Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/2659

16.10.2024

ΣΥΣΤΑΣΗ (ΕΕ) 2024/2659 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 11ης Οκτωβρίου 2024

σχετικά με κατευθυντήριες γραμμές για την εξαγωγή ειδών κυβερνοεπιτήρησης σύμφωνα με το άρθρο 5 του κανονισμού (ΕΕ) 2021/821 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 292,

Εκτιμώντας τα ακόλουθα:

(1) Με τον κανονισμό (ΕΕ) 2021/821 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1] θεσπίζεται ενωσιακό σύστημα ελέγχου των εξαγωγών, της μεσιτείας, της τεχνικής βοήθειας, της διαμετακόμισης και της μεταφοράς ειδών διπλής χρήσης.

(2) Ο κανονισμός (ΕΕ) 2021/821 έχει ως στόχο την αντιμετώπιση του κινδύνου χρήσης ειδών κυβερνοεπιτήρησης σε σχέση με εσωτερική καταστολή και/ή σε σχέση με τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου.

(3) Σύμφωνα με το άρθρο 5 παράγραφος 2 και το άρθρο 26 παράγραφος 1 του κανονισμού (ΕΕ) 2021/821, η Επιτροπή και το Συμβούλιο διαθέτουν στους εξαγωγείς κατευθυντήριες γραμμές αναφορικά με τα μη απαριθμούμενα είδη κυβερνοεπιτήρησης, δεδομένης της ανάγκης να διασφαλιστεί η αποτελεσματικότητα του ενωσιακού συστήματος ελέγχου των εξαγωγών όσον αφορά την ασφάλεια στον κυβερνοχώρο και τη συνοχή της εφαρμογής του κανονισμού (ΕΕ) 2021/821.

(4) Η παρούσα σύσταση και οι συνημμένες σ' αυτήν κατευθυντήριες γραμμές αποσκοπούν στη στήριξη των εξαγωγέων κατά την εφαρμογή ελέγχων σε μη απαριθμούμενα είδη κυβερνοεπιτήρησης, και συμπεριλαμβάνουν, μεταξύ άλλων, μέτρα δέουσας επιμέλειας για την εκτίμηση των κινδύνων που σχετίζονται με την εξαγωγή των εν λόγω ειδών.

(5) Οι κατευθυντήριες γραμμές που επισυνάπτονται στην παρούσα σύσταση αποτέλεσαν αντικείμενο εκτεταμένων διαβουλεύσεων στο πλαίσιο της ομάδας εμπειρογνωμόνων σε θέματα τεχνολογιών επιτήρησης το 2022 και το 2023 και έλαβαν υπόψη τις παρατηρήσεις που ελήφθησαν κατά τη διάρκεια δημόσιας διαβούλευσης [2] που πραγματοποιήθηκε το δεύτερο τρίμηνο του 2023.

(6) Υπενθυμίζεται ότι η παρούσα σύσταση και οι συνημμένες κατευθυντήριες γραμμές είναι μη δεσμευτικές. Ως εκ τούτου, οι εξαγωγείς θα πρέπει να διατηρήσουν την ευθύνη συμμόρφωσης με τις υποχρεώσεις που υπέχουν βάσει του κανονισμού (ΕΕ) 2021/821, ενώ η Επιτροπή θα πρέπει να διασφαλίσει ότι η παρούσα σύσταση παραμένει επίκαιρη,

[1] Κανονισμός (ΕΕ) 2021/821 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη θέσπιση ενωσιακού συστήματος ελέγχου των εξαγωγών, της μεσιτείας, της τεχνικής βοήθειας, της διαμετακόμισης και της μεταφοράς ειδών διπλής χρήσης (ΕΕ L 206 της 11.6.2021, σ. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

[2] https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en?prefLang=el.

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

Συνιστάται στις αρμόδιες αρχές και τους εξαγωγείς των κρατών μελών να λαμβάνουν υπόψη τις κατευθυντήριες γραμμές που προβλέπονται στο παράρτημα της παρούσας σύστασης, προκειμένου να εκπληρώσουν τις υποχρεώσεις που υπέχουν δυνάμει του άρθρου 5 παράγραφος 2 του κανονισμού (ΕΕ) 2021/821.

Βρυξέλλες, 11 Οκτωβρίου 2024.

Για την Επιτροπή
Valdis DOMBROVSKIS
Εκτελεστικός Αντιπρόεδρος

ΠΑΡΑΡΤΗΜΑ

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα

Εισαγωγή ... 4

1. Σχετικές νομικές διατάξεις, ορισμοί και βασικές έννοιες ... 4

1.1. Επισκόπηση των σχετικών νομικών διατάξεων ... 4

1.2. Βασικοί ορισμοί ... 5

1.2.1. «Ειδικά σχεδιασμένα» ... 5

1.2.2. «Συγκεκαλυμμένη επιτήρηση» ... 6

1.2.3. «Φυσικά πρόσωπα» ... 6

1.2.4. «Παρακολούθηση, εξαγωγή, συλλογή, ανάλυση δεδομένων» ... 6

1.2.5. «Από συστήματα πληροφοριών και τηλεπικοινωνιών» ... 7

1.2.6. «Γνωρίζει» και «προορίζονται για» ... 7

1.3. Εσωτερική καταστολή, σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου ... 7

1.3.1. Εσωτερική καταστολή ... 8

1.3.2. Διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων ... 8

1.3.3. Διάπραξη σοβαρών παραβιάσεων του διεθνούς ανθρωπιστικού δικαίου ... 9

2. Τεχνικό πεδίο εφαρμογής ... 9

2.1. Απαριθμούμενα είδη κυβερνοεπιτήρησης ... 9

2.2. Δυνητικά μη απαριθμούμενα είδη κυβερνοεπιτήρησης ... 9

2.2.1. Τεχνολογία αναγνώρισης προσώπου και συναισθημάτων ... 10

2.2.2. Συσκευές εντοπισμού θέσης ... 10

2.2.3. Συστήματα βιντεοεπιτήρησης ... 10

3. Μέτρα δέουσας επιμέλειας ... 10

Απαιτήσεις του άρθρου 5 παράγραφος 2 του κανονισμού (ΕΕ) 2021/821 ... 12

4. Προσάρτημα ... 12

Κατάλογος ειδών κυβερνοεπιτήρησης που υπόκεινται σε έλεγχο σύμφωνα με το παράρτημα I του κανονισμού (ΕΕ) 2021/821 ... 12

Συστήματα υποκλοπής τηλεπικοινωνιών (5A001.στ.) ... 12

Συστήματα επιτήρησης του διαδικτύου (5A001.ι.) ... 13

«Λογισμικό εισβολής» (4A005, 4D004 και συναφείς έλεγχοι βάσει των σημείων 4E001.α. και 4E001.γ.) ... 13

Λογισμικό παρακολούθησης επικοινωνιών (5D001.ε.) 14 ... 14

Είδη που χρησιμοποιούνται για τη διενέργεια κρυπτανάλυσης (5A004.α.) ... 14

Εγκληματολογικά/ερευνητικά εργαλεία (5A004.β., 5D002.α.3.β. και 5D002.γ.3.β.) ... 14

ΕΙΣΑΓΩΓΗ

Το ενωσιακό πλαίσιο ελέγχου των εξαγωγών που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/821 (στο εξής: κανονισμός) έχει ως στόχο να διασφαλίσει ότι τηρούνται οι διεθνείς υποχρεώσεις και δεσμεύσεις της Ένωσης και των κρατών μελών της, μεταξύ άλλων όσον αφορά την περιφερειακή ειρήνη, την ασφάλεια και σταθερότητα και τον σεβασμό των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου. Ως εκ τούτου, η Ένωση και τα κράτη μέλη της έχουν εφαρμόσει τις αποφάσεις που ελήφθησαν στο πλαίσιο των πολυμερών καθεστώτων ελέγχου των εξαγωγών και επικαιροποίησαν αναλόγως τον ενωσιακό κατάλογο ελέγχου του παραρτήματος I του κανονισμού ([1]). Επιπλέον, ήδη πριν από την εφαρμογή του άρθρου 5 του κανονισμού, οι αρμόδιες αρχές των κρατών μελών υπέβαλλαν σε έλεγχο την εξαγωγή ορισμένων απαριθμούμενων ειδών που ενδέχεται να έχουν εφαρμογές επιτήρησης ([2]), λαμβάνοντας υπόψη τους κινδύνους κατάχρησης σε ορισμένες ειδικές περιστάσεις. Σε εξαιρετικά σοβαρές περιστάσεις, η Ένωση επέβαλε κυρώσεις που περιόρισαν την εξαγωγή ορισμένου εξοπλισμού επιτήρησης ([3]).

Ο κανονισμός αντικατοπτρίζει τη δέσμευση της Ένωσης να αντιμετωπίσει αποτελεσματικά τον κίνδυνο χρήσης ειδών κυβερνοεπιτήρησης σε σχέση με εσωτερική καταστολή και/ή σε σχέση με τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου. Ειδικότερα, ο κανονισμός εισάγει νέες διατάξεις για τον έλεγχο των εξαγωγών μη απαριθμούμενων ειδών κυβερνοεπιτήρησης, συμπεριλαμβανομένης της υποχρέωσης των εξαγωγέων να ενημερώνουν την αρμόδια αρχή όταν γνωρίζουν, σύμφωνα με τα πορίσματα της δέουσας επιμέλειάς τους, ότι τα μη απαριθμούμενα είδη κυβερνοεπιτήρησης τα οποία οι εξαγωγείς προτίθενται να εξάγουν προορίζονται, εν όλω ή εν μέρει, για χρήση σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου. Ο κανονισμός καλεί επίσης την Επιτροπή και το Συμβούλιο να θέσουν στη διάθεση των εξαγωγέων κατευθυντήριες γραμμές για τη στήριξη της αποτελεσματικής εφαρμογής των νέων ελέγχων για τα μη απαριθμούμενα είδη κυβερνοεπιτήρησης.

Ως εκ τούτου, οι εν λόγω κατευθυντήριες γραμμές αποσκοπούν στη στήριξη των εξαγωγέων κατά τη διενέργεια ελέγχων σε μη απαριθμούμενα είδη κυβερνοεπιτήρησης, συμπεριλαμβανομένου, μεταξύ άλλων, ως προς τα μέτρα δέουσας επιμέλειας για την εκτίμηση των κινδύνων που σχετίζονται με την εξαγωγή των εν λόγω ειδών σε τελικούς χρήστες και τελικές χρήσεις βάσει των νέων διατάξεων του κανονισμού.

1. ΣΧΕΤΙΚΕΣ ΝΟΜΙΚΕΣ ΔΙΑΤΑΞΕΙΣ, ΟΡΙΣΜΟΙ ΚΑΙ ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

1.1. Επισκόπηση των σχετικών νομικών διατάξεων

Ο κανονισμός εισάγει νέες διατάξεις που προβλέπουν συγκεκριμένα ελέγχους των εξαγωγών ειδών κυβερνοεπιτήρησης που δεν απαριθμούνται στο παράρτημα I του κανονισμού, τα οποία προορίζονται ή μπορεί να προορίζονται, εν όλω ή εν μέρει, για χρήση σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου. Οι σχετικές αιτιολογικές σκέψεις και άρθρα είναι τα εξής:

α) Αιτιολογική σκέψη 8: «Προκειμένου να αντιμετωπιστεί ο κίνδυνος ορισμένα μη απαριθμούμενα είδη κυβερνοεπιτήρησης που έχουν εξαχθεί από το τελωνειακό έδαφος της Ένωσης να αποτελέσουν ενδεχομένως αντικείμενο κακής χρήσης από πρόσωπα που συνέργησαν ή ευθύνονται για την καθοδήγηση ή τη διάπραξη σοβαρών παραβιάσεων των ανθρώπινων δικαιωμάτων ή του διεθνούς ανθρωπιστικού δικαίου, είναι σκόπιμη η επιβολή ελέγχων στην εξαγωγή των εν λόγω ειδών. Οι συναφείς κίνδυνοι αφορούν, ιδίως, περιπτώσεις στις οποίες τα είδη κυβερνοεπιτήρησης είναι ειδικά σχεδιασμένα ώστε να επιτρέπουν την εισβολή

([1]) Βλέπε ιδίως ελέγχους σχετικά με τα συστήματα υποκλοπής τηλεπικοινωνιών (5A001.στ), τα συστήματα επιτήρησης του διαδικτύου (5A001.ι.), το λογισμικό εισβολής (4A005, 4D004 και τους σχετικούς ελέγχους βάσει των σημείων 4E001.α και 4E001.γ) και το λογισμικό παρακολούθησης της επιβολής του νόμου (5D001.ε). Βλέπε περαιτέρω, βάσει κατά περίπτωση αξιολόγησης, ελέγχους που αφορούν ορισμένα εγκληματολογικά/ερευνητικά εργαλεία (5A004.b 5D002.α.3.β και 5D002.γ.3.β).

([2]) Ιδίως τα συστήματα ασφάλειας πληροφοριών.

([3]) Βλέπε κανονισμό (ΕΚ) αριθ. 765/2006 του Συμβουλίου, της 18ης Μαΐου 2006, σχετικά με περιοριστικά μέτρα λόγω της κατάστασης στη Λευκορωσία και της εμπλοκής της Λευκορωσίας στην επίθεση της Ρωσίας κατά της Ουκρανίας (ΕΕ L 134 της 20.5.2006, σ. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj)· κανονισμό (ΕΕ) αριθ. 359/2011 του Συμβουλίου, της 12ης Απριλίου 2011, για περιοριστικά μέτρα κατά ορισμένων προσώπων, οντοτήτων και οργανισμών λόγω της κατάστασης στο Ιράν (ΕΕ L 100 της 14.4.2011, σ. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj)· κανονισμό (ΕΕ) αριθ. 36/2012 του Συμβουλίου, της 18ης Ιανουαρίου 2012, σχετικά με περιοριστικά μέτρα λόγω της κατάστασης στη Συρία και την κατάργηση του κανονισμού (ΕΕ) αριθ. 442/2011 (ΕΕ L 16 της 19.1.2012, σ. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj)· κανονισμό (ΕΕ) αριθ. 401/2013 του Συμβουλίου, της 2ας Μαΐου 2013, σχετικά με περιοριστικά μέτρα λόγω της κατάστασης στη Μιανμάρ/Βιρμανία και την κατάργηση του κανονισμού (ΕΚ) αριθ. 194/2008 (ΕΕ L 121 της 3.5.2013, σ. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj)· και κανονισμό (ΕΕ) 2017/2063 του Συμβουλίου, της 13ης Νοεμβρίου 2017, σχετικά με περιοριστικά μέτρα λόγω της κατάστασης στη Βενεζουέλα (ΕΕ L 295 της 14.11.2017, σ. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

ή την εις βάθος επιθεώρηση πακέτων σε συστήματα πληροφοριών και τηλεπικοινωνιών με σκοπό τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων μέσω παρακολούθησης, εξαγωγής, συλλογής ή ανάλυσης δεδομένων, συμπεριλαμβανομένων βιομετρικών δεδομένων, από τα εν λόγω συστήματα. Τα είδη που χρησιμοποιούνται για αμιγώς εμπορικές εφαρμογές, όπως η τιμολόγηση, η εμπορική προώθηση, οι υπηρεσίες ποιότητας, η ικανοποίηση των χρηστών ή η ασφάλεια του δικτύου, θεωρείται γενικά ότι δεν ενέχουν τέτοιους κινδύνους».

β) Αιτιολογική σκέψη 9: «Προκειμένου να ενισχυθεί ο αποτελεσματικός έλεγχος των εξαγωγών μη απαριθμούμενων ειδών κυβερνοεπιτήρησης, είναι σημαντικό να εναρμονιστεί περαιτέρω η εφαρμογή γενικών ελέγχων στον εν λόγω τομέα. Για τον σκοπό αυτό, τα κράτη μέλη δεσμεύονται να υποστηρίζουν τους ελέγχους αυτούς ανταλλάσσοντας πληροφορίες μεταξύ τους και με την Επιτροπή, ιδίως όσον αφορά τις τεχνολογικές εξελίξεις των ειδών κυβερνοεπιτήρησης, και επιδεικνύοντας επαγρύπνηση κατά την εφαρμογή των εν λόγω ελέγχων για την προώθηση ανταλλαγών σε επίπεδο Ένωσης».

γ) Το άρθρο 2 σημείο 20, το οποίο παρέχει ορισμό για τα «είδη κυβερνοεπιτήρησης» ως είδη διπλής χρήσης ειδικά σχεδιασμένα για να επιτρέπουν τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων μέσω παρακολούθησης, εξαγωγής, συλλογής ή ανάλυσης δεδομένων από συστήματα πληροφοριών και τηλεπικοινωνιών».

δ) Το άρθρο 5 εισάγει απαίτηση άδειας εξαγωγής για την εξαγωγή μη απαριθμούμενων ειδών κυβερνοεπιτήρησης εφόσον ο εξαγωγέας έχει ενημερωθεί από την αρμόδια αρχή ότι τα εν λόγω είδη προορίζονται ή μπορεί να προορίζονται, εν όλω ή εν μέρει, για χρήση σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου (άρθρο 5 παράγραφος 1). Περαιτέρω, απαιτεί από τους εξαγωγείς να ενημερώνουν την αρμόδια αρχή όταν γνωρίζουν, σύμφωνα με τα πορίσματά τους δέουσας επιμέλειας, ότι τα είδη προορίζονται, εν όλω ή εν μέρει, για χρήση σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου (άρθρο 5 παράγραφος 2). Η εν λόγω αρμόδια αρχή αποφασίζει αν θα υποβάλει την εν λόγω εξαγωγή σε αδειοδότηση.

ε) Το άρθρο 5 παράγραφος 2 ορίζει περαιτέρω ότι «Η Επιτροπή και το Συμβούλιο διαθέτουν κατευθυντήριες γραμμές στους εξαγωγείς, όπως αναφέρεται στο άρθρο 26 παράγραφος 1».

1.2. **Βασικοί ορισμοί**

Ο κανονισμός περιέχει ειδικές αιτιολογικές σκέψεις και διατάξεις που αποσαφηνίζουν συγκεκριμένους όρους σχετικά με τους ελέγχους στις εξαγωγές μη απαριθμούμενων ειδών κυβερνοεπιτήρησης, και οι οποίες είναι σημαντικές ώστε οι εξαγωγείς να τις κατανοούν σαφώς, προκειμένου να επιδεικνύουν τη δέουσα επιμέλεια και να διενεργούν αποτελεσματικά τους ελέγχους. Ιδιαίτερης σημασίας είναι το άρθρο 2 σημείο 20, το οποίο παρέχει τον ακόλουθο ακριβή ορισμό για τα «είδη κυβερνοεπιτήρησης»: *είδη διπλής χρήσης ειδικά σχεδιασμένα για να επιτρέπουν τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων μέσω παρακολούθησης, εξαγωγής, συλλογής ή ανάλυσης δεδομένων από συστήματα πληροφοριών και τηλεπικοινωνιών*.

Για τους σκοπούς των κατευθυντήριων γραμμών, θα πρέπει να αποσαφηνιστούν συγκεκριμένες πτυχές του εν λόγω ορισμού.

1.2.1. *«Ειδικά σχεδιασμένα»*

Ένα είδος είναι σχεδιασμένο για συγκεκαλυμμένη επιτήρηση όταν τα τεχνικά χαρακτηριστικά του είναι κατάλληλα για τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων και την καθιστούν αντικειμενικά εφικτή. Ως εκ τούτου, ο όρος «ειδικά σχεδιασμένα» σημαίνει ότι η συγκεκαλυμμένη επιτήρηση φυσικών προσώπων πρέπει να αποτελεί τον κύριο σκοπό της ανάπτυξης και του σχεδιασμού του προϊόντος. Ωστόσο, ο όρος αυτός δεν απαιτεί το αντικείμενο να μπορεί να χρησιμοποιηθεί αποκλειστικά για τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων.

Όπως διευκρινίζεται στην αιτιολογική σκέψη 8 του κανονισμού, τα είδη που χρησιμοποιούνται για αμιγώς εμπορικές εφαρμογές, όπως η τιμολόγηση, η εμπορική προώθηση, οι υπηρεσίες ποιότητας, η ικανοποίηση των χρηστών ή η ασφάλεια του δικτύου, δεν είναι ειδικά σχεδιασμένα για τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων και, ως εκ τούτου, δεν εμπίπτουν στον ορισμό των ειδών κυβερνοεπιτήρησης. Για παράδειγμα, παρόλο που είδη για την επιτήρηση λειτουργικών συστημάτων στη βιομηχανία ή για την παρακολούθηση της κυκλοφορίας των χρηστών θα μπορούσαν να χρησιμοποιηθούν για σκοπούς επιτήρησης, τα εν λόγω είδη δεν αποτελούν είδη κυβερνοεπιτήρησης σύμφωνα με τον ορισμό, δεδομένου ότι δεν είναι ειδικά σχεδιασμένα για να επιτρέπουν τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων.

1.2.2. *«Συγκεκαλυμμένη επιτήρηση»*

Τα είδη καθιστούν δυνατή τη συγκεκαλυμμένη επιτήρηση ιδίως όταν η επιτήρηση δεν είναι εμφανώς αντιληπτή στο θιγόμενο φυσικό πρόσωπο. Αυτό συμβαίνει όταν τα ενδιαφερόμενα πρόσωπα δεν γνωρίζουν την παρουσία και/ή τη δράση ειδών κυβερνοεπιτήρησης και, ως εκ τούτου, δεν έχουν τη δυνατότητα να απομακρυνθούν από την εν λόγω επιτήρηση ή τουλάχιστον να προσαρμόσουν αναλόγως τη συμπεριφορά τους. Ακόμη και αν η επιτήρηση διενεργείται μέσω ειδών εγκατεστημένων ή λειτουργούντων στον δημόσιο χώρο, η απόκτηση δεδομένων μπορεί σε ορισμένες περιπτώσεις να θεωρηθεί συναφής με τη συγκεκαλυμμένη επιτήρηση, ιδίως όταν τα συλλεγόμενα δεδομένα μπορούν να εκτραπούν, να αξιολογηθούν ή να υποβληθούν σε επεξεργασία για σκοπούς άλλους από εκείνους για τους οποίους έχει ενημερωθεί το θιγόμενο φυσικό πρόσωπο. Με άλλα λόγια, όταν ένα φυσικό πρόσωπο αντικειμενικά δεν μπορεί να αναμένει ότι βρίσκεται υπό επιτήρηση, η επιτήρηση μπορεί να θεωρηθεί συγκεκαλυμμένη σύμφωνα με το άρθρο 2 σημείο 20 του κανονισμού.

1.2.3. *«Φυσικά πρόσωπα»*

Ο όρος «φυσικό πρόσωπο» αναφέρεται σε ζωντανό ανθρώπινο ον, σε αντίθεση με νομικό πρόσωπο ή οντότητα, τα οποία, κατά συνέπεια, δεν υπόκεινται στις διατάξεις. Ο όρος δεν καλύπτει την επιτήρηση αντικειμένων, χώρων ή μηχανημάτων αυτών καθαυτών.

1.2.4. *«Παρακολούθηση, εξαγωγή, συλλογή, ανάλυση δεδομένων»*

Σύμφωνα με το αγγλικό λεξικό Oxford, οι λέξεις παρακολούθηση (monitoring), εξαγωγή (extracting), συλλογή (collecting) και ανάλυση (analysing) έχουν την ακόλουθη σημασία:

— «παρακολούθηση»: εποπτεία· επιτήρηση, συνακρόαση·

— «εξαγωγή»: αντλώ·

— «συλλογή»: συλλέγω, συγκεντρώνω;

— «ανάλυση»: διαφοροποιώ ή εξακριβώνω τα επιμέρους στοιχεία από κάτι (σύνθετο) προκειμένου να προσδιοριστεί η δομή ή η φύση του και, ως εκ τούτου, να εξηγηθεί ή να κατανοηθεί· εξετάζω ενδελεχώς και μεθοδικά για σκοπούς ερμηνείας· υποβάλλω σε κριτική ή υπολογιστική ανάλυση.

Από τους εν λόγω όρους συνάγεται ότι τα είδη που χρησιμοποιούνται για την επιτήρηση θα πρέπει να διαθέτουν ακριβείς τεχνικές ικανότητες για την επεξεργασία δεδομένων με σκοπό την παρακολούθηση, τη συλλογή, την εξαγωγή ή την ανάλυση δεδομένων, όπως, για παράδειγμα, τα ακόλουθα είδη:

α) είδη που χρησιμοποιούνται για την παρακολούθηση δεδομένων από συστήματα πληροφοριών και τηλεπικοινωνιών ([4]) (για παράδειγμα, μέγεθος αρχείου δεδομένων ή κίνηση πακέτου δεδομένων που διαβιβάζονται στο εν λόγω σύστημα)·

β) είδη που εξάγουν δεδομένα από συστήματα πληροφοριών και τηλεπικοινωνιών εκτελώντας εισβολή και εξαγωγή (για παράδειγμα, λογισμικό εισβολής)·

γ) είδη που καθιστούν δυνατή την ανάλυση δεδομένων που εξάγονται από συστήματα πληροφοριών και τηλεπικοινωνιών, συμπεριλαμβανομένων εκείνων που μπορούν να επεξεργάζονται εικόνες κάμερας αποθηκευμένες στα εν λόγω συστήματα (για παράδειγμα, ορισμένοι τύποι τεχνολογιών ανάλυσης δεδομένων που χρησιμοποιούνται στο πλαίσιο συστημάτων αναγνώρισης προσώπου).

Είδη που χρησιμοποιούνται απλώς για την παρακολούθηση συστημάτων πληροφοριών ή για την παρατήρηση του πληθυσμού μέσω καμερών βιντεοεπιτήρησης και τα οποία καθιστούν δυνατή τη συλλογή συνομιλιών, ανταλλαγών δεδομένων, κινήσεων και ατομικών συμπεριφορών, δεν αποτελούν είδη κυβερνοεπιτήρησης κατά τον ορισμό του κανονισμού, καθώς δεν είναι ειδικά σχεδιασμένα για τον σκοπό αυτό και πρέπει να συνδυάζονται με άλλες τεχνολογίες, όπως η τεχνητή νοημοσύνη ή τα μαζικά δεδομένα. Ωστόσο, ολόκληρο το σύστημα (σε συνεργασία με άλλες τεχνολογίες, όπως η τεχνητή νοημοσύνη ή οι τεχνολογίες μαζικών δεδομένων) θα μπορούσε δυνητικά να αποτελέσει στοιχείο κυβερνοεπιτήρησης σύμφωνα με τον ορισμό του άρθρου 2 σημείο 20 του κανονισμού.

Είναι σημαντικό να σημειωθεί ότι, αν και παρέχονται ορισμένα παραδείγματα χρήσιμα για επεξηγηματικούς σκοπούς, ο ορισμός και το πεδίο εφαρμογής των ειδών κυβερνοεπιτήρησης δεν περιορίζονται από τα παραδείγματα αυτά, δεδομένου ότι στόχος του άρθρου 5 είναι να καταστεί δυνατός ο αποτελεσματικός έλεγχος των εξαγωγών μη απαριθμούμενων ειδών.

([4]) Βλέπε σημείο 1.2.5. κατωτέρω για τον ορισμό.

Όπως δείχνει η χρήση του συνδέσμου «ή» στον ορισμό, οι απαριθμούμενες τεχνικές ικανότητες πρέπει να θεωρούνται εναλλακτικές, και δεν είναι απαραίτητο ένα είδος να διαθέτει όλες αυτές τις τεχνικές ικανότητες για την παρακολούθηση, την εξαγωγή, τη συλλογή ή την ανάλυση δεδομένων. Με άλλα λόγια, αρκεί ένα είδος να διαθέτει μία από αυτές τις τεχνικές ικανότητες ώστε να εμπίπτει στον ορισμό του είδους κυβερνοεπιτήρησης του άρθρου 2 σημείο 20.

1.2.5. *«Από συστήματα πληροφοριών και τηλεπικοινωνιών»*

Οι όροι αυτοί αναφέρονται σε συστήματα τα οποία επεξεργάζονται ηλεκτρονικά πληροφορίες, όπως π.χ. προγραμματισμός / δημιουργία κώδικα, λειτουργία συστημάτων Η/Υ (υλισμικό) και άλλα είδη διαχείρισης πληροφοριών, συμπεριλαμβανομένης της τεχνολογίας λογισμικού, της τεχνολογίας ιστού, της τεχνολογίας υπολογιστών, της τεχνολογίας αποθήκευσης κ.λπ., καθώς και σε ορισμένα συστήματα που μεταφέρουν πληροφορίες εξ αποστάσεως, για παράδειγμα τεχνικά συστήματα που εκπέμπουν ήχους, σήματα, κείμενο, άλλες ενδείξεις, εικόνες μέσω ενσύρματων και ασύρματων διαύλων, μέσω οπτικών ινών, ραδιοεπικοινωνιών και άλλων ηλεκτρομαγνητικών συστημάτων. Από κοινού, οι δύο αυτές έννοιες περιλαμβάνουν ευρύ φάσμα συστημάτων μετάδοσης ή επεξεργασίας πληροφοριών. Πρέπει να σημειωθεί ότι ο όρος αναφέρεται σε συστήματα και όχι σε εξοπλισμό.

1.2.6. *«Γνωρίζει» και «προορίζονται για»*

Σύμφωνα με το άρθρο 5 παράγραφος 2 του κανονισμού, ο εξαγωγέας ενημερώνει την αρμόδια αρχή όταν ο εξαγωγέας *«γνωρίζει […] ότι τα είδη κυβερνοεπιτήρησης […] προορίζονται […] για χρήση σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου».*

Ο όρος «γνωρίζει» δεν αποτελεί νέα νομική έννοια, αλλά έχει χρησιμοποιηθεί σε σχέση με τις σχετικές με την τελική χρήση απαιτήσεις αδειοδότησης (οι λεγόμενοι γενικοί έλεγχοι) σύμφωνα με τα άρθρα 4, 6, 7 και 8 του κανονισμού. Το να «γνωρίζει» σημαίνει ότι ο εξαγωγέας έχει βέβαιη γνώση της σκοπούμενης κατάχρησης. Η απλή πιθανότητα ενός τέτοιου κινδύνου δεν αρκεί για να αποδειχθεί η γνώση. Ωστόσο, ο όρος «γνωρίζει» δεν μπορεί να εξομοιωθεί με παθητικότητα: απαιτείται από τον εξαγωγέα να έχει λάβει μέτρα για να αποκτήσει επαρκείς και κατάλληλες γνώσεις για την εκτίμηση των κινδύνων που συνδέονται με την εξαγωγή, και για τη διασφάλιση της συμμόρφωσης με τον κανονισμό.

Η ένδειξη ότι τα είδη πρέπει να «προορίζονται για» σχετική ευαίσθητη τελική χρήση συνεπάγεται ότι ο εξαγωγέας θα πρέπει να αξιολογεί την τελική χρήση κατά περίπτωση, υπό το πρίσμα των ειδικών περιστάσεων της συγκεκριμένης περίπτωσης. Εξ αντιδιαστολής, ένας θεωρητικός κίνδυνος, ο οποίος δηλαδή δεν βασίζεται σε αξιολόγηση των πραγματικών περιστατικών της περίπτωσης, ότι τα είδη θα μπορούσαν να χρησιμοποιηθούν κατά τρόπο που παραβιάζει τα ανθρώπινα δικαιώματα, δεν αρκεί για να συναχθεί ότι «προορίζονται για» συγκεκριμένη κατάχρηση βάσει του άρθρου 5.

1.3. **Εσωτερική καταστολή, σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου**

Σύμφωνα με το άρθρο 15 του κανονισμού, στο οποίο καθορίζονται οι εκτιμήσεις για την αξιολόγηση μιας άδειας, τα κράτη μέλη πρέπει να λαμβάνουν υπόψη κάθε σχετικό ζήτημα, συμπεριλαμβανομένων εκείνων που καλύπτονται από την κοινή θέση 2008/944/ΚΕΠΠΑ του Συμβουλίου ([5]).

Το άρθρο 5 του κανονισμού επεκτείνει τους ελέγχους στην εξαγωγή ειδών κυβερνοεπιτήρησης που δεν περιλαμβάνονται στον κατάλογο, λαμβανομένου υπόψη του κινδύνου χρήσης τους σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου. Η κοινή θέση 2008/944/ΚΕΠΠΑ και οι οδηγίες χρήσης της οικείας κοινής θέσης ([6]) παρέχουν χρήσιμες οδηγίες ως προς αυτό.

([5]) Κοινή θέση 2008/944/ΚΕΠΠΑ του Συμβουλίου, της 8ης Δεκεμβρίου 2008, για τον καθορισμό κοινών κανόνων που διέπουν τον έλεγχο των εξαγωγών στρατιωτικής τεχνολογίας και εξοπλισμού (ΕΕ L 335 της 13.12.2008, σ. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Βλέπε οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ του Συμβουλίου για τον καθορισμό κοινών κανόνων που διέπουν τον έλεγχο των εξαγωγών στρατιωτικής τεχνολογίας και εξοπλισμού, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Εσωτερική καταστολή*

Σύμφωνα με το άρθρο 2 παράγραφος 2 της κοινής θέσης 2008/944/ΚΕΠΠΑ, «στην εσωτερική καταστολή περιλαμβάνονται, μεταξύ άλλων, τα βασανιστήρια και άλλοι τρόποι σκληρής, απάνθρωπης ή ταπεινωτικής μεταχείρισης ή τιμωρίας, οι αυθαίρετες ή με συνοπτικές διαδικασίες εκτελέσεις, οι εξαφανίσεις, οι αυθαίρετες κρατήσεις ή άλλες σημαντικές παραβιάσεις των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, όπως ορίζονται σε συναφείς διεθνείς πράξεις για τα ανθρώπινα δικαιώματα, μεταξύ των οποίων είναι η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου και το Διεθνές σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα». Οι οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ παρέχουν καθοδήγηση σχετικά με τα στοιχεία που πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση από τον εξαγωγέα, συμπεριλαμβανομένων των «νυν και των πρότερων επιδόσεων του προτεινόμενου τελικού χρήστη όσον αφορά το σεβασμό των ανθρώπινων δικαιωμάτων αλλά και τις επιδόσεις της αποδέκτριας χώρας εν γένει».

1.3.2. *Διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων*

Η κατάχρηση μη απαριθμούμενων ειδών κυβερνοεπιτήρησης μπορεί να επηρεάσει αρνητικά ένα ευρύ φάσμα ανθρωπίνων δικαιωμάτων και θίγει άμεσα το δικαίωμα στην ιδιωτική ζωή και στην προστασία των δεδομένων. Η αυθαίρετη ή παράνομη επιτήρηση μπορεί επίσης να παραβιάζει άλλα ανθρώπινα δικαιώματα, όπως το δικαίωμα στην ελευθερία της έκφρασης, του συνεταιρίζεσθαι και του συνέρχεσθαι, την ελευθερία σκέψης, συνείδησης και θρησκείας, καθώς και το δικαίωμα ίσης μεταχείρισης ή απαγόρευσης των διακρίσεων, και το δικαίωμα σε ελεύθερες, ισότιμες και μυστικές εκλογές. Σε ορισμένες περιπτώσεις, η επιτήρηση, συμπεριλαμβανομένης της παρακολούθησης ή της συλλογής πληροφοριών για φυσικά πρόσωπα, όπως υπερασπιστές των ανθρωπίνων δικαιωμάτων, ακτιβιστές, πολιτικές προσωπικότητες, ευάλωτους πληθυσμούς και δημοσιογράφους, μπορεί να οδηγήσει σε εκφοβισμό, καταπίεση, αυθαίρετη κράτηση, βασανιστήρια ή ακόμη και εξωδικαστικές εκτελέσεις. Ως εκ τούτου, οι εξαγωγείς θα πρέπει να συμπεριλαμβάνουν στις αξιολογήσεις τους αυτές τις πτυχές που σχετίζονται με σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων.

Η διεθνής πρακτική δείχνει ότι τυχόν περιορισμοί στα ανθρώπινα δικαιώματα πρέπει να είναι «ενδεδειγμένοι» και σύμφωνοι με τα διεθνή πρότυπα για τα ανθρώπινα δικαιώματα. Στην πράξη αυτό σημαίνει ότι υπάρχουν κατάλληλες εγγυήσεις ώστε να διασφαλίζεται ότι οι περιορισμοί προβλέπονται από τον νόμο και διαφυλάσσεται η ουσία των δικαιωμάτων. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί μπορούν να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και εξυπηρετούν πραγματικά έναν θεμιτό σκοπό —για παράδειγμα, την εθνική ή δημόσια ασφάλεια, τη δημόσια τάξη, την προστασία της δημόσιας υγείας ή την προστασία των δικαιωμάτων και ελευθεριών τρίτων.

Τα είδη κυβερνοεπιτήρησης μπορούν να περιλαμβάνουν νόμιμα και ρυθμιζόμενα εργαλεία για εφαρμογές στην επιβολή του νόμου, όπως για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων, μεταξύ άλλων στον τομέα της καταπολέμησης της τρομοκρατίας, ή την εκτέλεση ποινικών κυρώσεων. Παράλληλα, τα είδη κυβερνοεπιτήρησης μπορούν επίσης να χρησιμοποιηθούν καταχρηστικά για τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου όταν εξάγονται σε καταπιεστικά καθεστώτα ή σε ιδιωτικούς τελικούς χρήστες και/ή σε περιοχές συγκρούσεων.

Αυτό απαιτεί την κατά περίπτωση αξιολόγηση από τα αρμόδια όργανα, για παράδειγμα τα Ηνωμένα Έθνη, την Ένωση ή το Συμβούλιο της Ευρώπης, των περιστάσεων μιας περίπτωσης, καθώς και την εφαρμογή των σχετικών κανονισμών, υπό το πρίσμα τυχόν καταγγελιών για σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων. Η αναγνώριση των παραβιάσεων αυτών σε πληροφορίες που δημοσιεύονται από τα αρμόδια όργανα των Ηνωμένων Εθνών, από την Ένωση ή από το Συμβούλιο της Ευρώπης μπορεί να αποτελεί ένδειξη για τη «σοβαρότητα» των παραβιάσεων ανθρωπίνων δικαιωμάτων. Δεν είναι απολύτως αναγκαία η ρητή αυτή αναγνώριση από τα εν λόγω όργανα, αλλά αποτελεί σημαντικό παράγοντα για την εκπλήρωση των κριτηρίων.

Σύμφωνα με τους όρους του άρθρου 5, η παραβίαση των ανθρωπίνων δικαιωμάτων πρέπει να είναι «σοβαρή». Χρήσιμες οδηγίες για τον χαρακτηρισμό πιθανών παραβιάσεων ανθρωπίνων δικαιωμάτων ως «σοβαρών» περιλαμβάνονται στις οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ. Σύμφωνα με τις εν λόγω οδηγίες, η φύση και οι συνέπειες της παραβίασης είναι καθοριστικές. Οι συστηματικές και/ή εκτεταμένες παραβιάσεις των ανθρωπίνων δικαιωμάτων θεωρούνται κατά κανόνα σοβαρές· αλλά και παραβιάσεις που δεν είναι συστηματικές ή εκτεταμένες μπορούν να θεωρηθούν «σοβαρές» —για παράδειγμα, λόγω της σοβαρότητας των επιπτώσεων για τα θιγόμενα πρόσωπα.

Το παράρτημα ΙΙ των οδηγιών χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ προβλέπει μη εξαντλητικό κατάλογο των κύριων διεθνών και περιφερειακών πράξεων για τα ανθρώπινα δικαιώματα, συμπεριλαμβανομένων του Διεθνούς συμφώνου για τα ατομικά και πολιτικά δικαιώματα (ICCPR), της σύμβασης κατά των βασανιστηρίων και άλλων τρόπων σκληρής, απάνθρωπης ή ταπεινωτικής μεταχείρισης ή τιμωρίας, της Ευρωπαϊκής σύμβασης Δικαιωμάτων του Ανθρώπου (στο εξής: Σύμβαση) και του Χάρτη των Θεμελιωδών Δικαιωμάτων (στο εξής: Χάρτης), που μπορούν να παράσχουν σημαντική καθοδήγηση για την ερμηνεία και την εφαρμογή των κριτηρίων προς υποστήριξη αξιόπιστων αξιολογήσεων στο πεδίο των ανθρωπίνων δικαιωμάτων. Οι εν λόγω πράξεις και τα αντίστοιχα συμπληρωματικά τους πρωτόκολλα αντιπροσωπεύουν τους κύριους διεθνείς κανόνες και πρότυπα στο πεδίο των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών.

1.3.3. *Διάπραξη σοβαρών παραβιάσεων του διεθνούς ανθρωπιστικού δικαίου*

Το διεθνές ανθρωπιστικό δίκαιο (που ονομάζεται επίσης «δίκαιο της Γενεύης» ή «δίκαιο των ενόπλων συρράξεων») αναπτύχθηκε μέσω μιας σειράς διεθνών συνθηκών, κυρίως των Κανονισμών της Χάγης, των Συμβάσεων της Γενεύης και των δύο πρόσθετων πρωτοκόλλων τους του 1977, και προσδιορίζει κανόνες οι οποίοι, σε περιόδους ένοπλης σύρραξης, χρησιμεύουν για την προστασία ατόμων που δεν συμμετέχουν ή δεν συμμετέχουν πλέον σε εχθροπραξίες (για παράδειγμα, αμάχους και τραυματίες, ασθενείς ή αιχμάλωτους μαχητές) και επιβάλλουν περιορισμούς στα αντιμαχόμενα μέρη όσον αφορά τα μέσα και τις μεθόδους πολέμου (νόμος της Χάγης).

Η χρήση μη απαριθμούμενων ειδών κυβερνοεπιτήρησης θα πρέπει να συμμορφώνεται με το διεθνές ανθρωπιστικό δίκαιο όταν χρησιμοποιούνται ως μέσα και μέθοδοι πολεμικών επιχειρήσεων στο πλαίσιο ένοπλης σύρραξης. Υπό τέτοιες περιστάσεις, ο κίνδυνος σοβαρών παραβιάσεων του διεθνούς ανθρωπιστικού δικαίου εξετάζεται στο πλαίσιο του κανονισμού και, όσον αφορά τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων, αυτή θα πρέπει να αξιολογείται υπό το πρίσμα της σκοπούμενης τελικής χρήσης των ειδών στη συγκεκριμένη περίπτωση. Οι οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ παρέχουν καθοδήγηση σχετικά με τα στοιχεία που πρέπει να λαμβάνονται υπόψη, συμπεριλαμβανομένων των πρότερων και νυν επιδόσεων του παραλήπτη όσον αφορά τον σεβασμό του διεθνούς ανθρωπιστικού δικαίου, των προθέσεων του παραλήπτη όπως εκφράζονται μέσω επίσημων δεσμεύσεων και της ικανότητας του παραλήπτη να διασφαλίσει ότι ο εξοπλισμός ή η τεχνολογία που μεταβιβάζεται χρησιμοποιείται κατά τρόπο σύμφωνο με το διεθνές ανθρωπιστικό δίκαιο και δεν εκτρέπεται ούτε μεταφέρεται σε άλλους προορισμούς όπου θα μπορούσε να χρησιμοποιηθεί για σοβαρές παραβιάσεις του εν λόγω δικαίου.

Σύμφωνα με το άρθρο 5, η παραβίαση του διεθνούς ανθρωπιστικού δικαίου πρέπει να είναι «σοβαρή». Καθοδήγηση περιλαμβάνεται στις οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ, όπου αναγνωρίζεται ότι «μεμονωμένα περιστατικά παραβιάσεων του διεθνούς ανθρωπιστικού δικαίου δεν είναι κατ' ανάγκη ενδεικτικά της στάσης της αποδέκτριας χώρας έναντι του διεθνούς ανθρωπιστικού δικαίου», ενώ «όταν μπορεί να διαπιστωθεί κάποια μορφή παραβιάσεων ή η αποδέκτρια χώρα δεν έχει λάβει τα κατάλληλα μέτρα για την τιμωρία των παραβιάσεων, αυτό θα πρέπει να προκαλεί σοβαρή ανησυχία». Η Διεθνής Επιτροπή του Ερυθρού Σταυρού (ΔΕΕΣ) έχει παράσχει κατευθυντήριες γραμμές όσον αφορά την αξιολόγηση των παραβιάσεων του διεθνούς ανθρωπιστικού δικαίου για σκοπούς ελέγχου των εξαγωγών. Σύμφωνα με τη ΔΕΕΣ, «οι παραβιάσεις του διεθνούς ανθρωπιστικού δικαίου είναι σοβαρές εάν θέτουν σε κίνδυνο προστατευόμενα πρόσωπα (για παράδειγμα, αμάχους, αιχμαλώτους πολέμου, τραυματίες και ασθενείς) ή αντικείμενα (για παράδειγμα, μη στρατιωτικά αντικείμενα ή υποδομές) ή εάν παραβιάζουν σημαντικές οικουμενικές αξίες». Τα εγκλήματα πολέμου, για παράδειγμα, συνιστούν σοβαρές παραβιάσεις του διεθνούς ανθρωπιστικού δικαίου. Η ΔΕΕΣ αναφέρει επίσης παρόμοιους με τις οδηγίες χρήσης για την κοινή θέση 2008/944/ΚΕΠΠΑ παράγοντες που πρέπει να λαμβάνονται υπόψη, συμπεριλαμβανομένων των επίσημων δεσμεύσεων για την εφαρμογή των κανόνων του διεθνούς ανθρωπιστικού δικαίου, των ενδεδειγμένων μέτρων που διασφαλίζουν τη λογοδοσία για παραβιάσεις του διεθνούς ανθρωπιστικού δικαίου, της εκπαίδευσης του στρατού στο διεθνές ανθρωπιστικό δίκαιο, και της απαγόρευσης στρατολόγησης παιδιών στις ένοπλες δυνάμεις.

2. **ΤΕΧΝΙΚΟ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ**

2.1. **Απαριθμούμενα είδη κυβερνοεπιτήρησης**

Το προσάρτημα των παρουσών κατευθυντήριων γραμμών παρέχει πληροφορίες σχετικά με τα είδη κυβερνοεπιτήρησης που απαριθμούνται στο παράρτημα Ι του κανονισμού, προκειμένου να βοηθήσει τους εξαγωγείς στον εντοπισμό πιθανών μη απαριθμούμενων ειδών κυβερνοεπιτήρησης.

2.2. **Δυνητικά μη απαριθμούμενα είδη κυβερνοεπιτήρησης**

Μολονότι είναι εξ ορισμού αδύνατο να παρασχεθεί εξαντλητικός κατάλογος των ειδών που μπορούν να ελεγχθούν ως «μη απαριθμούμενα είδη» σύμφωνα με το άρθρο 5, τα ακόλουθα είδη θα μπορούσαν να αποτελέσουν αντικείμενο επιτήρησης και μπορεί να απαιτούν ιδιαίτερη επαγρύπνηση δυνάμει του κανονισμού.

Όπως διευκρινίζεται στην αιτιολογική σκέψη 8 του κανονισμού, τα είδη που χρησιμοποιούνται για αμιγώς εμπορικές εφαρμογές, όπως η τιμολόγηση, η εμπορική προώθηση, οι υπηρεσίες ποιότητας, η ικανοποίηση των χρηστών ή η ασφάλεια του δικτύου, θεωρείται γενικά ότι δεν ενέχουν κινδύνους κατάχρησης συναφείς στο πλαίσιο σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων ή του διεθνούς ανθρωπιστικού δικαίου και, ως εκ τούτου, γενικά δεν υπόκεινται σε έλεγχο δυνάμει του άρθρου 5. Πολλά από τα είδη αυτά διαθέτουν (κρυπτογραφικές ή ακόμη και κρυπταναλυτικές) λειτουργικότητες ασφάλειας πληροφοριών που πληρούν τις παραμέτρους ελέγχου της κατηγορίας 5 μέρος 2 της περιγραφής στο παράρτημα Ι του κανονισμού. Ο εξοπλισμός δικτύου ασφάλειας —συμπεριλαμβανομένων δρομολογητών, διακοπτών ή ηλεκτρονόμων, στους οποίους η λειτουργικότητα ασφάλειας πληροφοριών περιορίζεται στα καθήκοντα της «λειτουργίας, διαχείρισης ή συντήρησης» και εφαρμόζει μόνο δημοσιευμένα ή εμπορικά κρυπτογραφικά πρότυπα— επίσης δεν καλύπτεται από τον ορισμό των «ειδών κυβερνοεπιτήρησης», αν και, λαμβανομένων υπόψη των διαφόρων αναφορών κατάχρησης των εν λόγω ειδών για παραβιάσεις των ανθρωπίνων δικαιωμάτων, οι εξαγωγείς θα πρέπει να παραμένουν σε επαγρύπνηση.

2.2.1. *Τεχνολογία αναγνώρισης προσώπου και συναισθημάτων*

Οι τεχνολογίες αναγνώρισης προσώπου και συναισθημάτων έχουν πολλαπλές χρήσεις εκτός της κυβερνοεπιτήρησης —π.χ. ταυτοποίηση ή επαλήθευση ταυτότητας— και δεν εμπίπτουν αυτόματα στον ορισμό. Ωστόσο, σε ορισμένες περιπτώσεις, οι τεχνολογίες αναγνώρισης προσώπου και συναισθημάτων ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής του άρθρου 2 σημείο 20 του κανονισμού.

Οι τεχνολογίες αναγνώρισης προσώπου και συναισθημάτων που μπορούν να χρησιμοποιηθούν για την παρακολούθηση ή την ανάλυση αποθηκευμένων εικόνων βίντεο θα μπορούσαν να εμπίπτουν στο πεδίο εφαρμογής του ορισμού των ειδών κυβερνοεπιτήρησης. Ωστόσο, ακόμη και αν πληρούνται τα προαναφερθέντα κριτήρια, πρέπει να εξεταστεί προσεκτικά αν το λογισμικό είναι ειδικά σχεδιασμένο για συγκεκαλυμμένη επιτήρηση.

2.2.2. *Συσκευές εντοπισμού θέσης*

Οι συσκευές εντοπισμού θέσης καθιστούν δυνατό τον εντοπισμό της φυσικής θέσης μιας συσκευής σε βάθος χρόνου, ενώ ορισμένες τεχνολογίες εντοπισμού θέσης χρησιμοποιούνται εδώ και αρκετό καιρό από υπηρεσίες επιβολής του νόμου και υπηρεσίες πληροφοριών. Οι δυνατότητές τους για στοχευμένη και μαζική επιτήρηση έχουν αυξηθεί σημαντικά, καθώς οι τεχνολογίες εντοπισμού εξελίσσονται διαρκώς —συμπεριλαμβανομένων του δορυφορικού εντοπισμού θέσης, του εντοπισμού θέσης με βάση τις κυψέλες, και των πομποδεκτών Wi-Fi και Bluetooth— και λόγω του ότι οι «συσκευές εντοπισμού», όπως τα έξυπνα τηλέφωνα και άλλες ηλεκτρονικές συσκευές (π.χ. επί του οχήματος συστήματα σε αυτοκίνητα) είναι πλέον ευρέως διαδεδομένες.

Οι συσκευές εντοπισμού θέσης χρησιμοποιούνται από υπηρεσίες επιβολής του νόμου και υπηρεσίες πληροφοριών, για παράδειγμα για τη συλλογή αποδεικτικών στοιχείων κατά τη διάρκεια έρευνας ή για τον εντοπισμό υπόπτων, αλλά και από εταιρείες για εμπορικούς σκοπούς, για παράδειγμα καταγραφή συγκεντρωτικών μοτίβων μετακίνησης σε δρόμους με εμπορικά καταστήματα, εντοπισμό εργαζομένων που εργάζονται εκτός των εγκαταστάσεων ή για σκοπούς διαφήμισης βάσει τοποθεσίας.

2.2.3. *Συστήματα βιντεοεπιτήρησης*

Προκειμένου να βοηθηθούν οι εξαγωγείς να εντοπίσουν πιθανή κυβερνοεπιτήρηση, είναι επίσης χρήσιμο να διευκρινιστεί ποια είδη δεν καλύπτονται από τον ορισμό. Υπό την έννοια αυτή, για παράδειγμα τα συστήματα βιντεοεπιτήρησης και οι κάμερες —συμπεριλαμβανομένων των καμερών υψηλής ευκρίνειας— που χρησιμοποιούνται για την κινηματογράφηση ανθρώπων σε δημόσιους χώρους δεν καλύπτονται από τον ορισμό των ειδών κυβερνοεπιτήρησης, καθώς δεν παρακολουθούν ούτε συλλέγουν δεδομένα από συστήματα πληροφοριών και τηλεπικοινωνιών.

3. **ΜΕΤΡΑ ΔΕΟΥΣΑΣ ΕΠΙΜΕΛΕΙΑΣ**

Σύμφωνα με την αιτιολογική σκέψη 7 του κανονισμού, «η συμβολή των εξαγωγέων […] στον γενικό στόχο των εμπορικών ελέγχων είναι ζωτικής σημασίας. Προκειμένου να είναι σε θέση να ενεργούν σύμφωνα με τον παρόντα κανονισμό, η εκτίμηση των κινδύνων που σχετίζονται με συναλλαγές τις οποίες αφορά ο παρών κανονισμός πρέπει να διενεργείται μέσω μέτρων ελέγχου των συναλλαγών, γνωστών και ως αρχή δέουσας επιμέλειας, στο πλαίσιο εσωτερικών προγραμμάτων συμμόρφωσης (ΕΠΣ)».

Με το άρθρο 2 σημείο 21, το εσωτερικό πρόγραμμα συμμόρφωσης (ΕΠΣ) ορίζεται ως «συνεχείς αποτελεσματικές, κατάλληλες και αναλογικές πολιτικές και διαδικασίες που υιοθετούνται από τους εξαγωγείς προκειμένου να διευκολυνθεί η συμμόρφωση με τις διατάξεις και τους στόχους του παρόντος κανονισμού και με τους όρους και τις προϋποθέσεις των αδειών που εφαρμόζονται σύμφωνα με τον παρόντα κανονισμό, συμπεριλαμβανομένων, μεταξύ άλλων, μέτρων δέουσας επιμέλειας για την εκτίμηση των κινδύνων που σχετίζονται με την εξαγωγή των ειδών προς τελικούς χρήστες και τελικές χρήσεις».

Η σύσταση (ΕΕ) 2019/1318 της Επιτροπής ([7]) παρέχει ένα πλαίσιο που βοηθά τους εξαγωγείς να εντοπίζουν, να διαχειρίζονται και να μετριάζουν τους κινδύνους που συνδέονται με τους εμπορικούς ελέγχους ειδών διπλής χρήσης και να διασφαλίζουν τη συμμόρφωση με τις σχετικές νομοθετικές και κανονιστικές ρυθμίσεις της ΕΕ και των κρατών μελών.

Οι εν λόγω κατευθυντήριες γραμμές μπορούν να στηρίζουν τους εξαγωγείς κατά την εφαρμογή μέτρων ελέγχου συναλλαγών, γνωστών και ως αρχή δέουσας επιμέλειας, στο πλαίσιο ενός ΕΠΣ.

Σύμφωνα με το άρθρο 5 παράγραφος 2 του κανονισμού (ΕΕ) 2021/821, οι εξαγωγείς μη απαριθμούμενων ειδών κυβερνοεπιτήρησης υποχρεούνται να επιδεικνύουν τη δέουσα επιμέλεια μέσω μέτρων ελέγχου συναλλαγών, δηλαδή να λαμβάνουν μέτρα για την ταξινόμηση των ειδών και την εκτίμηση κινδύνου συναλλαγής. Επί της ουσίας, οι εξαγωγείς ενθαρρύνονται να εξετάζουν τα ακόλουθα:

([7]) Σύσταση (ΕΕ) 2019/1318 της Επιτροπής, της 30ής Ιουλίου 2019, για τα εσωτερικά προγράμματα συμμόρφωσης σχετικά με τους ελέγχους του εμπορίου ειδών διπλής χρήσης βάσει του κανονισμού (ΕΚ) αριθ. 428/2009 του Συμβουλίου (ΕΕ L 205 της 5.8.2019, σ. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Εξέταση του κατά πόσον το μη απαριθμούμενο είδος προς εξαγωγή ενδέχεται να είναι «είδος κυβερνοεπιτήρησης», δηλαδή ειδικά σχεδιασμένο για να επιτρέπει τη συγκεκαλυμμένη επιτήρηση φυσικών προσώπων μέσω παρακολούθησης, εξαγωγής, συλλογής ή ανάλυσης δεδομένων από συστήματα πληροφοριών και τηλεπικοινωνιών.**

Το στάδιο αυτό αφορά τον καθορισμό του είδους βάσει των διατάξεων που ισχύουν για τα είδη κυβερνοεπιτήρησης. Αυτό περιλαμβάνει εξέταση των τεχνικών χαρακτηριστικών του είδους, με βάση τις τεχνικές παραμέτρους που ορίζονται στο παράρτημα Ι του κανονισμού για τα απαριθμούμενα είδη, και υπό το πρίσμα των ειδικών όρων και εννοιών στον ορισμό των ειδών κυβερνοεπιτήρησης για τα μη απαριθμούμενα είδη, καθώς και της επακόλουθης ταξινόμησης του είδους (αγαθά, τεχνολογία ή λογισμικό).

3.2. **Εξέταση των δυνατοτήτων του υπό εξέταση είδους για να καθοριστεί εάν υπάρχει ενδεχόμενο κατάχρησης σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου από ξένους τελικούς χρήστες.**

Οι εξαγωγείς θα πρέπει να διενεργούν αξιολόγηση για να καθορίσουν εάν το προϊόν θα μπορούσε να χρησιμοποιηθεί καταχρηστικά για εσωτερική καταστολή, παραβίαση ή καταπάτηση ανθρωπίνων δικαιωμάτων, συμπεριλαμβανομένου του δικαιώματος στη ζωή, της απαγόρευσης των βασανιστηρίων και της απάνθρωπης και ταπεινωτικής μεταχείρισης, του δικαιώματος στην ιδιωτική ζωή, του δικαιώματος στην ελευθερία του λόγου, του δικαιώματος του συνεταιρίζεσθαι και του συνέρχεσθαι, του δικαιώματος στην ελευθερία σκέψης, συνείδησης και θρησκείας, του δικαιώματος ίσης μεταχείρισης ή απαγόρευσης των διακρίσεων ή του δικαιώματος σε ελεύθερες, ισότιμες και μυστικές εκλογές.

Περιλαμβάνει επίσης αξιολόγηση για να καθοριστεί αν το προϊόν θα μπορούσε να χρησιμοποιηθεί ως μέρος ή συστατικό ενός συστήματος που θα μπορούσε να οδηγήσει στις ίδιες παραβιάσεις και/ή καταχρήσεις.

Οι εξαγωγείς θα πρέπει να χρησιμοποιούν στην αξιολόγησή τους προειδοποιητικά σημάδια, τα οποία παραπέμπουν σε τυχόν ασυνήθεις περιστάσεις μιας συναλλαγής οι οποίες δείχνουν ότι η εξαγωγή μπορεί να προορίζεται για ακατάλληλη τελική χρήση, τελικό χρήστη ή προορισμό.

Προειδοποιητικά σημάδια:

α) το είδος διατίθεται στην αγορά με πληροφορίες σχετικά με τη δυνητική χρήση του για συγκεκαλυμμένη επιτήρηση·

β) πληροφορίες από τις οποίες προκύπτει ότι παρόμοιο είδος χρησιμοποιήθηκε καταχρηστικά σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου (βλέπε σημείο 1.3)·

γ) πληροφορίες από τις οποίες προκύπτει ότι το είδος χρησιμοποιήθηκε παράνομα σε δραστηριότητες επιτήρησης κατά κράτους μέλους ή σε σχέση με παράνομη επιτήρηση πολίτη της ΕΕ·

δ) πληροφορίες από τις οποίες προκύπτει ότι η συναλλαγή περιλαμβάνει είδη που θα μπορούσαν να χρησιμοποιηθούν για τη δημιουργία, την προσαρμογή ή τη διαμόρφωση συστήματος που είναι γνωστό ότι χρησιμοποιείται καταχρηστικά σε σχέση με εσωτερική καταστολή και/ή τη διάπραξη σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου (βλέπε σημείο 1.3)·

ε) το είδος ή παρόμοιο είδος περιλαμβάνεται στον κατάλογο που δημοσιεύεται στη σειρά C της *Επίσημης Εφημερίδας της Ευρωπαϊκής Ένωσης* σύμφωνα με το άρθρο 5 παράγραφος 6 του κανονισμού.

3.3. **Προς υποστήριξη των αρμόδιων αρχών, εξέταση των ενδιαφερόμενων μερών που εμπλέκονται στη συναλλαγή (συμπεριλαμβανομένων των τελικών χρηστών και των παραληπτών, όπως π.χ. διανομείς και μεταπωλητές).**

Οι εξαγωγείς θα πρέπει, προς υποστήριξη των αρμόδιων αρχών και στο μέτρο του δυνατού:

α) πριν και κατά τη διάρκεια οποιασδήποτε συναλλαγής, να εξετάζουν τον τρόπο με τον οποίο οι παραλήπτες και/ή οι τελικοί χρήστες προτίθενται να χρησιμοποιήσουν το προϊόν ή την υπηρεσία, με βάση τις δηλώσεις τελικής χρήσης·

β) να εξοικειώνονται με την κατάσταση στον σχετικό προορισμό των ειδών, ιδίως με τη γενική κατάσταση των ανθρωπίνων δικαιωμάτων, καθώς αυτό αποτελεί σημαντικό δείκτη του κινδύνου σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου που συνδέονται με μια εξαγωγή·

γ) να εξετάζουν τους κινδύνους εκτροπής του προϊόντος ή της υπηρεσίας σε διαφορετικό μη εξουσιοδοτημένο τελικό χρήστη, με βάση τα προειδοποιητικά σημάδια που παρατίθενται κατωτέρω.

Προειδοποιητικά σημάδια:

α) ο τελικός χρήστης έχει προφανή σχέση με ξένη κυβέρνηση που έχει ιστορικό διάπραξης εσωτερικής καταστολής και/ή σοβαρών παραβιάσεων των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου·

β) ο τελικός χρήστης αποτελεί δομικά μέρος των ενόπλων δυνάμεων ή άλλης ομάδας που εμπλέκεται σε ένοπλη σύρραξη η οποία περιλαμβάνει μέτρα εσωτερικής καταστολής και/ή σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου κατά το παρελθόν·

γ) ο τελικός χρήστης έχει εξαγάγει στο παρελθόν είδη κυβερνοεπιτήρησης σε χώρες όπου η χρήση των εν λόγω ειδών έχει οδηγήσει σε μέτρα εσωτερικής καταστολής και/ή σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου.

3.4. **Χρήση των πορισμάτων δέουσας επιμέλειας για την κατάρτιση σχεδίων για την πρόληψη και τον μετριασμό πιθανών μελλοντικών δυσμενών επιπτώσεων.**

Οι εξαγωγείς θα πρέπει, με βάση τα πορίσματά τους για τη δέουσα επιμέλεια, να διακόψουν τις δραστηριότητες που προκαλούν ή συμβάλλουν σε δυσμενείς επιπτώσεις που σχετίζονται με τα ανθρώπινα δικαιώματα, καθώς και να καταρτίζουν και να εφαρμόζουν σχέδιο διορθωτικών μέτρων. Οι δράσεις αυτές μπορούν να περιλαμβάνουν τα εξής:

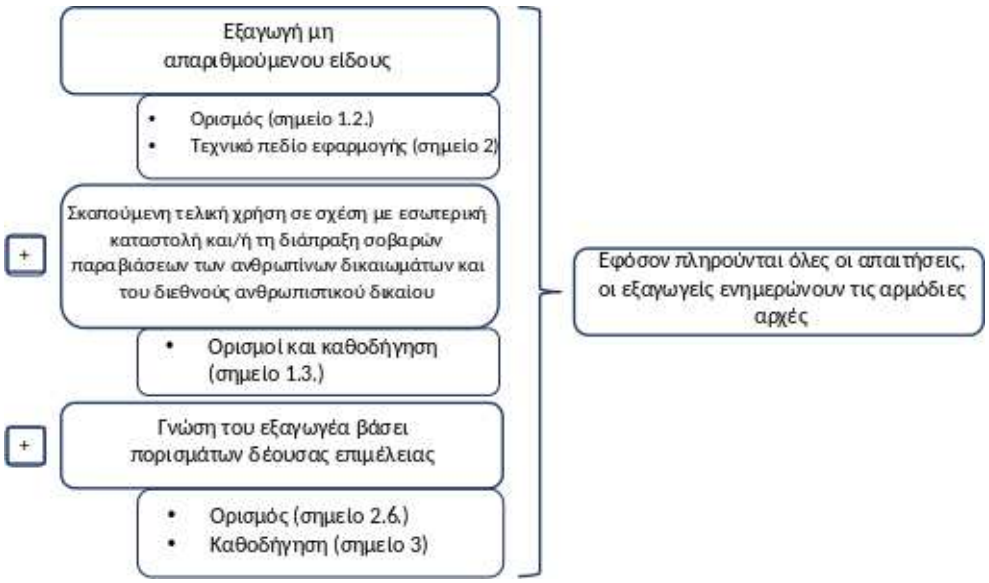
α) επικαιροποίηση των πολιτικών της επιχείρησης ώστε να παρέχεται καθοδήγηση σχετικά με τον τρόπο αποφυγής και αντιμετώπισης των δυσμενών επιπτώσεων στο μέλλον και να διασφαλίζεται η εφαρμογή τους·

β) αξιοποίηση των πορισμάτων της εκτίμησης των κινδύνων για την επικαιροποίηση και την ενίσχυση των συστημάτων διαχείρισης ώστε να διενεργείται καλύτερη παρακολούθηση των πληροφοριών και να επισημαίνονται οι κίνδυνοι πριν από την εμφάνιση δυσμενών επιπτώσεων·

γ) συλλογή πληροφοριών για την κατανόηση των υψηλού επιπέδου κινδύνων για δυσμενείς επιπτώσεις στον σχετικό τομέα·

δ) κοινοποίηση των πορισμάτων δέουσας επιμέλειας στις αρμόδιες αρχές των κρατών μελών για τη διευκόλυνση της ροής πληροφοριών όσον αφορά ορισμένα είδη, τελικούς χρήστες και προορισμούς.

Απαιτήσεις του άρθρου 5 παράγραφος 2 του κανονισμού (ΕΕ) 2021/821



4. **ΠΡΟΣΑΡΤΗΜΑ**

Απαριθμούμενα είδη κυβερνοεπιτήρησης που υπόκεινται σε έλεγχο σύμφωνα με το παράρτημα Ι του κανονισμού (ΕΕ) 2021/821

— **Συστήματα υποκλοπής τηλεπικοινωνιών (5A001.στ.)**

Στις περισσότερες χώρες, συμπεριλαμβανομένων των κρατών μελών, το απόρρητο των επικοινωνιών προστατεύεται από τον νόμο, αλλά η συγκεκαλυμμένη ηλεκτρονική επιτήρηση της επικοινωνίας από τις κυβερνητικές αρχές μπορεί να επιτραπεί εντός νομικού πλαισίου (η λεγόμενη νόμιμη υποκλοπή). Ωστόσο, η ψηφιακή εποχή κατέστησε δυνατή τη χρήση τεχνολογιών υποκλοπής σε μαζική κλίμακα. Η χρήση εργαλείων υποκλοπής από το λιβυκό καθεστώς ανέδειξε τις δυνατότητες χρήσης αυτών των τεχνολογιών σε μαζική κλίμακα και προώθησε την καθιέρωση ελέγχων των εξαγωγών στα συστήματα υποκλοπής τηλεπικοινωνιών το 2012.

Ο έλεγχος εφαρμόζεται στον εξοπλισμό που έχει σχεδιαστεί για την εξαγωγή του περιεχομένου μιας επικοινωνίας (φωνής ή δεδομένων), καθώς και σε αναγνωριστικά συνδρομητή ή άλλα μεταδεδομένα που μεταδίδονται μέσω ασύρματης επικοινωνίας, και σε εξοπλισμό παρακολούθησης ραδιοσυχνοτήτων. Ο έλεγχος αυτός εφαρμόζεται, για παράδειγμα, σε συσκευές υποκλοπής IMSI (International Mobile Subscriber Identity — διεθνής ταυτότητα κινητού συνδρομητή) που υποκλέπτουν την επικοινωνία κινητών τηλεφώνων και παρακολουθούν την κίνηση των χρηστών κινητών τηλεφώνων, ή σε εξοπλισμό που δημιουργεί ψευδή σημεία πρόσβασης Wi-Fi που μπορούν να εξάγουν αριθμούς IMSI από τηλέφωνο, καθώς και σε ορισμένους τύπους ειδών ειδικά σχεδιασμένων για να επιτρέπουν την «εις βάθος επιθεώρηση πακέτων» (deep packet inspection) σε τηλεπικοινωνιακά συστήματα. Ο εξοπλισμός ηλεκτρονικών παρεμβολών κινητών τηλεπικοινωνιών δεν εμπίπτει στο πεδίο εφαρμογής των ειδών κυβερνοεπιτήρησης, καθώς δεν συλλέγει δεδομένα.

Παρότι η τεχνολογία γενικής χρήσης μπορεί να χρησιμοποιηθεί για την κατασκευή τέτοιων συστημάτων, οι δυνατότητές τους υποκλοπής σε μαζική κλίμακα θα βασίζονται σε συγκεκριμένα εξαρτήματα και δομικά στοιχεία, όπως, για παράδειγμα, ειδικά λογισμικά, προηγμένα ή ενσωματωμένα κυκλώματα ειδικά για την εκάστοτε εφαρμογή (π.χ. FPGA, ASIC κ.λπ.) για την αύξηση του αριθμού των πακέτων ή των συνεδριών επικοινωνίας που μπορούν να υποβληθούν σε επεξεργασία ανά δευτερόλεπτο.

— **Συστήματα επιτήρησης του διαδικτύου (5A001.ι.)**

Παρά το γεγονός ότι πολλές διαδικτυακές επικοινωνίες είναι πλέον κατά κανόνα κρυπτογραφημένες εξ ορισμού, η υποκλοπή δεδομένων κίνησης (μεταδεδομένων) σχετικά με επικοινωνίες —όπως διευθύνσεις IP και συχνότητα και μεγέθη ανταλλαγής δεδομένων— μπορεί πάραυτα να χρησιμοποιηθεί για τον εντοπισμό συνδέσμων μεταξύ προσώπων και ονομάτων τομέα. Οι κυβερνήσεις μπορούν να χρησιμοποιούν τα συστήματα αυτά νόμιμα και με δικαστική εποπτεία, για νόμιμους σκοπούς, όπως η ταυτοποίηση προσώπων που επισκέπτονται τομείς που συνδέονται με εγκληματικό ή τρομοκρατικό περιεχόμενο. Ωστόσο, η παρακολούθηση και η ανάλυση της διαδικτυακής κίνησης βάσει εθνοτικού, θρησκευτικού, πολιτικού ή κοινωνικού χαρακτηρισμού μπορεί να οδηγήσει σε ολοκληρωμένη ανθρώπινη και κοινωνική χαρτογράφηση μιας χώρας για τον έλεγχο του πληθυσμού και την καταστολή, καθώς και για άλλους σκοπούς, για παράδειγμα για τον εντοπισμό πολιτικών αντιφρονούντων. Εκτός από τα ζητήματα που αφορούν τα ανθρώπινα δικαιώματα και την εσωτερική καταστολή, τα είδη αυτά μπορούν επίσης να συμβάλουν στην ενίσχυση των ικανοτήτων ασφάλειας και των στρατιωτικών ικανοτήτων.

Ο έλεγχος βάσει του σημείου 5A001.ι εφαρμόζεται σε συστήματα ελέγχου του διαδικτύου που λειτουργούν σε «δίκτυο κατηγορίας φορέων IP [δίκτυο IP κατηγορίας παρόχου] (για παράδειγμα, δίκτυο κορμού IP εθνικού επιπέδου)» για τη διενέργεια ανάλυσης, εξαγωγής και ευρετηρίασης μεταδιδόμενου περιεχομένου μεταδεδομένων (φωνή, βίντεο, μηνύματα, συνημμένα) με βάση «βασικούς επιλογείς» και τη χαρτογράφηση του σχεσιακού δικτύου των ατόμων. Πρόκειται για είδη που πραγματοποιούν «συγκεκαλυμμένη επιτήρηση» επειδή τα στοχευόμενα πρόσωπα αγνοούν την υποκλοπή των επικοινωνιών. Αντίθετα, οι έλεγχοι δεν στοχεύουν σε συστήματα στα οποία υπάρχει ενέργεια ή αλληλεπίδραση με χρήστη ή συνδρομητή και, για παράδειγμα, δεν εφαρμόζονται σε κοινωνικά δίκτυα ή εμπορικές μηχανές αναζήτησης. Επιπλέον, οι έλεγχοι εφαρμόζονται σε συστήματα που επεξεργάζονται δεδομένα τα οποία προέρχονται από κεντρικό δίκτυο παρόχου διαδικτύου, και δεν εφαρμόζονται σε κοινωνικά δίκτυα ή εμπορικές μηχανές αναζήτησης που επεξεργάζονται δεδομένα τα οποία παρέχονται από χρήστες.

— **«Λογισμικό εισβολής» (4A005, 4D004 και συναφείς έλεγχοι βάσει των σημείων 4E001.α. και 4E001.γ.)**

Το λογισμικό εισβολής επιτρέπει στον χειριστή του να αποκτήσει συγκεκαλυμμένη εξ αποστάσεως πρόσβαση σε ηλεκτρονική συσκευή, όπως έξυπνο τηλέφωνο, φορητό υπολογιστή, εξυπηρετητή ή συσκευή διαδικτύου των πραγμάτων, να αποκτήσει δεδομένα αποθηκευμένα στη συσκευή, να προβεί σε λαθρακρόαση μέσω ενσωματωμένης στη συσκευή ή συνδεδεμένης με τη συσκευή κάμερας ή μικροφώνου, και να χρησιμοποιήσει τη συσκευή ως εφαλτήριο για την πραγματοποίηση επιθέσεων σε εξοπλισμό με τον οποίο συνδέεται η συσκευή ή κατά των επαφών του χρήστη («δικτυοπαραβίαση μέσω συσκευών τρίτων»). Ενώ υπάρχουν νόμιμες χρήσεις ([8]) λογισμικού εισβολής, για παράδειγμα το «λογισμικό εξ αποστάσεως πρόσβασης» που χρησιμοποιείται για την εξ αποστάσεως υποστήριξη από τμήματα ΤΠ, ο συγκεκαλυμμένος χαρακτήρας της επιτήρησης και το μέγεθος των πληροφοριών που ενδέχεται να συλλεχθούν, ενέχει υψηλό κίνδυνο παραβίασης του δικαιώματος στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα, και μπορεί να υπονομεύσει σοβαρά το δικαίωμα στην ελευθερία της έκφρασης.

([8]) Για λόγους σαφήνειας, τα απαριθμούμενα είδη κυβερνοεπιτήρησης, όπως ελέγχονται από το παράρτημα Ι του κανονισμού για τα είδη διπλής χρήσης, θα πρέπει να διαθέτουν άδεια για να εξάγονται σε τρίτες χώρες, ανεξάρτητα από το αν η χρήση του είδους είναι νόμιμη.

Ο έλεγχος βάσει του σημείου 4A005 κ.ά. περιλαμβάνει λογισμικά, καθώς και συστήματα, εξοπλισμό, δομικά στοιχεία και συναφή τεχνολογία, που έχουν ειδικά σχεδιαστεί ή μετασκευαστεί για την παραγωγή, τον χειρισμό και τον έλεγχο ή την απόδοση «λογισμικού εισβολής», αλλά δεν εφαρμόζεται στο ίδιο το «λογισμικό εισβολής», όπως ορίζεται στο παράρτημα Ι του κανονισμού. Τα εν λόγω κυβερνοεργαλεία ελέγχονται υπό το πρίσμα των πιθανών διαταραχών και ζημιών που μπορούν να προκαλέσουν εάν χρησιμοποιηθούν και εκτελεστούν επιτυχώς, αλλά οι έλεγχοι δεν προορίζονται να επηρεάσουν τη δραστηριότητα των ερευνητών και της βιομηχανίας στον τομέα της κυβερνοασφάλειας για παράδειγμα, καθώς αυτοί χρειάζεται να ανταλλάσσουν πληροφορίες σχετικά με τα λογισμικά εισβολής προκειμένου να είναι σε θέση να αναπτύξουν διορθώσεις σφαλμάτων για τα προϊόντα τους και να τις έχουν εγκαταστήσει πριν από τη δημοσιοποίηση ενός τρωτού σημείου.

— **Λογισμικό παρακολούθησης επικοινωνιών (5D001.ε.)**

Το λογισμικό αυτό έχει σχεδιαστεί για την παρακολούθηση και την ανάλυση από εξουσιοδοτημένες αρχές επιβολής του νόμου δεδομένων που συλλέγονται μέσω στοχευμένων μέτρων υποκλοπής, τα οποία ζητούνται από πάροχο υπηρεσιών επικοινωνιών. Το λογισμικό αυτό επιτρέπει αναζητήσεις με βάση «βασικούς επιλογείς» περιεχομένου επικοινωνίας ή μεταδεδομένων, με τη χρήση διεπαφής για νόμιμη υποκλοπή, και τη χαρτογράφηση του σχεσιακού δικτύου ή την παρακολούθηση της κίνησης στοχευόμενων ατόμων με βάση τα αποτελέσματα των αναζητήσεων. Το λογισμικό προορίζεται για «συγκεκαλυμμένη επιτήρηση» διότι χρησιμοποιεί δεδομένα που συλλέγονται από την υποκλοπή επικοινωνιών χωρίς τα άτομα να έχουν γνώση της υποκλοπής. Επιπλέον, «αναλύει» δεδομένα που συλλέγονται μέσω «συστημάτων τηλεπικοινωνιών». Το λογισμικό είναι εγκατεστημένο στην κρατική αρχή [για παράδειγμα, εγκατάσταση της αρχής επιβολής του νόμου που χρησιμοποιείται για παρακολούθηση (LEMF)] και ο έλεγχος δεν εφαρμόζεται στα συστήματα ελέγχου της συμμόρφωσης νόμιμης υποκλοπής (για παράδειγμα, συστήματα διαχείρισης νόμιμης υποκλοπής και συσκευές διαμεσολάβησης) που αναπτύσσονται εμπορικά και εγκαθίστανται στον χώρο του παρόχου υπηρεσιών επικοινωνιών (π.χ. ενσωματώνονται στο δίκτυο επικοινωνιών) και τα οποία ο πάροχος υπηρεσιών λειτουργεί και συντηρεί. Όπως διευκρινίζεται στην περιγραφή, οι έλεγχοι δεν εφαρμόζονται στο «λογισμικό» που έχει ειδικά σχεδιαστεί ή τροποποιηθεί για καθαρά εμπορικούς σκοπούς, όπως η τιμολόγηση, η ποιότητα των υπηρεσιών δικτύου (QoS), η ποιότητα της εμπειρίας (QoE), οι συσκευές διαμεσολάβησης ή οι πληρωμές ή τραπεζικές συναλλαγές μέσω κινητής συσκευής.

— **Είδη που χρησιμοποιούνται για τη διενέργεια κρυπτανάλυσης (5A004.α.)**

Ο έλεγχος εφαρμόζεται σε είδη που έχουν σχεδιαστεί για την καταστολή κρυπτογραφικών μηχανισμών προκειμένου να εξαχθούν εμπιστευτικές μεταβλητές ή ευαίσθητα δεδομένα, συμπεριλαμβανομένων ακρυπτογράφητου κειμένου, κωδικών πρόσβασης ή κρυπτογραφικών κλειδιών. Η κρυπτογραφία χρησιμοποιείται για τη διασφάλιση της εμπιστευτικότητας των πληροφοριών υπό διαβίβαση και σε κατάσταση αποθήκευσης. Η κρυπτανάλυση χρησιμοποιείται για την άρση αυτής της εμπιστευτικότητας και, ως εκ τούτου, η τεχνολογία αυτή «καθιστά δυνατή» τη συγκεκαλυμμένη επιτήρηση μέσω της παρακολούθησης, της εξαγωγής, της συλλογής ή της ανάλυσης δεδομένων από συστήματα πληροφοριών και τηλεπικοινωνιών.

— **Εγκληματολογικά/ερευνητικά εργαλεία (5A004.β., 5D002.α.3.β. και 5D002.γ.3.β.)**

Τα εγκληματολογικά/ερευνητικά εργαλεία είναι σχεδιασμένα για την εξαγωγή ανεπεξέργαστων δεδομένων από μια συσκευή (για παράδειγμα, συσκευή επεξεργασίας δεδομένων ή επικοινωνίας), ώστε τα δεδομένα να μην παραποιούνται ή να αλλοιώνονται και να μπορούν να χρησιμοποιηθούν για δικαστικούς σκοπούς, δηλαδή σε ποινική έρευνα ή δικαστήριο. Τα προϊόντα αυτά παρακάμπτουν τους ελέγχους «επαλήθευσης ταυτότητας» ή έγκρισης μιας συσκευής, ώστε τα ανεπεξέργαστα δεδομένα να μπορούν να εξαχθούν από τη συσκευή. Τα προϊόντα αυτά χρησιμοποιούνται από την κυβέρνηση και τις υπηρεσίες επιβολής του νόμου, αλλά και από στρατιωτικές δυνάμεις για την εξαγωγή και ανάλυση δεδομένων από κατασχεθείσες συσκευές. Παρότι έχουν νόμιμες χρήσεις, μπορούν ωστόσο να χρησιμοποιηθούν καταχρηστικά και, ως εκ τούτου, να ενέχουν κίνδυνο για ευαίσθητα ή εμπορικά δεδομένα.

Ωστόσο, τα εγκληματολογικά/ερευνητικά εργαλεία που δεν είναι «ειδικά σχεδιασμένα» για συγκεκαλυμμένη επιτήρηση δεν εμπίπτουν στον ορισμό των ειδών κυβερνοεπιτήρησης του άρθρου 2 σημείο 20. Επίσης, τα εγκληματολογικά/ερευνητικά εργαλεία που εξάγουν μόνο δεδομένα χρήστη ή όταν τα δεδομένα δεν προστατεύονται στη συσκευή δεν καλύπτονται από την περιγραφή στο σημείο 5A004.β. κ.ά. Ταυτόχρονα, οι έλεγχοι δεν ισχύουν για τον εξοπλισμό παραγωγής ή δοκιμής του κατασκευαστή, τα εργαλεία διαχειριστή συστήματος ή τα προϊόντα αποκλειστικά για τον εμπορικό τομέα λιανικής, για παράδειγμα τα προϊόντα ξεκλειδώματος κινητών τηλεφώνων. Ως εκ τούτου, λαμβανομένης υπόψη της ποικιλίας αυτών των τύπων τεχνολογίας, η εφαρμογή των ελέγχων εξαρτάται από την κατά περίπτωση αξιολόγηση κάθε προϊόντος.

Τέλος, επισημαίνεται ότι στο παράρτημα Ι του κανονισμού απαριθμούνται και άλλα είδη που σχετίζονται με την επιτήρηση και τα οποία δεν θα πρέπει να θεωρούνται ότι εμπίπτουν στον ορισμό των ειδών κυβερνοεπιτήρησης, όπως ο εξοπλισμός ηλεκτρονικών παρεμβολών κινητών τηλεπικοινωνιών (5A001.στ.) που έχει σχεδιαστεί για να βλάπτει ή να διαταράσσει τις επικοινωνίες ή τα συστήματα, το λογισμικό εισβολής που τροποποιεί ένα σύστημα (4D004) και ο ηχητικός εξοπλισμός ανίχνευσης λέιζερ (6A005.ζ.) που συλλέγει ακουστικά δεδομένα με λέιζερ ή καθιστά δυνατή την ακρόαση συνομιλιών σε απόσταση (που ενίοτε ονομάζεται «μικρόφωνο λέιζερ»). Ομοίως, η χρήση απαριθμούμενων μη επανδρωμένων εναέριων οχημάτων για σκοπούς επιτήρησης δεν θα ενέθετε τα εν λόγω είδη στον ορισμό των ειδών κυβερνοεπιτήρησης.