



ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Στρασβούργο, 10.2.2026
COM(2026) 71 final

**ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ
ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ
ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ**

Σχέδιο δράσης κατά του κυβερνοεκφοβισμού

«Πιο ασφαλείς στο διαδίκτυο, πιο δυνατοί μαζί»

1. Εισαγωγή

«Αυτή η επιχειρηματική δραστηριότητα δεν γίνεται για φιλανθρωπικούς σκοπούς. Όμως οι γονείς ζουν καθημερινά με τους κινδύνους που ελλοχεύουν σε αυτή και τις βλάβες που προκαλεί: τον διαδικτυακό εκφοβισμό, την ενθάρρυνση του αυτοτραυματισμού, τα διαδικτυακά αρπακτικά, τους εθιστικούς αλγορίθμους. Σ' εμάς εναπόκειται να προστατεύσουμε την επόμενη γενιά μας.»

Ομιλία της προέδρου φον ντερ Λάιεν το 2025 στην εκδήλωση υψηλού επιπέδου με θέμα την «Προστασία των παιδιών στην ψηφιακή εποχή»

Ο ψηφιακός μετασχηματισμός έχει αλλάξει ριζικά την κοινωνία. Προσφέρει στα παιδιά, τις νέες και τους νέους τεράστιες ευκαιρίες για να αναπτύξουν τις δεξιότητες και τη δημιουργικότητά τους. Σήμερα, το 97 % των νέων στην ΕΕ χρησιμοποιεί το διαδίκτυο καθημερινά, και για τα άτομα ηλικίας μεταξύ 15 και 24 ετών, η πλέον χρησιμοποιούμενη πηγή πληροφοριών είναι οι πλατφόρμες των μέσων κοινωνικής δικτύωσης (65 %). Μαζί με εργαλεία τεχνητής νοημοσύνης, βιντεοπαιχνίδια, εφαρμογές ανταλλαγής μηνυμάτων και διαδικτυακές κοινότητες, συνδέονται και συμμετέχουν.

Ωστόσο, οι πλατφόρμες αυτές ενέχουν συγχρόνως κινδύνους: έκθεση σε διαδικτυακά αρπακτικά, ενθάρρυνση του αυτοτραυματισμού, εθιστικοί αλγόριθμοι, επικίνδυνες διαδικτυακές προκλήσεις και κυβερνοεκφοβισμός.

Τα θεμελιώδη δικαιώματα, συμπεριλαμβανομένων των δικαιωμάτων των παιδιών, συνιστούν ουσιαστικό στοιχείο των αξιών της ΕΕ και πρέπει να γίνονται σεβαστά τόσο στο διαδίκτυο όσο και εκτός διαδικτύου. Τα παιδιά, οι νέες και οι νέοι έχουν το δικαίωμα στην ασφάλεια όταν αναζητούν πληροφορίες, μαθαίνουν, συνδέονται σε ψηφιακά περιβάλλοντα και γίνονται ενεργά μέλη της κοινωνίας. Οι ελευθερίες και οι δυνατότητες που προσφέρει ο ψηφιακός κόσμος πρέπει επομένως να συνοδεύονται από την αποφασιστικότητά μας να προστατεύσουμε και να ενδυναμώσουμε τα παιδιά και τους νέους ανθρώπους. Οι υποσχέσεις της ψηφιακής εποχής δεν πρέπει να υπονομευθούν από συμπεριφορές που εξευτελίζουν, αποκλείουν ή βλάπτουν.

Ο κυβερνοεκφοβισμός διαβρώνει την εμπιστοσύνη και λειτουργεί σε βάρος της αυτοεκτίμησης. Αποκλείει ανθρώπους και περιορίζει τις δυνατότητές τους. Υπονομεύει την κοινή μας φιλοδοξία να προσφέρουμε στα παιδιά, τους νέους και τις νέες μας μια δυναμική ψηφιακή Ευρώπη χωρίς αποκλεισμούς.

Τα μέσα κοινωνικής δικτύωσης αποτελούν βασικό δίαυλο μέσω του οποίου τα παιδιά και οι έφηβοι εκτίθενται σε κυβερνοεκφοβισμό, ενώ υπάρχουν όλο και περισσότερα στοιχεία που δείχνουν ότι η έκθεσή τους σε ακατάλληλο διαδικτυακό περιεχόμενο έχει μακροχρόνιες, επιβλαβείς επιπτώσεις. Η ΕΕ διαθέτει ήδη ένα ολοκληρωμένο νομικό και πολιτικό πλαίσιο για την προστασία και την ενδυνάμωση των παιδιών στο διαδίκτυο, εντός του οποίου η πράξη για τις ψηφιακές υπηρεσίες αποτελεί το κύριο εργαλείο που διαθέτουμε σήμερα προς τον σκοπό αυτό.

Όπως ανακοινώθηκε στην κατάσταση της Ένωσης το 2025, η πρόεδρος φον ντερ Λάιεν ζητά τη γνώμη εμπειρογνομόνων σχετικά με πιθανούς ηλικιακούς περιορισμούς στα μέσα κοινωνικής δικτύωσης στην Ευρώπη λόγω των διαδικτυακών κινδύνων, και αναμένεται να διατυπωθούν συστάσεις έως το καλοκαίρι του 2026. Ορισμένα κράτη μέλη εξετάζουν το ενδεχόμενο να λάβουν μέτρα για τη θέσπιση ελάχιστων ηλικιακών ορίων που να μπορούν να εφαρμοστούν όσον αφορά την πρόσβαση στα μέσα κοινωνικής δικτύωσης, καθώς και απαιτήσεων για γονική συγκατάθεση και γονικό έλεγχο. Τα μέτρα αυτά περιλαμβάνουν την ευθυγράμμιση των κατώτατων ηλικιακών ορίων για την πρόσβαση στα μέσα κοινωνικής δικτύωσης με την ηλικία ψηφιακής συγκατάθεσης, την υποχρέωση εξ ορισμού προστασίας της ιδιωτικότητας των ανηλίκων και τη δημιουργία λύσεων για ανώνυμη επαλήθευση της ηλικίας.

Μια συντονισμένη ευρωπαϊκή προσέγγιση όσον αφορά τα κατώτατα ηλικιακά όρια θα διασφάλιζε ότι όλα τα παιδιά στην Ευρώπη λαμβάνουν ίση προστασία και θα απέτρεπε τον νομικό κατακερματισμό στην ενιαία ψηφιακή αγορά. Η ομάδα εμπειρογνομόνων θα προετοιμάσει το έδαφος για μια συντονισμένη, δυνητικά νομοθετική ευρωπαϊκή προσέγγιση όσον αφορά τα κατώτατα ηλικιακά όρια και μια τεκμηριωμένη εκστρατεία ευαισθητοποίησης ώστε να δοθεί στους γονείς η δυνατότητα να αναλάβουν τον αποτελεσματικό έλεγχο της πρόσβασης των παιδιών τους σε διαδικτυακό περιεχόμενο.

Η συμβουλευτική επιτροπή νέων κοινοποίησε επίσης στην πρόεδρο της Επιτροπής τις απόψεις των νέων σχετικά με το θέμα αυτό. Η Επιτροπή εφαρμόζει πιλοτικά με τα κράτη μέλη μια [λύση επαλήθευσης της ηλικίας](#) που είναι φιλική προς τον χρήστη, προστατεύει την ιδιωτική ζωή και καθορίζει ένα «πρότυπο αναφοράς» για την επαλήθευση της ηλικίας στο διαδίκτυο. Το Ευρωπαϊκό Κοινοβούλιο έχει [ζητήσει](#) να θεσπιστεί ένα εναρμονισμένο ευρωπαϊκό ψηφιακό ελάχιστο ηλικιακό όριο στα 16 έτη για την πρόσβαση στα μέσα κοινωνικής δικτύωσης, τις πλατφόρμες διαμοιρασμού βίντεο και τους συντρόφους TN, ενώ η πρόσβαση των ατόμων ηλικίας 13 έως 16 ετών να επιτρέπεται μόνο με γονική συγκατάθεση.

Η Επιτροπή θα δρομολογήσει επίσης έρευνα σε όλη την ΕΕ βάσει της οποίας θα διεξαχθεί εν συνεχεία μια τεκμηριωμένη συζήτηση σχετικά με τις συνέπειες των μέσων κοινωνικής δικτύωσης και του υπερβολικού χρόνου που καταναλώνεται στην οθόνη για την ευεξία και την ψυχική υγεία των νέων.

Όταν τα παιδιά συνδέονται στο διαδίκτυο, ο κυβερνοεκφοβισμός παραμένει σημαντική απειλή, για την αντιμετώπιση της οποίας χρειάζεται να αναληφθεί συντονισμένη αντίδραση σε ενωσιακό και εθνικό επίπεδο. Προτεραιότητα δίνεται στην ευθύνη που έχουν οι επιγραμμικές πλατφόρμες να εγγυώνται την ασφάλεια εκ σχεδιασμού. Για να αντιμετωπιστεί ο κυβερνοεκφοβισμός χρειάζεται συνεργασία σε όλα τα επίπεδα διακυβέρνησης, συμπεριλαμβανομένων των ρυθμιστικών αρχών και των αρχών επιβολής του νόμου, καθώς και μια προσέγγιση που αγκαλιάζει το σύνολο της κοινωνίας και περιλαμβάνει γονείς, επαγγελματίες, εκπαιδευτικούς, την κοινωνία των πολιτών και τους ίδιους τους νέους ανθρώπους.

Όπως ανακοινώθηκε στις [πολιτικές κατευθύνσεις της Επιτροπής για την περίοδο 2024-2029](#), η παρούσα ανακοίνωση καθορίζει ένα στοχευμένο σχέδιο δράσης για την αποφασιστική καταπολέμηση της αυξανόμενης τάσης κακοποιητικής συμπεριφοράς στο διαδίκτυο. Επικεντρώνεται κυρίως στα παιδιά, τις νέες και τους νέους, ενώ λαμβάνει επίσης υπόψη την

ιδιαίτερα ευάλωτη θέση ορισμένων ομάδων. Ωστόσο, πολλές από τις προτεινόμενες δράσεις θα συμβάλουν στην αντιμετώπιση του κυβερνοεκφοβισμού στον ευρύτερο πληθυσμό.

Η Επιτροπή θα κάνει χρήση όλων των εργαλείων που έχει στη διάθεσή της για να συμπληρώσει την πράξη για τις ψηφιακές υπηρεσίες ώστε να διασφαλίσει ότι οι ψηφιακές πλατφόρμες θα αναλάβουν πλήρως την ευθύνη τους όσον αφορά τον εντοπισμό και την καταπολέμηση του κυβερνοεκφοβισμού. Θα υποστηρίζει όλα τα κράτη μέλη στην υιοθέτηση των βέλτιστων πρακτικών που είναι διαθέσιμες στην ΕΕ, ώστε να μεγιστοποιηθεί η αποτελεσματικότητα της δράσης τους κατά του κυβερνοεκφοβισμού. Θα εντείνει επίσης τις προσπάθειες για την προσέγγιση όλων των τμημάτων της κοινωνίας με σκοπό την ενημέρωση και την ευαισθητοποίησή τους όσον αφορά τις μορφές που μπορεί να λάβει ο κυβερνοεκφοβισμός, τους τρόπους πρόληψής του και τους τρόπους υποστήριξης των θυμάτων.

Με το παρόν σχέδιο δράσης, η Επιτροπή καλεί τα κράτη μέλη, τις περιφερειακές και τοπικές αρχές, τις επιγραμμικές πλατφόρμες, την κοινωνία των πολιτών, τα εκπαιδευτικά ιδρύματα, τις οικογένειες, και τα ίδια τα παιδιά και τους νέους ανθρώπους να δεσμευτούν σε μια κοινή προσπάθεια με σκοπό να επιτευχθεί ένα ασφαλές, συμπεριληπτικό και υποστηρικτικό ψηφιακό περιβάλλον στο οποίο να επικρατεί σεβασμός. Η πρόταση της Επιτροπής έχει ως στόχο να σταθεί η Ένωσή μας ενωμένη υπέρ της ψυχικής ευεξίας και της αξιοπρέπειας όλων των παιδιών και των νέων.

2. Διαδικτυακός εκφοβισμός: το πρόβλημα

Ο κυβερνοεκφοβισμός επηρεάζει τα παιδιά παντού: το 18,3 % των παιδιών στον κόσμο έχει υποστεί κυβερνοεκφοβισμό μέσω άμεσων μηνυμάτων, αναρτήσεων στα μέσα κοινωνικής δικτύωσης, μηνυμάτων ηλεκτρονικού ταχυδρομείου ή γραπτών μηνυμάτων. Μπορεί να εκδηλωθεί όχι μόνο μέσω κειμενικών μηνυμάτων, αλλά και μέσω οπτικοακουστικού περιεχομένου, όπως [εικόνες ή βίντεο](#) που κοινοποιούνται στο διαδίκτυο.

Στην Ευρώπη, περίπου [1 στα 6 παιδιά](#) ηλικίας 11 έως 15 ετών αναφέρει ότι έχει πέσει θύμα κυβερνοεκφοβισμού, ενώ περίπου 1 στα 8 παραδέχεται ότι έχει ασκήσει κυβερνοεκφοβισμό. Μεταξύ των ετών 2018 και 2022, ο αριθμός των [εφήβων που υπέστησαν κυβερνοεκφοβισμό](#) αυξήθηκε κατά ένα τέταρτο για τα αγόρια και σχεδόν κατά ένα τέταρτο για τα κορίτσια. Την τελευταία πενταετία, ο κυβερνοεκφοβισμός υπήρξε σταθερά [ο κύριος λόγος](#) για τις κλήσεις στις γραμμές βοήθειας των Κέντρων Ασφαλούς Διαδικτύου (SIC).

Τα 6 343 άτομα ηλικίας 12-17 ετών που συμμετείχαν στη διαβούλευση για το παρόν σχέδιο δράσης ανέφεραν [εκτεταμένη έκθεση σε κυβερνοεκφοβισμό](#): 1 στα 4 παιδιά και έφηβοι/έφηβες ηλικίας 12-17 ετών έχει βιώσει προσωπικά κυβερνοεκφοβισμό, ενώ πάνω από 1 στα 3 υπήρξαν μάρτυρες κυβερνοεκφοβισμού.

2.1 Τι είναι ο κυβερνοεκφοβισμός;

Οι ψηφιακές τεχνολογίες έχουν διευρύνει τις ευκαιρίες σύνδεσης, αλλά έχουν επίσης επιτείνει τους διαδικτυακούς κινδύνους, όπως ο κοινωνικός αποκλεισμός, τα αδικήματα μίσους, η παρενόχληση, ο εξευτελισμός και η κακοποίηση, που μπορεί να υπερβαίνουν τα φυσικά όρια και να επιμένουν σε εικοσιτετράωρη βάση 7 ημέρες την εβδομάδα.

Για τους σκοπούς του παρόντος σχεδίου δράσης, η Επιτροπή προτίθεται να προωθήσει μια **κοινή αντίληψη για τον κυβερνοεκφοβισμό**:

Ο όρος «κυβερνοεκφοβισμός» αναφέρεται σε **συμπεριφορές που εκδηλώνονται μέσω ψηφιακών τεχνολογιών, με πρωταρχική πρόθεση ή αποτέλεσμα τον επαναλαμβανόμενο ή συνεχή εξευτελισμό, κοινωνικό αποκλεισμό, κακοποίηση, παρενόχληση ή βλάβη, ιδίως παιδιών ή νέων.**

Η επανάληψη θεωρείται βασικό χαρακτηριστικό του εκφοβισμού και του κυβερνοεκφοβισμού διότι σχετίζεται με τις μακροχρόνιες επιπτώσεις που έχει στο θύμα, το οποίο μπορεί επίσης να φοβάται ότι ένα μεμονωμένο συμβάν θα μπορούσε να κοινοποιηθεί επανειλημμένα στο διαδίκτυο, με αποτέλεσμα να παρατείνεται η τραυματική του εμπειρία και να θυματοποιείται ξανά και ξανά χωρίς ο δράστης να εμπλέκεται άμεσα πλέον.

Η ανισορροπία ισχύος είναι στοιχείο καίριας σημασίας για τον εκφοβισμό, αλλά μπορεί να εκδηλωθεί με διαφορετικό τρόπο στο διαδίκτυο. Στο πλαίσιο του παραδοσιακού εκφοβισμού, η ανισορροπία ισχύος εξαρτάται συχνά από τη σωματική δύναμη, την κοινωνική θέση ή τα ομαδικά πρότυπα. Στην περίπτωση του κυβερνοεκφοβισμού, απορρέει επίσης από τα άνισα επίπεδα ψηφιακής επιρροής, ψηφιακών δεξιοτήτων, πρόσβασης στην τεχνολογία ή ελέγχου επί του περιεχομένου.

Ο κυβερνοεκφοβισμός είναι όλο και πιο δύσκολο να αντιμετωπιστεί, διότι μπορεί να συμβεί σε ιδιωτικές συσκευές ανά πάσα στιγμή, οπουδήποτε, χωρίς τη φυσική παρουσία του δράστη. Επιπλέον, συμβαίνει και σε διαύλους που δεν είναι διαθέσιμοι στο κοινό.

Οι συνηθέστερες μορφές κυβερνοεκφοβισμού περιλαμβάνουν τη διατύπωση κακόβουλων ή προσβλητικών σχολίων, τη διάδοση φημών στο διαδίκτυο ή τη δημοσίευση αναρτήσεων που θέτουν σε δύσκολη θέση ή εξευτελίζουν το θύμα.

Η ανωνυμία, η δυνατότητα προσέγγισης μεγαλύτερου κοινού και η ικανότητα αποστολής ιδιωτικών μηνυμάτων σε μεμονωμένους χρήστες ανά πάσα στιγμή διογκώνουν τη βλάβη που προκαλεί ο παραδοσιακός εκφοβισμός. Επιπλέον, τα ψηφιακά περιβάλλοντα ευνοούν την ηθική αποστασιοποίηση, τη μείωση της ενσυναίσθησης και την απουσία αναστολών στο διαδίκτυο, χαμηλώνοντας έτσι τους φραγμούς στη διαδικτυακή επιθετικότητα.

Το επιβλαβές περιεχόμενο μπορεί να παραμείνει στο διαδίκτυο επ' αόριστον. Μπορεί να είναι προσβάσιμο και να κοινοποιείται εκ νέου συνεχώς ή να διαδίδεται ιότροπα, γεγονός που επιτείνει τη βλάβη, προκαλεί εκ νέου θυματοποίηση και εμποδίζει την αποκατάσταση της βλάβης. Οι παράγοντες αυτοί πρέπει να λαμβάνονται υπόψη για την παροχή αποτελεσματικής στήριξης. Οι συνθήκες αυτές διευρύνουν επίσης το δυνητικό κοινό, διότι καθιστούν δυνατή τη συνεχή μετακίνηση της επιθετικότητας μεταξύ διαδικτυακών και μη διαδικτυακών χώρων, ή αντιστρόφως.

Ως αποτέλεσμα της ταχείας ανάπτυξης των ψηφιακών τεχνολογιών που παρατηρούμε στις μέρες μας, τα περιβάλλοντα και τα εργαλεία που χρησιμοποιούνται για την πρόκληση βλάβης μεταβάλλονται συνεχώς. Για να διασφαλίζεται ευελιξία, θα πρέπει να χρησιμοποιούνται οι πλέον πρόσφατες τεχνολογίες για τον εντοπισμό και την αντιμετώπιση του φαινομένου.

Ειδικότερα, η τεχνητή νοημοσύνη (TN) μπορεί μεν να συμβάλει στον εντοπισμό του κυβερνοεκφοβισμού, όμως η αυξανόμενη χρήση της, ιδίως η χρήση της παραγωγικής TN, και η ενσωμάτωσή της σε διαδικτυακές εφαρμογές και υπηρεσίες, αυξάνει τους κινδύνους και τα εργαλεία κυβερνοεκφοβισμού ή δημιουργεί ακόμη και νέους τέτοιους κινδύνους και εργαλεία. Για παράδειγμα, τα προϊόντα βαθυπαραποίησης (deepfake) αυξάνονται και χρησιμοποιούνται όλο και περισσότερο για σαφή σεξουαλική κακοποίηση μέσω προϊόντων βαθυπαραποίησης που στη συντριπτική τους πλειονότητα στοχοποιούν γυναίκες και κορίτσια, μεταξύ άλλων σε περιπτώσεις κυβερνοεκφοβισμού, και κυμαίνονται από επιβλαβή συμπεριφορά έως ποινικά αδικήματα όταν περιλαμβάνουν τη δημιουργία εικόνων που συνιστούν σεξουαλική κακοποίηση παιδιών ή έμφυλη βία στο διαδίκτυο. Οι εξελίξεις αυτές δημιουργούν μια πρόσθετη δυνατότητα πρόκλησης βλάβης που όχι μόνο θίγει την υπόληψη του θύματος, αλλά, όπως και άλλες συμπεριφορές διαδικτυακού εκφοβισμού, θα μπορούσε να προκαλέσει ψυχολογικό τραύμα, γεγονός που καταδεικνύει την επείγουσα ανάγκη παρακολούθησης και αντιμετώπισης αυτών των αναδυόμενων κινδύνων σε επίπεδο ΕΕ.

Ο κυβερνοεκφοβισμός και τα αδικήματα μίσους ενδέχεται να αλληλεπικαλύπτονται όταν ο κυβερνοεκφοβισμός έχει ως κίνητρο το μίσος ή υποκινεί βία και μίσος και στοχοποιεί άτομα που προσδιορίζονται βάσει ορισμένων προστατευόμενων χαρακτηριστικών. Η απόφαση-πλαίσιο 2008/913/ΔΕΥ του Συμβουλίου απαιτεί από τα κράτη μέλη να ποινικοποιήσουν τη δημόσια υποκίνηση πράξεων βίας ή μίσους που στρέφεται κατά ομάδας προσώπων ή μέλους ομάδας, που προσδιορίζεται βάσει της φυλής, του χρώματος, της θρησκείας, των γενεαλογικών καταβολών ή της εθνικής καταγωγής. Απαιτεί επίσης από τα κράτη μέλη να διασφαλίζουν ότι προβλέπονται πρόσθετες κυρώσεις για ποινικά αδικήματα που διαπράττονται με ρατσιστικά ή ξενοφοβικά κίνητρα.

Ο κυβερνοεκφοβισμός μπορεί να αλληλεπικαλύπτεται με τη σεξουαλική κακοποίηση παιδιών κατά την έννοια της οδηγίας 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας.

Η οδηγία 2024/1385 για την καταπολέμηση της βίας κατά των γυναικών και της εξ οικείων βίας απαιτεί από τα κράτη μέλη να διασφαλίζουν ότι η έμφυλη κυβερνοϋποκίνηση βίας ή μίσους τιμωρείται ως ποινικό αδίκημα. Ποινικοποιεί επίσης άλλα αδικήματα κυβερνοβίας που συχνά προκύπτουν στο πλαίσιο κυβερνοεκφοβισμού: τη μη συναινετική κοινοχρησία υλικού προσωπικής φύσης ή παραποιημένου υλικού, την παρενοχλητική κυβερνοπαρακολούθηση και την κυβερνοπαρενόχληση. Η οδηγία περιλαμβάνει επίσης διατάξεις που επιτρέπουν την άμεση αφαίρεση παράνομου υλικού κυβερνοβίας.

2.2 Ομάδες που διατρέχουν κίνδυνο κυβερνοεκφοβισμού

Ο κυβερνοεκφοβισμός είναι ιδιαίτερα διαδεδομένος μεταξύ **των παιδιών και των εφήβων σχολικής ηλικίας**, ιδίως καθώς αυξάνεται η διαδικτυακή τους δραστηριότητα.

Οι γυναίκες και τα κορίτσια εκτίθενται σε σεξιστικό και μισογυνικό εκφοβισμό και επηρεάζονται δυσανάλογα, για παράδειγμα, από τη μη συναινετική κοινοχρησία εικόνων προσωπικής φύσης και βαθυπαραποιήσεων σαφώς σεξουαλικού χαρακτήρα.

Οι **ευάλωτες ομάδες** εκτίθενται δυσανάλογα στον κυβερνοεκφοβισμό, δεδομένου ότι αυτός μπορεί να ασκηθεί κατά ενός ατόμου επειδή θεωρείται ότι ανήκει σε τέτοιες ομάδες.

Τα παιδιά από νοικοκυριά χαμηλού εισοδήματος είναι πιθανότερο να εκτεθούν σε κυβερνοεκφοβισμό από ό,τι άλλα συνομήλικά τους παιδιά.

Τα παιδιά, οι νέες και οι νέοι με αναπηρία βιώνουν υψηλότερα επίπεδα διαδικτυακής θυματοποίησης, συμπεριλαμβανομένης της σεξουαλικής και έμφυλης βίας. Ορισμένα μάλιστα από τα άτομα αυτά αποσύρονται από τους ψηφιακούς χώρους λόγω της συνεχούς κακοποίησης που υφίστανται.

Οι εθνοτικές και θρησκευτικές μειονότητες, οι μετανάστες και οι πρόσφυγες αντιμετωπίζουν αυξημένους κινδύνους ρατσιστικού εκφοβισμού ή εκφοβισμού που εισάγει διακρίσεις. Για παράδειγμα, οι Ρομά και άλλες φυλετικές ή εθνοτικές μειονότητες είναι ιδιαίτερα εκτεθειμένοι σε διαδικτυακή παρενόχληση και παράνομη ρητορική μίσους που συνδέεται με συστημικό αποκλεισμό, ενώ το 90 % των Εβραίων Ευρωπαίων ανέφερε ότι βίωσε αντισιμιτισμό στο διαδίκτυο κατά το προηγούμενο έτος.

Μεταξύ των **ατόμων ΛΟΑΤΚΙ+**, το 63 % έχει βρεθεί συχνά αντιμέτωπο με βίαιο διαδικτυακό περιεχόμενο κατά της κοινότητας ΛΟΑΤΚΙ+. Επιπλέον, το 11 % ανέφερε ότι αναρτήθηκαν προσβλητικά ή απειλητικά σχόλια εναντίον του στο διαδίκτυο κατά το προηγούμενο έτος, ενώ τα δύο τρίτα έχουν βιώσει χλευασμό ή παρενόχληση στο σχολείο.

Οι δράσεις που προτείνονται στο παρόν σχέδιο δράσης θα συμβάλουν στην αντιμετώπιση του κυβερνοεκφοβισμού για κάθε θύμα. Τα ζητήματα ισότητας που περιγράφονται ανωτέρω θα ληφθούν υπόψη κατά την εφαρμογή με σκοπό την ενίσχυση του αντικτύπου των δράσεων.

2.3 Ο αντίκτυπος του κυβερνοεκφοβισμού

Οι συνέπειες του κυβερνοεκφοβισμού μπορεί να είναι σοβαρές και μακροχρόνιες, τόσο για τα άτομα όσο και για την κοινωνία γενικότερα. Βραχυπρόθεσμα, ο κυβερνοεκφοβισμός μπορεί να αποτελέσει ένα πρώτο βήμα προς σοβαρότερα εγκλήματα ή κακοποίηση, συμπεριλαμβανομένης της σεξουαλικής κακοποίησης.

Τα θύματα κυβερνοεκφοβισμού αντιμετωπίζουν αυξημένο κίνδυνο άγχους, κατάθλιψης, μοναξιάς, αυτοτραυματισμού και αυτοκτονικής συμπεριφοράς, και είναι πιο επιρρεπή σε προβλήματα συμπεριφοράς, συμπεριλαμβανομένων επιβλαβών συμπεριφορών αντιμετώπισης. Επιπλέον, τα άτομα που υφίστανται κυβερνοεκφοβισμό ενδέχεται να ασκήσουν και τα ίδια κυβερνοεκφοβισμό, αν μη τι άλλο σε μια απόπειρα να ξεφύγουν από τον ρόλο τους ως θυμάτων. Για να αντιμετωπιστεί η κατάσταση αυτή απαιτείται μια προσεκτική και φιλική προς τα παιδιά αντίδραση.

Ο κυβερνοεκφοβισμός μπορεί επίσης να λειτουργήσει σε βάρος των επιδόσεων στο σχολείο ή το πανεπιστήμιο, της ευημερίας των μαθητών και του σχολικού περιβάλλοντος, γεγονός που μπορεί να έχει μακροπρόθεσμες συνέπειες για την εκπαιδευτική και επαγγελματική τους εξέλιξη, καθώς και για τη συνολική ευημερία και ικανοποίησή τους από τη ζωή.

Ως εκ τούτου, ο αντίκτυπος στα παιδιά, τις νέες και τους νέους μπορεί να έχει εκτεταμένες συνέπειες για την κοινωνία, καθώς επιδεινώνει υφιστάμενες ανισότητες.

3. Μελλοντική πορεία

Υπάρχει ανάγκη για μια πιο αποφασιστική, συνεπή και συντονισμένη αντίδραση της ΕΕ στον κυβερνοεκφοβισμό η οποία, αφενός, θα ενισχύσει τις προσπάθειες πρόληψης και ψηφιακού γραμματισμού και, αφετέρου, θα βελτιώσει και θα απλουστεύσει την υποβολή αναφορών και την υποστήριξη των θυμάτων σε ολόκληρη την Ένωση. Το όραμά μας είναι μια Ευρώπη στην οποία κάθε παιδί, κάθε νέος και κάθε νέα θα μπορεί να μεγαλώνει χωρίς κυβερνοεκφοβισμό, να προστατεύεται η αξιοπρέπεία του/της και να ενδυναμώνεται ώστε να ευδοκίμει σε έναν ψηφιακό κόσμο που σέβεται τις ευρωπαϊκές αξίες. Για τον σκοπό αυτό, το παρόν σχέδιο δράσης εδράζεται σε τρεις αλληλένδετους πυλώνες: Συντονισμένη προσέγγιση της ΕΕ, πρόληψη και ευαισθητοποίηση, και υποβολή αναφορών και υποστήριξη.

Αυτή η έκκληση για ανάληψη δράσης υποστηρίζεται από την κοινή γνώμη: [περισσότεροι/περισσότερες από 9 στους 10 Ευρωπαίους και Ευρωπαϊές](#) δηλώνουν ότι χρειάζεται να αναλάβουν οι δημόσιες αρχές επείγοντως δράση για την προστασία των παιδιών από τον κυβερνοεκφοβισμό. Η [δημόσια διαβούλευση](#) για το σχέδιο αυτό έδειξε έντονη υποστήριξη στον ψηφιακό γραμματισμό και τα προγράμματα οικοδόμησης ενσυναίσθησης στα σχολεία και την κατάρτιση των εκπαιδευτικών, καθώς και για τη βελτίωση των εργαλείων υποβολής αναφορών και των υπηρεσιών υποστήριξης των θυμάτων.

3.1 Πυλώνας I: Μια συντονισμένη προσέγγιση της ΕΕ για την προστασία

Η Επιτροπή θα αξιοποιήσει πλήρως τα υφιστάμενα πολιτικά και νομικά μέσα και θα εντοπίσει ευκαιρίες για την καταπολέμηση του κυβερνοεκφοβισμού στο πλαίσιο μελλοντικών πρωτοβουλιών. Επιπλέον, **τα κράτη μέλη καλούνται να μετατρέψουν τους κοινούς στόχους σε αποτελεσματικά εθνικά μέτρα και να οικοδομήσουν ένα ολοκληρωμένο και λειτουργικό οικοσύστημα για την αντιμετώπιση του κυβερνοεκφοβισμού.**

Η πράξη για τις ψηφιακές υπηρεσίες παραμένει κεντρικής σημασίας για τις προσπάθειες επιβολής δεδομένου ότι απαιτεί από τους παρόχους επιγραμμικών πλατφορμών που είναι προσβάσιμες σε ανηλίκους να διασφαλίζουν υψηλό επίπεδο ιδιωτικότητας, ασφάλειας και προστασίας των ανηλίκων στην υπηρεσία τους.

Επιπλέον, οι [κατευθυντήριες γραμμές για την πράξη για τις ψηφιακές υπηρεσίες](#) σχετικά με την προστασία των ανηλίκων στο διαδίκτυο καθορίζουν μέτρα που θα πρέπει να εφαρμόζουν οι πάροχοι επιγραμμικών πλατφορμών για τη συμμόρφωση με την εν λόγω υποχρέωση, συμπεριλαμβανομένων κατάλληλων μέτρων για τη μείωση του κινδύνου έκθεσης των

ανηλίκων σε επιβλαβές περιεχόμενο, όπως ο σχεδιασμός συστημάτων συστάσεων προς το βέλτιστο συμφέρον των ανηλίκων, ή σε επιβλαβή συμπεριφορά, συμπεριλαμβανομένων των κινδύνων που σχετίζονται με την επαφή από αλληλεπιδράσεις με συνομιλήκους. Για την προστασία των θυμάτων κυβερνοεκφοβισμού, περιλαμβάνουν εξάλλου μέτρα ελέγχου και ενδυνάμωσης των χρηστών, φιλικούς προς τα παιδιά μηχανισμούς και εργαλεία υποβολής καταγγελιών, καθώς και έλεγχο περιεχομένου στις επίσημες γλώσσες του κράτους μέλους στο οποίο παρέχεται η υπηρεσία. Η πράξη για τις ψηφιακές υπηρεσίες απαιτεί επίσης από τους παρόχους επιγραμμικών πλατφορμών να θέτουν σε εφαρμογή εύκολα προσβάσιμους και εύχρηστους μηχανισμούς που παρέχουν σε κάθε χρήστη, συμπεριλαμβανομένων των ανηλίκων, τη δυνατότητα υποβολής αναφορών για παράνομο περιεχόμενο, π.χ. ορισμένες μορφές παράνομης ρητορικής μίσους ή υλικό παιδικής πορνογραφίας. Ανάλογα με την εθνική νομοθεσία, μορφές κυβερνοεκφοβισμού μπορεί επίσης να είναι παράνομες. Οι πάροχοι πρέπει να λαμβάνουν άμεσα αποφάσεις μόλις λάβουν τέτοιες ειδοποιήσεις.

Το παρόν σχέδιο δράσης θα τροφοδοτήσει την επικείμενη επανεξέταση και επικαιροποίηση των κατευθυντήριων γραμμών για την πράξη για τις ψηφιακές υπηρεσίες όσον αφορά την προστασία των ανηλίκων στο διαδίκτυο. Ειδικότερα, οι κατευθυντήριες γραμμές θα μπορούσαν να βοηθούν τους παρόχους επιγραμμικών πλατφορμών να σχεδιάζουν αποτελεσματικότερα εργαλεία υποβολής αναφορών, π.χ. όσον αφορά την ορατότητα, την τεχνική προσβασιμότητα και τη γλωσσική τους κάλυψη, και να χρησιμοποιούν αποτελεσματικές τεχνολογίες για την πρόληψη της έκθεσης σε κυβερνοεκφοβισμό. Οι κατευθυντήριες γραμμές θα μπορούσαν επίσης να βοηθούν τους παρόχους στον σχεδιασμό κατάλληλων μέτρων αντίδρασης σε ειδοποιήσεις από ανηλίκους, π.χ. βοηθώντας τους χρήστες να αποθηκεύουν πληροφορίες που μπορούν να χρησιμεύσουν ως αποδεικτικά στοιχεία.

Η πράξη για τις ψηφιακές υπηρεσίες προβλέπει επίσης τη δυνατότητα ύπαρξης «αξιόπιστων πηγών επισήμανσης παράνομου περιεχομένου», εξειδικευμένων οντοτήτων στις ειδοποιήσεις των οποίων πρέπει να δίνεται προτεραιότητα. Οι διατάξεις αυτές μπορούν να χρησιμοποιούνται για την αντιμετώπιση του κυβερνοεκφοβισμού παρέχοντας στις αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου τη δυνατότητα να συμβάλλουν στην αντιμετώπιση της διάδοσης παράνομου περιεχομένου κυβερνοεκφοβισμού. Η Επιτροπή θα εκδώσει κατευθυντήριες γραμμές σχετικά με τις αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου για να βοηθήσει να αποσαφηνιστεί ο ρόλος τους στην αντιμετώπιση του παράνομου περιεχομένου, συμπεριλαμβανομένου του παράνομου κυβερνοεκφοβισμού. Οι εν λόγω κατευθυντήριες γραμμές θα συμβάλουν επίσης στην αποσαφήνιση των υποχρεώσεων των παρόχων επιγραμμικών πλατφορμών όσον αφορά τις ειδοποιήσεις που υποβάλλονται από αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου.

Κυβερνοεκφοβισμός μπορεί επίσης να ασκηθεί μέσω οπτικοακουστικού περιεχομένου στο διαδίκτυο. Η οδηγία για τις υπηρεσίες οπτικοακουστικών μέσων (οδηγία YOAM) καθορίζει γενικές απαιτήσεις για την προστασία των ανηλίκων, ιδίως στο διαδίκτυο, από επιβλαβές περιεχόμενο που δύναται να υπονομεύσει τη σωματική, πνευματική ή ηθική τους ανάπτυξη. Σε αυτό περιλαμβάνεται το περιεχόμενο που συνιστά κυβερνοεκφοβισμό. Η οδηγία YOAM επιβάλλει στις πλατφόρμες διαμοιρασμού βίντεο την υποχρέωση να λαμβάνουν κατάλληλα μέτρα ώστε να αποφεύγεται η πρόσβαση των ανηλίκων σε επιβλαβές περιεχόμενο μέσω της συμπερίληψης προτύπων για το περιεχόμενο των μέσων ενημέρωσης στους όρους και τις προϋποθέσεις τους ή συστημάτων γονικού ελέγχου και διαβάθμισης περιεχομένου. Επιπλέον,

τα κράτη μέλη έχουν την υποχρέωση να προστατεύουν την ανθρώπινη αξιοπρέπεια κατά την εφαρμογή της οδηγίας YOAM. Κατά την εν εξελίξει αξιολόγηση και επανεξέταση της οδηγίας θα αξιολογηθεί πόσο αποτελεσματικά έχουν εφαρμόσει οι πλατφόρμες διαμοιρασμού βίντεο τους εν λόγω κανόνες και κατά πόσον πρέπει να γίνουν περισσότερα για την προστασία των ανηλίκων από επιβλαβές περιεχόμενο στο διαδίκτυο, μεταξύ άλλων σε σχέση με τον κυβερνοεκφοβισμό, και σε ευθυγράμμιση με την πράξη για τις ψηφιακές υπηρεσίες.

Ο κανονισμός για την τεχνητή νοημοσύνη απαγορεύει τα συστήματα ΤΝ που χειραγωγούν ή παραπλανούν πρόσωπα εκμεταλλευόμενα τρωτά σημεία που συνδέονται με την ηλικία τους, προκειμένου να στρεβλώσουν τη συμπεριφορά τους προκαλώντας σημαντική βλάβη. Οι απαγορεύσεις αυτές μπορούν να αποτρέψουν τον κυβερνοεκφοβισμό. Η Επιτροπή εξέδωσε κατευθυντήριες γραμμές σχετικά με τις απαγορευμένες πρακτικές ΤΝ προκειμένου να διευκολύνει τη συνεπή και αποτελεσματική εφαρμογή σε ολόκληρη την Ένωση. Ο κανονισμός για την ΤΝ θεσπίζει επίσης απαιτήσεις διαφάνειας, συμπεριλαμβανομένης της υποχρέωσης ενημέρωσης των χρηστών όταν αλληλεπιδρούν με την ΤΝ και σαφούς επισήμανσης του περιεχομένου που έχει παραχθεί ή υποστεί χειρισμό από ΤΝ, όπως τα προϊόντα βαθυπαραποίησης, για την πρόληψη της παραπλάνησης.

Επιπλέον, οι πολιτικές αυτές πρέπει να συμπληρώνονται με τη συλλογή δεδομένων σχετικά με τον κυβερνοεκφοβισμό, η οποία επί του παρόντος δεν γίνεται με συνεπή τρόπο και δυσχεραίνει τη σφαιρική κατανόηση των τάσεων σε όλα τα κράτη μέλη. Ανταποκρινόμενη στην έκκληση που προέκυψε από τη δημόσια διαβούλευση, η Επιτροπή θα διευκολύνει τη συνεπή και συγκρίσιμη συλλογή δεδομένων σχετικά με τον κυβερνοεκφοβισμό σε ολόκληρη την ΕΕ, για παράδειγμα με την παροχή καθοδήγησης, όπως ένα κοινό πλαίσιο για τη συλλογή δεδομένων και σχετικοί δείκτες, και με τη δρομολόγηση ερευνών σε επίπεδο ΕΕ μέσω της πλατφόρμας «Καλύτερο διαδίκτυο για τα παιδιά» (BIK) σε συνεργασία με άλλους μηχανισμούς συμμετοχής των παιδιών και των νέων. Θα παρασχεθούν επαρκείς πόροι ώστε το δίκτυο των Κέντρων Ασφαλούς Διαδικτύου (SIC) να μπορέσει να αναλάβει αυτά τα πρόσθετα καθήκοντα και να διασφαλίσει τη μακροπρόθεσμη συνέχεια των εργασιών αυτών.

Η Επιτροπή:

1. θα επεκτείνει την εστίαση στην αντιμετώπιση του κυβερνοεκφοβισμού κατά την **επανεξέταση των κατευθυντήριων γραμμών για την πράξη για τις ψηφιακές υπηρεσίες σχετικά με την προστασία των ανηλίκων**, ιδίως όσον αφορά μέτρα για την περαιτέρω πρόληψη της έκθεσης σε επιβλαβές περιεχόμενο, και τη βελτίωση των συστημάτων των επιγραμμικών πλατφορμών για την υποβολή αναφορών – έχει προγραμματιστεί για το **2026**·
2. θα εκδώσει **κατευθυντήριες γραμμές για την πράξη για τις ψηφιακές υπηρεσίες σχετικά με τις αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου** με σκοπό να συμβάλει στην αποσαφήνιση του ρόλου τους στην αντιμετώπιση παράνομου περιεχομένου, όπως ο παράνομος κυβερνοεκφοβισμός – έως το **2ο τρίμηνο του 2026**·
3. θα εξετάσει τρόπους για την αντιμετώπιση του κυβερνοεκφοβισμού στις πλατφόρμες διαμοιρασμού βίντεο κατά την εν εξελίξει **αξιολόγηση της οδηγίας για τις**

υπηρεσίες οπτικοακουστικών μέσων (οδηγία YOAM) και την επανεξέτασή της – έως το 3ο τρίμηνο του 2026·

- 4. Θα υποστηρίξει την αποτελεσματική εφαρμογή των διατάξεων του κανονισμού για την TN σχετικά με τις απαγορευμένες πρακτικές TN, μεταξύ άλλων όταν χρησιμοποιούνται για κυβερνοεκφοβισμό, μέσω συντονισμού στο πλαίσιο του Συμβουλίου TN και της καθοδήγησης που παρέχεται με τις κατευθυντήριες γραμμές της Επιτροπής σχετικά με τις απαγορευμένες πρακτικές TN – από το 3ο τρίμηνο του 2026·**
- 5. Θα διευκολύνει την αποτελεσματική εφαρμογή των υποχρεώσεων διαφάνειας του κανονισμού για την TN, μεταξύ άλλων μέσω κώδικα ορθής πρακτικής για τη σήμανση και την επισήμανση περιεχομένου που παράγεται από TN, ο οποίος αποσκοπεί στην υποστήριξη της συμμόρφωσης με τις υποχρεώσεις διαφάνειας του κανονισμού για την TN όσον αφορά τη σήμανση και την επισήμανση περιεχομένου που παράγεται από TN, μεταξύ άλλων αυτού που χρησιμοποιείται για κυβερνοεκφοβισμό – από το 3ο τρίμηνο του 2026.**

Τα κράτη μέλη καλούνται:

1. να καταρτίσουν **ολοκληρωμένα εθνικά σχέδια κατά του εκφοβισμού, συμπεριλαμβανομένου του κυβερνοεκφοβισμού**, αξιοποιώντας την υποστήριξη που παρέχει το δίκτυο της ΕΕ για τα δικαιώματα του παιδιού σύμφωνα με την [ανακοίνωση και τη σύσταση της Επιτροπής σχετικά με ολοκληρωμένα συστήματα προστασίας των παιδιών](#)·
2. να χρησιμοποιήσουν την κοινή αντίληψη για τον κυβερνοεκφοβισμό που προτείνεται στο παρόν σχέδιο δράσης για τη **συλλογή συνεκτικών και συγκρίσιμων δεδομένων σχετικά με τον κυβερνοεκφοβισμό**, έργο που διευκολύνεται από την υποστήριξη που παρέχει η Επιτροπή μέσω του δικτύου των Κέντρων Ασφαλούς Διαδικτύου και της πλατφόρμας «Καλύτερο διαδίκτυο για τα παιδιά», και να συνεργαστούν για την επίτευξη κοινών προτύπων για την αντιμετώπιση του κυβερνοεκφοβισμού σε ολόκληρη την ΕΕ.

3.2 Πυλώνας II: Πρόληψη και ευαισθητοποίηση

Ο καλύτερος τρόπος για την καταπολέμηση του κυβερνοεκφοβισμού είναι η ανάληψη δράσης πριν από την εμφάνιση επιβλαβών περιστατικών. Για την πρόληψη του κυβερνοεκφοβισμού είναι αναγκαίες υγιείς ψηφιακές πρακτικές εξ απαλών ονύχων. Πρόκειται για τον εφοδιασμό των παιδιών, των νέων και των ενηλίκων με τις δεξιότητες και την αυτοπεποίθηση που χρειάζονται για να μιλούν για τους κινδύνους στο διαδίκτυο και να τους αναγνωρίζουν. Είναι επίσης σημαντικό να αντιμετωπίζονται οι υποκείμενες συμπεριφορές που μπορούν να οδηγήσουν σε επιβλαβή συμπεριφορά στο διαδίκτυο.

Για να είναι αποτελεσματικές οι προσπάθειες πρόληψης, πρέπει να περιλαμβάνουν και τα άτομα που γίνονται μάρτυρες περιστατικών κυβερνοεκφοβισμού, τους συνομιλήκους, τους δράστες, τους γονείς, τους φροντιστές, τους εκπαιδευτικούς και την ευρύτερη σχολική

κοινότητα, με την υποστήριξη όλων των σχετικών φορέων, ιδίως των οργανώσεων της κοινωνίας των πολιτών. Αυτό υποστηρίχθηκε από το 62 % όσων συμμετείχαν στη δημόσια διαβούλευση, οι οποίοι τόνισαν την ανάγκη να στηριχθεί η επαγγελματική κατάρτιση των εκπαιδευτικών, των αρχών επιβολής του νόμου και των κοινωνικών λειτουργών.

Πρωτοβουλίες πρόληψης και ευαισθητοποίησης θα πρέπει επίσης να υλοποιούνται σε περιβάλλοντα τόσο άτυπης όσο και μη τυπικής μάθησης, όπως κέντρα νεολαίας, αθλητικοί σύλλογοι και κοινοτικά περιβάλλοντα, όπου παιδιά, νέες και νέοι περνούν μεγάλο μέρος του χρόνου τους. Οι πρωτοβουλίες αυτές θα πρέπει επίσης να ενσωματώνουν την πρόληψη και την καταπολέμηση κάθε μορφής διακρίσεων, σε συνέργεια με τις στρατηγικές της ΕΕ για την ισότητα.

Η ψηφιακή εκπαίδευση και ο ψηφιακός γραμματισμός καθίστανται όλο και πιο αναγκαία εφόδια για την ασφαλή και υπεύθυνη πλοήγηση στον διαδικτυακό κόσμο. Η ενημέρωση των παιδιών και των νέων για τη σημασία του σεβασμού και της υπευθυνότητας σε ψηφιακά περιβάλλοντα μπορεί να μειώσει τις πιθανότητες να υποστούν εκούσια ή ακούσια βλάβη. Η ενημέρωση αυτή προβλέπεται επίσης ως προληπτικό μέτρο στην οδηγία για την καταπολέμηση της βίας κατά των γυναικών και της εξ οικείων βίας.

Τα παιδιά οι νέοι και οι νέες, συμπεριλαμβανομένων όσων έχουν ειδικές ανάγκες, αναπηρία ή βρίσκονται σε ευάλωτη κατάσταση, θα πρέπει να συμμετέχουν ενεργά στον σχεδιασμό και την υλοποίηση προσβάσιμων δραστηριοτήτων ευαισθητοποίησης που ενδυναμώνουν και δεν εισάγουν αποκλεισμούς, ώστε να σπάσει η σιωπή γύρω από τον κυβερνοεκφοβισμό.

Η Επιτροπή θα καταστήσει διαθέσιμη μια σειρά εργαλείων πρόληψης και ευαισθητοποίησης σε επίπεδο ΕΕ, τα οποία θα αναπτυχθούν σε συνεργασία με παιδιά, νέες και νέους, γονείς, εκπαιδευτικούς, επαγγελματίες ψυχικής υγείας και κράτη μέλη, καθώς και οργανώσεις της κοινωνίας των πολιτών.

Στο πλαίσιο του σχεδίου δράσης για την ψηφιακή εκπαίδευση (2021-2027), η Ευρωπαϊκή Επιτροπή θα επικαιροποιήσει τις κατευθυντήριες γραμμές της για διδάσκοντες και εκπαιδευτικούς σχετικά με την αντιμετώπιση της παραπληροφόρησης και την προώθηση του ψηφιακού γραμματισμού μέσω της εκπαίδευσης και της κατάρτισης. Επιπλέον, όπως εξαγγέλθηκε στην ανακοίνωση σχετικά με την Ευρωπαϊκή Ασπίδα Δημοκρατίας, οι επικαιροποιήσεις θα αποτυπώνουν τις εξελίξεις στην ΤΝ και τα μέσα κοινωνικής δικτύωσης και θα περιλαμβάνουν διδακτικό υλικό και δραστηριότητες σχετικά με τον κυβερνοεκφοβισμό με ιδιαίτερη προσοχή στην ένταξη και την πολυμορφία. Η Ευρωπαϊκή Επιτροπή θα αναπτύξει επίσης ένα πλαίσιο ικανοτήτων για την ιθαγένεια της ΕΕ μαζί με κατευθυντήριες γραμμές για την ενίσχυση της αγωγής του πολίτη στα σχολεία.

Επιπλέον, ο ψηφιακός γραμματισμός, η πρόληψη του κυβερνοεκφοβισμού και η ψηφιακή ευημερία θα αποτελέσουν τομείς εστίασης στον χάρτη πορείας του 2030 για το μέλλον της ψηφιακής εκπαίδευσης και των ψηφιακών δεξιοτήτων. Ο χάρτης πορείας του 2030 θα έχει ως στόχο να διασφαλίσει ότι οι νέες και οι νέοι θα υποστηρίζονται ώστε να αποκτήσουν υγιείς διαδικτυακές συνήθειες και θα ενημερώνονται σχετικά με την υπεύθυνη χρήση των ψηφιακών συσκευών, τόσο εντός όσο και εκτός της αίθουσας διδασκαλίας.

Το έργο αυτό για τον ψηφιακό γραμματισμό βασίζεται σε πρωτοβουλίες που υλοποιεί η Επιτροπή μέσω του προγράμματος Erasmus+ και του Ευρωπαϊκού Σώματος Αλληλεγγύης, της Ευρωπαϊκής Πλατφόρμας Σχολικής Εκπαίδευσης (ESEP) και του δικτύου ηλεκτρονικής αδελφοποίησης (eTwinning). Στο πλαίσιο της ESEP, η Επιτροπή θα μεριμνήσει για την καλύτερη και μόνιμη προβολή όλου του υλικού που μπορεί να χρησιμεύσει στα σχολεία όσον αφορά τον εκφοβισμό, συμπεριλαμβανομένου του κυβερνοεκφοβισμού. Από την πρόσκληση υποβολής προτάσεων στο πλαίσιο του Erasmus+ του 2026, η ευημερία στο σχολείο θα ενισχυθεί με σκοπό την καλύτερη στήριξη, παρακολούθηση και ενθάρρυνση έργων για την αντιμετώπιση του εκφοβισμού και του κυβερνοεκφοβισμού.

Το δίκτυο της ΕΕ για την πρόληψη της σεξουαλικής κακοποίησης παιδιών θα συμβάλει στην προώθηση της εκπαίδευσης και της ευαισθητοποίησης των παιδιών σε σχέση με τη σεξουαλική κακοποίηση παιδιών, συμπεριλαμβανομένων πρωτοβουλιών που συμβάλλουν στην πρόληψη της κλιμάκωσης περιπτώσεων κυβερνοεκφοβισμού σε εγκληματική συμπεριφορά (π.χ. διάδοση υλικού σεξουαλικής κακοποίησης παιδιών). Επιπλέον, η πρόληψη του κυβερνοεκφοβισμού θα εξεταστεί επίσης στο επικείμενο σχέδιο δράσης της ΕΕ για την προστασία των παιδιών από την εγκληματικότητα. Το σχέδιο δράσης θα επιδιώξει να παράσχει συνεκτική και ολοκληρωμένη απόκριση στους διάφορους κινδύνους που αντιμετωπίζουν τα παιδιά σε σχέση με την εγκληματικότητα, τόσο στο διαδίκτυο όσο και εκτός διαδικτύου.

Η πλατφόρμα «Καλύτερο διαδίκτυο για τα παιδιά» (BIK) και το δίκτυο των SIC παρέχουν εργαλεία υποστήριξης για παιδιά, γονείς, εκπαιδευτικούς και επαγγελματίες σε επίπεδο ΕΕ (η BIK) και σε εθνικό επίπεδο (τα SIC). Οι πόροι αυτοί θα επεκταθούν περαιτέρω ώστε να ενισχύονται οι ικανότητες, να προσεγγίζονται περισσότερα ενδιαφερόμενα μέρη και να αντιμετωπίζονται νέες προκλήσεις όσον αφορά τον κυβερνοεκφοβισμό.

Δεδομένου ότι τα σχολεία διαδραματίζουν καίριο ρόλο στην πρόληψη του κυβερνοεκφοβισμού, θα διοργανώνονται στην αρχή κάθε νέου σχολικού έτους δραστηριότητες ευαισθητοποίησης με την υποστήριξη των SIC και της πλατφόρμας BIK, αρχής γενομένης από την ετήσια εκστρατεία «Back to School», με σκοπό τον εφοδιασμό των διδασκόντων και των παιδιών με εκπαιδευτικό υλικό, εργαλεία και πληροφορίες σχετικά με τρόπους πρόληψης και αναφοράς του κυβερνοεκφοβισμού.

Οι πόροι και η κατάρτιση σχετικά με τον κυβερνοεκφοβισμό για τη μη τυπική και την άτυπη εκπαίδευση θα ενισχυθούν μέσω ευρωπαϊκών πλατφορμών. Σε αυτές περιλαμβάνονται η Ευρωπαϊκή Δικτυακή Πύλη της Νεολαίας, η οποία είναι η υπηρεσία μίας στάσης για την ευαισθητοποίηση και την προώθηση ευκαιριών για νέες και νέους, η Ευρωπαϊκή Πλατφόρμα Σχολικής Εκπαίδευσης, η οποία αποτελεί το σημείο συνάντησης για την κοινότητα της σχολικής εκπαίδευσης, και η Γωνιά μάθησης, η οποία παρέχει σε διδάσκοντες και επαγγελματίες του τομέα της εκπαίδευσης πόρους και εργαλείοι σχετικά με τις πρωτοβουλίες της ΕΕ.

Εκδηλώσεις όπως η Ευρωπαϊκή Εβδομάδα Νεολαίας και η Ευρωπαϊκή Εβδομάδα Αθλητισμού διευκολύνουν την ενεργό συμμετοχή σε διάφορους θεματικούς τομείς, συμπεριλαμβανομένης της καταπολέμησης του κυβερνοεκφοβισμού. Η ομάδα της ανοικτής μεθόδου συντονισμού για την καταπολέμηση της ρητορικής μίσους στον αθλητισμό, η οποία συστάθηκε στο πλαίσιο του προγράμματος εργασίας της ΕΕ για τον αθλητισμό, καταρτίζει επί του παρόντος συστάσεις

προς τα κράτη μέλη και τα ενδιαφερόμενα μέρη για το ευρύτερο αθλητικό περιβάλλον, περιλαμβανομένου του διαδικτύου. Η έκθεσή της αναμένεται έως το τέλος του 2026 και θα περιλαμβάνει συστάσεις για την αντιμετώπιση του κυβερνοεκφοβισμού.

Η Επιτροπή:

6. **θα εξετάσει το ζήτημα του κυβερνοεκφοβισμού κατά την επικαιροποίηση των κατευθυντήριων γραμμών για διδάσκοντες και εκπαιδευτικούς σχετικά με την αντιμετώπιση της παραπληροφόρησης και την προώθηση του ψηφιακού γραμματισμού μέσω της εκπαίδευσης και της κατάρτισης – έως το 2ο τρίμηνο του 2026·**
7. **θα ενισχύσει την αγωγή του πολίτη στα σχολεία μέσω ενός πλαισίου ικανοτήτων για την ιθαγένεια της ΕΕ και σχετικών κατευθυντήριων γραμμών – το 2027·**
8. **θα ενισχύσει τις ψηφιακές ικανότητες, την πρόληψη του κυβερνοεκφοβισμού και την ψηφιακή ευημερία μέσω του χάρτη πορείας του 2030 για το μέλλον της ψηφιακής εκπαίδευσης και των ψηφιακών δεξιοτήτων – έως το 3ο τρίμηνο του 2026·**
9. **θα συμβάλει στην πρόληψη του κυβερνοεκφοβισμού στο επικείμενο σχέδιο δράσης της ΕΕ για την προστασία των παιδιών από την εγκληματικότητα – έως το 3ο τρίμηνο του 2026·**
10. **θα επεκτείνει τους πόρους κατά του κυβερνοεκφοβισμού και τη σχετική κατάρτιση για τα σχολεία και για τη μη τυπική και άτυπη εκπαίδευση, κατά τρόπο προσβάσιμο για τα άτομα με αναπηρία, μέσω της πλατφόρμας BIK, των SIC, της Ευρωπαϊκής Δικτυακής Πύλης της Νεολαίας και της Ευρωπαϊκής Πλατφόρμας Σχολικής Εκπαίδευσης – από το 2ο τρίμηνο του 2026·**
11. **θα υποστηρίξει την ομάδα ανοικτής μεθόδου συντονισμού για την καταπολέμηση της ρητορικής μίσους στον αθλητισμό στο πλαίσιο των εργασιών της σχετικά με συστάσεις για την καταπολέμηση του κυβερνοεκφοβισμού στο αθλητικό περιβάλλον – έκθεση που αναμένεται έως το 4ο τρίμηνο του 2026.**

Τα κράτη μέλη καλούνται:

3. **να ενισχύσουν την πρόληψη και τον έγκαιρο εντοπισμό του κυβερνοεκφοβισμού παρέχοντας σαφή καθοδήγηση και κατάρτιση στα ενδιαφερόμενα μέρη, όπως εκπαιδευτικούς, φροντιστές, επαγγελματίες που εργάζονται με παιδιά σε διάφορους τομείς (π.χ. υγεία, αθλητισμός, δικαιοσύνη, επιβολή του νόμου)·**
4. **να ενισχύσουν τη συμμετοχή των παιδιών στη χάραξη των πολιτικών και στην εφαρμογή μέτρων για την ευημερία των παιδιών.**

3.3 Πυλώνας III: Υποβολή αναφορών και ολοκληρωμένη υποστήριξη

Τα θύματα κυβερνοεκφοβισμού πρέπει να διαθέτουν σαφείς, αξιόπιστους και προσβάσιμους διαύλους για να αναφέρουν την κακοποίηση και να λαμβάνουν βοήθεια, συμπεριλαμβανομένων των περιπτώσεων κυβερνοεκφοβισμού μέσω προσωπικών μηνυμάτων. Για να είναι αποτελεσματικές, οι προσπάθειες υποστήριξης πρέπει να επεκταθούν πέραν της παροχής βοήθειας μόνο στα θύματα κυβερνοεκφοβισμού, ώστε να προσεγγίσουν επίσης τα άτομα που γίνονται μάρτυρες περιστατικών κυβερνοεκφοβισμού, τους δράστες, τους γονείς, τους φροντιστές, τους εκπαιδευτικούς και την ευρύτερη σχολική κοινότητα.

Η Επιτροπή θα προωθήσει συνεκτικές, πανενωσιακές δυνατότητες υποβολή αναφορών του κυβερνοεκφοβισμού και υποστήριξης των θυμάτων. Οι αναφορές θα πρέπει να οδηγούν γρήγορα σε διεπιστημονική υποστήριξη, τόσο στο διαδίκτυο όσο και εκτός διαδικτύου. Στην προσφορά υποστήριξης θα πρέπει να εμπλακούν όλες οι αρμόδιες αρχές σε κάθε επίπεδο, ιδιωτικοί φορείς, οργανώσεις της κοινωνίας των πολιτών, καθώς και γονείς, φροντιστές και τα ίδια τα παιδιά, οι νέοι και οι νέες.

Λαμβάνοντας υπόψη τις πληροφορίες που συγκέντρωσε μέσω διαφόρων στοχευμένων διαβουλεύσεων, **η Επιτροπή θα στηρίξει την ανάπτυξη μιας διαδικτυακής εφαρμογής για την ασφάλεια σε όλα τα κράτη μέλη**, με βάση επιτυχημένα υφιστάμενα υποδείγματα εθνικών πρακτικών, όπως η γαλλική εφαρμογή *App 3018*. Η εφαρμογή θα προσφέρει ένα ασφαλές, εύχρηστο και εμπιστευτικό εργαλείο που θα παρέχει στα παιδιά, τους νέους και τις νέες τη δυνατότητα:

- i. να υποβάλλουν εύκολα αναφορά σχετικά με τον κυβερνοεκφοβισμό σε τηλεφωνική γραμμή βοήθειας,
- ii. να αποθηκεύουν και να διαβιβάζουν με ασφάλεια αποδεικτικά στοιχεία σύμφωνα με τα εθνικά νομικά πλαίσια, και
- iii. να λαμβάνουν εξατομικευμένη βοήθεια μέσω της συντονισμένης παραπομπής τους, π.χ. σε υπηρεσίες επιβολής του νόμου, εκπαίδευσης και προστασίας των παιδιών.

Η Επιτροπή θα στηρίξει τα κράτη μέλη, όπου είναι αναγκαίο και σκόπιμο, ώστε:

- i. να προσαρμόσουν την εν λόγω εφαρμογή στις εθνικές συνθήκες και ανάγκες (π.χ. μετάφραση, επικοινωνιακή προώθησή της, σύνδεση με τις σχετικές εθνικές υπηρεσίες για υποστήριξη και με τις πλατφόρμες για την υποβολή αναφορών), παροχή χαρακτηριστικών όπως η ασφαλής υποβολή αναφορών, η διατήρηση των αποδεικτικών στοιχείων σύμφωνα με το εθνικό δίκαιο και η εγγυημένη εμπιστευτικότητα·
- ii. να διασφαλίσουν τη διαλειτουργικότητα με τις υφιστάμενες υποδομές και συστήματα υποστήριξης, και
- iii. να υποστηρίξουν την προώθηση της χρήσης της εφαρμογής μεταξύ των κρατών μελών, των χρηστών και των επιγραμμικών πλατφορμών.

Οι επιγραμμικές πλατφόρμες θα παραμείνουν υπεύθυνες για τη θέσπιση αποτελεσματικών μηχανισμών υποβολής αναφορών. Αυτό μπορεί να αντιστοιχεί σε ένα από τα μέτρα που έχουν θεσπιστεί για τη διασφάλιση της συμμόρφωσης με τις υποχρεώσεις που προβλέπει η πράξη για τις ψηφιακές υπηρεσίες όσον αφορά την προστασία των ανηλίκων. Συμπληρωματικά προς τις προσπάθειες αυτές, η εφαρμογή θα τεθεί στη διάθεση των επιγραμμικών πλατφορμών για να την ενσωματώσουν στα εργαλεία υποβολής αναφορών και υποστήριξης των χρηστών, μεταξύ άλλων μέσω διεπαφών προγραμματισμού εφαρμογών (API), ώστε να καταστεί αποδοτική ως προς τη χρήση των πόρων και αποτελεσματική για την υποβολή αναφορών και την απόκριση σε αναφορές.

Η επιτυχία της εφαρμογής εξαρτάται από τη διαθεσιμότητα υποστήριξης και μεταπαρακολούθησης από τις εθνικές αρχές. Τα κράτη μέλη θα διαδραματίσουν σημαντικό ρόλο, αφενός, στις προσπάθειες να διασφαλιστεί ότι η υποβολή αναφορών μέσω της εφαρμογής θα συνοδεύεται με προσφορά συντονισμένης υποστήριξης εκτός διαδικτύου (π.χ. νομική, κοινωνική, ψυχολογική και εκπαιδευτική υποστήριξη) και, αφετέρου, στην ενημέρωση για τα οφέλη της εφαρμογής. Η εφαρμογή θα επιδιώξει συνέργειες με καθιερωμένους μηχανισμούς υποβολής αναφορών στα κράτη μέλη για την αναφορά υλικού σεξουαλικής κακοποίησης παιδιών και βίας κατά γυναικών στο διαδίκτυο, καθώς και με ενωσιακές, εθνικές και διεθνείς γραμμές βοήθειας, ιδίως τις τηλεφωνικές γραμμές βοήθειας για παιδιά (116 111) και τις ανοικτές τηλεφωνικές γραμμές για αγνοούμενα παιδιά (116 000).

Η Επιτροπή θα εκδώσει την επόμενη [στρατηγική της ΕΕ για τα δικαιώματα των θυμάτων το 2026](#) για να συμπληρώσει τους κανόνες της ΕΕ με μη νομοθετικά μέτρα. Η στρατηγική αυτή θα προωθήσει δομές για στοχευμένη υποστήριξη (π.χ. ιατρική εξέταση, συναισθηματική και ψυχολογική υποστήριξη) και υπηρεσίες προστασίας για τα παιδιά-θύματα, συμπεριλαμβανομένων των υπηρεσιών προστασίας από το ηλεκτρονικό έγκλημα. Τα μέτρα αυτά θα αφορούν επίσης τα θύματα κυβερνοεκφοβισμού στα κράτη μέλη στα οποία οι εν λόγω πράξεις ποινικοποιούνται βάσει του εθνικού δικαίου.

Σύμφωνα με τον [γενικό κανονισμό για την προστασία δεδομένων](#), το δικαίωμα διαγραφής δεδομένων προσωπικού χαρακτήρα είναι ιδιαίτερα σημαντικό όταν το υποκείμενο των δεδομένων παρέσχε τη συγκατάθεσή του ως παιδί και ενδέχεται να μην είχε πλήρη επίγνωση των σχετικών κινδύνων, μεταξύ άλλων στο πλαίσιο κυβερνοεκφοβισμού. Η Επιτροπή θα συνεχίσει να υποστηρίζει τις αρχές προστασίας δεδομένων όσον αφορά την ανάπτυξη εργαλείων που εστιάζουν στα παιδιά, με σκοπό την προστασία των δεδομένων στα μέσα κοινωνικής δικτύωσης, την πρόληψη της κλοπής δεδομένων ή λογαριασμών και τη διευκόλυνση της άσκησης των δικαιωμάτων τους.

Η Επιτροπή:

- 12. Θα υποστηρίξει την ανάπτυξη σε όλα τα κράτη μέλη μιας προσβάσιμης διαδικτυακής εφαρμογής για την ασφάλεια που θα καθιστά δυνατή την εύκολη υποβολή αναφορών περιστατικών κυβερνοεκφοβισμού, προσαρμοσμένης στις εθνικές συνθήκες, σε συνέργειες με τους υφιστάμενους μηχανισμούς υποβολής αναφορών, συμπεριλαμβανομένων των τηλεφωνικών γραμμών βοήθειας και των ανοικτών τηλεφωνικών γραμμών, και θα προωθήσει την προσφορά διεπιστημονικής**

υποστήριξης, τόσο στο διαδίκτυο όσο και εκτός διαδικτύου – **από το 3ο τρίμηνο του 2026.**

13. θα αντιμετωπίσει το ζήτημα των παιδιών που καθίστανται θύματα και τη διαδικτυακή θυματοποίηση, η οποία μπορεί να περιλαμβάνει τον κυβερνοεκφοβισμό, στην επόμενη **στρατηγική της ΕΕ για τα δικαιώματα των θυμάτων – το 2026.**

Τα κράτη μέλη καλούνται:

5. να αναλύσουν το εθνικό τους πλαίσιο με σκοπό να καταστήσουν διαθέσιμη μια **εθνική διαδικτυακή εφαρμογή για την ασφάλεια** με εξατομικευμένη υποστήριξη και, με βάση επιτυχημένα υφιστάμενα υποδείγματα εθνικών πρακτικών, **να προσαρμόσουν το εν λόγω υπόδειγμα στις εθνικές τους συνθήκες**, συμπεριλαμβανομένης π.χ. της μετάφρασης, της επικοινωνιακής προώθησης, της σύνδεσης με τις σχετικές εθνικές υπηρεσίες για υποστήριξη και με τις πλατφόρμες για την υποβολή αναφορών, διασφαλίζοντας παράλληλα βασικά χαρακτηριστικά όπως η ασφαλής υποβολή αναφορών, η διατήρηση των αποδεικτικών στοιχείων σύμφωνα με το εθνικό δίκαιο και η εγγυημένη εμπιστευτικότητα·
6. να μεριμνήσουν ώστε η υποβολή αναφορών μέσω της εθνικής διαδικτυακής εφαρμογής για την ασφάλεια να ενσωματωθεί σε ένα **ολιστικό και λειτουργικό οικοσύστημα για τη διαχείριση υποθέσεων και την παροχή υποστήριξης**, συμπεριλαμβανομένης της συντονισμένης υποστήριξης εκτός διαδικτύου (π.χ. νομικές, αστυνομικές, κοινωνικές, ψυχολογικές και εκπαιδευτικές υπηρεσίες υποστήριξης)·
7. **να θέσουν την εθνική διαδικτυακή εφαρμογή για την ασφάλεια στη διάθεση των επιγραμμικών πλατφορμών ώστε να την ενσωματώσουν στα εργαλεία υποβολής αναφορών και υποστήριξης των χρηστών**, μεταξύ άλλων μέσω διεπαφών προγραμματισμού εφαρμογών (API), ώστε να καταστεί αποδοτική ως προς τη χρήση των πόρων και αποτελεσματική για την υποβολή αναφορών και την απόκριση σε αναφορές·
8. **να προωθήσουν την ευρεία υιοθέτηση και χρήση της εθνικής εφαρμογής ασφάλειας από όλα τα σχετικά ενδιαφερόμενα μέρη·**
9. **να προωθήσουν εργαλεία που αναπτύσσονται από τις αρχές προστασίας δεδομένων** στις εθνικές τους γλώσσες για την προστασία των παιδιών από κινδύνους στο διαδίκτυο, όπως ο κυβερνοεκφοβισμός, η κλοπή δεδομένων ή λογαριασμών, οι απόπειρες εξαπάτησης, ο σεξουαλικός εκβιασμός.

4. Διεθνής προβολή και πολυμερής συνεργασία

Η ΕΕ έχει στόχο να διασφαλίσει την ευημερία και τα δικαιώματα των παιδιών εντός των συνόρων της, αλλά και να συμβάλει σημαντικά στην προώθηση ενός ασφαλέστερου και πιο συμπεριληπτικού ψηφιακού περιβάλλοντος παγκοσμίως. Η Ημέρα Ασφαλούς Διαδικτύου αποτελεί πλέον μια παγκόσμια εκστρατεία που καλεί τα ενδιαφερόμενα μέρη να αναλάβουν από κοινού δράση για να καταστήσουν το διαδίκτυο έναν ασφαλέστερο και καλύτερο χώρο για όλους, ιδίως για τα παιδιά, τους νέους και τις νέες μέσω της ευαισθητοποίησης σχετικά με τις βασικές διαδικτυακές προκλήσεις και τις αναδυόμενες πηγές ανησυχίας και τάσεις.

Η προστασία και ενδυνάμωση των ανηλίκων στο διαδίκτυο αποτελεί παγκόσμια προτεραιότητα, όπως αποτυπώνεται στη [διεθνή ψηφιακή στρατηγική της ΕΕ](#). Το συγχρηματοδοτούμενο από την ΕΕ δίκτυο ανοικτών τηλεφωνικών γραμμών στα κράτη μέλη για την αντιμετώπιση της διάδοσης υλικού σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο αποτελεί μέρος του [δικτύου INHOPE](#), το οποίο διαθέτει επί του παρόντος 57 ανοικτές τηλεφωνικές γραμμές παγκοσμίως.

Η Επιτροπή θα συνεχίσει να συνεργάζεται με ρυθμιστικές αρχές που συμμερίζονται τους στόχους της για την ασφάλεια στο διαδίκτυο, συμπεριλαμβανομένης της πρόληψης και της αντιμετώπισης του κυβερνοεκφοβισμού, στο πλαίσιο διοικητικών ρυθμίσεων —π.χ. επί του παρόντος με την Ofcom στο Ηνωμένο Βασίλειο και την επίτροπο Ηλεκτρονικής Ασφάλειας (eSafety Commissioner) στην Αυστραλία— και ψηφιακών εταιρικών σχέσεων (π.χ. με τον Καναδά, τη Σιγκαπούρη, την Ινδία).

Η ΕΕ θα προωθήσει τη συνεργασία κατά του κυβερνοεκφοβισμού σε διεθνή φόρουμ, σύμφωνα με το [παγκόσμιο ψηφιακό σύμφωνο](#). Οι οργανώσεις των Ηνωμένων Εθνών έχουν καταρτίσει κατευθυντήριες γραμμές και εργαλεία που μπορούν να χρησιμοποιηθούν ως ορθές πρακτικές και σημεία αναφοράς, μεταξύ άλλων η UNICEF (ιστότοπος και API ανοικτού κώδικα), η Διεθνή Ένωση Τηλεπικοινωνιών (κατευθυντήριες γραμμές για την προστασία των παιδιών στο διαδίκτυο), καθώς και η Ειδική Εκπρόσωπος του Γενικού Γραμματέα των Ηνωμένων Εθνών για τη βία κατά των παιδιών. Η ΕΕ στηρίζει τις δραστηριότητες προβολής της UNESCO προς τις ρυθμιστικές αρχές για την εφαρμογή των κατευθυντήριων γραμμών της UNESCO σχετικά με τη διακυβέρνηση των επιγραμμικών πλατφορμών.

Η ΕΕ χρηματοδοτεί ειδικά προγράμματα στήριξης της ευαισθητοποίησης και της προστασίας των παιδιών σε τρίτες χώρες, ιδίως σε υποψήφιες και γειτονικές χώρες, τόσο στο διαδίκτυο όσο και εκτός διαδικτύου, από τον ΜΓΑΔΣ–Παγκόσμια Ευρώπη. Η ΕΕ υποστηρίζει επίσης την ευθυγράμμιση των υποψήφιων και δυνάμει υποψήφιων χωρών με τους κανόνες της ΕΕ στο πλαίσιο της διαδικασίας προσχώρησής τους, και προωθεί τη διαδικτυακή ασφάλεια των παιδιών και των νέων στις γειτονικές χώρες μέσω της ανταλλαγής γνώσεων και βέλτιστων πρακτικών στο πλαίσιο του προγράμματος «Κέντρα Ασφαλούς Διαδικτύου+» (SIC+).

5. Επόμενα βήματα

Η Επιτροπή θα παρακολουθεί την εφαρμογή του σχεδίου δράσης και στους τρεις πυλώνες, σε στενή συνεργασία με τα κράτη μέλη, τα SIC και άλλα ενδιαφερόμενα μέρη. Η πρόοδος, οι

προκλήσεις και οι ορθές πρακτικές θα καταγράφονται μέσω των υφιστάμενων εργαλείων, όπως ο ετήσιος χάρτης πολιτικής της πρωτοβουλίας «Καλύτερο διαδίκτυο για τα παιδιά» (BIK), οι εκθέσεις των SIC και οι τακτικές ανταλλαγές μέσω φόρουμ εμπειρογνομόνων, ενώ θα ληφθεί μέριμνα για τη διαφανή και συμμετοχική παρακολούθηση.

Η Επιτροπή θα συνεργαστεί με τα κράτη μέλη για την ενσωμάτωση πλαισίων παρακολούθησης στις εθνικές στρατηγικές ή πολιτικές κατά του κυβερνοεκφοβισμού, και θα αξιολογεί την εφαρμογή, την προσβασιμότητα, τη συμπεριληπτικότητα και την προσαρμοστικότητα στα εξελισσόμενα ψηφιακά πλαίσια, με τη συμμετοχή παιδιών και νέων. Τα πορίσματα θα κοινοποιούνται σε επίπεδο ΕΕ για την υποστήριξη της αμοιβαίας μάθησης και της ευθυγράμμισης των πολιτικών, ώστε να επικαιροποιούνται οι πρωτοβουλίες στο πλαίσιο της στρατηγικής BIK+ και της πράξης για τις ψηφιακές υπηρεσίες.

Η Επιτροπή θα προβεί σε απολογισμό του παρόντος σχεδίου δράσης το 2029, μεταξύ άλλων μέσω διαβουλεύσεων με παιδιά, νέες και νέους.

6. Συμπεράσματα

«Θέλουμε έναν ασφαλή διαδικτυακό χώρο για τα παιδιά, για τη νεολαία και για την επόμενη γενιά, αλλά δεν τον έχουμε ακόμη. Αντιμετωπίζουμε κάποια προβλήματα — προβλήματα που δεν αφορούν μόνο αυτή τη γενιά. Χρειαζόμαστε γι' αυτό βοήθεια από την ΕΕ προκειμένου να δημιουργήσουμε τους ασφαλείς διαδικτυακούς χώρους μας. Κάποτε έρχεται η στιγμή που πρέπει να αναληφθεί δράση. Αυτή η στιγμή είναι τώρα. Για το μέλλον.»

Απόσπασμα από δήλωση παιδιών που είναι μέλη της Πλατφόρμας της ΕΕ για τη Συμμετοχή των Παιδιών

Τα παιδιά, οι νέες και οι νέοι επικοινωνούν μαζί μας ζητώντας βοήθεια ώστε οι διαδικτυακοί χώροι να καταστούν ασφαλείς, για τους ίδιους, τους συνομηλίκους τους και τις μελλοντικές γενιές. Πρέπει να ανταποκριθούμε στην πρόκληση αυτή σε ολόκληρη την Ένωσή μας, γιατί η προστασία και η ενδυνάμωση των παιδιών και των νέων μας δεν θα πρέπει να εξαρτώνται από τον ταχυδρομικό τους κώδικα.

Αξιοποιώντας την ήδη σημαντική εργαλειοθήκη νομικών μέτρων και μέτρων πολιτικής της ΕΕ κατά των κινδύνων στο διαδίκτυο, και με βάση τις συνεισφορές ευρέος φάσματος ενδιαφερόμενων μερών, το παρόν σχέδιο δράσης θα συμβάλει στη δημιουργία ενός ασφαλούς, συμπεριληπτικού και ενδυναμωτικού ψηφιακού περιβάλλοντος για τα παιδιά, τους νέους και τις νέες στην Ευρώπη. Θα συμπληρώσει και θα εμπνεύσει τις εν εξελίξει πρωτοβουλίες της ΕΕ για ασφαλέστερο διαδίκτυο, την ευθύνη των πλατφορμών, τις ψηφιακές δεξιότητες και την ψηφιακή εκπαίδευση, την ενδυνάμωση των παιδιών και των νέων, τη συλλογή δεδομένων και τη διεθνή συνεργασία.

Η Επιτροπή καλεί το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο να εγκρίνουν το παρόν σχέδιο δράσης και να συνεργαστούν για την εφαρμογή του. Η Επιτροπή καλεί την Επιτροπή των Περιφερειών και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή να προωθήσουν τον διάλογο με τις τοπικές και περιφερειακές αρχές, τους οικονομικούς και κοινωνικούς εταίρους και την κοινωνία των πολιτών.

ΠΑΡΑΡΤΗΜΑ: Βασικές δράσεις και χρονοδιάγραμμα

Πυλώνας Ι: Συντονισμένη προσέγγιση της ΕΕ για την προστασία

Η Επιτροπή:	
θα επεκτείνει την εστίαση στην αντιμετώπιση του κυβερνοεκφοβισμού κατά την αναθεώρηση των κατευθυντήριων γραμμών για την πράξη για τις ψηφιακές υπηρεσίες σχετικά με την προστασία των ανηλίκων .	το 2026
θα εκδώσει κατευθυντήριες γραμμές για την πράξη για τις ψηφιακές υπηρεσίες σχετικά με τις αξιόπιστες πηγές επίσημης παράνομης περιεχομένου με σκοπό να συμβάλει στην αποσαφήνιση του ρόλου τους στην αντιμετώπιση παράνομης περιεχομένου όπως ο παράνομος κυβερνοεκφοβισμός.	έως το 2ο τρίμηνο του 2026
θα εξετάσει τρόπους για την αντιμετώπιση του κυβερνοεκφοβισμού στις πλατφόρμες διαμοιρασμού βίντεο κατά την εν εξελίξει αξιολόγηση της οδηγίας για τις υπηρεσίες οπτικοακουστικών μέσων και την επανεξέτασή της.	έως το 3ο τρίμηνο του 2026
θα υποστηρίξει την αποτελεσματική εφαρμογή των διατάξεων του κανονισμού για την τεχνητή νοημοσύνη σχετικά με τις απαγορευμένες πρακτικές ΤΝ , μεταξύ άλλων όταν χρησιμοποιούνται για κυβερνοεκφοβισμό.	από το 3ο τρίμηνο του 2026
θα διευκολύνει την αποτελεσματική εφαρμογή των υποχρεώσεων διαφάνειας του κανονισμού για την ΤΝ όσον αφορά τη σήμανση και την επίσημηση περιεχομένου που παράγεται από ΤΝ , μεταξύ άλλων όταν αφορά κυβερνοεκφοβισμό.	από το 3ο τρίμηνο του 2026

Τα κράτη μέλη καλούνται:
να καταρτίσουν ολοκληρωμένα εθνικά σχέδια κατά του εκφοβισμού, συμπεριλαμβανομένου του κυβερνοεκφοβισμού , ιδίως με την υποστήριξη του δικτύου της ΕΕ για τα δικαιώματα του παιδιού.
να συλλέγουν συνεκτικά, συγκρίσιμα δεδομένα σχετικά με τον κυβερνοεκφοβισμό με τη βοήθεια του δικτύου των Κέντρων Ασφαλούς Διαδικτύου και της πλατφόρμας «Καλύτερο διαδίκτυο για τα παιδιά».

Πυλώνας ΙΙ: Πρόληψη και ευαισθητοποίηση

Η Επιτροπή:

θα εξετάσει το ζήτημα του κυβερνοεκφοβισμού κατά την επικαιροποίηση των κατευθυντήριων γραμμών για διδάσκοντες και εκπαιδευτικούς σχετικά με την αντιμετώπιση της παραπληροφόρησης και την προώθηση του ψηφιακού γραμματισμού ·	έως το 2ο τρίμηνο του 2026
θα ενισχύσει την αγωγή του πολίτη στα σχολεία μέσω ενός πλαισίου ικανοτήτων για την ιθαγένεια της ΕΕ και σχετικών κατευθυντήριων γραμμών·	το 2027

θα ενισχύσει τις ψηφιακές ικανότητες, την πρόληψη του κυβερνοεκφοβισμού και την ψηφιακή ευημερία μέσω του χάρτη πορείας του 2030 για το μέλλον της ψηφιακής εκπαίδευσης και των ψηφιακών δεξιοτήτων ·	έως το 3ο τρίμηνο του 2026
θα συμβάλει στην πρόληψη του κυβερνοεκφοβισμού στο επικείμενο σχέδιο δράσης της ΕΕ για την προστασία των παιδιών από την εγκληματικότητα ·	έως το 3ο τρίμηνο του 2026
θα επεκτείνει τους πόρους κατά του κυβερνοεκφοβισμού και τη σχετική κατάρτιση για τα σχολεία και για τη μη τυπική και άτυπη εκπαίδευση, κατά τρόπο προσβάσιμο για τα άτομα με αναπηρία, μέσω της πλατφόρμας BIK, των SIC, της Ευρωπαϊκής Δικτυακής Πύλης της Νεολαίας και της Ευρωπαϊκής Πλατφόρμας Σχολικής Εκπαίδευσης·	από το 2ο τρίμηνο του 2026
θα υποστηρίξει την ομάδα ανοικτής μεθόδου συντονισμού για την καταπολέμηση της ρητορικής μίσους στον αθλητισμό στο πλαίσιο των εργασιών της σχετικά με συστάσεις για την καταπολέμηση του κυβερνοεκφοβισμού στο αθλητικό περιβάλλον .	έως το 4ο τρίμηνο του 2026

Τα κράτη μέλη καλούνται:
να ενισχύσουν την πρόληψη και τον έγκαιρο εντοπισμό του κυβερνοεκφοβισμού με κατευθυντήριες γραμμές και κατάρτιση για τα ενδιαφερόμενα μέρη , όπως εκπαιδευτικούς, φροντιστές, επαγγελματίες που εργάζονται με παιδιά σε διάφορους τομείς·
να ενισχύσουν τη συμμετοχή των παιδιών στη χάραξη των πολιτικών και στην εφαρμογή μέτρων για την ευημερία των παιδιών.

Πυλώνας III: Υποβολή αναφορών και ολοκληρωμένη υποστήριξη

<u>Η Επιτροπή:</u>

θα υποστηρίξει την ανάπτυξη σε όλα τα κράτη μέλη μιας προσβάσιμης διαδικτυακής εφαρμογής για την ασφάλεια ·	από το 3ο τρίμηνο του 2026
θα αντιμετωπίσει το ζήτημα των παιδιών που καθίστανται θύματα και τη διαδικτυακή θυματοποίηση, η οποία μπορεί να περιλαμβάνει τον κυβερνοεκφοβισμό, στη στρατηγική της ΕΕ για τα δικαιώματα των θυμάτων .	το 2026

<u>Τα κράτη μέλη καλούνται:</u>	
να αναλύσουν το εθνικό τους πλαίσιο με σκοπό να καταστήσουν διαθέσιμη μια εθνική διαδικτυακή εφαρμογή για την ασφάλεια και, με βάση επιτυχημένα υφιστάμενα υποδείγματα εθνικών πρακτικών, να προσαρμόσουν το εν λόγω υπόδειγμα στις εθνικές τους συνθήκες·	
να μεριμνήσουν ώστε η υποβολή αναφορών μέσω της εθνικής διαδικτυακής εφαρμογής για την ασφάλεια να ενσωματωθεί σε ένα ολιστικό και λειτουργικό οικοσύστημα υποστήριξης ·	
να θέσουν την εθνική διαδικτυακή εφαρμογή για την ασφάλεια στη διάθεση των επιγραμμικών πλατφορμών ώστε να την ενσωματώσουν στα εργαλεία υποβολής αναφορών και υποστήριξης των χρηστών·	
να προωθήσουν την εθνική διαδικτυακή εφαρμογή για την ασφάλεια μεταξύ των σχετικών ενδιαφερόμενων μερών·	
να προωθήσουν εργαλεία που αναπτύσσονται από τις αρχές προστασίας δεδομένων στις εθνικές τους γλώσσες για την προστασία των παιδιών από κινδύνους στο διαδίκτυο, όπως ο κυβερνοεκφοβισμός.	