συμμετοχή σε δραστηριότητες τρομοκρατικής ομάδας ή εξυμνεί τρομοκρατικές δραστηριότητες, συμπεριλαμβανομένης της διάδοσης υλικού που απεικονίζει τρομοκρατική επίθεση. Ο ορισμός θα πρέπει επίσης να περιλαμβάνει το περιεχόμενο που παρέχει οδηγίες για την κατασκευή ή χρήση εκρηκτικών, πυροβόλων όπλων ή άλλων όπλων ή επιβλαβών ή επικίνδυνων ουσιών, καθώς και χημικών,

βιολογικών, ραδιολογικών και πυρηνικών ουσιών (ΧΒΡΠ), ή σχετικά με άλλες ειδικές μεθόδους ή τεχνικές, συμπεριλαμβανομένης της επιλογής στόχων, με σκοπό την τέλεση ή τη συμβολή στην τέλεση τρομοκρατικών εγκλημάτων». ([Κανονισμός ΤΠΔ, 11](#))

Ο ορισμός δεν περιλαμβάνει «υλικό που διαδίδεται για εκπαιδευτικούς, δημοσιογραφικούς, καλλιτεχνικούς ή ερευνητικούς σκοπούς ή για σκοπούς αύξησης της ευαισθητοποίησης κατά της τρομοκρατικής δραστηριότητας» ([Κανονισμός ΤΠΔ, 12](#)) και θεμελιώδη δικαιώματα, όπως η ελευθερία της έκφρασης, της πληροφόρησης και της επιστήμης, πρέπει πάντα να λαμβάνονται προσεκτικά υπόψη. «Επιπλέον, η έκφραση ριζοσπαστικών, επιθετικών ή αμφιλεγόμενων απόψεων στο πλαίσιο δημόσιας συζήτησης για ευαίσθητα πολιτικά θέματα δεν θα πρέπει να θεωρείται ότι συνιστά τρομοκρατικό περιεχόμενο». ([Κανονισμός ΤΠΔ, 12](#))

2) Υποστήριξη μέσω της χρήσης αυτοματοποιημένων εργαλείων

Συχνά μπορεί να είναι βοηθητική η χρήση αυτοματοποιημένων εργαλείων για τον προκαταρκτικό εντοπισμό δυνητικά προβληματικού περιεχομένου. Για παράδειγμα, η αυτοματοποίηση μπορεί να χρησιμοποιηθεί για την αναγνώριση συγκεκριμένων [λέξεων-κλειδιών](#) που σχετίζονται με εξτρεμιστικές κοσμοθεωρίες ή [οπτικά στοιχεία](#) όπως λογότυπα ή σύμβολα τρομοκρατικών οργανώσεων. Υπάρχουν επίσης πρωτοβουλίες για τον αυτόματο εντοπισμό δυνητικά τρομοκρατικού περιεχομένου σε όλες τις πλατφόρμες με αναφορά σε μια κοινή βάση δεδομένων (π.χ. η Πλατφόρμα Ανάλυσης Τρομοκρατικού Περιεχομένου [[Terrorist Content Analytics Platform](#) – TCAP] της Tech Against Terrorism ή η [βάση ανταλλαγής ετικετών \(hash\)](#) που διατηρεί το Παγκόσμιο Διαδικτυακό Φόρουμ για την Καταπολέμηση της Τρομοκρατίας [Global Internet Forum to Counter Terrorism – GIFCT]).

3) Υποστήριξη από συστήματα αναφοράς

Εάν ένας ΠΥΦ εκτίθεται σε τρομοκρατικό περιεχόμενο - τυπικά αυτό σημαίνει εάν η αρμόδια αρχή της χώρας που φιλοξενεί την κύρια εγκατάσταση του ΠΥΦ ή ο νόμιμος εκπρόσωπος έχει εκδώσει τουλάχιστον δύο νομικά δεσμευτικές εντολές αφαίρεσης και ο ΠΥΦ έχει ενημερωθεί σχετικά - ο κανονισμός ΤΠΔ απαιτεί ρητά τη λήψη μέτρων για την αποτροπή της περαιτέρω διάδοσης του εν λόγω περιεχομένου ([Κανονισμός ΤΠΔ, άρθρο 5.2](#)). Συνιστάται επίσης η λήψη προληπτικών μέτρων για την επίδειξη προληπτικής συμπεριφοράς. Ένα τέτοιο μέτρο μπορεί να είναι ένα σύστημα αναφοράς που επιτρέπει στους χρήστες να αναφέρουν ύποπτο και απαγορευμένο περιεχόμενο στον ΠΥΦ. Είναι λογικό οι χρήστες να καθορίζουν μια κατηγορία που θα αποδίδουν σε ύποπτο περιεχόμενο, με την τρομοκρατία να αποτελεί μια τέτοια κατηγορία. Αυτό επιτρέπει στους υπαλλήλους που επεξεργάζονται τις αναφορές να ιεραρχούν και να επεξεργάζονται περιεχόμενο ύποπτο για διάδοση τρομοκρατικών ιδεών ταχύτερα. Αυτή η προ-κατηγοριοποίηση μπορεί επίσης να διευκολύνει την προετοιμασία μεταγενέστερων εκθέσεων διαφάνειας - περισσότερα σχετικά στο ► [κεφάλαιο 6](#).

4) Ανάθεση και εξέταση από ανθρώπους διαχειριστές

Η επισήμανση του περιεχομένου μέσω αυτοματοποιημένων εργαλείων ή αναφορών από μεμονωμένους χρήστες είναι το πρώτο βήμα για την ανάδειξη ύποπτου, δυνητικά επικίνδυνου

περιεχομένου. Στη συνέχεια, ωστόσο, είναι συνήθως απαραίτητη η επανεξέταση από ανθρώπους διαχειριστές μέχρι να ληφθεί τελική απόφαση σχετικά με τη δράση που πρέπει να αναληφθεί. Αυτοί οι διαχειριστές θα πρέπει (1) να γνωρίζουν καλά τους κανονισμούς που ισχύουν για την πλατφόρμα, (2) να είναι σε θέση να διακρίνουν το απαγορευμένο περιεχόμενο από το υλικό που εμπλέκει το δικαίωμα στην ελευθερία της έκφρασης και (3) να έχουν ακριβή γνώση των διαφόρων επιλογών διαχείρισης στην πλατφόρμα. Είναι σημαντικό αυτοί οι διαχειριστές να εκπαιδεύονται διαρκώς σχετικά με τις διαδικτυακές στρατηγικές των τρομοκρατών, όμως δεν είναι λιγότερο σημαντική, από δεοντολογική άποψη, η λήψη συμβουλών σχετικά με τις ψυχολογικές επιπτώσεις της αντιμετώπισης προβληματικού περιεχομένου.

5) Απόφαση για τον τρόπο αντιμετώπισης του περιεχομένου

Η διαδικασία που περιγράφεται παραπάνω καταλήγει σε μια απόφαση σχετικά με τον τρόπο αντιμετώπισης του περιεχομένου. Μπορεί να μη γίνει τίποτα και το περιεχόμενο να παραμείνει ενεργό, εάν, αφού σταθμιστούν όλες οι εκτιμήσεις, το περιεχόμενο κριθεί ότι είναι ακίνδυνο. Στο άλλο άκρο, στην περίπτωση εξαιρετικά προβληματικού, επικίνδυνου ή άλλου είδους απαγορευμένου περιεχομένου, όπως οι εκκλήσεις για τρομοκρατικές επιθέσεις, το περιεχόμενο και οι χρήστες μπορεί να μπλοκαριστούν. Ενδιάμεσα, ωστόσο, υπάρχουν επίσης πολυάριθμοι άλλοι τρόποι για να προχωρήσετε με το περιεχόμενο - το περιεχόμενο που δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού ΤΠΔ μπορεί να απαιτεί μια πιο διαφοροποιημένη αντιμετώπιση. Λεπτομέρειες και πρακτικές συστάσεις μπορείτε να βρείτε στο ακόλουθο ► [τρίτο κεφάλαιο](#) σχετικά με τις αποτελεσματικές στρατηγικές ελέγχου.

6) Ειδοποίηση του παρόχου περιεχομένου

Εάν το περιεχόμενο έχει αποκλειστεί, πρέπει να ειδοποιηθεί ο πάροχος περιεχομένου. Για το σκοπό αυτό συνιστάται ένα σύστημα αυτόματης ειδοποίησης και καταγγελίας. Γενικά, για το σκοπό αυτό θα πρέπει να αναπτυχθεί και να δημιουργηθεί μια διαδικασία κατάλληλη για τον ΠΥΦ. Λεπτομέρειες και προτάσεις για το πώς μπορεί να γίνει αυτό σύμφωνα με τον Κανονισμό ΤΠΔ θα βρείτε στο ► [πέμπτο κεφάλαιο](#).

3. Πρακτικές συμβουλές και οδηγίες: Τι βοηθά στην αξιολόγηση του κατά πόσον το περιεχόμενο είναι παράνομο;

Όσον αφορά τον Κανονισμό ΤΠΔ, οι ΠΥΦ δεν υποχρεούνται να αξιολογούν τη νομιμότητα του περιεχομένου, καθώς είναι ευθύνη των αρμόδιων αρχών να το πράξουν πριν από την έκδοση εντολής αφαίρεσης. Ωστόσο, **οι ΠΥΦ υποχρεούνται να εντοπίζουν προληπτικά το τρομοκρατικό περιεχόμενο στις πλατφόρμες τους μόλις εκτεθούν σε τρομοκρατικό περιεχόμενο**. Συχνά είναι δύσκολο να εκτιμηθεί κατά πόσον το περιεχόμενο υπερβαίνει τα νομικά όρια και πρέπει συνεπώς να απαγορευτεί. Επιπλέον, δεν θα πρέπει να παραγνωρίζεται το ψυχολογικό στρες που προκαλείται από τη θέαση προβληματικού περιεχομένου. Οι εργαζόμενοι που συντονίζουν το περιεχόμενο θα πρέπει να έχουν τακτικές ευκαιρίες να αναστοχάζονται για το έργο τους και, αν χρειαστεί, να λαμβάνουν ψυχολογική υποστήριξη.

Για να αξιολογήσετε την παρανομία του περιεχομένου, θα βρείτε παρακάτω ορισμένες ενδείξεις και πρακτικές συμβουλές. Πριν από αυτό, ας ρίξουμε μια ματιά στα σχετικά σημεία σχετικά με την αξιολόγηση του περιεχομένου στον κανονισμό ΤΠΔ:

Η παράγραφος 11 αναφέρει, μεταξύ άλλων:

«Όταν αξιολογούν κατά πόσον ένα συγκεκριμένο υλικό συνιστά τρομοκρατικό περιεχόμενο κατά την έννοια του παρόντος κανονισμού, οι αρμόδιες αρχές και οι πάροχοι υπηρεσιών φιλοξενίας θα πρέπει να λαμβάνουν υπόψη παράγοντες όπως η φύση και η διατύπωση των δηλώσεων, το πλαίσιο στο οποίο διατυπώνονται οι δηλώσεις και η δυνατότητά τους να έχουν επιβλαβείς συνέπειες, επηρεάζοντας κατ'αυτόν τον τρόπο την προστασία και την ασφάλεια προσώπων.» ([Κανονισμός ΤΠΔ, 11](#))

Επιπλέον, τα θεμελιώδη δικαιώματα πρέπει πάντα να σταθμίζονται:

«Όταν κρίνεται κατά πόσον το υλικό που παρέχεται από πάροχο περιεχομένου συνιστά «τρομοκρατικό περιεχόμενο» κατά την έννοια του παρόντος κανονισμού, θα πρέπει να λαμβάνονται υπόψη ιδίως η ελευθερία έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της ελευθερίας και πολυφωνίας των μέσων ενημέρωσης, και η ελευθερία της τέχνης και της επιστήμης. Ειδικότερα στις περιπτώσεις που ο πάροχος περιεχομένου φέρει συντακτική ευθύνη, οποιαδήποτε απόφαση αφαίρεσης του διαδοθέντος υλικού θα πρέπει να λαμβάνει υπόψη τα δημοσιογραφικά πρότυπα που έχουν καθιερωθεί σχετικά με τον Τύπο ή τα μέσα ενημέρωσης σύμφωνα με το δίκαιο της Ένωσης, συμπεριλαμβανομένου του Χάρτη.» ([Κανονισμός ΤΠΔ, 12](#))

Εάν οι ΠΥΦ λάβουν εντολή αφαίρεσης, το περιεχόμενο έχει ήδη χαρακτηριστεί ως τρομοκρατικό από την αρμόδια αρχή. Σε δύο περιπτώσεις είναι χρήσιμο οι ΠΥΦ να είναι αρμόδιοι να μπορούν να ταξινομήσουν το περιεχόμενο ως τρομοκρατικό ή μη τρομοκρατικό:

5. Εάν ένας ΠΥΦ δεν έχει λάβει ακόμη επίσημη εντολή αφαίρεσης, αλλά θέλει **να ενεργήσει προληπτικά** ή/και να επιβάλει τη συμμόρφωση με τους δικούς του ΟΠΥ σε σχέση με ύποπτο περιεχόμενο.
1. Εάν ένας ΠΥΦ λάβει επίσημη εντολή αφαίρεσης, αλλά **έχει αμφιβολίες** σχετικά με την αξιολόγηση του περιεχομένου ως τρομοκρατικού από την αρμόδια αρχή και επιθυμεί να επανεξετάσει τη διαταγή (ως πρώτο βήμα προς την άσκηση ένδικου μέσου).

Παρακάτω θα βρείτε διάφορες μορφές πρακτικής αρωγής για την ταξινόμηση του περιεχομένου ως τρομοκρατικού ή μη τρομοκρατικού.



Χρήση ονομαστικών καταλόγων

Οι εθνικοί και διεθνείς [ονομαστικοί κατάλογοι](#) που κατονομάζουν τρομοκρατικές οργανώσεις παρέχουν ένα καλό πλαίσιο και σημείο αναφοράς για την ταξινόμηση του περιεχομένου. Για παράδειγμα, η υιοθέτηση καταλόγων χαρακτηρισμού ως βάση για την απαγόρευση ή τον αποκλεισμό, οι οποίοι θα πρέπει να αναφέρονται στους ΟΠΥ ([► κεφάλαιο 1](#)), παρέχει στις κυρώσεις μιας πλατφόρμας την υποστήριξη του νόμου. Η παράγραφος 11

του [Κανονισμού ΤΠΔ](#) υποδεικνύει ρητά ότι ο κατάλογος της Ευρωπαϊκής Ένωσης μπορεί να χρησιμοποιηθεί κατά την αξιολόγηση του περιεχομένου.



Χρήση βάσεων δεδομένων με λέξεις-κλειδιά, σύμβολα και λογότυπα

Τα άτομα που ελέγχουν χειροκίνητα το περιεχόμενο θα πρέπει όχι μόνο να έχουν άμεσα διαθέσιμο τον ορισμό του τρομοκρατικού περιεχομένου, αλλά και να γνωρίζουν και να διατηρούν τις γνώσεις τους σχετικά με τις [λέξεις-κλειδιά και τις φράσεις](#) που χρησιμοποιούνται συνήθως από τρομοκρατικές οργανώσεις. Όσο πιο εντατικά ένα άτομο που αξιολογεί το περιεχόμενο είναι εξοικειωμένο με ένα τρομοκρατικό φαινόμενο (π.χ. δεξιό, αριστερό, ισλαμιστικό), τόσο πιο εύκολα μπορεί να αναγνωρίσει τακτικές απόκρυψης, όπως το λεγόμενο «dog whistling», δηλαδή η χρήση φαινομενικά ακίνδυνων λέξεων που έχουν ιδεολογική σημασία εντός του εκάστοτε πλαισίου³. Μια βάση δεδομένων με λογότυπα και σύμβολα, δηλαδή [οπτικά στοιχεία](#) που υποδηλώνουν τρομοκρατικό υπόβαθρο, είναι εξίσου απαραίτητη για την ακριβή και με ρυθμό αξιολόγηση του περιεχομένου.



Συμπερίληψη παραγόντων που σχετίζονται με το πλαίσιο

Η διαχείριση θα πρέπει να λαμβάνει υπόψη το πλαίσιο στο οποίο είναι πιθανό να έχει δημοσιευθεί το περιεχόμενο. Οι σχετικοί παράγοντες του πλαισίου περιλαμβάνουν, μεταξύ άλλων, α) τις πολιτικές συνθήκες, β) τα τρέχοντα γεγονότα, συμπεριλαμβανομένων των πρόσφατων εξελίξεων στις ειδήσεις, και γ) τις πολιτιστικές συνθήκες που ενδέχεται να διαμορφώνουν απόψεις για ορισμένα θέματα. Αυτό είναι συχνά δύσκολο να κριθεί -ιδιαίτερα όταν οι χρήστες είναι ανώνυμοι και το περιεχόμενο που δημοσιεύουν περιέχει ελάχιστες ή καθόλου ενδείξεις κειμένου για την ταυτότητά τους- αλλά σε ορισμένες περιπτώσεις, όταν στο περιεχόμενο γίνεται αναφορά σε εξωτερικούς παράγοντες, οι εκτιμήσεις του πλαισίου αποδεικνύονται χρήσιμες.

Επιπλέον, όταν πρόκειται για **περιεχόμενο που δεν είναι τρομοκρατικό αλλά επιβλαβές με άλλο τρόπο** (π.χ. διάφορες μορφές ρητορικής μίσους), μπορούν να ληφθούν υπόψη τα ακόλουθα σημεία.



Εκτίμηση έκτασης της δυνητικής ζημίας που προκαλείται από το περιεχόμενο

Το τρομοκρατικό, εξτρεμιστικό και περαιτέρω επιβλαβές περιεχόμενο, όπως η ρητορική μίσους ή η υποκίνηση σε βία, ιδίως όταν υποκινεί στη διάπραξη τρομοκρατικών εγκλημάτων, μπορεί να προκαλέσει σημαντική βλάβη. Κατά την αξιολόγηση του περιεχομένου, μπορεί να είναι χρήσιμο να λαμβάνεται υπόψη ο βαθμός στον οποίο το περιεχόμενο μπορεί να αποτελεί αιτιολογικό παράγοντα για την εν λόγω ζημία. Όσο μεγαλύτερη είναι η ζημία που μπορεί να προκληθεί, τόσο πιο γρήγορα και πιο συνειδητά πρέπει να ληφθούν μέτρα. Οι δυσμενείς ψυχολογικές επιπτώσεις σε όσους επηρεάζονται από το επιβλαβές περιεχόμενο θα πρέπει να θεωρούνται ως μορφή ζημίας.

³ Åkerlund, M. (2022). Dog whistling far-right code words: the case of 'culture enricher' on the Swedish web. Information, Communication & Society, 25(12), 1808–1825. <https://doi.org/10.1080/1369118X.2021.1889639>



Εξέταση του πιθανού αντίκτυπου της αφαίρεσης περιεχομένου

Ο κανονισμός ΤΠΔ απαιτεί μια ευαίσθητη εξισορρόπηση των θεμελιωδών δικαιωμάτων που κατοχυρώνονται στον Χάρτη (π.χ. ελευθερία της έκφρασης και της πληροφόρησης) κατά την εξέταση της αφαίρεσης περιεχομένου. Εάν η αφαίρεση δεν έχει διαταχθεί από αρμόδια αρχή, υπάρχουν άλλοι τρόποι με τους οποίους μπορεί να αντιμετωπιστεί το επιβλαβές περιεχόμενο - παραδείγματα των οποίων μπορείτε να βρείτε στο ► [κεφάλαιο 3](#).

4. Τι πρέπει να κάνω αν κρίνω διαφορετικά; Πώς να αμφισβητήσετε μια ληφθείσα εντολή αφαίρεσης

Τι πρέπει να γίνει όταν οι εκτιμήσεις του ΠΥΦ και της αρμόδιας αρχής αντικρούονται;

Οι ΠΥΦ καθώς και ο πάροχος περιεχομένου έχουν το δικαίωμα να αμφισβητήσουν τις εντολές αφαίρεσης σύμφωνα με το [άρθρο 9](#) του κανονισμού ΤΠΔ. Το δικαίωμα αυτό αποτελεί σημαντικό αντίβαρο, ικανό να προασπίσει τα θεμελιώδη δικαιώματα.

Η αμφισβήτηση των αποφάσεων αφαίρεσης γίνεται ενώπιον των δικαστηρίων του κράτους μέλους της ΕΕ του οποίου η αρμόδια αρχή διέταξε την αφαίρεση. **Οι ΠΥΦ υποχρεούνται να φυλάσσουν σε ασφαλείς συνθήκες και για περίοδο έξι μηνών όλο το περιεχόμενο που έχει αφαιρεθεί (είτε ως αποτέλεσμα εντολής αφαίρεσης είτε άλλων μέτρων), καθώς και όλα τα δεδομένα που σχετίζονται με το περιεχόμενο (π.χ. χρόνος δημοσίευσης, πληροφορίες λογαριασμού).** Αυτό βοηθά στη διερεύνηση και την πρόληψη τρομοκρατικών εγκλημάτων ή απειλών και διασφαλίζει ότι υπάρχει επαρκής χρόνος για την άσκηση νομικών προσφυγών κατά της αφαίρεσης του περιεχομένου και, εάν είναι απαραίτητο, για την αποκατάσταση του περιεχομένου ([Κανονισμός ΤΠΔ, 27 & 28](#)).

Ειδική περίπτωση: Διασυνοριακές εντολές αφαίρεσης ([Κανονισμός ΤΠΔ, Άρθρο 4](#))

Εάν οι ΠΥΦ λάβουν εντολή αφαίρεσης από αρμόδια αρχή σε κράτος μέλος της ΕΕ διαφορετική από την «αρχή της έδρας» τους (δηλ. την αρμόδια αρχή του κράτους μέλους στο οποίο ο ΠΥΦ έχει την κύρια εγκατάστασή του ή τον νόμιμο αντιπρόσωπό του- λεπτομέρειες σχετικά με τους νόμιμους αντιπροσώπους ακολουθούν στο ► [κεφάλαιο 4](#)), εφαρμόζεται ειδική διαδικασία.

Κατά την έκδοση της εντολής αφαίρεσης, η αρμόδια αρχή πρέπει επίσης να αποστείλει αντίγραφο της εν λόγω εντολής στην «αρχή της έδρας», η οποία έχει προθεσμία 72 ωρών για να επανεξετάσει την εντολή. Εάν διαπιστωθεί ότι η εντολή αφαίρεσης παραβιάζει θεμελιώδη δικαιώματα και ελευθερίες που κατοχυρώνονται στον Χάρτη, μπορεί να εκδώσει αιτιολογημένη απόφαση, η οποία μπορεί να αποτελέσει ένσταση.

Ο ΠΥΦ πρέπει να απομακρύνει και να ασφαλίσει το περιεχόμενο μόλις λάβει την εντολή αφαίρεσης (όπως και στην περίπτωση εντολής αφαίρεσης από την «αρχή της έδρας»). Ο ΠΥΦ (και ο πάροχος του αφαιρούμενου περιεχομένου) μπορεί να υποβάλει αίτηση επανεξέτασης στην «αρχή της έδρας» εντός 48 ωρών, η οποία δικαιούται να επανεξετάσει την εντολή αφαίρεσης και

να απαντήσει εντός 72 ωρών από την παραλαβή της αίτησης, αφού ενημερώσει την αρμόδια αρχή που διέταξε αρχικά την αφαίρεση ότι διενεργείται επανεξέταση.

Αφότου η αρχή, που αναθεωρεί την εντολή αφαίρεσης, εκδώσει αιτιολογημένη απόφαση, ειδοποιούνται οι σχετικοί φορείς (δηλαδή η αρχή έκδοσης της εντολής, ο ΠΥΦ, ο πάροχος περιεχομένου και η Ευροpol, κατά περίπτωση) και, εάν έχει εντοπιστεί παραβίαση, ο ΠΥΦ μπορεί να αποκαταστήσει αμέσως το περιεχόμενο.

Κεφάλαιο 3

Καθιέρωση Αποτελεσματικών Μηχανισμών Εποπτείας Τρομοκρατικού Περιεχομένου στο Διαδίκτυο



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Κατά την εποπτεία περιεχομένου, το **περιεχόμενο των χρηστών εξετάζεται για να εκτιμηθεί εάν έχουν τηρηθεί ή παραβιαστεί οι νομικοί** (π.χ. Κανονισμός ΤΠΔ, ΠΨΥ) **και ειδικοί κανονισμοί της πλατφόρμας** (π.χ. ΟΠΥ).
- **Εάν ένας κανονισμός παραβιάζεται, το περιεχόμενο «μετριάζεται».** Με άλλα λόγια, λαμβάνονται μέτρα για να περιοριστεί η διάδοση του περιεχομένου.
- Όταν λαμβάνεται **εντολή αφαίρεσης** από αρμόδια αρχή με βάση τον Κανονισμό ΤΠΔ, η **εποπτεία περιλαμβάνει πάντοτε την αφαίρεση του** αντίστοιχου τρομοκρατικού περιεχομένου, αν και οι ΠΥΦ και οι χρήστες μπορούν να το αμφισβητήσουν αν διαφωνούν.
- Διάφορα σημεία πρέπει να λαμβάνονται υπόψη πριν, κατά τη διάρκεια ή αμέσως μετά την ανάληψη των εποπτικών ενεργειών από τον ΠΥΦ, καθώς και σε μεταγενέστερη επανεξέταση. Σε αυτά περιλαμβάνονται η ενημέρωση των χρηστών των οποίων το περιεχόμενο έχει υποστεί μετριοπάθεια και η δυνατότητα προσφυγής κατά της απόφασης.
- Εάν οι πλατφόρμες αναλάβουν **προληπτική δράση κατά άλλων δυνητικά επιβλαβών μορφών περιεχομένου**, όπως η ρητορική μίσους ή οι εξύβριση, ανεξαρτήτως του Κανονισμού ΤΠΔ, μπορούν επίσης να εξεταστούν άλλες **εναλλακτικές προσεγγίσεις εποπτείας**.

1. Τι είναι η εποπτεία περιεχομένου και για ποιό λόγο είναι απαραίτητη σε ορισμένες περιπτώσεις;

Η εποπτεία περιεχομένου περιλαμβάνει την **εξέταση του περιεχομένου που δημιουργείται από χρήστες** στο διαδίκτυο, προκειμένου να **αξιολογηθεί η καταλληλότητα του περιεχομένου** με βάση τους κανονισμούς της πλατφόρμας (π.χ. ΟΠΥ) και τα νομικά πλαίσια (π.χ. [Κανονισμός ΤΠΔ, ΠΨΥ](#))⁴. Οι **κανονισμοί της πλατφόρμας και οι νομικές απαιτήσεις επιβάλλονται μέσω της εποπτείας του περιεχομένου**, ώστε να λαμβάνονται τα απαιτούμενα μέτρα κατά του απαγορευμένου ή/και προβληματικού περιεχομένου. Οι ΠΥΦ οφείλουν να είναι **διαφανείς** όσον αφορά τα συγκεκριμένα μέτρα που λαμβάνονται για τον εντοπισμό και την αφαίρεση τρομοκρατικού περιεχομένου, συμπεριλαμβανομένων των προληπτικών και κατασταλτικών

⁴ Roberts, S.T. (2017). Content Moderation. In L. Schintler & C. McNeely (eds.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1

διαδικασιών εποπτείας περιεχομένου και τυχόν αυτοματοποιημένων εργαλείων που χρησιμοποιούνται.

Η εποπτεία περιεχομένου είναι μια πολύ σημαντική, αλλά και πολύ περίπλοκη και **ευαίσθητη διαδικασία**. Η ύπαρξη των κατάλληλων τεχνικών και γνωστικών πόρων μπορεί να αποτελέσει σημαντική οικονομική επιβάρυνση για τις μικρότερες εταιρείες. Επιπλέον, τρομοκρατικό περιεχόμενο μπορεί να παραχθεί σε όλες τις γλώσσες και είναι εξαιρετικά δαπανηρό να διασφαλιστεί ότι οι συντονιστές είναι σε θέση να αξιολογήσουν το περιεχόμενο σε όλες αυτές τις γλώσσες.

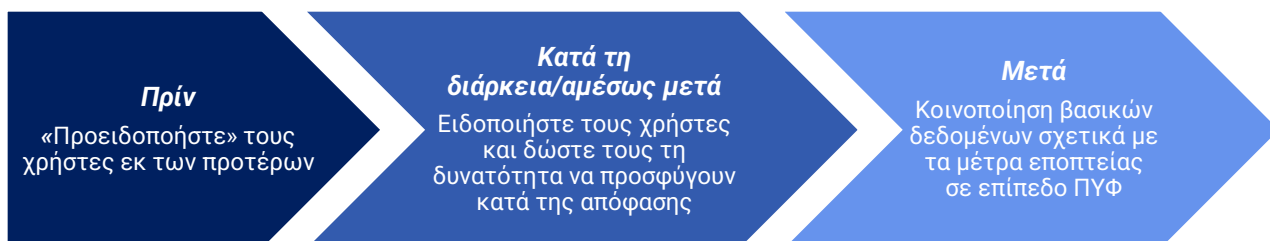
Τα θεμελιώδη δικαιώματα που κατοχυρώνονται στη Διακήρυξη των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα, ιδίως το δικαίωμα στην ελευθερία της έκφρασης, πρέπει πάντα να σταθμίζονται έναντι της βλάβης που προκαλείται από το εν λόγω περιεχόμενο. Από την άλλη πλευρά, οι ΠΥΦ έχουν την κοινωνική ευθύνη να μετριάσουν το επιβλαβές περιεχόμενο στις πλατφόρμες τους.

Ο κατανοητός και διαφανής έλεγχος του περιεχομένου συμβάλλει στην προστασία των χρηστών και των εμπλεκόμενων μερών από τις επιπτώσεις του επιβλαβούς περιεχομένου αλλά και στην οικοδόμηση εμπιστοσύνης. Από τη σκοπιά των ΠΥΦ, η εποπτεία περιεχομένου μπορεί να ενισχύσει τη θέση της προλαμβάνοντας τη νομική ευθύνη μέσω της συμμόρφωσης με την ισχύουσα νομοθεσία και την εξασφάλιση της φήμης έναντι ζημιών που προκαλούνται από την κακή χρήση της πλατφόρμας.

Η εποπτεία περιεχομένου δεν σημαίνει απαραίτητα αφαίρεση περιεχομένου. Αν και η διαγραφή περιεχομένου μπορεί να είναι υποχρεωτική λόγω νομικών απαιτήσεων - όπως συμβαίνει με τις εντολές αφαίρεσης βάσει του Κανονισμού ΤΠΔ - υπάρχουν και άλλοι τρόποι αντιμετώπισης του επιβλαβούς περιεχομένου. Ανάλογα με το πόσο προβληματικό και σοβαρό είναι το περιεχόμενο και τη ζημία που μπορεί να προκαλέσει, μπορούν να εξεταστούν εναλλακτικές επιλογές. Παραδείγματα και προτάσεις εναλλακτικών στρατηγικών μετριασμού μπορείτε να βρείτε στην [ενότητα 3 του παρόντος κεφαλαίου](#).

Οι τεχνικές εποπτείας διαφέρουν από πλατφόρμα σε πλατφόρμα ανάλογα με τη λειτουργικότητά τους, τις προσφερόμενες υπηρεσίες, τις αξίες της πλατφόρμας και την ανοχή στον κίνδυνο⁵. Είναι σημαντικό να είστε όσο το δυνατόν πιο διαφανείς με τον έλεγχο του περιεχομένου. Αυτό περιλαμβάνει διάφορους παράγοντες που πρέπει να λαμβάνονται υπόψη πριν, κατά τη διάρκεια και μετά την εποπτεία, ώστε να διασφαλίζεται ότι οι χρήστες γνωρίζουν τους περιορισμούς στους οποίους μπορεί να υποβληθεί το περιεχόμενό τους.

⁵ Roberts, S.T. (2017). Content Moderation. In L. Schintler & C. McNeely (eds.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1



1. Πρίν: «Προειδοποιήστε» τους χρήστες εκ των προτέρων

Ενημερώστε τους χρήστες σε πρώιμο στάδιο για τις ενέργειες που ενδέχεται να ακολουθήσουν μετά από συμπεριφορά ή περιεχόμενο που απαγορεύεται από τους ΟΠΥ ή από το νόμο. Δηλαδή θα πρέπει να συμπεριλάβετε πληροφορίες σχετικά με τις στρατηγικές εποπτείας στη δεσμευτική συμφωνία με τους χρήστες στους ΟΠΥ ([► κεφάλαιο 1](#)). Αυτό διασφαλίζει επίσης την οικοδόμηση εμπιστοσύνης με τους χρήστες πριν ή κατά τη στιγμή της σύναψης της σχέσης και κάνει κατανοητό ότι δίνετε μια δεσμευτική και ξεκάθαρη διαβεβαίωση ως προς το ότι το προβληματικό και παράνομο περιεχόμενο δεν θα είναι ανεκτό στην πλατφόρμα και ότι εσείς, ως ΠΥΦ, θέλετε να προστατεύσετε τους χρήστες από αυτό.

2. Κατά τη διάρκεια (και αμέσως μετά): Ειδοποιήστε τους χρήστες και δώστε τους τη δυνατότητα να προσφύγουν κατά της απόφασης

Το άρθρο 11 του Κανονισμού ΤΠΔ υποχρεώνει τις ΠΥΦ, πρώτον, να ενημερώνουν τον χρήστη που παρείχε (δηλ. συνέταξε ή/και ανέβασε) το απαγορευμένο (τρομοκρατικό) περιεχόμενο ότι αυτό έχει αποκλειστεί από την πλατφόρμα, και, δεύτερον, να παρέχουν πληροφορίες στον χρήστη σχετικά με το ιστορικό ή την εντολή αφαίρεσης κατόπιν αιτήματος του χρήστη. Η γνωστοποίηση μπορεί να ανασταλλεί προσωρινά από τους ΠΥΦ για περίοδο όχι μεγαλύτερη των έξι εβδομάδων, εάν η αρμόδια αρχή θεωρεί ότι η κοινοποίηση της αφαίρεσης στον χρήστη ενέχει ιδιαίτερο κίνδυνο. Όταν η μη δημοσιοποίηση εξακολουθεί να είναι σημαντική και σκόπιμη, η αρμόδια αρχή μπορεί να παρατείνει την προθεσμία κατά έξι επιπλέον εβδομάδες (Κανονισμός ΤΠΔ, Άρθρο. 11.3). Ο Κανονισμός ΤΠΔ (Άρθρο 10) παρέχει συγκεκριμένους μηχανισμούς για τον χειρισμό τέτοιων καταστάσεων. Συνίσταται η δημιουργία μιας τυποποιημένης αυτόματης διαδικασίας με την οποία οι χρήστες θα ενημερώνονται για τις διαγραφές και θα έχουν τη δυνατότητα να υποβάλουν καταγγελία εναντίον τους. Ο εν λόγω μηχανισμός κοινοποίησης και ένστασης θα πρέπει επίσης να εφαρμόζεται σε περιπτώσεις που δεν εμπίπτουν στον κανονισμό για την ΤΠΔ, αλλά έχουν λάβει χώρα μέσω προληπτικών μέτρων εκ μέρους των παρόχων ΠΥΦ.

3. **Μετά:** Κοινοποίηση βασικών δεδομένων σχετικά με τα μέτρα εποπτείας σε επίπεδο ΠΥΦ

Η διαφάνεια σχετικά με τις αποφάσεις και τα αποτελέσματα της εποπτικής διαδικασίας είναι σημαντική για την εδραίωση της εμπιστοσύνης και της λογοδοσίας μεταξύ των ΠΥΦ και των χρηστών τους και επιβάλλεται όλο και περισσότερο από διάφορους διαδικτυακούς κανονισμούς. Οι εκθέσεις διαφάνειας καταγράφουν πληροφορίες σχετικά με τις εποπτικές αποφάσεις των πλατφορμών, συμπεριλαμβανομένου όχι μόνο του αριθμού και του είδους των παραβιάσεων που εντοπίστηκαν, αλλά και του ακριβούς τρόπου με τον οποίο αντιμετωπίστηκαν οι εν λόγω παραβιάσεις (Περισσότερες λεπτομέρειες σχετικά με τις εκθέσεις διαφάνειας και τις απαιτήσεις διαφάνειας του Κανονισμού ΤΠΔ μπορείτε να βρείτε στο ► [κεφάλαιο 6.](#))

2. Πρακτικές συμβουλές και οδηγίες: Πώς πρέπει να εφαρμόζεται η εποπτεία περιεχομένου;

Είναι σημαντικό για τους ΠΥΦ να διαθέτουν μια σαφή διαδικασία για την εποπτεία περιεχομένου, η οποία μπορεί να προσαρμοστεί σε συγκεκριμένες επαγγελματικές υπηρεσίες και ανάγκες. Είναι ζωτικής σημασίας να εντοπίζεται πρώτα το απαγορευμένο περιεχόμενο και να είναι σε θέση να αξιολογείται η νομιμότητά του, όπως αναλύεται λεπτομερέστερα στο ► [κεφάλαιο 2](#). Προς υπενθύμιση, τα βασικά βήματα είναι:

1. Ορισμός τρομοκρατικού περιεχομένου
2. Υποστήριξη μέσω της χρήσης αυτοματοποιημένων εργαλείων
3. Υποστήριξη από συστήματα αναφοράς
4. Ανάθεση και εξέταση από ανθρώπους διαχειριστές
5. **Απόφαση για τον τρόπο αντιμετώπισης του περιεχομένου**
6. Ειδοποίηση του παρόχου περιεχομένου

Στην παρούσα ενότητα ασχολούμαστε με το βήμα 5. Στο ► [κεφάλαιο 2](#), ονομάσαμε το βήμα αυτό «Απόφαση για τον τρόπο αντιμετώπισης του περιεχομένου». Έχοντας λάβει εντολή αφαίρεσης από αρμόδια αρχή, οι ΠΥΦ πρέπει να αφαιρέσουν το περιεχόμενο και έχουν τη δυνατότητα να ασκήσουν έφεση κατά της εντολής. Οι ΠΥΦ μπορούν επίσης να αποφασίσουν να εντοπίζουν και να αφαιρούν τρομοκρατικό ή απαγορευμένο περιεχόμενο προληπτικά (δηλ. χωρίς εντολές αφαίρεσης).

Ο παρών οδηγός διακρίνει πέντε διαφορετικούς τύπους εποπτείας και ελέγχου: προ-εποπτεία, μετα-εποπτεία, αντιδραστική εποπτεία, αποκεντρωμένη εποπτεία και αυτοματοποιημένη εποπτεία. Σύντομες επεξηγήσεις για τον καθένα, καθώς και τα πλεονεκτήματα και τα μειονεκτήματά τους μπορείτε να βρείτε παρακάτω.

Είδη εποπτείας και ελέγχου	Επεξήγηση
Προ-εποπτεία	Οι συντονιστές ελέγχουν το περιεχόμενο πριν από τη δημοσίευσή του. Πλεονεκτήματα: Υψηλός βαθμός ασφάλειας και συμμόρφωσης του περιεχομένου με τα νομικά πρότυπα και τους ειδικούς κανονισμούς της πλατφόρμας Μειονεκτήματα: Μεγάλη επιβάρυνση από πλευράς πόρων, προσωπικού και οικονομικού κόστους
Μετά-εποπτεία	Οι συντονιστές ελέγχουν το περιεχόμενο αμέσως μετά τη δημοσίευση. Πλεονεκτήματα: Δυνατότητα γρήγορης αλληλεπίδρασης των χρηστών με το περιεχόμενο (λόγω άμεσης δημοσίευσης) Μειονεκτήματα: Σημαντικό κόστος σε χρόνο, προσωπικό και οικονομικούς πόρους - στην περίπτωση απαγορευμένου/βλαβερού περιεχομένου, οι χρήστες εκτίθενται στο περιεχόμενο
Αντιδραστική εποπτεία	Οι συντονιστές ελέγχουν το περιεχόμενο αφότου αναφερθεί από τους χρήστες. Πλεονεκτήματα: Μικρότερη απαίτηση σε πόρους από τους ΠΥΦ. Οικοδόμηση εμπιστοσύνης με χρήστες (λόγω της δυνατότητας υποβολής αναφοράς) Μειονεκτήματα: Responsibility of the users; in the case of prohibited/harmful content, users are still exposed to the content; potential for false alarms requiring additional effort on the part of the HSP
Αποκεντρωμένη εποπτεία	Η κοινότητα των χρηστών ενεργούν ως συντονιστές, συχνά μέσω ενός μηχανισμού ανοδικών (upvote) και καθοδικών (downvote) ψήφων, ο οποίος χρησιμεύει ως μέτρηση της αξιοπιστίας του περιεχομένου και τελικά καθορίζει τη δημόσια εμβέλεια του περιεχομένου (δηλ. το περιεχόμενο με πολλές ανοδικές ψήφους κατατάσσεται υψηλότερα και αποκτά μεγαλύτερη εμβέλεια). Πλεονεκτήματα: Λιγότερη απαίτηση σε πόρους από τους ΠΥΦ. Ενθάρρυνση εμπλοκής χρηστών. Αυτορύθμιση Μειονεκτήματα: Αυξάνεται η ευθύνη των χρηστών. οι χρήστες εκτίθενται σε απογερευμένο/επιβλαβές περιεχόμενο. Επιρρέπεια σε συντονισμένες χειριστικές συμπεριφορές εκ μέρους κακόβουλων χρηστών
Αυτοματοποιημένη εποπτεία	Μοντέλα βασισμένα στην τεχνητή νοημοσύνη (π.χ. φίλτρα, αλγόριθμοι) λειτουργούν ως συντονιστές. Πλεονεκτήματα: Λιγότερο απαιτητική σε πόρους μετά την εγκατάστασή της. Έγκαιρος, γρήγορος και εξαιρετικά ευέλικτος εντοπισμός δυνητικά κακόβουλου περιεχομένου Μειονεκτήματα: Επιρρέπεια σε σφάλματα, ιδίως όσον αφορά τη λανθασμένη διαγραφή περιεχομένου (προβληματική στο πλαίσιο της ελευθερίας της

έκφρασης, επομένως σημαντική η ανθρώπινη αξιολόγηση). Απαραίτητη η συνεχής συντήρηση και προσαρμογή σε νέες εξελίξεις

(Σύμφωνα με Grimes-Viort, 2010)⁶

Συνιστάται ο συνδυασμός διαφόρων προσεγγίσεων για τη διαχείριση του περιεχομένου. Η αντιδραστική εποπτεία, για παράδειγμα, μπορεί εύκολα να συνδυαστεί με την προ-εποπτεία ή τη μετα-εποπτεία. Στις περισσότερες περιπτώσεις, **οι συνδυασμοί είναι πολύ χρήσιμοι και σε ορισμένες περιπτώσεις μπορεί να είναι ακόμη και απαραίτητοι**. Οι αυτοματοποιημένες αποφάσεις εποπτείας πρέπει πάντοτε να επανεξετάζονται ή τουλάχιστον να ενημερώνονται με ανθρώπινη επανεξέταση, ώστε να αποφεύγονται συστηματικές παραβιάσεις των θεμελιωδών δικαιωμάτων των χρηστών και κίνδυνοι για την ελευθερία της έκφρασης.

Να έχετε υπόψη σας ότι οι εξτρεμιστικοί και τρομοκρατικοί δρώντες μπορούν να χρησιμοποιούν **τακτικές για να αποφεύγουν τις γνωστές μεθόδους εποπτείας περιεχομένου**, λειτουργώντας κρυφά και παρακάμπτοντας έτσι την εποπτεία, ιδίως τους αυτοματοποιημένους μηχανισμούς. Γνωστές τακτικές περιλαμβάνουν τη χρήση συντόμευσης URL (*Ενιαίος Ενοπιστής Πόρων - Uniform Resource Locator*) για να παρακάμψουν τα φίλτρα ή τα συστήματα αποκλεισμού ιστοσελίδων, την ανάρτηση ή τη δημιουργία πανομοιότυπου περιεχομένου/λογαριασμών πολλές φορές για να παρακάμψουν τους συντονιστές και να έχουν εφεδρικά αντίγραφα διαθέσιμα σε περίπτωση διαγραφής, ή την *εσκεμμένη επιλογή (λανθασμένης) ορθογραφίας μιας λέξης* για να ξεφύγουν από τα αυτοματοποιημένα φίλτρα λέξεων. Το εύρος των τεχνικών αποφυγής υπογραμμίζει τη σημασία της ανθρώπινης αξιολόγησης.

Η ενασχόλησή σας με τον παρόντα οδηγό ή η συμμετοχή σας στο διαδικτυακό μάθημα που προσφέρεται επίσης στο πλαίσιο του προγράμματος TATE (με δυνατότητα πιστοποίησης), δείχνει ότι ενδιαφέρεστε για αυτές τις τάσεις. Μπορείτε να βρείτε περισσότερα παραδείγματα αποφυγής της εποπτείας περιεχομένου, καθώς και εφικτές και αποτελεσματικές λύσεις στην πλατφόρμα ανταλλαγής γνώσεων “Tech Against Terrorism’s Knowledge Sharing Platform”, η οποία είναι διαθέσιμη [εδώ](#).

3. Εναλλακτικές μεθόδους εποπτείας

Εποπτεία δεν συνεπάγεται πάντοτε διαγραφή περιεχομένου. Εναλλακτικές προσεγγίσεις, όπως αυτές που προτείνονται παρακάτω, μπορεί να ενδιαφέρουν τους ΠΥΦ που επιδιώκουν να ελέγχουν προληπτικά το περιεχόμενο πέραν των απαιτήσεων του κανονισμού ΤΠΔ. Είναι σημαντικό να τονιστεί ότι τέτοιες εναλλακτικές μεθόδους εποπτείας **δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού ΤΠΔ και μπορούν να χρησιμοποιηθούν μόνο όταν οι πλατφόρμες δεν έχουν λάβει εντολή αφαίρεσης, αλλά θέλουν να ελέγχουν προληπτικά για μη τρομοκρατικό, αλλά κατά τα άλλα επιβλαβές περιεχόμενο**. Όταν λαμβάνετε εντολή αφαίρεσης, η διαδικασία είναι σαφής: πρέπει να αφαιρέσετε το περιεχόμενο και δεν τίθεται θέμα εναλλακτικών προσεγγίσεων.

⁶ Grimes-Viort, B. (2010, December 7). 6 types of content moderation you need to know about. *Social Media Today*. <https://www.socialmediatoday.com/content/6-types-content-moderation-you-need-know-about>



ΕΠΙΘΥΜΕΙΤΕ ΝΑ ΚΑΝΕΤΕ ΠΕΡΙΣΣΟΤΕΡΑ ΓΙΑ ΝΑ ΔΙΑΤΗΡΗΣΕΤΕ ΤΗΝ ΠΛΑΤΦΟΡΜΑ ΣΑΣ ΑΣΦΑΛΗ;

Αποκρύψτε περιεχόμενο

Οι ΠΥΦ μπορούν να αποκρύπτουν μερικώς/πλήρως περιεχόμενο και να αποφεύγουν τον αποκλεισμό του, εάν πιστεύουν ότι οι χρήστες μπορεί να θεωρούν το περιεχόμενο προσβλητικό ή δυσάρεστο, αλλά είναι ωστόσο θεμιτό, νόμιμο και επιτρεπτό σε ολόκληρη την πλατφόρμα. Η απόκρυψη περιεχομένου από άτομα που ανήκουν σε ευάλωτες ομάδες ή από άτομα που βρίσκονται σε χώρα που το περιεχόμενο είναι παράνομο (ενώ επιτρέπεται σε άλλες χώρες) είναι μια τέτοια περίπτωση. Για την απόκρυψη περιεχομένου μπορούν να χρησιμοποιηθούν διάφορες τεχνικές λειτουργίες, όπως φίλτρα σύνδεσης ή ιστοδιοδίων (paywall), ασφαλής λειτουργία (αναζήτησης) για την εμφάνιση περιεχομένου κατάλληλου για την ηλικία και γεωγραφικό ή χρονικό αποκλεισμό.

Αποδέσμευση περιεχομένου από τους μηχανισμούς ανταμοιβής («απεμπλοκή»)

Η αποδέσμευση/απεμπλοκή στερεί από συγκεκριμένο περιεχόμενο ή χρήστες τις μετρήσεις εμπλοκής, αποθαρρύνει τη δραστηριότητα γύρω από την ανάρτηση και δεν «ανταμείβει» το περιεχόμενο της ανάρτησης. Ωστόσο, το περιεχόμενο και ο λογαριασμός του χρήστη παραμένουν στην πλατφόρμα. Η αποδέσμευση/απεμπλοκή περιορίζει την προβολή αναρτήσεων ή λογαριασμών στην πλατφόρμα. Τυπικές τακτικές απεμπλοκής περιλαμβάνουν την απενεργοποίηση λειτουργιών της πλατφόρμας, όπως, στην περίπτωση πολλών κοινωνικών δικτύων, τη δυνατότητα διάδρασης (να κάνετε like), να σχολιάζετε ή να μοιράζεστε αναρτήσεις, έτσι ώστε η ανάρτηση να μπορεί μόνο να διαβαστεί, τη στέρηση δυνατότητας αποκόμισεις οικονομικού οφέλους από το περιεχόμενο, ή την κατάργηση της πιστοποίησης (δηλ. την αφαίρεση κάθε πιστοποίησης της ταυτότητας του λογαριασμού ή του χρήστη). Τέτοιου είδους κυρώσεις μπορεί να δημιουργούνται αλλά και να ενισχύονται από την αλλαγή της αντιμετώπισης του περιεχομένου ή του λογαριασμού από τον αλγόριθμο της πλατφόρμας: η υποβάθμιση του περιεχομένου σημαίνει ότι είναι πιο δύσκολο να διαδοθεί ευρέως και να προωθηθεί μέσω των μηχανισμών της πλατφόρμας (αλγοριθμικά συστήματα συστάσεων).

Επισυνάψτε ενημερωτικές επισημάνσεις στο περιεχόμενο

Ο στόχος των ενημερωτικών ή επικοινωνιακών τακτικών είναι να προσφέρουν στους χρήστες πρόσθετες πληροφορίες, ώστε να μπορούν τελικά να αποφασίσουν οι ίδιοι αν θέλουν να δουν το περιεχόμενο ή όχι. Εντέλει είναι η πλατφόρμα που αποφασίζει ποιο περιεχόμενο προβάλλεται με τέτοιες σημειώσεις, τι περιλαμβάνουν αυτές οι σημειώσεις, για ποια κατηγορία επιβλαβών στοιχείων προειδοποιούνται οι χρήστες και πόσες πρόσθετες πληροφορίες προσφέρονται.

Μια γνωστή πρακτική που χρησιμοποιούσε το (προηγουμένως) Twitter είναι να προειδοποιεί τους χρήστες ότι μπορεί να υπάρχει επιβλαβές περιεχόμενο σε μια ανάρτηση, όπως παραπληροφόρηση ή θεωρίες συνωμοσίας, και να επιτρέπει στους χρήστες να βλέπουν το περιεχόμενο μόνο αφού επιβεβαιώσουν ενεργά ότι το επιθυμούν κάνοντας κλικ σε ένα κουμπί. Ιδιαίτερα στην περίπτωση πολιτικο-ιδεολογικού περιεχομένου που μπορεί να προάγει τη ριζοσπαστικοποίηση, οι εναλλακτικές αφηγήσεις και οι σύνδεσμοι με εκπαιδευτικές πληροφορίες μπορούν να ευαισθητοποιήσουν τους ανθρώπους για τις πιθανές επιπτώσεις αυτού του περιεχομένου.

Παραχωρήστε ευθύνες και αρμοδιότητες στους χρήστες (ενδυνάμωση κοινότητας)

Η λογική των μηχανισμών εποπτείας που βασίζονται στην ενδυνάμωση της κοινότητας είναι να επιτρέπουν στους ίδιους τους χρήστες να δημιουργούν τον ψηφιακό χώρο που φαντάζονται. Οι στρατηγικές αυτές μπορεί να έχουν ιδιαίτερο ενδιαφέρον για πλατφόρμες στις οποίες η ιδέα της κοινότητας είναι σημαντική ή των οποίων οι πρακτικές συντονισμού εξαρτώνται ήδη σε κάποιο βαθμό από την υποστήριξη των χρηστών. Αυτές οι προσεγγίσεις εποπτείας ακολουθούν μια μέθοδο αποκεντρωμένης εποπτείας. Εκτός από τη λειτουργία ανοδικής (upvote) και καθοδικής (downvote) ψηφοφορίας που έχει ήδη αναφερθεί, περιλαμβάνεται επίσης και η δυνατότητα των χρηστών να αποκλείουν ή να θέτουν σε σίγαση συγκεκριμένους λογαριασμούς, κάτι που προσφέρει ήδη μεγάλος αριθμός πλατφορμών, ή τη χρήση διαχειριστών/συντονιστών από την ίδια την κοινότητα. Με αυτό συνδέεται στενά η έννοια των «αξιόπιστων πηγών επισήμανσης παράνομου περιεχομένου», η οποία εξετάζεται στην Πράξη για της Ψηφιακές Υπηρεσίες ([Άρθρο 22](#)). Η έννοια αναφέρεται σε χρήστες οι οποίοι είναι ιδιαίτερα αξιόπιστοι και ικανοί να αξιολογούν την παρανομία του περιεχομένου και να το αναφέρουν (αντικειμενικά και γρήγορα). Οι χρήστες αυτοί εκπροσωπούν συλλογικά συμφέροντα (προσανατολισμένα στη δημόσια ευημερία) ανεξάρτητα από τη συγκεκριμένη διαδικτυακή πλατφόρμα. Το περιεχόμενο που αναφέρεται με αυτόν τον τρόπο πρέπει να επεξεργάζεται κατά προτεραιότητα και άμεσα από την πλευρά του ΠΥΦ.

Αυτές οι εναλλακτικές μέθοδοι εποπτείας μπορεί να είναι σχετικές ακόμη και όταν οι πλατφόρμες δεν υποχρεώνονται από τον Κανονισμό ΤΠΔ να αναλάβουν δράση. Ανεξαρτήτως της μορφής που θα λάβει, ο Κανονισμός ΤΠΔ επιτρέπει μια προληπτική προσέγγιση: εάν, κατά τη διάρκεια των προληπτικών, δικών του μέτρων μετριασμού, ο ΠΥΦ συναντήσει περιεχόμενο που αφορά επικείμενη απειλή για τη ζωή ή τρομοκρατική ενέργεια, αυτό πρέπει να διαγραφεί και να ενημερωθεί αμέσως η αρμόδια αρχή του κράτους μέλους της ΕΕ που επηρεάζεται από αυτό ([Κανονισμός ΤΠΔ, Άρθρο 14.5](#)).

Περισσότερες λεπτομέρειες σχετικά με τις (τεχνικές) μεθόδους που απαιτούνται για αυτές τις εναλλακτικές προσεγγίσεις, καθώς και τα πλεονεκτήματα και μειονεκτήματά τους αλλά και μελέτες περιπτώσεων, παρέχονται από το Tech Against Terrorism [εδώ](#).

Κεφάλαιο 4

Καθορισμός Σημείων Επαφής και Νόμιμων Εκπροσώπων



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Ο Κανονισμός ΤΠΔ διακρίνει μεταξύ σημείων επαφής και νομίμων εκπροσώπων.
- **Σημεία επαφής οφείλουν να οριστούν από κάθε ΠΥΦ και είναι υπεύθυνα για τη λήψη των εντολών αφαίρεσης και την άμεση διεκπεραίωσή τους.**
- **Εάν ο ΠΥΦ δεν εδρεύει εντός της ΕΕ, πρέπει να οριστεί, επίσης, ένας νόμιμος εκπρόσωπος.** Το πρόσωπο αυτό είναι υπεύθυνο για την παραλαβή, τη συμμόρφωση και την εφαρμογή του Κανονισμού ΤΠΔ. Ο νόμιμος εκπρόσωπος μπορεί, αλλά δεν είναι υποχρεωμένος, να ενεργεί ταυτόχρονα ως σημείο επαφής.
- Κάθε ΠΥΦ, ανεξάρτητα από το αν έχει εκτεθεί ή όχι σε τρομοκρατικό περιεχόμενο, πρέπει να δημιουργήσει ένα σημείο επαφής και, όπου είναι απαραίτητο, έναν νομικό εκπρόσωπο σύμφωνα με τον Κανονισμό ΤΠΔ.

Ο Κανονισμός ΤΠΔ ορίζει ότι όλοι οι ΠΥΦ που επηρεάζονται από τον εν λόγω κανονισμό (δηλαδή εμπίπτουν στο πεδίο εφαρμογής του κανονισμού εξ ορισμού: ► [δείτε την ενότητα σχετικά με τις πλατφόρμες που επηρεάζονται στην εισαγωγή](#)) υποχρεούνται να ορίσουν σημείο επαφής ή νόμιμο εκπρόσωπο.

1. Τι είναι τα σημεία επαφής και οι νόμιμοι εκπρόσωποι;

Σημείο επαφής (Κανονισμός ΤΠΔ, παράγραφος 42 & άρθρο 15)

- **Σκοπός:** Τα σημεία επαφής των ΠΥΦ διευκολύνουν την άμεση διεκπεραίωση των εντολών απομάκρυνσης. Συνεπώς, το σημείο επαφής εξυπηρετεί μόνο επιχειρησιακούς σκοπούς.
- **Διοικητική μέριμνα:** Το σημείο επαφής θα πρέπει να είναι σε θέση να λαμβάνει και να διαβιβάζει ηλεκτρονικά τις εντολές απομάκρυνσης, είτε βρίσκεται εντός της επιχείρησης είτε είναι εξωτερικός συνεργάτης.
- **Απαραίτητοι πόροι:** Το σημείο επαφής πρέπει να διαθέτει επαρκή τεχνική ικανότητα, πρόσβαση και να είναι στελεχωμένο κατά τρόπο ώστε να μπορούν να διεκπεραιώνονται οι εντολές αφαίρεσης δίχως καθυστέρηση. Δεδομένου ότι το τρομοκρατικό περιεχόμενο πρέπει να αφαιρείται εντός μίας ώρας από την παραλαβή της εντολής αφαίρεσης, αυτό σημαίνει ότι το σημείο επαφής πρέπει να είναι διαθέσιμο 24/7.
- **Τοποθεσία:** Το σημείο επαφής δεν είναι απαραίτητο να βρίσκεται εντός της ΕΕ.
- **Επικοινωνία:** Η γλώσσα επικοινωνίας με το σημείο επαφής θα πρέπει να αναφέρεται στις πληροφορίες σχετικά με τη διαθεσιμότητά του. Προκειμένου να καταστεί δυνατή η επικοινωνία μεταξύ των ΠΥΦ και των αρμόδιων αρχών των κρατών μελών, θα πρέπει να

χρησιμοποιείται τουλάχιστον μία επίσημη γλώσσα της ΕΕ. Η γλώσσα αυτή θα πρέπει να είναι η γλώσσα στην οποία είναι επίσης διαθέσιμοι οι όροι παροχής υπηρεσιών (ΟΠΥ) της πλατφόρμας.

Νόμιμος εκπρόσωπος (Κανονισμός ΤΠΔ, Άρθρο 17)

- **Αναγκαιότητα:** Εάν ο ΠΥΦ δεν έχει την κύρια έδρα του στην ΕΕ, πρέπει να οριστεί νόμιμος εκπρόσωπος. Πρόκειται για ένα φυσικό ή νομικό πρόσωπο που βρίσκεται σε ένα από τα κράτη μέλη της ΕΕ στα οποία ο ΠΥΦ προσφέρει τις υπηρεσίες του.
- **Σκοπός:** Ο εν λόγω νόμιμος εκπρόσωπος είναι αρμόδιος για τη λήψη, τη συμμόρφωση και την εφαρμογή του Κανονισμού ΤΠΔ και συγκεκριμένα τις εντολές αφαίρεσης.
- **Πόροι:** Οι ΠΥΦ πρέπει να παρέχουν στους νόμιμους εκπροσώπους τους την εξουσία, τις ικανότητες και τους πόρους για τη συμμόρφωση με τον Κανονισμό ΤΠΔ και να συνεργάζονται με τις αρμόδιες αρχές.
- **Ευθύνη:** Οι νόμιμοι εκπρόσωποι μπορούν να θεωρηθούν υπεύθυνοι για παραβάσεις του Κανονισμού ΤΠΔ.
- **Σχέση με το σημείο επαφής:** Ο νόμιμος εκπρόσωπος μπορεί επίσης να ενεργεί ταυτόχρονα ως σημείο επαφής, αλλά δεν είναι υποχρεωμένος να το κάνει.

2. Για ποιο λόγο είναι απαραίτητο να υπάρχει σημείο επαφής ή νόμιμος εκπρόσωπος;

Στα άλλα κεφάλαια εξετάζονται πολλές επιλογές που μπορεί να είναι ελκυστικές για τους ΠΥΦ και από επιχειρηματική άποψη, αλλά ο κύριος λόγος και το κύριο επιχείρημα για τη **δημιουργία ενός σημείου επαφής ή τον ορισμό ενός νομικού εκπροσώπου** είναι ότι **είναι υποχρεωτικό**. Αυτό μπορεί να συνεπάγεται κάποια ανακατανομή πόρων, προβαίνοντας εγκαίρως στον ορισμό των αρμόδιων, αλλά είναι αναμφισβήτητη προς το συμφέρον των ΠΥΦ να συμμορφωθούν με τον νόμο και να αποφύγουν τις αρνητικές συνέπειες της μη συμμόρφωσης, όπως η μείωση της υπόληψης, της εμπιστοσύνης και των χρημάτων, εάν επιβληθούν πρόστιμα.

Οι ΠΥΦ πρέπει να επιτρέπουν στις αρμόδιες αρχές να εξετάζουν τις πληροφορίες σχετικά με το σημείο επαφής και στη συνέχεια να παρέχουν ηλεκτρονικές κοινοποιήσεις (π.χ. να υποβάλλουν ηλεκτρονικά εντολή αφαίρεσης). Συνήθως, αυτό συνεπάγεται την παροχή μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου (για παράδειγμα, στην ενότητα «Επικοινωνία» του δικτυακού τόπου του ΠΥΦ) μέσω της οποίας η αρμόδια αρχή μπορεί να προσεγγίσει το σημείο επαφής.

Πρέπει να τονιστούν δύο πτυχές του διορισμού νόμιμου εκπροσώπου. Πρώτον, **η ταυτότητα του νόμιμου εκπροσώπου πρέπει να δημοσιοποιηθεί** (βλ. σημείο επαφής). Δεύτερον, **ο ΠΥΦ πρέπει να κοινοποιεί ενεργά τον διορισμό στην «αρμόδια αρχή του τόπου προέλευσής»** (δηλαδή στην αρμόδια αρχή του κράτους μέλους όπου είναι εγκατεστημένος ο νόμιμος εκπρόσωπος).

Η Europol έχει επίσης αναπτύξει μια πλατφόρμα, [Plateforme Européenne de Retraits de Contenus illicites sur Internet \(European platform for takedown of illicit content online\)](#), ή εργαλείο **PERCI**, για την υποστήριξη της εφαρμογής του Κανονισμού ΤΠΔ. Σκοπός του εργαλείου PERCI είναι να διασφαλίσει ότι οι ΠΥΦ μπορούν να λαμβάνουν εντολές απομάκρυνσης από τα Κράτη Μέλη (Κ-Μ)

μέσω ενός κοινού ασφαλούς καναλιού, αντί για 27 ξεχωριστά συστήματα ανά Κ-Μ. Το σύστημα συντονίζει τις εντολές αφαίρεσης από διαφορετικά Κ-Μ και λειτουργεί ως ένα ενιαίο σημείο επαφής για τις παραπομπές και τις εντολές αφαίρεσης. Το εργαλείο PERCI έχει ως στόχο να αποτρέψει τη διπλή έκδοση εντολών αφαίρεσης, δηλαδή την έκδοση της ίδιας εντολής από δύο Κ-Μ. Είναι επίσης χρήσιμο για τους ΠΥΦ να διαθέτουν κεντρικά τις εντολές αφαίρεσης και τις παραπομπές που λαμβάνουν με την πάροδο του χρόνου, ώστε να υποστηρίζονται οι υποχρεώσεις υποβολής εκθέσεων διαφάνειας. Μέσω του εργαλείου PERCI, οι ΠΥΦ μπορούν επίσης να ζητήσουν τον έλεγχο και την επανεξέταση μιας εντολή απομάκρυνσης.

3. Ποια είναι η αρμόδια αρχή ενός κράτους μέλους της ΕΕ και πώς μπορώ να επικοινωνήσω μαζί της;

Η επικοινωνία με την αρμόδια αρχή από τον νόμιμο εκπρόσωπο είναι απαραίτητη σε ορισμένες περιπτώσεις. Μια τέτοια «περίσταση» προκύπτει κατά την προσφυγή κατά εντολής αφαίρεσης. Μια άλλη περίπτωση θα ήταν, για παράδειγμα, εάν ο ΠΥΦ αντιληφθεί τρομοκρατικό περιεχόμενο που συνεπάγεται άμεση απειλή για τη ζωή ή τρομοκρατική πράξη χωρίς εντολή αφαίρεσης. Στην περίπτωση αυτή, ο ΠΥΦ υποχρεούται να το διαγράψει αμέσως και να ενημερώσει την αρμόδια αρχή του κράτους μέλους της ΕΕ που επηρεάζεται από αυτό ([Κανονισμός ΤΠΔ, Άρθρο 14.5](#)).

Οι περισσότερες αρμόδιες αρχές των κρατών μελών της ΕΕ έχουν ήδη δημιουργήσει σημεία επαφής. Ένας ενημερωμένος κατάλογος με τα στοιχεία επικοινωνίας βρίσκεται στον δικτυακό τόπο της Ευρωπαϊκής Επιτροπής [εδώ](#).

Κεφάλαιο 5

Καθορισμός Συστήματος Ειδοποίησης Χρηστών και Υποβολής Καταγγελιών για Αφαιρεθέν Περιεχόμενο



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Οι χρήστες των οποίων το περιεχόμενο έχει αφαιρεθεί, **μπορούν να χρησιμοποιήσουν τις διαδικασίες υποβολής καταγγελιών για να υποβάλουν καταγγελία κατά των εντολών αφαίρεσης** (και, εάν είναι απαραίτητο και πέρα από το πεδίο εφαρμογής της ΤΠΔ, βάσει άλλων προληπτικών μέτρων επιτήρησης).
- Οι διαδικασίες υποβολής καταγγελιών αποτελούν σημαντικό **μηχανισμό ελέγχου και ανατροφοδότησης**, από τη σκοπιά των χρηστών, των επιχειρήσεων και του νομικού πλαισίου.
- Κάθε ΠΥΦ «καθιερώνει έναν αποτελεσματικό και προσβάσιμο» μηχανισμό υποβολής καταγγελιών ([Κανονισμός ΤΠΔ, Άρθρο 10.1](#)).
- Σύμφωνα με τον κανονισμό ΤΠΔ, οι μηχανισμοί υποβολής καταγγελιών πρέπει να πληρούν ορισμένες προδιαγραφές ως προς το περιεχόμενο και τις τεχνικές πτυχές.
- Μια διαδικασία υποβολής καταγγελίας μπορεί να οδηγήσει σε δύο διαφορετικά αποτελέσματα, πιο συγκεκριμένα (1) η καταγγελία γίνεται δεκτή διότι διαπιστώνεται ότι το περιεχόμενο έχει αποκλειστεί εσφαλμένα, ή (2) η καταγγελία απορρίπτεται, διότι το περιεχόμενο κρίθηκε δικαιολογημένα αποκλεισμένο.
- Αναλόγως της έκβασης της διαδικασίας καταγγελίας, το περιεχόμενό μπορεί να υπόκειται σε άλλα μέτρα.
- Το κεφάλαιο αυτό παρέχει επιπλέον καθοδήγηση για τον σχεδιασμό και την εφαρμογή μιας διαδικασίας υποβολής καταγγελιών ειδικά για ΠΥΦ.

Οι **διαδικασίες υποβολής καταγγελίας** επιτρέπουν στους χρήστες να εγείρουν την ένστασή τους κατά της αφαίρεσης περιεχομένου, επικοινωνώντας με την πλατφόρμα και αποτελούν το **πρώτο βήμα για την (νομική) αμφισβήτηση μιας εντολής αφαίρεσης**. Μπορείτε να διαβάσετε περισσότερα για τη διαδικασία επίλυσης διαφορών στο ► [κεφάλαιο 2](#).

1. Για ποιο λόγο είναι απαραίτητη η δημιουργία ενός διαφανούς μηχανισμού υποβολής καταγγελιών;

Είναι απαραίτητο να δημιουργηθεί ένας μηχανισμός υποβολής καταγγελιών από τρεις βασικές οπτικές γωνίες: (α) τη νομική, (β) του χρήστη και (γ) της επιχείρησης.

α) Νομική Οπτική Γωνία

Οι διαδικασίες υποβολής καταγγελιών είναι σύμφωνες με τις νομοθετικές ρυθμίσεις που καθιστούν τους μηχανισμούς αυτούς αναγκαίους. Για παράδειγμα, ο Κανονισμός ΤΠΔ ([Κανονισμός ΤΠΔ, Άρθρο 10](#)) ορίζει ότι οι ΠΥΦ οφείλουν να συστήσουν έναν αποτελεσματικό και προσβάσιμο μηχανισμό καταγγελιών, ώστε οι χρήστες να έχουν τη δυνατότητα να αμφισβητήσουν την αφαίρεση ή τον αποκλεισμό του περιεχομένου βάσει συγκεκριμένου μέτρου. Σύμφωνα με τον Κανονισμό ΤΠΔ, ο πάροχος περιεχομένου πρέπει να ενημερώνεται για το τελικό αποτέλεσμα εντός δύο εβδομάδων.

β) Οπτική Γωνία Χρήστη

Ο μηχανισμός καταγγελιών δεν είναι απλώς μια νομική απαίτηση. Ένας σαφής και προσβάσιμος μηχανισμός καταγγελιών συμβάλλει στην οικοδόμηση εμπιστοσύνης με τους χρήστες - τόσο με εκείνους των οποίων το περιεχόμενο έχει υποστεί περιορισμούς αλλά, ακόμα περισσότερο, με μη επηρεαζόμενους χρήστες που χρησιμοποιούν την πλατφόρμα όπως προβλέπεται. Με τον τρόπο αυτό, οι ΠΥΦ καταδεικνύουν ότι οι χρήστες μπορούν να βασίζονται στις διαδικασίες ελέγχου, ότι οι διαδικασίες αυτές βασίζονται σε **αίσθημα ευθύνης απέναντι στους χρήστες** και ότι οι πλατφόρμες λαμβάνουν υπόψη τα **θεμελιώδη δικαιώματα**, όπως η ελευθερία της έκφρασης και της πληροφόρησης.

γ) Οπτική Γωνία Επιχείρησης

Οι μηχανισμοί καταγγελιών μπορούν να αποτελέσουν μια **χρήσιμη μορφή αυτοελέγχου**, με την οποία τα μέτρα και τα πρότυπα ελέγχου μπορούν να αξιολογηθούν ως προς την αποτελεσματικότητα, τη δίκαιη αντιμετώπιση και τη συνέπεια. Τέτοιοι μηχανισμοί μπορούν να παρέχουν τη διαβεβαίωση ότι η πλατφόρμα σας χρησιμοποιείται με τον προβλεπόμενο τρόπο, γεγονός που συμβάλλει περαιτέρω στην **προστασία της φήμης** των διαδικτυακών υπηρεσιών και στην περαιτέρω προστασία του δικαιώματος της ελευθερίας της έκφρασης στο διαδίκτυο.

2. Ποιες είναι οι απαιτήσεις για ένα σύστημα υποβολής καταγγελιών;

Σύμφωνα με τον Κανονισμό ΤΠΔ ([33 & Άρθρο 10](#)), η διαδικασία υποβολής καταγγελιών οφείλει:

- Να είναι φιλική προς το χρήστη,
- Να είναι αποτελεσματική και (εύκολα) προσβάσιμη,
- Να προσφέρει ένα ασφαλές πλαίσιο στο οποίο οι καταγγελίες θα εξετάζονται άμεσα και με διαφάνεια, έτσι ώστε το άτομο που προσφεύγει να λαμβάνει ενημέρωση για το αποτέλεσμα της καταγγελίας εντός δύο εβδομάδων.

Τα συστήματα υποβολής καταγγελιών πρέπει να δημιουργηθούν για τους σκοπούς του Κανονισμού ΤΠΔ για την αποκατάσταση του περιεχομένου που έχει αφαιρεθεί εσφαλμένα. Ωστόσο, μπορούν επίσης να υποβληθούν καταγγελίες κατά των μέτρων που λαμβάνονται για την επιβολή των ΟΠΥ της πλατφόρμας πέραν του πεδίου εφαρμογής του κανονισμού ΤΠΔ.

3. Πώς πρέπει να διαχειρίζονται οι καταγγελίες και ποια είναι τα πιθανά αποτελέσματα;

Μόλις τεθεί σε εφαρμογή το σύστημα υποβολής καταγγελιών και οι χρήστες υποβάλουν μια καταγγελία, ο ΠΥΦ **θα εξετάσει την καταγγελία και θα κοινοποιήσει την απόφαση στον καταγγέλλοντα εντός δύο εβδομάδων το αργότερο για τις περιπτώσεις που αφορούν τον Κανονισμό ΤΠΔ.**

Υπάρχουν δύο πιθανές εκβάσεις της διαδικασίας επανεξέτασης, τα οποία παρατίθενται στον ακόλουθο πίνακα.

Έκβαση Α	Έκβαση Β
Η καταγγελία του χρήστη κατά της αφαίρεσης περιεχομένου γίνεται δεκτή	Η καταγγελία του χρήστη κατά της αφαίρεσης περιεχομένου απορρίπτεται
Αποτέλεσμα: Η καταγγελία κατά της αφαίρεσης του περιεχομένου είναι δικαιολογημένη και ως εκ τούτου γίνεται δεκτή.	Αποτέλεσμα: Η καταγγελία κατά της αφαίρεσης του περιεχομένου δεν είναι δικαιολογημένη και ως εκ τούτου απορρίπτεται.
Σημασία: Το περιεχόμενο έχει αφαιρεθεί, διαγραφεί ή τροποποιηθεί εσφαλμένα.	Σημασία: Το περιεχόμενο έχει αφαιρεθεί, διαγραφεί ή τροποποιηθεί με ορθό τρόπο.
Περαιτέρω διαδικασία: Ο ΠΥΦ (1) ενημερώνει τον καταγγέλλοντα για το αποτέλεσμα της επανεξέτασης και (2) αποκαθιστά το περιεχόμενο.	Περαιτέρω διαδικασία: Ο ΠΥΦ (1) ενημερώνει τον καταγγέλλοντα για το αποτέλεσμα της επανεξέτασης και (2) παρέχει στον χρήστη τους λόγους για την απόφαση αυτή.

4. Πρακτικές συμβουλές και οδηγίες: Ποια στοιχεία είναι χρήσιμα κατά την δημιουργία ενός συστήματος υποβολής καταγγελιών;

Το γεγονός ότι ένα σύστημα υποβολής καταγγελιών πρέπει να διαθέτει ορισμένα χαρακτηριστικά αποτελεί απαίτηση όχι μόνο του νόμου, αλλά και της **φιλικότητας προς τον χρήστη**.

Όμοια με άλλα βασικά ζητήματα όπως ότι αφορά τους ΟΠΥ ([► κεφάλαιο 1](#)), την καθιέρωση διαδικασίας για τον εντοπισμό παράνομου περιεχομένου ([► κεφάλαιο 2](#)), ή την επιλογή μηχανισμών ελέγχου για κάθε πλατφόρμα ([► κεφάλαιο 3](#)), η μέθοδος υποβολής μιας καταγγελίας μπορεί να διαφέρει σημαντικά από πλατφόρμα σε πλατφόρμα. Ενώ ορισμένες πλατφόρμες μπορούν να προσφέρουν τη δυνατότητα υποβολής καταγγελιών μέσω ηλεκτρονικού ταχυδρομείου, άλλες επιλέγουν να εφαρμόσουν τυποποιημένες εφαρμογές που βασίζονται σε ηλεκτρονικές φόρμες.

Τα συστήματα υποβολής καταγγελιών θα πρέπει να προσαρμόζονται στο σκοπό, τη δομή και την οργάνωση μιας πλατφόρμας. Οδηγίες για τη δημιουργία ενός συστήματος παραπόνων μπορείτε να βρείτε στην ακόλουθη λίστα.



Δώστε σαφείς πληροφορίες σχετικά με την αφαίρεση του περιεχομένου

Ενημερώστε το άτομο του οποίου το περιεχόμενο έχει αφαιρεθεί. Εξετάστε το ενδεχόμενο να το κάνετε αυτό ακόμη και αν το περιεχόμενο έχει περιοριστεί με άλλο τρόπο. Σε αυτό το πλαίσιο, ενημερώστε επίσης το άτομο για τους λόγους για τους οποίους το περιεχόμενο αφαιρέθηκε (βλ. παρακάτω το ακόλουθο σημείο σχετικά με τις πληροφορίες για το εκπαιδευτικό και παιδαγωγικό υπόβαθρο) και για τον τρόπο με τον οποίο μπορεί να υποβληθεί προσφυγή κατά της απόφασης αφαίρεσης (βλ. παρακάτω το σημείο σχετικά με την επεξήγηση της διαδικασίας υποβολής καταγγελίας).



Εξηγήστε τη διαδικασία υποβολής καταγγελιών

Εξηγήστε στους χρήστες σας τη διαδικασία υποβολής καταγγελιών. Αυτό θα πρέπει να γίνεται κατά τη διάρκεια της κοινοποίησης σχετικά με την αφαίρεση περιεχομένου ή τον περιορισμό περιεχομένου με άλλο τρόπο. Οι πληροφορίες σχετικά με τη διαδικασία υποβολής καταγγελιών μπορούν επίσης να συμπεριληφθούν στους ΟΠΥ. Η επεξήγηση της διαδικασίας υποβολής καταγγελιών θα πρέπει να περιλαμβάνει: (1) τον τρόπο με τον οποίο μπορούν να υποβληθούν καταγγελίες, (2) τον τρόπο με τον οποίο λειτουργεί η διαδικασία επανεξέτασης και (3) τον τρόπο με τον οποίο οι χρήστες ενημερώνονται για το αποτέλεσμα της επανεξέτασης.



Παροχή επιπρόσθετων επεξηγηματικών πληροφοριών

Προσφέρετε στους χρήστες επεξηγηματικές πληροφορίες για να κάνετε σαφές το λόγο που αφαιρέθηκε το περιεχόμενο και ποιους όρους παραβιάζει. Για παράδειγμα, το περιεχόμενο μπορεί να αφαιρεθεί εάν παραβιάζει τους ΟΠΥ ή εάν έχει ληφθεί αίτημα αφαίρεσης από αρμόδια αρχή στο πλαίσιο του Κανονισμού ΤΠΔ. Στην πρώτη περίπτωση, οι πληροφορίες αυτές μπορούν να διευκρινιστούν προσθέτοντας ποιος από τους ειδικούς όρους για την πλατφόρμα έχει παραβιαστεί (π.χ. κατά της ρητορικής μίσους, της υποκίνησης σε βία, του σεξουαλικού περιεχομένου και της παρενόχλησης). Στη δεύτερη περίπτωση, συνιστάται να προστεθεί στο σύστημα καταγγελιών μια σύντομη ενημερωτική επισκόπηση του κανονισμού ΤΠΔ, έτσι ώστε το νομικό πλαίσιο να γίνεται σαφές στον χρήστη



Παρέχετε τακτικές ενημερώσεις σχετικά με την πρόοδο της καταγγελίας

Οι χρήστες θα πρέπει να ενημερώνονται τακτικά για την πρόοδο της καταγγελίας, ώστε να διαπιστώνεται ότι η διαδικασία είναι σε εξέλιξη. Οι ενημερώσεις αυτές θα πρέπει να περιλαμβάνουν τουλάχιστον μια ειδοποίηση για την ολοκλήρωση της εξέτασης και την έγκαιρη κοινοποίηση του αποτελέσματος. Λεπτομερέστερη επικοινωνία θα μπορούσε να ενημερώνει τον χρήστη ότι η καταγγελία έχει παραληφθεί και εξετάζεται τώρα από υπαλλήλους του ΠΥΦ. Η βέλτιστη πρακτική θα έδινε στον χρήστη ένα χρονοδιάγραμμα για την εξέταση της καταγγελίας του. Αυτές οι ενημερώσεις μπορούν να δοθούν μέσω ηλεκτρονικού ταχυδρομείου ή να εμφανιστούν σε μια ηλεκτρονική πύλη.



Καταγράψτε τη διαδικασία (ατομικής) καταγγελίας

Το έγγραφο αυτό θα χρησιμεύσει ως αναφορά για τυχόν μεταγενέστερες ερωτήσεις ή διαφωνίες για το λόγο αυτό είναι σημαντικό να τεκμηριώνεται η διαδικασία υποβολής καταγγελιών. Το έγγραφο μπορεί να χρησιμεύσει ως σημείο αναφοράς για τυχόν μεταγενέστερες ερωτήσεις ή ενστάσεις.

Κεφάλαιο 6

Πρακτικές Επιστημονικές και Συμβουλές Σχετικά με την Υποβολή Εκθέσεων Διαφάνειας



Σύνοψη: Περιεχόμενο και κύρια σημεία του παρόντος κεφαλαίου

- Οι εκθέσεις διαφάνειας επιτρέπουν στους ΠΥΦ να **επικοινωνούν δημοσίως** τον τρόπο με τον οποίο τηρούνται οι **αξίες** τους στην πλατφόρμα, καθώς και τις **ενέργειες που έχουν ληφθεί κατά απαγορευμένου και παράνομου περιεχομένου και συμπεριφοράς**.
- Οι εκθέσεις διαφάνειας αποτελούν **σημαντικό εργαλείο για την ανάληψη δημόσιας ευθύνης και την επίδειξη φερεγγυότητας και αξιοπιστίας**.
- Διάφοροι **νόμοι**, συμπεριλαμβανομένου του Κανονισμού ΤΠΔ, **απαιτούν ρητά την υποβολή εκθέσεων διαφάνειας**.
- Κατά την προετοιμασία των εκθέσεων διαφάνειας, είναι συνετό να ακολουθείτε συγκεκριμένα βήματα πριν, κατά τη διάρκεια και μετά τη διαδικασία.
- Ο **κανονισμός ΤΠΔ απαιτεί από τους ΠΥΦ που εκτίθενται σε τρομοκρατικό περιεχόμενο ή έχουν λάβει μέτρα κατά αυτού, να δημοσιεύουν σχετική ετήσια έκθεση διαφάνειας**. Η έκθεση οφείλει να περιλαμβάνει ορισμένα βασικά στοιχεία και πληροφορίες, όπως ο αριθμός των περιεχομένων που έχουν αφαιρεθεί. Η έκθεση, αυτή, πρέπει να δημοσιεύεται το αργότερο έως την 1η Μαρτίου του επόμενου έτους ([Κανονισμός ΤΠΔ, Άρθρο 7.2](#)).

1. Τι είναι οι εκθέσεις διαφάνειας;

Οι εκθέσεις διαφάνειας είναι ένα **σημαντικό εργαλείο για τους ΠΥΦ ώστε να αποδεικνύουν την υπευθυνότητα, την αξιοπιστία και την φερεγγυότητά τους και να δημοσιεύουν κοινωνικά σημαντικές πληροφορίες**. Οι εκθέσεις διαφάνειας **περιέχουν σημαντικά στοιχεία σχετικά με τα αιτήματα που λαμβάνουν οι ΠΥΦ από κρατικούς φορείς παγκοσμίως και τον τρόπο με τον οποίο αντιμετωπίζονται τα αιτήματα αυτά**, τα οποία αποσκοπούν στο να διασφαλίσουν τη διαφάνεια της συνεργασίας και της συνεργασίας με τις αρχές και άλλους κρατικούς φορείς⁷.

Οι εκθέσεις διαφάνειας παρέχουν επίσης μια επισκόπηση των μέτρων που έχει λάβει ο ΠΥΦ για την επιβολή των κανονισμών (π.χ. μέσω της αφαίρεσης περιεχομένου ή άλλων μέτρων επιτήρησης). Αυτό περιλαμβάνει την επιβολή (1) των πολιτικών που αφορούν την πλατφόρμα

⁷ Urman, A., & Makhortykh, M. (2023). How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms. *Telecommunications Policy*, 47(3), 102477. <https://doi.org/10.1016/j.telpol.2022.102477>

(συνήθως ΟΠΥ; ► [κεφάλαιο 1](#)), (2) δικαιώματων όπως η νομοθεσία περί πνευματικών δικαιωμάτων ή εμπορικών σημάτων και (3) (τοπικής) νομοθεσίας και κανονισμών που οδηγούν σε αφαίρεση περιεχομένου. Στην ΕΕ, η τοπική νομοθεσία περιλαμβάνει τον κανονισμό ΤΠΔ και την Πράξη για τις Ψηφιακές Υπηρεσίες. Ενδέχεται να τίθεται επίσης σε εφαρμογή και σχετική νομοθεσία συγκεκριμένης χώρας, όπως ο αυτή, για τη βελτίωση της επιβολής του νόμου στα κοινωνικά δίκτυα, στη Γερμανία.

Οι εκθέσεις διαφάνειας δημοσιεύονται συνήθως σε τακτική βάση. Ο Κανονισμός ΤΠΔ αναφέρει ότι αυτό θα πρέπει να γίνεται (τουλάχιστον) μία φορά το χρόνο, εάν ένας ΠΥΦ έχει λάβει μέτρα κατά τρομοκρατικού περιεχομένου ([Κανονισμός ΤΠΔ, 30](#)).

Οι εκθέσεις διαφάνειας και οι μετρήσεις που αναφέρονται σε αυτές μπορεί να διαφέρουν σημαντικά από ΠΥΦ σε ΠΥΦ⁸. **Για τις εκθέσεις διαφάνειας σύμφωνα με τον Κανονισμό ΤΠΔ, υπάρχουν συγκεκριμένες απαιτήσεις σχετικά με τις πληροφορίες που πρέπει να περιλαμβάνονται.** Μπορείτε να διαβάσετε περισσότερα σχετικά ► [ενότητα 4 παρόντος κεφαλαίου](#).

2. Γιατί είναι απαραίτητες οι εκθέσεις διαφάνειας;

Οι εκθέσεις διαφάνειας επιτρέπουν στους χρήστες και άλλα ενδιαφερόμενα μέρη να αξιολογούν τον βαθμό στον οποίο οι ΠΥΦ παραμένουν πιστοί στις αρχές τους, στις νομικές απαιτήσεις και στην προστασία των δεδομένων και της ιδιωτικής ζωής⁹. Ας εξετάσουμε τις διαφορετικές οπτικές γωνίες σχετικά με το γιατί οι εκθέσεις διαφάνειας είναι σημαντικές.

α) Νομική Οπτική Γωνία

Οι εκθέσεις διαφάνειας είναι χρήσιμες και συχνά αναγκαίες για τη συμμόρφωση με τους κανονισμούς της ΕΕ, όπως ο Κανονισμός ΤΠΔ, η Πράξη για τις Ψηφιακές Υπηρεσίες και οι νόμοι της εκάστοτε χώρας, κατά περίπτωση. Εάν οι ΠΥΦ έχουν λάβει μέτρα κατά της διάδοσης τρομοκρατικού περιεχομένου εντός ενός ημερολογιακού έτους, είτε προληπτικά είτε σε συμμόρφωση με εντολή αφαίρεσης, **πρέπει να δημοσιεύσουν έκθεση διαφάνειας το αργότερο έως την 1η Μαρτίου του επόμενου έτους** ([Κανονισμός ΤΠΔ, Άρθρο 7.2](#)). Αυτό σημαίνει ότι οι εκθέσεις διαφάνειας είναι πιθανότερο να είναι υποχρεωτικές παρά το αντίθετο. Οι αρμόδιες αρχές υποχρεούνται και αυτές να δημοσιεύουν ετήσιες εκθέσεις διαφάνειας ([Κανονισμός ΤΠΔ, 31](#)).

β) Οπτική Γωνία Χρηστών και Ενδιαφερομένων Μερών

Οι εκθέσεις διαφάνειας βοηθούν τους χρήστες και άλλα ενδιαφερόμενα μέρη να αξιολογήσουν τον βαθμό στον οποίο οι ΠΥΦ εκπληρώνουν την **ευθύνη τους απέναντι στην κοινωνία**. Ταυτόχρονα, η τακτική δημοσίευση των εκθέσεων διαφάνειας βοηθά τον ΠΥΦ, να **οικοδομήσει εμπιστοσύνη και καλή δημόσια φήμη**, επιδεικνύοντας συμμόρφωση, δέσμευση και αξιοπιστία.

⁸ Woolery, L., Budish, R., & Bankston, K. (2016). The transparency reporting toolkit. *New America and The Berkman Center for Internet & Society at Harvard University*.

γ) Οπτική Γωνία Επιχείρησης

Όμοια με τους μηχανισμούς υποβολής καταγγελιών, οι εκθέσεις διαφάνειας μπορούν επίσης να αποτελέσουν ένα **εργαλείο αυτοελέγχου** που εντοπίζει τους τομείς στους οποίους οι επιχειρηματικές διαδικασίες μπορούν να βελτιωθούν. Δεδομένου ότι οι μικρότεροι ΠΥΦ είναι ιδιαίτερα δημοφιλείς στους τρομοκρατικούς δρώντες (για περαιτέρω πληροφορίες δείτε [εδώ: Tech Against Terrorism](#)), οφείλουν να αναλάβουν δράση κατά της διάδοσης τρομοκρατικού περιεχομένου. Οι εκθέσεις διαφάνειας είναι ένας τρόπος για τους μικρότερους ΠΥΦ να αποδείξουν τη δέσμευσή τους σε αυτή την προσπάθεια.

3. Διαδικασία προετοιμασίας των εκθέσεων διαφάνειας

Η αρχική προετοιμασία και υποβολή μιας έκθεσης διαφάνειας μπορεί να μοιάζει ένα δύσκολο έργο. Ωστόσο, μόλις καθιερωθεί **μια διαδικασία και μια κανονικότητα για την προετοιμασία των ετήσιων εκθέσεων διαφάνειας**, συνήθως δεν υπάρχει ανάγκη για πλήρη αναμόρφωση της δομής της έκθεσης και τυπικά αρκεί μια απλή επικαιροποίηση. Ο παρών οδηγός θα περιγράψει τον τρόπο δημιουργίας μιας έκθεσης διαφάνειας από την οπτική γωνία του ΠΥΦ, καθώς και τι πρέπει να ληφθεί υπόψη εκ των προτέρων, κατά τη διάρκεια και μετά τη διαδικασία δημιουργίας.

α) Πριν τη σύνταξη της έκθεσης διαφάνειας

Διερεύνηση νομικού πλαισίου

Ενημερωθείτε για τους νομικούς κανονισμούς που ισχύουν για τον ΠΥΦ σας. Για παράδειγμα, ο Κανονισμός ΤΠΔ και η Πράξη για τις Ψηφιακές Υπηρεσίες αφορούν όλη την ΕΕ. Ενδέχεται να υπάρχουν ειδικοί κανονισμοί ανά χώρα, καθώς και απαιτήσεις για άλλα θέματα που αφορούν τον ΠΥΦ σας πέραν του τρομοκρατικού περιεχομένου. Εάν έχετε έμμισθους συνεργάτες ή δικηγόρους, είναι συνετό να συνομιλήσετε μαζί τους για να καθορίσετε ποιοι κανονισμοί (εκτός από τον κανονισμό ΤΠΔ με τον οποίο ασχολείστε εδώ) ισχύουν για τον ΠΥΦ σας.

Καθορισμός των στόχων της έκθεσης διαφάνειας

Σκεφτείτε ποιοι είναι οι στόχοι της έκθεσης διαφάνειας. Βασικές ερωτήσεις που μπορούν να σας βοηθήσουν σε αυτό είναι οι εξής: Θέλετε να εκπληρώσετε «απλά και μόνο» τις νομικές σας υποχρεώσεις ή θέλετε να ασχοληθείτε και με άλλα θέματα και τη δέσμευσή σας σε αυτά; Ποιον θέλετε να προσεγγίσετε, δηλαδή ποια ομάδα-στόχος έχει νόημα για τον ΠΥΦ σας (π.χ. πολιτικοί φορείς, χρήστες, χρηματοδότες); Πόσο συχνά θέλετε να δημοσιεύετε εκθέσεις διαφάνειας και ποιος είναι ο καλύτερος χρόνος για το εκάστοτε οικονομικό σας έτος;

Καθορισμός δεδομένων που μπορούν και πρέπει να συμπεριληφθούν

Καθορίστε ποια δεδομένα θα συμπεριλάβετε στην έκθεση διαφάνειας. Αφενός, η δυνατότητα συλλογής είναι σχετική, δηλαδή ποια δεδομένα είναι διαθέσιμα ή ποιά είναι εφικτό να τα συλλέξετε στο μέλλον; Από την άλλη πλευρά, το τι οφείλει και πρέπει να δηλωθεί είναι καθοριστικό, δηλαδή: ποιες νομικές απαιτήσεις πρέπει να ικανοποιήσετε και ποια δεδομένα είναι απαραίτητα για αυτό; Μπορείτε να μάθετε ποιες πληροφορίες και ποια δεδομένα πρέπει να συμπεριλάβετε σύμφωνα με τον Κανονισμό ΤΠΔ στο ► [επόμενο υποκεφάλαιο](#).

β) Κατά τη διάρκεια σύνταξης της έκθεσης διαφάνειας

Χρήση σαφούς και συνοπτικής γλώσσας

Κατά τη σύνταξη της έκθεσης διαφάνειας, βεβαιωθείτε ότι χρησιμοποιείται σαφής και συνοπτική γλώσσα. Αυτό βοηθά στην κατανόηση του πολύπλοκου υλικού. Η γλώσσα θα πρέπει να προσαρμόζεται περαιτέρω στο προβλεπόμενο αναγνωστικό κοινό.

Παροχή σχετικών πληροφοριών και επεξηγήσεων

Παρέχετε στους αναγνώστες σας πληροφορίες και επεξηγήσεις που σχετίζονται με το πλαίσιο αναφοράς. Οι εξηγήσεις αυτές επιτρέπουν στους χρήστες να κατανοήσουν καλύτερα τον τρόπο με τον οποίο λειτουργεί ο ΠΥΦ σας και τους λόγους για τους οποίους (ίσως) παρέχει μια λεπτομερέστερη έκθεση διαφάνειας παρά μια «απλή» έκθεση που πληροί μόνο τις ελάχιστες απαιτήσεις.

Ενσωμάτωση εσωτερικής ανατροφοδότησης

Όταν προγραμματίζετε μια έκθεση διαφάνειας, να λαμβάνετε υπόψη και τους γύρους ανατροφοδότησης στο χρονοδιάγραμμα. Η τακτική ανατροφοδότηση που προσφέρει διορθώσεις στο περιεχόμενο και τη γλώσσα της έκθεσης μπορεί να είναι πολύτιμη για όλους τους εμπλεκόμενους φορείς, ιδίως για όσους έχουν αναλάβει την προετοιμασία της έκθεσης.

γ) Μετά τη σύνταξη της έκθεσης διαφάνειας

Δημοσίευση της έκθεσης διαφάνειας

Αναλογιστείτε τις γλώσσες στις οποίες θέλετε να δημοσιεύσετε την έκθεση διαφάνειας και δημιουργήστε τις κατάλληλες μεταφράσεις. Καθορίστε επίσης σε ποιο σημείο του ιστότοπού σας θα πρέπει να είναι προσβάσιμη. Μπορείτε επίσης να εξετάσετε το ενδεχόμενο να συμπεριλάβετε την έκθεση διαφάνειας σε διάφορα υλικά επικοινωνίας για να αποκτήσει μεγαλύτερη προβολή. Αυτό θα μπορούσε να περιλαμβάνει την ενσωμάτωσή της στον ιστότοπό σας, την αποστολή της σε newsletter ή την κοινοποίησή της στα μέσα κοινωνικής δικτύωσης.

Τακτική επικαιροποίηση των δεδομένων και της έκθεσης διαφάνειας.

Όταν ολοκληρωθεί η πρώτη έκθεση διαφάνειας, έχετε ήδη δημιουργήσει τα θεμέλια που θα διευκολύνουν την επόμενη, δεδομένου ότι έχετε ήδη δημιουργήσει το υπόδειγμα. Η διαδικασία συλλογής των σχετικών δεδομένων καθ' όλη τη διάρκεια του έτους και η οργάνωσή τους ώστε να είναι άμεσα διαθέσιμα θα διευκολύνει την παραγωγή της επόμενης έκθεσης διαφάνειας και θα είναι λιγότερο χρονοβόρα και απαιτητική σε πόρους.

Αφήστε περιθώρια βελτίωσης

Να είστε ανοιχτοί σε αλλαγές και προσαρμογές. Εάν λάβετε εξωτερική ανατροφοδότηση, εξετάστε το ενδεχόμενο να την ενσωματώσετε στην επόμενη έκθεση διαφάνειας. Ωστόσο, η σχετική ανατροφοδότηση μπορεί να μην είναι μόνο εξωτερική. Μετά τη δημοσίευση, ο ΠΥΦ μπορεί επίσης να εξετάσει κριτικά την προηγούμενη έκθεση διαφάνειας, την επικοινωνία γύρω από αυτήν και τις αντιδράσεις σε αυτήν, λαμβάνοντας υπόψη δηλώσεις στον Τύπο ή άλλες σχετικές πηγές. Τόσο η εσωτερική όσο και η εξωτερική ανατροφοδότηση μπορούν να προσδιορίσουν τα σημεία προς βελτίωση.

4. Ποιες πληροφορίες και μετρήσεις πρέπει να περιλαμβάνονται στην έκθεση διαφάνειας;

Ο Κανονισμός ΤΠΔ διευκρινίζει στο [Άρθρο 7.3](#) τις ελάχιστες απαιτήσεις για τις εκθέσεις διαφάνειας, δηλαδή τι ακριβώς πρέπει να περιλαμβάνεται για τη συμμόρφωση με την εν λόγω νομοθεσία της ΕΕ. Παρουσιάζουμε τις απαιτήσεις αυτές στον παρακάτω κατάλογο:

1) Πληροφορίες σχετικά με τα μέτρα που έχει λάβει ο ΠΥΦ για:

- ☒ τον εντοπισμό τρομοκρατικού περιεχομένου;
- ☒ την αφαίρεση ή την κατάργηση τρομοκρατικού περιεχομένου;
- ☒ την αποτροπή της επανεμφάνισης και επαναφόρτωσης διαδικτυακού υλικού που είχε προηγουμένως αποκλειστεί (αυτό είναι ιδιαίτερα σημαντικό όταν χρησιμοποιούνται αυτοματοποιημένες διαδικασίες).

2) Μετρήσεις και, πρόσθετες πληροφορίες σχετικά με τον αριθμό των:

- ☒ των αφαιρεθέντων στοιχείων που περιλαμβάνουν τρομοκρατικό περιεχόμενο (βάσει εντολών αφαίρεσης ή άλλων μέτρων);
- ☒ εντολών αφαίρεσης που δεν εκτελέστηκαν και πρόσθετες πληροφορίες για τους λόγους που δεν συνέβη αυτό;
- ☒ καταγγελιών που διεκπεραιώθηκαν από τον ΠΥΦ μέσω της διαδικασίας υποβολής καταγγελιών, καθώς και πρόσθετες πληροφορίες ως προς την έκβαση αυτών;
- ☒ περιπτώσεων στις οποίες ο ΠΥΦ αποκατέστησε το περιεχόμενο μετά από καταγγελία;
- ☒ νομικών ενεργειών που εκκινήθηκαν από τον ΠΥΦ και πρόσθετες πληροφορίες σχετικά με την έκβασή τους;
- ☒ περιπτώσεων όπου ο ΠΥΦ αποκατέστησε το περιεχόμενο έπειτα από νομικές ενέργειες.

Γ. Ευχαριστούμε για τη Συνδρομή σας στην Αντιμετώπιση της Τρομοκρατικής Απειλής!

Συγχαρητήρια!

Έχετε φτάσει ως εδώ, και αυτό σημαίνει ότι έχετε ήδη αποκτήσει βασικές γνώσεις σχετικά με τις απαιτήσεις του Κανονισμού ΤΠΔ καθώς και άλλων πρόσθετων μέτρων για την αντιμετώπιση του τρομοκρατικού και επικίνδυνου διαδικτυακού περιεχομένου. Με αυτόν τον τρόπο, θα συμβάλλετε προς ένα ασφαλέστερο διαδίκτυο.

Αντιλαμβανόμαστε ότι η εφαρμογή αυτών των μέτρων απαιτεί σημαντική μέριμνα και πόρους. Το γεγονός ότι έχετε ήδη ολοκληρώσει τον παρόντα οδηγό είναι ένα σημαντικό βήμα και αν σας βοηθήσει να σκεφτείτε μια στρατηγική για την εφαρμογή των μέτρων κατά του τρομοκρατικού περιεχομένου που είναι κατάλληλη για το δικό σας πλαίσιο, τότε θα έχουμε ήδη πετύχει ένα σημαντικό αποτέλεσμα! Είμαστε πεπεισμένοι ότι ο οδηγός αυτός, μαζί με τους άλλους εκπαιδευτικούς μας πόρους, θα αποτελέσει ένα ανεκτίμητο εργαλείο για να μπορέσει ένας ΠΥΦ να ανταποκριθεί πλήρως στις υποχρεώσεις του όσον αφορά την αντιμετώπιση μιας διαδικτυακής τρομοκρατικής απειλής.

Σας ευχαριστούμε πολύ για τη δέσμευσή σας στην αντιμετώπιση της διαδικτυακής τρομοκρατικής απειλής και για την προστασία του ΠΥΦ αλλά και των χρηστών σας.



ΥΓ: Το πρόγραμμα Tech Against Terrorism Europe περιλαμβάνει επίσης ένα **αναγνωρισμένο και δωρεάν διαθέσιμο, διαδικτυακό μάθημα** για την περαιτέρω διερεύνηση της συμμόρφωσης με τον Κανονισμό ΤΠΔ της ΕΕ. Στο μάθημα αυτό, μπορείτε να εμβαθύνετε στο θέμα και να βρείτε λεπτομέρειες σχετικά με τον κανονισμό, παραδείγματα για το πώς άλλες πλατφόρμες εφαρμόζουν επιμέρους μέτρα, καθώς και γενικότερες πληροφορίες σχετικά με την τρομοκρατική συμπεριφορά στο διαδίκτυο. **Μετά την επιτυχή ολοκλήρωση του μαθήματος, θα λάβετε ένα επίσημο πιστοποιητικό υπογεγραμμένο από αναγνωρισμένα πανεπιστήμια.** (Πανεπιστήμιο Λούντβιχ-Μαξιμίλιαν Μόναχο, Πανεπιστήμιο της Γάνδης). Επιπρόσθετα, το έργο TATE προσφέρει ένα εκπαιδευτικό πρόγραμμα για την ανάπτυξη δεξιοτήτων, στο πλαίσιο του οποίου οι ΠΥΦ μπορούν να λάβουν πρακτική υποστήριξη για τις απαιτήσεις που σχετίζονται με τον Κανονισμό ΤΔΠ.

Δ. Γλωσσάρι

Όρος	Επεξήγηση
Αρμόδια αρχή	Οι αρχές ενός κράτους μέλους της ΕΕ που είναι υπεύθυνες για την εφαρμογή του κανονισμού ΤCO. Μια επισκόπηση των αντίστοιχων αρμόδιων αρχών των κρατών μελών μπορείτε να βρείτε εδώ .
Πάροχος περιεχομένου	Το άτομο που παρέχει περιεχόμενο στην αντίστοιχη πλατφόρμα, για παράδειγμα δημοσιεύει μια ανάρτηση.
ΠΥΦ	Πάροχοι υπηρεσιών φιλοξενίας – ο Κανονισμός ΤΠΔ εφαρμόζεται στους ΠΥΦ. Περισσότερες λεπτομέρειες σχετικά με το ποιοι πάροχοι υπηρεσιών φιλοξενίας εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού ΤΠΔ μπορείτε να βρείτε ►εδώ .
Εργαλείο PERCI	Το PERCI είναι ένα εργαλείο που συντονίζεται από την Europol και αποσκοπεί στην ενίσχυση και διευκόλυνση της επικοινωνίας μεταξύ των ΠΥΦ και των αρμόδιων αρχών.
Εντολή αφαίρεσης	Αίτημα που λαμβάνει ένας ΠΥΦ από μια αρμόδια αρχή. Ενημερώνει τον πάροχο υπηρεσιών φιλοξενίας ότι έχει κυκλοφορήσει τρομοκρατικό περιεχόμενο στην πλατφόρμα και τον υποχρεώνει να το αφαιρέσει γρήγορα εντός μίας ώρας από την παραλαβή του αιτήματος.
Κανονισμός ΤΠΔ (επίσης: LEX 2021/784 & Κανονισμός σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο)	Ο κανονισμός της ΕΕ κατά της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο που τέθηκε σε ισχύ το 2022. Εφαρμόζεται στους παρόχους υπηρεσιών φιλοξενίας (ΠΥΦ) που προσφέρουν τις υπηρεσίες τους εντός της ΕΕ.
Τρομοκρατικό Περιεχόμενο στο Διαδίκτυο (ΤΠΔ)	Περιεχόμενο που ενέχει τρομοκρατικά στοιχεία ή προορίζεται για την προώθηση τρομοκρατικών σκοπών. Λεπτομερής ορισμός αυτού του περιεχομένου βρίσκεται στην ►εισαγωγή . Το τρομοκρατικό περιεχόμενο στο διαδίκτυο συνδέεται στενά με τα ►τρομοκρατικά αδικήματα , τα οποία μπορεί να είναι πολυποίκιλα από τη φύση τους.
ΟΠΥ/Ο&Π	Όροι παροχής υπηρεσιών- δεσμευτικοί κανόνες που θεσπίζονται από και για την εκάστοτε πλατφόρμα οι οποίοι (1) καθορίζουν το πεδίο εφαρμογής και την ευθύνη των ΠΥΦ έναντι των χρηστών και (2) τις κατάλληλες και επιτρεπόμενες, αλλά και απαγορευμένες πρακτικές χρήσης. Οι χρήστες οφείλουν να συμμορφώνονται με αυτούς εάν επιθυμούν να συνεχίσουν να χρησιμοποιούν την υπηρεσία που προσφέρουν οι ΠΥΦ. Υπάρχουν πολυάριθμα συνώνυμα του ΟΠΥ, π.χ., Όροι Χρήσης, Όροι και Προϋποθέσεις, ή Κοινοτικά Πρότυπα.