Translations proofread by EDPB Members.

This language version has not yet been proofread.

Κατευθυντήριες γραμμές 05/2022 σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου

Έκδοση 2.0

Εγκρίθηκε στις 26 Απριλίου 2023

Ιστορικό έκδοσης

Έκδοση 1.0	12 Μαΐου 2022	Έγκριση κατευθυντήριων γραμμών για δημόσια διαβούλευση
Έκδοση 2.0	26 Απριλίου 2023	Έγκριση κατευθυντήριων γραμμών μετά από δημόσια διαβούλευση

Πίνακας περιεχομένων

Περίληψη 5

1 Εισαγωγή 9

2 Τεχνολογία 10

2.1 Μία βιομετρική τεχνολογία, δύο διαφορετικές λειτουργίες 10

2.2 Μεγάλη ποικιλία σκοπών και εφαρμογών 13

2.3 Αξιοπιστία, ακρίβεια και κίνδυνοι για τα υποκείμενα των δεδομένων 15

3 Ισχύον νομικό πλαίσιο 16

3.1 Γενικό νομικό πλαίσιο — Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ και η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) 17

3.1.1 Εφαρμογή του Χάρτη 17

3.1.2 Παρέμβαση στα δικαιώματα που ορίζονται στον Χάρτη 18

3.1.3 Αιτιολόγηση της παρέμβασης 19

3.2 Ειδικό νομικό πλαίσιο — η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου 23

3.2.1 Επεξεργασία ειδικών κατηγοριών δεδομένων για σκοπούς επιβολής του νόμου 24

3.2.2 Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ 27

3.2.3 Κατηγορίες των υποκειμένων των δεδομένων 28

3.2.4 Δικαιώματά του υποκειμένου των δεδομένων 29

3.2.5 Άλλες νομικές απαιτήσεις και διασφαλίσεις 33

4 Συμπέρασμα 37

5 Παραρτήματα 38

Παράρτημα I — Υπόδειγμα για την περιγραφή σεναρίων 39

Παράρτημα II— Πρακτική καθοδήγηση για τη διαχείριση έργων με τεχνολογία αναγνώρισης προσώπου στις αρχές επιβολής του νόμου 41

1. ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ 41

2. ΈΝΑΡΞΗ/ΠΡΙΝ ΑΠΟ ΤΗΝ ΠΡΟΜΗΘΕΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ 43

3. ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ ΤΗΣ ΠΡΟΜΗΘΕΙΑΣ ΚΑΙ ΠΡΙΝ ΑΠΟ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ 46

4. ΣΥΣΤΑΣΕΙΣ ΜΕΤΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ 48

Παράρτημα III — ΠΡΑΚΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ 49

1 Σενάριο 1 49

1.1. Περιγραφή 49

1.2. Εφαρμοστέο νομικό πλαίσιο 50

1.3. Αναγκαιότητα και αναλογικότητα — σκοπός/σοβαρότητα του εγκλήματος 51
1.4. Συμπέρασμα 51
2 Σενάριο 2 51
2.1. Περιγραφή 51
2.2. Ισχύον νομικό πλαίσιο 53
2.3. Αναγκαιότητα και αναλογικότητα — σκοπός/σοβαρότητα του εγκλήματος/αριθμός των προσώπων που δεν εμπλέκονται αλλά επηρεάζονται από την επεξεργασία 53
2.4. Συμπέρασμα 54
3 Σενάριο 3: 54
3.1. Περιγραφή 54
3.2. Ισχύον νομικό πλαίσιο 55
3.3. Αναγκαιότητα και αναλογικότητα 56
3.4. Συμπέρασμα 57
4 Σενάριο 4 57
4.1. Περιγραφή 57
4.2. Ισχύον νομικό πλαίσιο 58
4.3. Αναγκαιότητα και αναλογικότητα 58
4.4. Συμπέρασμα 58
5 Σενάριο 5 59
5.1. Περιγραφή 59
5.2. Ισχύον νομικό πλαίσιο 60
5.3. Αναγκαιότητα και αναλογικότητα 60
5.4. Συμπέρασμα 63
6 Σενάριο 6 63
6.1. Περιγραφή 63
6.2. Ισχύον νομικό πλαίσιο 64
6.3. Αναγκαιότητα και αναλογικότητα 65
6.4. Συμπέρασμα 65

ΠΕΡΙΛΗΨΗ

Όλο και περισσότερες αρχές επιβολής του νόμου εφαρμόζουν ή προτίθενται να εφαρμόσουν τεχνολογία αναγνώρισης προσώπου. Μπορεί να χρησιμοποιηθεί για τον **έλεγχο της ταυτότητας** ή για την **ταυτοποίηση** ενός ατόμου και μπορεί να εφαρμοστεί σε βίντεο (π.χ. CCTV) ή φωτογραφίες. Μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, συμπεριλαμβανομένης της αναζήτησης ατόμων που περιλαμβάνονται σε καταλόγους υπόπτων της αστυνομίας ή για την παρακολούθηση των κινήσεων ενός ατόμου στον δημόσιο χώρο.

Η τεχνολογία αναγνώρισης προσώπου βασίζεται στην επεξεργασία **βιομετρικών δεδομένων**, επομένως, περιλαμβάνει την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Συχνά, η τεχνολογία αναγνώρισης προσώπου χρησιμοποιεί συνιστώσες **τεχνητής νοημοσύνης** (ΤΝ) ή μηχανικής μάθησης (ΜΜ). Αν και αυτό επιτρέπει την επεξεργασία δεδομένων μεγάλης κλίμακας, δημιουργεί επίσης τον κίνδυνο διακρίσεων και ψευδών αποτελεσμάτων. Η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί σε ελεγχόμενες καταστάσεις 1:1, αλλά και σε μεγάλα πλήθη και σημαντικούς κόμβους μεταφορών.

Η τεχνολογία αναγνώρισης προσώπου είναι ένα **ευαίσθητο εργαλείο για τις αρχές επιβολής του νόμου.** Οι αρχές επιβολής του νόμου είναι εκτελεστικές αρχές και έχουν κυριαρχικές εξουσίες. Η τεχνολογία αναγνώρισης προσώπου τείνει να παρεμβαίνει στα θεμελιώδη δικαιώματα —και πέραν του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα— και μπορεί να επηρεάσει την κοινωνική και δημοκρατική πολιτική μας σταθερότητα.

Για την προστασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επιβολής του νόμου, πρέπει να πληρούνται οι **απαιτήσεις της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου**. Στην οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου προβλέπεται συγκεκριμένο πλαίσιο σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου, ιδίως το άρθρο 3 παράγραφος 13 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (όρος «βιομετρικά δεδομένα»), το άρθρο 4 (αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα), το άρθρο 8 (νομιμότητα της επεξεργασίας), το άρθρο 10 (επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα) και το άρθρο 11 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (αυτοματοποιημένη ατομική λήψη αποφάσεων).

Διάφορα άλλα θεμελιώδη δικαιώματα ενδέχεται επίσης να επηρεαστούν από την εφαρμογή της τεχνολογίας αναγνώρισης προσώπου. Ως εκ τούτου, ο **Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ** (στο εξής «ο Χάρτης») είναι απαραίτητος για την ερμηνεία της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, ιδίως του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα του άρθρου 8 του Χάρτη, αλλά και του δικαιώματος στην ιδιωτική ζωή που κατοχυρώνεται στο άρθρο 7 του Χάρτη.

Τα **νομοθετικά μέτρα** που χρησιμεύουν ως νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα παρεμβαίνουν άμεσα στα δικαιώματα που κατοχυρώνονται από τα άρθρα 7 και 8 του Χάρτη. Η επεξεργασία βιομετρικών δεδομένων υπό οποιεσδήποτε περιστάσεις συνιστά αφ' εαυτής σοβαρή παρέμβαση. Αυτό δεν εξαρτάται από το αποτέλεσμα, π.χ. μια θετική αντιστοίχιση. Κάθε περιορισμός στην άσκηση των θεμελιωδών δικαιωμάτων και ελευθεριών πρέπει να προβλέπεται από τον νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών.

Η νομική βάση πρέπει να είναι **επαρκώς σαφής** ως προς τους όρους της ώστε να παρέχει στους πολίτες επαρκή ένδειξη των προϋποθέσεων και των περιστάσεων υπό τις οποίες οι αρχές

εξουσιοδοτούνται να προσφεύγουν σε οποιαδήποτε μέτρα συλλογής δεδομένων και μυστικής παρακολούθησης. Η απλή μεταφορά στο εθνικό δίκαιο της γενικής ρήτρας του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου θα στερούνταν ακρίβειας και προβλεψιμότητας.

Προτού ο εθνικός νομοθέτης δημιουργήσει νέα νομική βάση για οποιαδήποτε μορφή επεξεργασίας βιομετρικών δεδομένων με τη χρήση αναγνώρισης προσώπου, θα πρέπει να **συμβουλευτεί** την αρμόδια εποπτική αρχή προστασίας δεδομένων.

Τα νομοθετικά μέτρα πρέπει να είναι **κατάλληλα** για την επίτευξη των θεμιτών στόχων που επιδιώκονται από την επίμαχη νομοθεσία. Ένας **στόχος γενικού συμφέροντος** —όσο θεμελιώδης και αν είναι— δεν δικαιολογεί από μόνος του τον περιορισμό ενός θεμελιώδους δικαιώματος. Τα νομοθετικά μέτρα θα πρέπει να **διαφοροποιούν** και να στοχεύουν τα άτομα που καλύπτονται από αυτά υπό το πρίσμα του στόχου, π.χ. την καταπολέμηση συγκεκριμένων σοβαρών εγκλημάτων. Εάν το μέτρο καλύπτει όλα τα άτομα κατά γενικό τρόπο χωρίς τέτοια διαφοροποίηση, περιορισμό ή εξαίρεση, εντείνει την παρέμβαση. Εντείνει επίσης την παρέμβαση εάν η επεξεργασία δεδομένων καλύπτει σημαντικό μέρος του πληθυσμού.

Η επεξεργασία των δεδομένων πρέπει να γίνεται με τρόπο που να διασφαλίζει την εφαρμογή και την αποτελεσματικότητα των κανόνων και αρχών της ΕΕ για την προστασία των δεδομένων. Με βάση κάθε κατάσταση, η **αξιολόγηση της αναγκαιότητας και της αναλογικότητας** πρέπει επίσης να προσδιορίζει και να εξετάζει όλες τις πιθανές επιπτώσεις σε άλλα θεμελιώδη δικαιώματα. Εάν τα δεδομένα υποβάλλονται σε συστηματική επεξεργασία χωρίς τη γνώση των υποκειμένων των δεδομένων, είναι πιθανό να δημιουργηθεί ένα **γενικό αίσθημα συνεχούς παρακολούθησης**. Αυτό μπορεί να οδηγήσει σε αποτρεπτικά αποτελέσματα όσον αφορά ορισμένα ή όλα τα σχετικά θεμελιώδη δικαιώματα, όπως η ανθρώπινη αξιοπρέπεια σύμφωνα με το άρθρο 1 του Χάρτη, η ελευθερία της σκέψης, της συνείδησης και της θρησκείας σύμφωνα με το άρθρο 10 του Χάρτη, η ελευθερία της έκφρασης σύμφωνα με το άρθρο 11 του Χάρτη, καθώς και η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι σύμφωνα με το άρθρο 12 του Χάρτη.

Η επεξεργασία ειδικών κατηγοριών δεδομένων, όπως τα βιομετρικά δεδομένα, μπορεί να θεωρηθεί «**απολύτως αναγκαία**» (άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου) μόνον εάν η παρέμβαση στην προστασία των δεδομένων προσωπικού χαρακτήρα και οι περιορισμοί της περιορίζονται σε ό, τι είναι απολύτως αναγκαίο, δηλαδή απαραίτητο, και αποκλείεται κάθε επεξεργασία γενικού ή συστηματικού χαρακτήρα.

Το γεγονός ότι μια φωτογραφία έχει **προδήλως δημοσιοποιηθεί** (άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου) από το υποκείμενο των δεδομένων δεν συνεπάγεται ότι τα σχετικά βιομετρικά δεδομένα, τα οποία μπορούν να ανακτηθούν από τη φωτογραφία με ειδικά τεχνικά μέσα, θεωρείται ότι έχουν προδήλως δημοσιοποιηθεί. Οι προεπιλεγμένες ρυθμίσεις μιας υπηρεσίας, π.χ. η δημοσιοποίηση υποδειγμάτων, ή η απουσία επιλογής, π.χ. υποδείγματα δημοσιοποιούνται χωρίς ο χρήστης να είναι σε θέση να τροποποιήσει την εν λόγω ρύθμιση, σε καμία περίπτωση δεν θα πρέπει να εκλαμβάνονται ως δεδομένα που έχουν προδήλως δημοσιοποιηθεί.

Το άρθρο 11 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου θεσπίζει ένα πλαίσιο για **την αυτοματοποιημένη ατομική λήψη αποφάσεων**. Η χρήση της τεχνολογίας αναγνώρισης προσώπου συνεπάγεται τη χρήση ειδικών κατηγοριών δεδομένων και μπορεί να οδηγήσει σε κατάρτιση προφίλ, ανάλογα με τον τρόπο και τον σκοπό για τον οποίο εφαρμόζεται η τεχνολογία αναγνώρισης προσώπου. Σε κάθε περίπτωση, σύμφωνα με το δίκαιο της Ένωσης και το άρθρο 11 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο

της επιβολής του νόμου, η κατάρτιση προφίλ που έχει ως αποτέλεσμα διακρίσεις εις βάρος φυσικών προσώπων με βάση τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα απαγορεύεται.

Το άρθρο 6 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αφορά την αναγκαιότητα **διάκρισης μεταξύ διαφορετικών κατηγοριών υποκειμένων των δεδομένων**. Όσον αφορά τα υποκείμενα των δεδομένων για τα οποία δεν υπάρχουν αποδεικτικά στοιχεία που να υποδεικνύουν ότι η συμπεριφορά τους μπορεί να συνδέεται, ακόμη και έμμεσα ή εξ αποστάσεως, με τον θεμιτό σκοπό σύμφωνα με την οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, κατά πάσα πιθανότητα η παρέμβαση δεν είναι δικαιολογημένη.

Η **αρχή της ελαχιστοποίησης των δεδομένων** (άρθρο 4 παράγραφος 1 στοιχείο ε) της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου) απαιτεί επίσης ότι κάθε υλικό βίντεο που δεν είναι σχετικό με τον σκοπό της επεξεργασίας θα πρέπει πάντα να αφαιρείται ή να ανωνυμοποιείται (π.χ. με θόλωση χωρίς αναδρομική δυνατότητα ανάκτησης των δεδομένων) πριν από την ανάπτυξη.

Ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει προσεκτικά πώς (ή εάν μπορεί) να εκπληρώσει τις απαιτήσεις για τα **δικαιώματα του υποκειμένου των δεδομένων** πριν από την έναρξη οποιασδήποτε επεξεργασίας με τεχνολογία αναγνώρισης προσώπου, δεδομένου ότι η τεχνολογία αναγνώρισης προσώπου συχνά περιλαμβάνει την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα χωρίς καμία προφανή αλληλεπίδραση με το υποκείμενο των δεδομένων.

Η αποτελεσματική άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων εξαρτάται από την εκπλήρωση των **υποχρεώσεων ενημέρωσης** του υπευθύνου επεξεργασίας (άρθρο 13 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου). Κατά την αξιολόγηση του εάν υφίσταται «συγκεκριμένη περίπτωση» σύμφωνα με το άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, πρέπει να λαμβάνονται υπόψη διάφοροι παράγοντες, μεταξύ άλλων εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται εν αγνοία του υποκειμένου των δεδομένων, καθώς αυτός θα ήταν ο μόνος τρόπος για να μπορούν τα υποκείμενα των δεδομένων να ασκούν αποτελεσματικά τα δικαιώματά τους. Εάν η λήψη αποφάσεων πραγματοποιείται αποκλειστικά με βάση την τεχνολογία αναγνώρισης προσώπου, τότε τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τα χαρακτηριστικά της αυτοματοποιημένης λήψης αποφάσεων.

Όσον αφορά τα **αιτήματα πρόσβασης**, όταν τα βιομετρικά δεδομένα αποθηκεύονται και συνδέονται με μια ταυτότητα και μέσω αλφαριθμητικών δεδομένων, σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, αυτό θα πρέπει να επιτρέπει στην αρμόδια αρχή να επιβεβαιώνει ένα αίτημα πρόσβασης βάσει αναζήτησης από τα εν λόγω αλφαριθμητικά δεδομένα και χωρίς να προβαίνει σε περαιτέρω επεξεργασία βιομετρικών δεδομένων τρίτων (π.χ. με αναζήτηση με τεχνολογία αναγνώρισης προσώπου σε βάση δεδομένων).

Οι κίνδυνοι για τα υποκείμενα των δεδομένων είναι ιδιαίτερα σοβαροί εάν ανακριβή δεδομένα αποθηκευτούν σε βάση δεδομένων της αστυνομίας ή/και κοινοποιηθούν σε άλλες οντότητες. Ο υπεύθυνος επεξεργασίας πρέπει να **διορθώσει** τα αποθηκευμένα δεδομένα και τα συστήματα τεχνολογίας αναγνώρισης προσώπου αναλόγως (βλ. επίσης αιτιολογική σκέψη 47 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου).

Το δικαίωμα **περιορισμού** καθίσταται ιδιαίτερα σημαντικό όταν πρόκειται για τεχνολογία αναγνώρισης προσώπου (βάσει αλγορίθμου(-ων) και συνεπώς δεν παρουσιάζει ποτέ οριστικό αποτέλεσμα) σε περιπτώσεις όπου συλλέγονται μεγάλες ποσότητες δεδομένων και η ακρίβεια και η ποιότητα της ταυτοποίησης μπορεί να ποικίλλει.

Η **εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)** πριν από τη χρήση της τεχνολογίας αναγνώρισης προσώπου αποτελεί υποχρεωτική απαίτηση, πρβλ. άρθρο 27 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Το ΕΣΠΔ συνιστά τη δημοσιοποίηση των αποτελεσμάτων των εν λόγω εκτιμήσεων ή τουλάχιστον των βασικών διαπιστώσεων και συμπερασμάτων της ΕΑΠΔ, ως μέτρο ενίσχυσης της εμπιστοσύνης και της διαφάνειας.

Οι περισσότερες περιπτώσεις εγκατάστασης και χρήσης τεχνολογίας αναγνώρισης προσώπου ενέχουν εγγενή υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Ως εκ τούτου, η αρχή που εγκαθιστά τεχνολογία αναγνώρισης προσώπου θα πρέπει να **συμβουλευτεί** την αρμόδια εποπτική αρχή πριν από την εγκατάσταση του συστήματος.

Δεδομένης της μοναδικής φύσης των βιομετρικών δεδομένων, η αρχή που εφαρμόζει ή/και χρησιμοποιεί τεχνολογία αναγνώρισης προσώπου θα πρέπει να δώσει ιδιαίτερη προσοχή στην **ασφάλεια της επεξεργασίας**, σύμφωνα με το άρθρο 29 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο επιβολής του νόμου. Ειδικότερα, η αρχή επιβολής του νόμου θα πρέπει να διασφαλίζει ότι το σύστημα συμμορφώνεται με τα σχετικά πρότυπα και εφαρμόζει μέτρα προστασίας βιομετρικών υποδειγμάτων. Οι αρχές και οι εγγυήσεις προστασίας των δεδομένων πρέπει να ενσωματώνονται στην τεχνολογία πριν από την έναρξη της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ως εκ τούτου, ακόμη και όταν μια αρχή επιβολής του νόμου προτίθεται να εφαρμόσει και να χρησιμοποιήσει τεχνολογία αναγνώρισης προσώπου από εξωτερικούς παρόχους, πρέπει να διασφαλίζει, π.χ. μέσω της διαδικασίας σύναψης συμβάσεων, ότι χρησιμοποιούνται μόνο τεχνολογίες αναγνώρισης προσώπου που βασίζονται στις αρχές της **προστασίας των δεδομένων από τον σχεδιασμό και εξ ορισμού**.

Οι καταχωρίσεις (πρβλ. άρθρο 25 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου) αποτελούν σημαντική διασφάλιση για την επαλήθευση της νομιμότητας της επεξεργασίας, τόσο σε εσωτερικό επίπεδο (δηλ. αυτοπαρακολούθηση από τον οικείο υπεύθυνο επεξεργασίας/εκτελούντα την επεξεργασία) όσο και από εξωτερικές εποπτικές αρχές. Στο πλαίσιο των συστημάτων αναγνώρισης προσώπου, συνιστώνται επίσης οι καταχωρίσεις για αλλαγές της βάσης δεδομένων αναφοράς και για προσπάθειες ταυτοποίησης ή επαλήθευσης, συμπεριλαμβανομένης της βαθμολογίας χρήστη, αποτελέσματος και εμπιστοσύνης. Ωστόσο, οι καταχωρίσεις αποτελούν μόνο ένα ουσιώδες στοιχείο της συνολικής **αρχής της λογοδοσίας** (πρβλ. άρθρο 4 παράγραφος 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου). Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση της επεξεργασίας με τις βασικές αρχές προστασίας δεδομένων του άρθρου 4 παράγραφοι 1 έως 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

Το ΕΣΠΔ υπενθυμίζει την κοινή **έκκληση** του ΕΣΠΔ και του ΕΕΠΔ **για την απαγόρευση** ορισμένων ειδών επεξεργασίας σε σχέση με 1) την εξ αποστάσεως βιομετρική ταυτοποίηση ατόμων σε δημόσιους χώρους, 2) τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη που κατηγοριοποιούν άτομα με βάση τα βιομετρικά τους στοιχεία σε ομάδες ανάλογα με την εθνικότητα, το φύλο, καθώς και τον πολιτικό ή σεξουαλικό προσανατολισμό ή άλλους λόγους διάκρισης 3) τη χρήση αναγνώρισης προσώπου ή παρόμοιων τεχνολογιών, για την εξαγωγή συμπερασμάτων σχετικά με τα συναισθήματα ενός φυσικού προσώπου και 4) την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε πλαίσιο επιβολής του νόμου που θα βασίζεται σε μια βάση δεδομένων η οποία θα εμπλουτίζεται από τη συλλογή δεδομένων προσωπικού χαρακτήρα σε μαζική κλίμακα και κατά τρόπο αδιάκριτο, π.χ. με την «εξαγωγή» φωτογραφιών και εικόνων προσώπου που είναι προσβάσιμες στο διαδίκτυο.

Κεντρική διασφάλιση ως προς τα διακυβευόμενα θεμελιώδη δικαιώματα είναι η **αποτελεσματική εποπτεία** από τις αρμόδιες εποπτικές αρχές προστασίας δεδομένων. Ως εκ τούτου, τα κράτη μέλη πρέπει να διασφαλίζουν ότι οι πόροι των εποπτικών αρχών είναι κατάλληλοι και επαρκείς ώστε να τους επιτρέπουν να εκπληρώσουν την εντολή τους.

Οι παρούσες **κατευθυντήριες γραμμές απευθύνονται** στους νομοθέτες σε ενωσιακό και εθνικό επίπεδο, καθώς και στις αρχές επιβολής του νόμου και τους υπαλλήλους τους που εφαρμόζουν και χρησιμοποιούν τα συστήματα τεχνολογίας αναγνώρισης προσώπου. Στα φυσικά πρόσωπα απευθύνονται στον βαθμό που αυτά ενδιαφέρονται γενικά ή ως υποκείμενα των δεδομένων, ιδίως όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων.

Οι **κατευθυντήριες γραμμές αποσκοπούν** στην ενημέρωση σχετικά με ορισμένες ιδιότητες της τεχνολογίας αναγνώρισης προσώπου και το εφαρμοστέο νομικό πλαίσιο στο πλαίσιο της επιβολής του νόμου (ιδίως της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου).

- Επιπλέον, παρέχουν ένα **εργαλείο για την υποστήριξη μιας πρώτης ταξινόμησης της ευαισθησίας μιας δεδομένης περίπτωσης χρήσης** (παράρτημα I).
- Περιλαμβάνουν επίσης **πρακτικές οδηγίες για τις αρχές επιβολής του νόμου που επιθυμούν να προμηθευτούν και να λειτουργήσουν ένα σύστημα τεχνολογίας αναγνώρισης προσώπου** (παράρτημα II).
- Οι κατευθυντήριες γραμμές περιγράφουν επίσης αρκετές τυπικές **περιπτώσεις χρήσης και απαριθμούν πολυάριθμες συναφείς παραμέτρους**, ιδίως όσον αφορά τον έλεγχο αναγκαιότητας και αναλογικότητας (παράρτημα III).

1 ΕΙΣΑΓΩΓΗ

1. Η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί για την αυτόματη αναγνώριση ατόμων με βάση το πρόσωπο τους. Η τεχνολογία αναγνώρισης προσώπου συχνά βασίζεται στην τεχνητή νοημοσύνη, όπως οι τεχνολογίες μηχανικής μάθησης. Οι εφαρμογές τεχνολογίας αναγνώρισης προσώπου υποβάλλονται ολοένα και περισσότερο σε δοκιμές και χρησιμοποιούνται σε διάφορους τομείς, από την ατομική χρήση έως τους ιδιωτικούς οργανισμούς και τη χρήση από τη δημόσια διοίκηση. Οι αρχές επιβολής του νόμου αναμένουν επίσης οφέλη από τη χρήση της τεχνολογίας αναγνώρισης προσώπου. Υπόσχεται λύσεις σε σχετικά νέες προκλήσεις, όπως έρευνες που αφορούν μεγάλο όγκο συλλεχθέντων αποδεικτικών στοιχείων, αλλά και σε γνωστά προβλήματα, ιδίως όσον αφορά την έλλειψη προσωπικού για καθήκοντα παρατήρησης και αναζήτησης.

2. Μεγάλο μέρος του αυξημένου ενδιαφέροντος για την τεχνολογία αναγνώρισης προσώπου βασίζεται στην αποτελεσματικότητα και την επεκτασιμότητά της. Μαζί με αυτές έρχονται και τα μειονεκτήματα που είναι συνυφασμένα με την τεχνολογία και την εφαρμογή της —επίσης σε μεγάλη κλίμακα. Αν και μπορεί να υπάρχουν χιλιάδες σύνολα δεδομένων προσωπικού χαρακτήρα που αναλύονται με το πάτημα ενός κουμπιού, οι ήδη μικρές επιπτώσεις των αλγοριθμικών διακρίσεων ή της εσφαλμένης ταυτοποίησης μπορεί να επιφέρουν μεγάλο αριθμό ατόμων που επηρεάζονται σοβαρά στη συμπεριφορά και την καθημερινή ζωή τους. Το ίδιο το μέγεθος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και ιδίως βιομετρικών δεδομένων, αποτελεί ένα ακόμη βασικό στοιχείο της τεχνολογίας αναγνώρισης προσώπου, καθώς η επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστά παρέμβαση στο θεμελιώδες δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα

σύμφωνα με το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (στο εξής: ο Χάρτης).

3. Η εφαρμογή της τεχνολογίας αναγνώρισης προσώπου των αρχών επιβολής του νόμου θα έχει —και σε κάποιο βαθμό ήδη έχει— σημαντικές επιπτώσεις σε φυσικά πρόσωπα και ομάδες ατόμων, συμπεριλαμβανομένων των μειονοτήτων. Οι εν λόγω επιπτώσεις θα έχουν επίσης σημαντικό αντίκτυπο στον τρόπο με τον οποίο συμβιώνουμε και στην κοινωνική και δημοκρατική πολιτική μας σταθερότητα, εκτιμώντας την υψηλή σημασία του πλουραλισμού και της πολιτικής αντιπολίτευσης. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί συχνά βασική προϋπόθεση για τη διασφάλιση άλλων θεμελιωδών δικαιωμάτων. Η εφαρμογή της τεχνολογίας αναγνώρισης προσώπου τείνει ιδιαίτερα να παρεμβαίνει σε θεμελιώδη δικαιώματα πέραν του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα.

4. Ως εκ τούτου, το ΕΣΠΔ θεωρεί σημαντικό να συμβάλει στη συνεχιζόμενη ενσωμάτωση της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου που καλύπτεται από την οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου[1] αντίστοιχα με τις εθνικές νομοθεσίες που τη μεταφέρουν στο εθνικό δίκαιο και να παράσχει τις παρούσες κατευθυντήριες γραμμές. Οι κατευθυντήριες γραμμές έχουν ως στόχο να παρέχουν σχετικές πληροφορίες στους νομοθέτες σε ενωσιακό και σε εθνικό επίπεδο, καθώς και στις αρχές επιβολής του νόμου και στους υπαλλήλους τους, κατά την εφαρμογή και τη χρήση συστημάτων τεχνολογίας αναγνώρισης προσώπου. Το πεδίο εφαρμογής των κατευθυντήριων γραμμών περιορίζεται στην τεχνολογία αναγνώρισης προσώπου. Ωστόσο, άλλες μορφές επεξεργασίας δεδομένων προσωπικού χαρακτήρα βάσει βιομετρικών στοιχείων από τις αρχές επιβολής του νόμου, ιδίως εάν η επεξεργασία τους πραγματοποιείται εξ αποστάσεως, ενδέχεται να ενέχουν παρόμοιους ή πρόσθετους κινδύνους για τα φυσικά πρόσωπα, τις ομάδες και την κοινωνία. Σύμφωνα με τις αντίστοιχες περιστάσεις, ορισμένες πτυχές των εν λόγω κατευθυντήριων γραμμών ενδέχεται επίσης να αποτελέσουν χρήσιμη πηγή στις εν λόγω περιπτώσεις. Τέλος, τα φυσικά πρόσωπα που ενδιαφέρονται γενικά ή ως υποκείμενα των δεδομένων μπορούν επίσης να βρουν σημαντικές πληροφορίες, ιδίως όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων.

5. Οι κατευθυντήριες γραμμές αποτελούνται από το κύριο έγγραφο και τρία παραρτήματα. Το επικείμενο κύριο έγγραφο παρουσιάζει την τεχνολογία και το ισχύον νομικό πλαίσιο. Για να διευκολυνθεί ο προσδιορισμός ορισμένων από τις σημαντικότερες πτυχές για την ταξινόμηση της σοβαρότητας της παρέμβασης στα θεμελιώδη δικαιώματα σε ένα δεδομένο πεδίο εφαρμογής, στο παράρτημα Ι παρατίθεται υπόδειγμα. Οι αρχές επιβολής του νόμου που επιθυμούν να προμηθευτούν και να διαχειριστούν ένα σύστημα τεχνολογίας αναγνώρισης προσώπου μπορούν να βρουν πρακτική καθοδήγηση στο παράρτημα ΙΙ. Ανάλογα με το πεδίο εφαρμογής της τεχνολογίας αναγνώρισης προσώπου, θα μπορούσαν να θεωρηθούν σημαντικές διάφορες εκτιμήσεις. Στο παράρτημα ΙΙΙ περιλαμβάνεται ένα σύνολο υποθετικών σεναρίων και σχετικών εκτιμήσεων.

2 ΤΕΧΝΟΛΟΓΙΑ

2.1 Μία βιομετρική τεχνολογία, δύο διαφορετικές λειτουργίες

[1] Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.

6. Η αναγνώριση προσώπου είναι μια πιθανολογική τεχνολογία που μπορεί να αναγνωρίζει αυτομάτως τα άτομα με βάση το πρόσωπό τους με σκοπό τον έλεγχο της ταυτότητάς τους ή την ταυτοποίησή τους.

7. Η τεχνολογία αναγνώρισης προσώπου εμπίπτει στην ευρύτερη κατηγορία της βιομετρικής τεχνολογίας. Τα βιομετρικά δεδομένα περιλαμβάνουν όλες τις αυτοματοποιημένες διαδικασίες που χρησιμοποιούνται για την αναγνώριση ενός ατόμου μέσω της ποσοτικοποίησης φυσικών, φυσιολογικών ή συμπεριφορικών χαρακτηριστικών (δακτυλικά αποτυπώματα, δομή της ίριδας, φωνή, βάδισμα, μοτίβα των αιμοφόρων αγγείων, κ.λπ.). Τα εν λόγω χαρακτηριστικά ορίζονται ως «βιομετρικά δεδομένα», επειδή επιτρέπουν ή επιβεβαιώνουν τη μοναδική ταυτοποίηση του εν λόγω προσώπου.

8. Αυτό ισχύει για τα πρόσωπα των ατόμων ή, πιο συγκεκριμένα, για την τεχνική επεξεργασία τους μέσω συσκευών αναγνώρισης προσώπου: λαμβάνοντας την εικόνα ενός προσώπου (φωτογραφία ή βίντεο) που ονομάζεται βιομετρικό «δείγμα», είναι δυνατόν να εξαχθεί μια ψηφιακή αναπαράσταση διακριτών χαρακτηριστικών αυτού του προσώπου (το οποίο ονομάζεται «υπόδειγμα»).

9. Ένα βιομετρικό υπόδειγμα είναι μια ψηφιακή αναπαράσταση των μοναδικών χαρακτηριστικών που έχουν εξαχθεί από ένα βιομετρικό δείγμα και μπορεί να αποθηκευτεί σε μια βιομετρική βάση δεδομένων[2]. Το εν λόγω υπόδειγμα θεωρείται ότι είναι μοναδικό και συγκεκριμένο για κάθε άτομο και παραμένει, κατ' αρχήν, αναλλοίωτο με την πάροδο του χρόνου[3]. Στη φάση της αναγνώρισης, η συσκευή συγκρίνει αυτό το υπόδειγμα με άλλα υποδείγματα που έχουν προηγουμένως παραχθεί ή υπολογιστεί απευθείας από βιομετρικά δείγματα, όπως πρόσωπα που βρίσκονται σε μια εικόνα, φωτογραφία ή βίντεο. Ως εκ τούτου, η «αναγνώριση προσώπου» είναι μια διαδικασία δύο σταδίων: η συλλογή της εικόνας προσώπου και η μετατροπή της σε υπόδειγμα, ακολουθούμενη από την αναγνώριση του προσώπου αυτού μέσω της σύγκρισης του αντίστοιχου υποδείγματος με ένα ή περισσότερα άλλα υποδείγματα.

10. Όπως κάθε βιομετρική διαδικασία, η αναγνώριση προσώπου μπορεί να επιτελέσει δύο διακριτές λειτουργίες:

    - τον **έλεγχο της ταυτότητας** ενός προσώπου, με σκοπό να επαληθευτεί ότι το εν λόγω πρόσωπο είναι αυτό που ισχυρίζεται ότι είναι. Στην εν λόγω περίπτωση, το σύστημα θα συγκρίνει ένα προ-καταγεγραμμένο βιομετρικό υπόδειγμα ή δείγμα (π.χ. αποθηκευμένο σε μια έξυπνη κάρτα ή βιομετρικό διαβατήριο) με ένα πρόσωπο, όπως αυτό ενός ατόμου που εμφανίζεται σε ένα σημείο ελέγχου, προκειμένου να επαληθεύσει αν πρόκειται για το ίδιο πρόσωπο. Συνεπώς, η λειτουργία αυτή βασίζεται στη σύγκριση δύο υποδειγμάτων. Αυτό ονομάζεται επίσης **επαλήθευση** 1 προς 1.

    - την **ταυτοποίηση** ενός προσώπου, με στόχο την εύρεση ενός προσώπου μεταξύ μιας ομάδας ατόμων, εντός μιας συγκεκριμένης περιοχής, μιας εικόνας ή μιας βάσης δεδομένων. Σε αυτή την περίπτωση, το σύστημα πρέπει να επεξεργαστεί κάθε πρόσωπο που καταγράφεται, να δημιουργήσει ένα βιομετρικό υπόδειγμα και στη συνέχεια να ελέγξει αν ταιριάζει με ένα άτομο γνωστό στο σύστημα. Επομένως, αυτή η λειτουργία βασίζεται στη σύγκριση ενός υποδείγματος με μια βάση δεδομένων υποδειγμάτων ή δειγμάτων (βάση αναφοράς). Αυτό ονομάζεται επίσης ταυτοποίηση 1 προς πολλά. Για παράδειγμα, μπορεί να συνδέσει μια καταγραφή ονόματος

[2] Κατευθυντήριες γραμμές για την αναγνώριση προσώπου, Συμβουλευτική Επιτροπή της Σύμβασης 108 της Σύμβασης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, Συμβούλιο της Ευρώπης, Ιούνιος 2021.

[3] Αυτό μπορεί να εξαρτάται από τον τύπο της βιομετρίας και την ηλικία του υποκειμένου των δεδομένων.

(επώνυμο, όνομα) με ένα πρόσωπο, εάν η αντιπαραβολή πραγματοποιείται με βάση δεδομένων φωτογραφιών που συνδέονται με επώνυμα και ονόματα. Μπορεί επίσης να περιλαμβάνει την παρακολούθηση ενός ατόμου μέσα στο πλήθος, χωρίς απαραίτητα να γίνεται σύνδεση με την πολιτική ταυτότητα του ατόμου.

11. Και στις δύο περιπτώσεις, οι χρησιμοποιούμενες τεχνικές αναγνώρισης προσώπου βασίζονται σε εκτιμώμενη αντιστοιχία μεταξύ των υποδειγμάτων: το υπόδειγμα που συγκρίνεται και τη βάση ή τις βάσεις αναφοράς. Από την άποψη αυτή, είναι πιθανολογικές: από τη σύγκριση προκύπτει μεγαλύτερη ή μικρότερη πιθανότητα το πρόσωπο να είναι πράγματι το πρόσωπο που πρέπει να ελεγχθεί ή να ταυτοποιηθεί· εάν η πιθανότητα αυτή υπερβαίνει ένα ορισμένο όριο στο σύστημα, το οποίο καθορίζεται από τον χρήστη ή τον προγραμματιστή του συστήματος, το σύστημα θα θεωρήσει ότι υπάρχει αντιστοιχία.

12. Ενώ και οι δύο λειτουργίες —έλεγχος της ταυτότητας και ταυτοποίηση— είναι διακριτές, αφορούν αμφότερες την επεξεργασία βιομετρικών δεδομένων που σχετίζονται με φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί και, ως εκ τούτου, συνιστούν επεξεργασία δεδομένων προσωπικού χαρακτήρα, και πιο συγκεκριμένα επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

13. Η αναγνώριση προσώπου αποτελεί μέρος ενός ευρύτερου φάσματος τεχνικών επεξεργασίας εικόνας βίντεο. Ορισμένες βιντεοκάμερες μπορούν να βιντεοσκοπήσουν ανθρώπους σε μια καθορισμένη περιοχή, ιδίως τα πρόσωπά τους, αλλά δεν μπορούν να χρησιμοποιηθούν ως τέτοιες για την αυτόματη αναγνώριση ατόμων. Το ίδιο ισχύει και για την απλή φωτογράφηση: μια φωτογραφική μηχανή δεν είναι σύστημα αναγνώρισης προσώπου, διότι οι φωτογραφίες των ανθρώπων πρέπει να υποστούν επεξεργασία με συγκεκριμένο τρόπο προκειμένου να εξαχθούν βιομετρικά δεδομένα.

14. Ούτε η απλή ανίχνευση προσώπων από τις λεγόμενες «έξυπνες» κάμερες συνιστά κατ' ανάγκη σύστημα αναγνώρισης προσώπου. Παρότι εγείρουν επίσης σημαντικά ερωτήματα όσον αφορά τη δεοντολογία και την αποτελεσματικότητα, οι ψηφιακές τεχνικές για την ανίχνευση μη φυσιολογικών συμπεριφορών ή βίαιων γεγονότων ή για την αναγνώριση συναισθημάτων προσώπου ή ακόμη και περιγραμμάτων, δεν μπορούν να θεωρηθούν ως βιομετρικά συστήματα που επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, υπό την προϋπόθεση ότι δεν αποσκοπούν στη μοναδική ταυτοποίηση ενός ατόμου και ότι η σχετική επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν περιλαμβάνει άλλες ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Τα παραδείγματα αυτά δεν είναι εντελώς άσχετα με την αναγνώριση προσώπου και εξακολουθούν να υπόκεινται στους κανόνες προστασίας των δεδομένων προσωπικού χαρακτήρα.[4] Επιπλέον, αυτό το είδος συστήματος ανίχνευσης μπορεί να χρησιμοποιείται σε συνδυασμό με άλλα συστήματα που αποσκοπούν στην ταυτοποίηση ενός ατόμου και, ως εκ τούτου, θεωρούνται τεχνολογία αναγνώρισης προσώπου.

15. Σε αντίθεση με τα συστήματα λήψης και επεξεργασίας βίντεο, για παράδειγμα, που απαιτούν την εγκατάσταση φυσικών συσκευών, η αναγνώριση προσώπου είναι μια λειτουργικότητα λογισμικού που μπορεί να εφαρμοστεί στο πλαίσιο υφιστάμενων συστημάτων (κάμερες, βάσεις δεδομένων εικόνων κ.λπ.). Συνεπώς, μια τέτοια λειτουργικότητα μπορεί να συνδεθεί ή να διασυνδεθεί με πλήθος συστημάτων και να συνδυαστεί με άλλες λειτουργίες. Μια τέτοια ενσωμάτωση σε μια ήδη υφιστάμενη υποδομή απαιτεί ιδιαίτερη προσοχή, διότι συνεπάγεται εγγενείς κινδύνους λόγω του

[4] Το άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (ή το άρθρο 9 του ΓΚΠΔ) εφαρμόζεται, ωστόσο, σε συστήματα που χρησιμοποιούνται για την κατηγοριοποίηση ατόμων με βάση τα βιομετρικά τους στοιχεία σε ομάδες ανάλογα με την εθνικότητα, καθώς και τον πολιτικό ή σεξουαλικό προσανατολισμό ή άλλες ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

γεγονότος ότι η τεχνολογία αναγνώρισης προσώπου θα μπορούσε να λειτουργεί απρόσκοπτα και να αποκρύπτεται εύκολα[5].

2.2 Μεγάλη ποικιλία σκοπών και εφαρμογών

16. Πέρα από το πεδίο εφαρμογής των παρόντων κατευθυντήριων γραμμών και εκτός του πεδίου εφαρμογής της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η αναγνώριση προσώπου μπορεί να χρησιμοποιηθεί για μια ευρεία ποικιλία στόχων, τόσο για εμπορική χρήση όσο και για την αντιμετώπιση ζητημάτων δημόσιας ασφάλειας ή επιβολής του νόμου. Μπορεί να εφαρμόζεται σε πολλά διαφορετικά πλαίσια: στην προσωπική σχέση μεταξύ ενός χρήστη και μιας υπηρεσίας (πρόσβαση σε μια εφαρμογή), για την πρόσβαση σε έναν συγκεκριμένο τόπο (φυσικό φιλτράρισμα) ή χωρίς κανέναν ιδιαίτερο περιορισμό στον δημόσιο χώρο (ζωντανή αναγνώριση προσώπου). Μπορεί να εφαρμοστεί σε κάθε είδους υποκείμενο δεδομένων: έναν πελάτη μιας υπηρεσίας, έναν υπάλληλο, έναν απλό θεατή, ένα καταζητούμενο πρόσωπο ή ένα πρόσωπο που εμπλέκεται σε νομικές ή διοικητικές διαδικασίες κ.λπ. Ορισμένες χρήσεις είναι ήδη κοινές και διαδεδομένες· άλλες βρίσκονται, προς το παρόν, σε πειραματικό ή υποθετικό στάδιο. Μολονότι οι παρούσες κατευθυντήριες γραμμές δεν θα καλύπτουν όλες τις εν λόγω χρήσεις και εφαρμογές, το ΕΣΠΔ υπενθυμίζει ότι μπορούν να εφαρμοστούν μόνο εάν συμμορφώνονται με το ισχύον νομικό πλαίσιο, και ιδίως με τον ΓΚΠΔ και τη σχετική εθνική νομοθεσία.[6] Ακόμη και στο πλαίσιο της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, πέραν των λειτουργιών του ελέγχου της ταυτότητας ή της ταυτοποίησης, τα δεδομένα που υποβάλλονται σε επεξεργασία με τη χρήση τεχνολογίας αναγνώρισης προσώπου μπορούν επίσης να υποβληθούν σε περαιτέρω επεξεργασία για άλλους σκοπούς, όπως η κατηγοριοποίηση.

17. Πιο συγκεκριμένα, θα μπορούσε να εξεταστεί μια κλίμακα δυνητικών χρήσεων, ανάλογα με τον βαθμό ελέγχου που έχουν τα άτομα επί των δεδομένων προσωπικού χαρακτήρα που τους αφορούν, τα αποτελεσματικά μέσα που διαθέτουν για την άσκηση του εν λόγω ελέγχου και το δικαίωμά τους να αναλάβουν πρωτοβουλίες για την ενεργοποίηση και τη χρήση αυτής της τεχνολογίας, τις συνέπειες για αυτούς (σε περίπτωση αναγνώρισης ή μη αναγνώρισης) και την κλίμακα της πραγματοποιούμενης επεξεργασίας. Η αναγνώριση προσώπου με βάση ένα υπόδειγμα το οποίο είναι αποθηκευμένο σε μια προσωπική συσκευή (έξυπνη κάρτα, έξυπνο τηλέφωνο κ.λπ.) που ανήκει στο εν λόγω πρόσωπο, η οποία χρησιμοποιείται για έλεγχο της ταυτότητας και αυστηρά προσωπική χρήση μέσω μιας ειδικής διεπαφής, δεν ενέχει τους ίδιους κινδύνους όπως, για παράδειγμα, η χρήση για σκοπούς ταυτοποίησης, σε μη ελεγχόμενο περιβάλλον, χωρίς την ενεργό συμμετοχή των υποκειμένων των δεδομένων, όπου το υπόδειγμα κάθε προσώπου που εισέρχεται στην περιοχή παρακολούθησης συγκρίνεται με υποδείγματα από μια ευρεία ομάδα του πληθυσμού που είναι αποθηκευμένα σε μια βάση δεδομένων. Μεταξύ αυτών των δύο άκρων βρίσκεται ένα εξαιρετικά ποικιλόμορφο φάσμα χρήσεων και συναφών ζητημάτων που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα.

18. Προκειμένου να αποσαφηνιστεί περαιτέρω το πλαίσιο εντός του οποίου συζητούνται ή εφαρμόζονται επί του παρόντος οι τεχνολογίες αναγνώρισης προσώπου, είτε για τον έλεγχο της ταυτότητας είτε για την ταυτοποίηση, το ΕΣΠΔ θεωρεί σκόπιμο να αναφέρει μια σειρά παραδειγμάτων. Τα ακόλουθα παραδείγματα είναι απλώς περιγραφικά και δεν θα πρέπει να θεωρούνται ως κάποιου είδους

[5] Για παράδειγμα, στις προσαρτώμενες στο σώμα κάμερες που χρησιμοποιούνται όλο και περισσότερο στην πράξη.

[6] Βλ. επίσης τις κατευθυντήριες γραμμές με τίτλο «EDPB guidelines 3/2019 on processing of personal data through video devices» (3/2019 Κατευθυντήριες γραμμές του ΕΣΠΔ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών), οι οποίες εκδόθηκαν στις 29 Ιανουαρίου 2020, για περαιτέρω καθοδήγηση.

προκαταρκτική αξιολόγηση της συμμόρφωσής τους με το κεκτημένο της ΕΕ στον τομέα της προστασίας των δεδομένων.

Παραδείγματα ελέγχου της ταυτότητας με αναγνώριση προσώπου

19. Ο έλεγχος της ταυτότητας μπορεί να σχεδιαστεί έτσι ώστε οι χρήστες να έχουν πλήρη έλεγχο επ' αυτού, για παράδειγμα για να καταστεί δυνατή η πρόσβαση σε υπηρεσίες ή εφαρμογές αποκλειστικά εντός οικιακού περιβάλλοντος. Ως εκ τούτου, χρησιμοποιείται εκτενώς από τους ιδιοκτήτες έξυπνων τηλεφώνων για να ξεκλειδώσουν τη συσκευή τους, αντί του ελέγχου της ταυτότητας με κωδικό πρόσβασης.

20. Ο έλεγχος της ταυτότητας με αναγνώριση προσώπου μπορεί επίσης να χρησιμοποιηθεί για τον έλεγχο της ταυτότητας ενός προσώπου που επιθυμεί να επωφεληθεί από δημόσιες ή ιδιωτικές υπηρεσίες τρίτων. Τέτοιες διαδικασίες προσφέρουν έτσι έναν τρόπο δημιουργίας μιας ψηφιακής ταυτότητας με τη χρήση μιας εφαρμογής για κινητά τηλέφωνα (έξυπνα τηλέφωνα, ταμπλέτες κ.λπ.), η οποία μπορεί στη συνέχεια να χρησιμοποιηθεί για την πρόσβαση σε επιγραμμικές διοικητικές υπηρεσίες.

21. Επιπλέον, ο έλεγχος ταυτότητας με αναγνώριση προσώπου μπορεί να αποσκοπεί στον έλεγχο της φυσικής πρόσβασης σε μία ή περισσότερες προκαθορισμένες τοποθεσίες, όπως είσοδοι κτιρίων ή συγκεκριμένα σημεία διέλευσης. Αυτή η λειτουργία εφαρμόζεται, για παράδειγμα, σε ορισμένες περιπτώσεις επεξεργασίας για τους σκοπούς της διέλευσης των συνόρων, όπου το πρόσωπο του ατόμου στη συσκευή του σημείου ελέγχου συγκρίνεται με εκείνο που είναι αποθηκευμένο στο έγγραφο ταυτότητάς του (διαβατήριο ή ασφαλή άδεια διαμονής).

Παραδείγματα ταυτοποίησης με αναγνώριση προσώπου

22. Η ταυτοποίηση μπορεί να εφαρμοστεί με πολλούς, ακόμη πιο διαφορετικούς τρόπους. Σε αυτούς περιλαμβάνονται, μεταξύ άλλων, οι χρήσεις που απαριθμούνται κατωτέρω, οι οποίες επί του παρόντος παρατηρούνται, δοκιμάζονται ή σχεδιάζονται στην ΕΕ.

- αναζήτηση, σε μια βάση δεδομένων φωτογραφιών, της ταυτότητας ενός αγνώστου ατόμου (θύμα, ύποπτος κ.λπ.)·
- παρακολούθηση των κινήσεων ενός ατόμου στον δημόσιο χώρο. Το πρόσωπό του/της συγκρίνεται με τα βιομετρικά υποδείγματα των ατόμων που ταξιδεύουν ή έχουν ταξιδέψει στην ελεγχόμενη περιοχή, για παράδειγμα όταν αφήνεται πίσω μια αποσκευή ή μετά τη διάπραξη ενός εγκλήματος,
- αναπαράσταση του ταξιδιού ενός ατόμου και των επακόλουθων αλληλεπιδράσεών του με άλλα άτομα, μέσω ετεροχρονισμένης σύγκρισης των ίδιων στοιχείων σε μια προσπάθεια προσδιορισμού, για παράδειγμα, των επαφών του·
- εξ αποστάσεως βιομετρική ταυτοποίηση καταζητούμενων ατόμων σε δημόσιους χώρους. Όλα τα πρόσωπα που καταγράφονται ζωντανά από τις κάμερες προστασίας βίντεο διασταυρώνονται, σε πραγματικό χρόνο, με μια βάση δεδομένων που τηρούν οι δυνάμεις ασφαλείας·
- αυτόματη αναγνώριση ατόμων σε μια εικόνα για τον εντοπισμό, για παράδειγμα, των σχέσεών τους σε ένα κοινωνικό δίκτυο, το οποίο τη χρησιμοποιεί. Η εικόνα συγκρίνεται με τα υποδείγματα όλων των συμμετεχόντων στο δίκτυο που έχουν συναινέσει σε αυτή τη λειτουργία, προκειμένου να προταθεί η ονομαστική ταυτοποίηση αυτών των σχέσεων·

- πρόσβαση σε υπηρεσίες, με ορισμένα μηχανήματα αυτόματης ανάληψης μετρητών να αναγνωρίζουν τους πελάτες τους, συγκρίνοντας το πρόσωπο που καταγράφεται από κάμερα με τη βάση δεδομένων εικόνων προσώπου που τηρεί η τράπεζα·

- παρακολούθηση του ταξιδιού ενός επιβάτη σε ένα συγκεκριμένο στάδιο του ταξιδιού. Το υπόδειγμα, που υπολογίζεται σε πραγματικό χρόνο, για κάθε άτομο που πραγματοποιεί έλεγχο στις πύλες που βρίσκονται σε ορισμένα στάδια του ταξιδιού (σημεία παράδοσης αποσκευών, πύλες επιβίβασης κ.λπ.), συγκρίνεται με τα υποδείγματα των ατόμων που ήταν προηγουμένως εγγεγραμμένα στο σύστημα.

23. Εκτός από τη χρήση της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου, το ευρύ φάσμα εφαρμογών που παρατηρείται απαιτεί οπωσδήποτε μια ολοκληρωμένη συζήτηση και πολιτική προσέγγιση προκειμένου να διασφαλιστεί η συνοχή και η συμμόρφωση με το κεκτημένο της ΕΕ στον τομέα της προστασίας των δεδομένων.

2.3 Αξιοπιστία, ακρίβεια και κίνδυνοι για τα υποκείμενα των δεδομένων

24. Όπως κάθε τεχνολογία, η αναγνώριση προσώπου μπορεί επίσης να υπόκειται σε προκλήσεις όσον αφορά την εφαρμογή της, ιδίως όσον αφορά την αξιοπιστία και την αποτελεσματικότητά της από άποψη ελέγχου της ταυτότητας ή ταυτοποίησης, καθώς και το συνολικό ζήτημα της ποιότητας και της ακρίβειας των δεδομένων «πηγής» και του αποτελέσματος της επεξεργασίας της τεχνολογίας αναγνώρισης προσώπου.

25. Οι εν λόγω τεχνολογικές προκλήσεις ενέχουν ιδιαίτερους κινδύνους για τα ενδιαφερόμενα υποκείμενα των δεδομένων, οι οποίοι είναι ακόμη σημαντικότεροι ή σοβαρότεροι στον τομέα της επιβολής του νόμου, λαμβανομένων υπόψη των πιθανών επιπτώσεων για τα υποκείμενα των δεδομένων είτε νομικών είτε άλλων που τα επηρεάζουν με παρόμοιο τρόπο σε σημαντικό βαθμό. Στο πλαίσιο αυτό, φαίνεται επίσης χρήσιμο να υπογραμμιστεί ότι η εκ των υστέρων χρήση της τεχνολογίας αναγνώρισης προσώπου δεν είναι αυτή καθαυτή ασφαλέστερη, καθώς τα άτομα μπορεί να παρακολουθούνται σε βάθος χρόνου και τόπου. Επομένως, η εκ των υστέρων χρήση ενέχει επίσης συγκεκριμένους κινδύνους οι οποίοι πρέπει να αξιολογούνται κατά περίπτωση.[7]

26. Όπως επισημαίνεται από τον Οργανισμό Θεμελιωδών Δικαιωμάτων της ΕΕ στην έκθεσή του για το 2019, «ο καθορισμός του αναγκαίου επιπέδου ακρίβειας του λογισμικού αναγνώρισης προσώπου παρουσιάζει δυσκολίες: υπάρχουν πολλοί διαφορετικοί τρόποι για την αξιολόγηση και την εκτίμηση της ακρίβειας, οι οποίοι εξαρτώνται επίσης από το έργο, τον σκοπό και το πλαίσιο της χρήσης του. Όταν εφαρμόζεται η τεχνολογία σε μέρη τα οποία επισκέπτονται εκατομμύρια άτομα —όπως σιδηροδρομικοί σταθμοί ή αεροδρόμια— ένα σχετικά μικρό ποσοστό σφαλμάτων (π.χ. 0,01 %)[8] εξακολουθεί να σημαίνει ότι εκατοντάδες άτομα επισημαίνονται εσφαλμένα. Επιπλέον, ορισμένες κατηγορίες ατόμων ενδέχεται να είναι πιθανότερο να αντιστοιχιστούν εσφαλμένα από άλλες, όπως περιγράφεται στην ενότητα 3. Υπάρχουν διάφοροι τρόποι υπολογισμού και ερμηνείας των ποσοστών σφάλματος, οπότε απαιτείται προσοχή. Επιπλέον, όσον αφορά την ακρίβεια και τα σφάλματα, τα ερωτήματα σχετικά με το πόσο εύκολο είναι ένα σύστημα να παραπλανηθεί, για παράδειγμα, από

[7] Βλ. τα παραδείγματα που παρουσιάζονται στο παράρτημα ΙΙΙ.

[8] Αυτό το ποσοστό ακρίβειας προέρχεται από την παρατιθέμενη έκθεση και αντικατοπτρίζει ένα ποσοστό πολύ καλύτερο από τις τρέχουσες επιδόσεις των αλγορίθμων στις εφαρμογές της τεχνολογίας αναγνώρισης προσώπου.

ψεύτικες εικόνες προσώπου (που αποκαλείται «πλαστοπροσωπία») είναι σημαντικά ιδίως για τους σκοπούς της επιβολής του νόμου.»[9]

27. Στο πλαίσιο αυτό, το ΕΣΠΔ θεωρεί σημαντικό να υπενθυμίσει ότι η τεχνολογία αναγνώρισης προσώπου, είτε χρησιμοποιείται για σκοπούς ελέγχου της ταυτότητας είτε για σκοπούς ταυτοποίησης, δεν παρέχει οριστικό αποτέλεσμα, αλλά βασίζεται σε πιθανότητες ότι δύο πρόσωπα ή εικόνες προσώπων αντιστοιχούν στο ίδιο πρόσωπο.[10] Το αποτέλεσμα αυτό υποβαθμίζεται περαιτέρω όταν η ποιότητα των βιομετρικών δειγμάτων που εισάγονται στην αναγνώριση προσώπου είναι χαμηλή. Η θολότητα των εισερχόμενων εικόνων, η χαμηλή ανάλυση της κάμερας, η κίνηση και ο χαμηλός φωτισμός μπορεί να είναι παράγοντες χαμηλής ποιότητας. Άλλες πτυχές με σημαντικό αντίκτυπο στα αποτελέσματα είναι η συχνότητα εμφάνισης και η πλαστοπροσωπία, π.χ. όταν οι εγκληματίες προσπαθούν είτε να αποφύγουν να περάσουν από τις κάμερες είτε να ξεγελάσουν την τεχνολογία αναγνώρισης προσώπου. Πολυάριθμες μελέτες έχουν επίσης επισημάνει ότι τέτοια στατιστικά αποτελέσματα της αλγοριθμικής επεξεργασίας μπορεί επίσης να υπόκεινται σε μεροληψία, ιδίως ως αποτέλεσμα της ποιότητας των δεδομένων προέλευσης, καθώς και των βάσεων δεδομένων κατάρτισης, ή άλλων παραγόντων, όπως η επιλογή της τοποθεσίας εγκατάστασης. Επιπλέον, θα πρέπει επίσης να επισημανθεί ο αντίκτυπος της τεχνολογίας αναγνώρισης προσώπου σε άλλα θεμελιώδη δικαιώματα, όπως ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, η ελευθερία της έκφρασης και της πληροφόρησης, η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι κ.λπ.

28. Ως εκ τούτου, είναι σημαντικό να λαμβάνονται υπόψη η αξιοπιστία και η ακρίβεια της τεχνολογίας αναγνώρισης προσώπου ως κριτήρια για την αξιολόγηση της συμμόρφωσης με τις βασικές αρχές προστασίας των δεδομένων, σύμφωνα με το άρθρο 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, και ιδίως όσον αφορά τη δικαιοσύνη και την ακρίβεια.

29. Επισημαίνοντας ότι τα υψηλής ποιότητας δεδομένα είναι απαραίτητα για αλγορίθμους υψηλής ποιότητας, το ΕΣΠΔ υπογραμμίζει επίσης την ανάγκη οι υπεύθυνοι επεξεργασίας δεδομένων, στο πλαίσιο της υποχρέωσής τους για λογοδοσία, να προβαίνουν σε τακτική και συστηματική αξιολόγηση της αλγοριθμικής επεξεργασίας, προκειμένου ιδίως να διασφαλίζουν την ακρίβεια, τη δικαιοσύνη και την αξιοπιστία του αποτελέσματος της εν λόγω επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται για τους σκοπούς της αξιολόγησης, της κατάρτισης και της περαιτέρω ανάπτυξης των συστημάτων τεχνολογίας αναγνώρισης προσώπου μπορούν να αποτελέσουν αντικείμενο επεξεργασίας μόνο βάσει επαρκούς νομικής βάσης και σύμφωνα με τις κοινές αρχές προστασίας δεδομένων.

3 ΙΣΧΥΟΝ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

30. Η χρήση τεχνολογιών αναγνώρισης προσώπου είναι άρρηκτα συνδεδεμένη με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων. Επιπλέον, έχει άμεσο ή έμμεσο αντίκτυπο σε ορισμένα θεμελιώδη δικαιώματα, τα οποία κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Αυτό είναι ιδιαίτερα σημαντικό στον τομέα της επιβολής του νόμου και της ποινικής δικαιοσύνης. Ως εκ τούτου, οποιαδήποτε χρήση τεχνολογιών αναγνώρισης προσώπου θα πρέπει να πραγματοποιείται σε αυστηρή συμμόρφωση με το ισχύον νομικό πλαίσιο.

[9] Facial recognition technology: fundamental rights considerations in the context of law enforcement (Τεχνολογία αναγνώρισης προσώπου: ζητήματα θεμελιωδών δικαιωμάτων στο πλαίσιο της επιβολής του νόμου), Οργανισμός Θεμελιωδών Δικαιωμάτων της ΕΕ, 21 Νοεμβρίου 2019.
[10] Αυτή η πιθανότητα αναφέρεται ως «βαθμολογία εμπιστοσύνης».

31. Οι ακόλουθες πληροφορίες προορίζονται να χρησιμοποιηθούν για εξέταση κατά την αξιολόγηση μελλοντικών νομοθετικών και διοικητικών μέτρων, καθώς και κατά την εφαρμογή της ισχύουσας νομοθεσίας κατά περίπτωση σε σχέση με την τεχνολογία αναγνώρισης προσώπου. Η συνάφεια των αντίστοιχων απαιτήσεων ποικίλλει ανάλογα με τις ιδιαίτερες περιστάσεις. Δεδομένου ότι δεν μπορούν να προβλεφθούν όλες οι μελλοντικές περιστάσεις, θεωρείται ότι παρέχουν μόνο υποστήριξη και δεν πρέπει να ερμηνεύονται ως εξαντλητική απαρίθμηση.

3.1 Γενικό νομικό πλαίσιο — Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ και η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)

3.1.1 Εφαρμογή του Χάρτη

32. Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ (στο εξής «ο Χάρτης») απευθύνεται στα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και στα κράτη μέλη όταν εφαρμόζουν το δίκαιο της Ένωσης.

33. Η ρύθμιση της επεξεργασίας βιομετρικών δεδομένων για σκοπούς επιβολής του νόμου σύμφωνα με το άρθρο 1 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου εγείρει αναπόφευκτα το ζήτημα της συμμόρφωσης με τα θεμελιώδη δικαιώματα, ιδίως όσον αφορά τον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών βάσει του άρθρου 7 του Χάρτη και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα βάσει του άρθρου 8 του Χάρτη.

34. Η συλλογή και ανάλυση βιντεοσκοπημένου οπτικοακουστικού υλικού φυσικών προσώπων, συμπεριλαμβανομένων των προσώπων τους, συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Κατά την τεχνική επεξεργασία της εικόνας, η επεξεργασία καλύπτει επίσης τα βιομετρικά δεδομένα. Η τεχνική επεξεργασία δεδομένων που αφορούν το πρόσωπο ενός φυσικού προσώπου σε σχέση με τον χρόνο και τον τόπο επιτρέπει την εξαγωγή συμπερασμάτων σχετικά με την ιδιωτική ζωή των ενδιαφερόμενων ατόμων. Τα συμπεράσματα αυτά μπορούν να αφορούν τη φυλετική ή εθνοτική καταγωγή, την υγεία, τη θρησκεία, τις καθημερινές συνήθειες, τους μόνιμους ή προσωρινούς τόπους διαμονής, τις καθημερινές ή άλλες μετακινήσεις, τις ασκούμενες δραστηριότητες, τις κοινωνικές σχέσεις των εν λόγω ατόμων και τα κοινωνικά περιβάλλοντα στα οποία συχνάζουν. Το ευρύ φάσμα των πληροφοριών που μπορεί να αποκαλυφθούν από την εφαρμογή της τεχνολογίας αναγνώρισης προσώπου καταδεικνύει σαφώς τον πιθανό αντίκτυπο στο δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που προβλέπεται στο άρθρο 8 του Χάρτη, αλλά και στο δικαίωμα στην ιδιωτική ζωή που προβλέπεται στο άρθρο 7 του Χάρτη.

35. Υπό αυτές τις συνθήκες, δεν αποκλείεται επίσης το ενδεχόμενο η συλλογή, η ανάλυση και η περαιτέρω επεξεργασία των εν λόγω βιομετρικών δεδομένων (προσώπου) να επηρεάσει τον τρόπο με τον οποίο οι άνθρωποι αισθάνονται ελεύθεροι να ενεργούν, ακόμη και αν η πράξη αυτή βρίσκεται πλήρως εντός του πλαισίου μιας ελεύθερης και ανοικτής κοινωνίας. Θα μπορούσε επίσης να έχει σοβαρές επιπτώσεις στην άσκηση των θεμελιωδών δικαιωμάτων τους, όπως το δικαίωμά τους στην ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και την ελευθερία της ειρηνικής συνάθροισης και του συνεταιρίζεσθαι σύμφωνα με τα άρθρα 1, 10, 11 και 12 του Χάρτη. Η επεξεργασία αυτή ενέχει και άλλους κινδύνους, όπως τον κίνδυνο κατάχρησης των πληροφοριών προσωπικού χαρακτήρα που συλλέγονται από τις αρμόδιες αρχές ως αποτέλεσμα παράνομης πρόσβασης και χρήσης των δεδομένων προσωπικού χαρακτήρα, παραβίασης της ασφάλειας κ.λπ. Οι κίνδυνοι συχνά εξαρτώνται από την επεξεργασία και τις περιστάσεις της, όπως τον κίνδυνο παράνομης πρόσβασης και χρήσης από αστυνομικούς ή άλλα μη εξουσιοδοτημένα μέρη. Ωστόσο, ορισμένοι κίνδυνοι είναι απλώς εγγενείς στη μοναδική φύση των βιομετρικών δεδομένων. Σε

αντίθεση με μια διεύθυνση ή έναν αριθμό τηλεφώνου, το υποκείμενο των δεδομένων είναι αδύνατον να αλλάξει τα μοναδικά χαρακτηριστικά του, όπως το πρόσωπο ή την ίριδα. Σε περίπτωση μη εξουσιοδοτημένης πρόσβασης ή τυχαίας δημοσίευσης βιομετρικών δεδομένων, αυτό θα είχε ως αποτέλεσμα την παραβίαση των δεδομένων κατά τη χρήση τους ως κωδικών πρόσβασης ή κρυπτογραφικών κλειδιών ή θα μπορούσε να χρησιμοποιηθεί για περαιτέρω, μη εξουσιοδοτημένες δραστηριότητες παρακολούθησης εις βάρος του υποκειμένου των δεδομένων.

3.1.2 Παρέμβαση στα δικαιώματα που ορίζονται στον Χάρτη

36. Η επεξεργασία βιομετρικών δεδομένων υπό οποιεσδήποτε περιστάσεις συνιστά αφ' εαυτής σοβαρή παρέμβαση. Αυτό δεν εξαρτάται από το αποτέλεσμα, π.χ. μια θετική αντιστοίχιση. Η επεξεργασία συνιστά παρέμβαση ακόμη και αν το βιομετρικό υπόδειγμα διαγράφεται αμέσως μετά την αντιστοίχιση με βάση δεδομένων της αστυνομίας χωρίς θετικό αποτέλεσμα.

37. Η παρέμβαση στα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων μπορεί να απορρέει από νομοθετική πράξη η οποία είτε αποσκοπεί είτε έχει ως αποτέλεσμα τον περιορισμό του αντίστοιχου θεμελιώδους δικαιώματος[11]. Μπορεί επίσης να προκύπτει από πράξη δημόσιας αρχής με τον ίδιο σκοπό ή αποτέλεσμα ή ακόμη και ιδιωτικής οντότητας στην οποία ο νόμος αναθέτει την άσκηση δημόσιας αρχής και την άσκηση δημόσιων εξουσιών.

38. Ένα νομοθετικό μέτρο που χρησιμεύει ως νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα παρεμβαίνει άμεσα στα δικαιώματα που εγγυώνται τα άρθρα 7 και 8 του Χάρτη[12].

39. Η χρήση βιομετρικών δεδομένων και ιδίως η τεχνολογία αναγνώρισης προσώπου σε πολλές περιπτώσεις επηρεάζουν επίσης το δικαίωμα στην ανθρώπινη αξιοπρέπεια, το οποίο κατοχυρώνεται στο άρθρο 1 του Χάρτη. Η ανθρώπινη αξιοπρέπεια προϋποθέτει ότι τα άτομα δεν αντιμετωπίζονται ως απλά αντικείμενα. Η τεχνολογία αναγνώρισης προσώπου υπολογίζει υπαρξιακά και άκρως προσωπικά χαρακτηριστικά, τα χαρακτηριστικά του προσώπου, σε μια μηχανικά αναγνώσιμη μορφή με σκοπό τη χρήση της ως ανθρώπινη πινακίδα κυκλοφορίας ή ταυτότητα, αντικειμενοποιώντας έτσι το πρόσωπο.

40. Μια τέτοια επεξεργασία μπορεί επίσης να θίγει άλλα θεμελιώδη δικαιώματα, όπως τα δικαιώματα που απορρέουν από τα άρθρα 10, 11 και 12 του Χάρτη, στον βαθμό που τα αποτρεπτικά αποτελέσματα είτε προορίζονται είτε απορρέουν από τη σχετική βιντεοπαρακολούθηση των υπηρεσιών επιβολής του νόμου.

41. Επιπλέον, θα πρέπει επίσης να εξεταστούν προσεκτικά οι πιθανοί κίνδυνοι που προκύπτουν από τη χρήση τεχνολογιών αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου όσον αφορά το δικαίωμα σε δίκαιη δίκη και το τεκμήριο αθωότητας σύμφωνα με τα άρθρα 47 και 48 του Χάρτη. Το αποτέλεσμα της εφαρμογής της τεχνολογία αναγνώρισης προσώπου, π.χ. μια αντιστοιχία, μπορεί όχι μόνο να οδηγήσει σε περαιτέρω αστυνόμευση ενός ατόμου, αλλά και να αποτελέσει αποφασιστικό αποδεικτικό στοιχείο σε δικαστικές διαδικασίες. Οι ελλείψεις της τεχνολογίας αναγνώρισης προσώπου, όπως η πιθανή μεροληψία, οι διακρίσεις ή ο εσφαλμένος εντοπισμός («ψευδώς θετικό») μπορεί επομένως να έχουν σοβαρές επιπτώσεις και στις ποινικές διαδικασίες. Επιπλέον, κατά την αξιολόγηση των αποδεικτικών στοιχείων, το αποτέλεσμα της εφαρμογής της τεχνολογίας αναγνώρισης προσώπου μπορεί να ευνοηθεί, ακόμη και αν υπάρχουν αντικρουόμενα στοιχεία («μεροληψία αυτοματισμού»).

---

[11] ΔΕΕ, C-219/91 – Ter Voort, RoC 1992 I-05485, σκέψη 36στ· ΔΕΕ, C-200/96 – Metronome, RoC 1998 I-1953, σκέψη 28.

[12] ΔΕΕ, C-594/12, σκέψη 36· ΔΕΕ, C-291/12, σκέψη 23 και εξής.

3.1.3 Αιτιολόγηση της παρέμβασης

42. Σύμφωνα με το άρθρο 52 παράγραφος 1 του Χάρτη, κάθε περιορισμός στην άσκηση των θεμελιωδών δικαιωμάτων και ελευθεριών πρέπει να προβλέπεται από τον νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ευρωπαϊκή Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.

3.1.3.1 Προβλέπεται από τον νόμο

43. Το άρθρο 52 παράγραφος 1 του Χάρτη ορίζει την απαίτηση ειδικής νομικής βάσης. Η εν λόγω νομική βάση πρέπει να είναι επαρκώς σαφής ως προς τους όρους της, ώστε να παρέχει στους πολίτες κατάλληλη ένδειξη των προϋποθέσεων και των περιστάσεων υπό τις οποίες οι αρχές εξουσιοδοτούνται να προσφεύγουν σε οποιαδήποτε μέτρα συλλογής δεδομένων και μυστικής παρακολούθησης[13]. Πρέπει να υποδεικνύει με εύλογη σαφήνεια το πεδίο εφαρμογής και τον τρόπο άσκησης της σχετικής διακριτικής ευχέρειας που παρέχεται στις δημόσιες αρχές, ώστε να διασφαλίζεται στα άτομα ο ελάχιστος βαθμός προστασίας που δικαιούνται σύμφωνα με το κράτος δικαίου σε μια δημοκρατική κοινωνία[14]. Επιπλέον, η νομιμότητα απαιτεί επαρκείς εγγυήσεις για να διασφαλιστεί ιδίως ο σεβασμός του δικαιώματος του ατόμου σύμφωνα με το άρθρο 8 του Χάρτη. Οι εν λόγω αρχές ισχύουν επίσης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αξιολόγησης, κατάρτισης και περαιτέρω ανάπτυξης των συστημάτων τεχνολογίας αναγνώρισης προσώπου.

44. Δεδομένου ότι τα βιομετρικά δεδομένα, όταν υποβάλλονται σε επεξεργασία με σκοπό την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου, αποτελούν ειδικές κατηγορίες δεδομένων που απαριθμούνται στο άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, οι διαφορετικές εφαρμογές της τεχνολογίας αναγνώρισης προσώπου απαιτούν στις περισσότερες περιπτώσεις ειδικό νόμο ο οποίος θα περιγράφει με ακρίβεια την εφαρμογή και τους όρους χρήσης της. Αυτό περιλαμβάνει ιδίως τα είδη των εγκλημάτων και, κατά περίπτωση, το κατάλληλο κατώτατο όριο σοβαρότητας των εν λόγω εγκλημάτων, ώστε, μεταξύ άλλων, να αποκλείονται αποτελεσματικά τα μικροαδικήματα.[15]

3.1.3.2 Η ουσία του θεμελιώδους δικαιώματος στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα που ορίζεται στα άρθρα 7 και 8 του Χάρτη

45. Οι περιορισμοί των θεμελιωδών δικαιωμάτων που είναι επικείμενοι σε κάθε κατάσταση εξακολουθούν να πρέπει να ορίζουν την ουσία του συγκεκριμένου δικαιώματος που πρέπει να γίνεται σεβαστό. Η ουσία αναφέρεται στον ίδιο τον πυρήνα του σχετικού θεμελιώδους δικαιώματος[16]. Η ανθρώπινη αξιοπρέπεια δεν μπορεί να θιγεί ούτε κατά τον περιορισμό δικαιώματος[17].

46. Οι ενδείξεις πιθανής παραβίασης του απαραβίαστου πυρήνα είναι οι ακόλουθες:

- Μια διάταξη που επιβάλλει περιορισμούς ανεξάρτητα από την ατομική συμπεριφορά ενός ατόμου ή τις εξαιρετικές περιστάσεις[18].

[13] ΕΔΔΑ, Shimovolos κατά Ρωσίας, σκέψη 68· Vukota-Bojić κατά Ελβετίας.
[14] ΕΔΔΑ, Piechowicz κατά Πολωνίας, σκέψη 212.
[15] Βλ. π.χ. αποφάσεις του ΔΕΕ στις υποθέσεις C-817/19 Ligue des droits humains, σκέψη 151στ, C-207/16 Ministerio Fiscal, σκέψη 56.
[16] ΔΕΕ C-279/09, RoC 2010 I-13849, σκέψη 60.
[17] Επεξηγήσεις σχετικά με τον Χάρτη των Θεμελιωδών Δικαιωμάτων, Τίτλος I, Επεξήγηση σχετικά με το άρθρο 1, ΕΕ C 303 της 14.12.2007, σ. 17–35.
[18] ΔΕΕ C-601/15, σκέψη 52.

- Η προσφυγή στα δικαστήρια δεν είναι δυνατή ή παρεμποδίζεται[19].
- Πριν από τον αυστηρό περιορισμό, δεν λαμβάνονται υπόψη οι περιστάσεις του ενδιαφερόμενου ατόμου[20].
- Λαμβάνοντας υπόψη τα δικαιώματα που απορρέουν από τα άρθρα 7 και 8 του Χάρτη: Εκτός από την ευρεία συλλογή μεταδεδομένων επικοινωνίας, η απόκτηση της γνώσης του περιεχομένου της ηλεκτρονικής επικοινωνίας θα μπορούσε να παραβιάσει την ουσία των δικαιωμάτων αυτών[21].
- Όσον αφορά τα δικαιώματα βάσει των άρθρων 7, 8 και 11 του Χάρτη: Ρύθμιση η οποία επιβάλλει στους παρόχους πρόσβασης σε υπηρεσίες ηλεκτρονικής επικοινωνίας προς το κοινό και στους παρόχους υπηρεσιών αποθήκευσης τη γενική και χωρίς διάκριση διατήρηση, μεταξύ άλλων, των δεδομένων προσωπικού χαρακτήρα που σχετίζονται με τις υπηρεσίες αυτές[22].
- Ενόψει των δικαιωμάτων που απορρέουν από το άρθρο 8 του Χάρτη: Η έλλειψη βασικών αρχών προστασίας και ασφάλειας των δεδομένων θα μπορούσε επίσης να παραβιάζει τον πυρήνα του δικαιώματος[23].

3.1.3.3 Νόμιμος στόχος

47. Όπως διευκρινίστηκε ήδη στο σημείο 3.1.3., οι περιορισμοί των θεμελιωδών δικαιωμάτων πρέπει να ανταποκρίνονται πραγματικά σε στόχους γενικού συμφέροντος που αναγνωρίζονται από την Ευρωπαϊκή Ένωση ή να ανταποκρίνονται στην ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών των άλλων.

48. Αναγνωρισμένοι από την Ένωση είναι τόσο οι στόχοι που αναφέρονται στο άρθρο 3 της Συνθήκης για την Ευρωπαϊκή Ένωση όσο και άλλα συμφέροντα που προστατεύονται από ειδικές διατάξεις των Συνθηκών[24], δηλαδή, μεταξύ άλλων, ένας χώρος ελευθερίας, ασφάλειας και δικαιοσύνης, πρόληψη και καταστολή της εγκληματικότητας. Στις σχέσεις της με τον ευρύτερο κόσμο, η Ένωση θα πρέπει να συμβάλλει στην ειρήνη και την ασφάλεια και στην προστασία των ανθρωπίνων δικαιωμάτων.

49. Η ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών τρίτων αφορά τα δικαιώματα των ατόμων που προστατεύονται από το δίκαιο της Ευρωπαϊκής Ένωσης ή των κρατών μελών της. Η αξιολόγηση πρέπει να διενεργείται με σκοπό τον συμβιβασμό των απαιτήσεων προστασίας των αντίστοιχων δικαιωμάτων και την επίτευξη δίκαιης ισορροπίας μεταξύ τους[25].·

3.1.3.4 Έλεγχος αναγκαιότητας και αναλογικότητας

50. Όταν πρόκειται για παρεμβάσεις στα θεμελιώδη δικαιώματα, η έκταση της διακριτικής ευχέρειας του εθνικού νομοθέτη και του νομοθέτη της Ένωσης μπορεί να αποδειχθεί περιορισμένη. Αυτό εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του σχετικού τομέα, της φύσης του εν λόγω δικαιώματος που κατοχυρώνεται από τον Χάρτη, της φύσης και της σοβαρότητας της παρέμβασης και του στόχου που επιδιώκεται από την παρέμβαση[26].· Τα νομοθετικά μέτρα πρέπει να είναι κατάλληλα για την επίτευξη των θεμιτών στόχων που επιδιώκονται από την επίμαχη νομοθεσία. Επιπλέον, το μέτρο δεν πρέπει να υπερβαίνει τα όρια του τι είναι κατάλληλο και αναγκαίο για την

[19] ΔΕΕ C-400/10, RoC 2010 I-08965, σκέψη. 55.
[20] ΔΕΕ C-408/03, RoC 2006 I-02647, σκέψη 68.
[21] ΔΕΕ - 203/15 - Tele2 Sverige, σκέψη. 101 με παραπομπή στο ΔΕΕ - C-293/12 και C-594/12, σκέψη 39.
[22] ΔΕΕ C-512/18, La Quadrature du Net, σκέψεις 209 και εξής.
[23] ΔΕΕ - C-594/12, σκέψη 40.
[24] Επεξηγήσεις σχετικά με τον Χάρτη των Θεμελιωδών Δικαιωμάτων, Τίτλος I, Επεξήγηση σχετικά με το άρθρο 52, ΕΕ C 303 της 14.12.2007, σ. 17–35.
[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.
[26] ΔΕΕ - C-594/12, σκέψη 47 με τις ακόλουθες πηγές: βλ. κατ' αναλογία, όσον αφορά το άρθρο 8 της ΕΣΔΑ, Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, S. και Marper κατά Ηνωμένου Βασιλείου [τμήμα μείζονος συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, σκέψη 102, ECHR 2008-V.

επίτευξη των εν λόγω στόχων[27]. Ένας στόχος γενικού συμφέροντος —όσο θεμελιώδης και αν είναι— δεν δικαιολογεί από μόνος του τον περιορισμό ενός θεμελιώδους δικαιώματος[28].·

51. Σύμφωνα με την πάγια νομολογία του ΔΕΕ, οι αποκλίσεις και οι περιορισμοί της προστασίας των δεδομένων προσωπικού χαρακτήρα δεν πρέπει να υπερβαίνουν τα όρια του απολύτως αναγκαίου[29]. Αυτό σημαίνει επίσης ότι δεν υπάρχουν διαθέσιμα λιγότερο παρεμβατικά μέσα για την επίτευξη του σκοπού. Πρέπει να εντοπιστούν και να αξιολογηθούν προσεκτικά πιθανές εναλλακτικές λύσεις, όπως —ανάλογα με τον επιδιωκόμενο σκοπό— η πρόσθετη στελέχωση, η συχνότερη αστυνόμευση ή ο πρόσθετος φωτισμός των δρόμων. Τα νομοθετικά μέτρα θα πρέπει να διαφοροποιούν και να στοχεύουν τα άτομα που καλύπτονται από αυτά υπό το πρίσμα του στόχου, π.χ. την καταπολέμηση σοβαρών εγκλημάτων. Εάν καλύπτουν όλα τα άτομα κατά γενικό τρόπο χωρίς τέτοια διαφοροποίηση, περιορισμό ή εξαίρεση, εντείνουν την παρέμβαση[30]. Εντείνουν επίσης την παρέμβαση εάν η επεξεργασία δεδομένων καλύπτει σημαντικό μέρος του πληθυσμού[31].

52. Η προστασία δεδομένων προσωπικού χαρακτήρα, η οποία απορρέει από τη ρητή υποχρέωση που προβλέπει το άρθρο 8, παράγραφος 1, του Χάρτη, αποκτά ιδιαίτερη σημασία για το δικαίωμα στον σεβασμό της ιδιωτικής ζωής που κατοχυρώνεται στο άρθρο 7 του Χάρτη[32]. Η νομοθεσία πρέπει να ορίζει σαφείς και ακριβείς κανόνες που να διέπουν το πεδίο εφαρμογής και την εφαρμογή του εν λόγω μέτρου και να επιβάλλει διασφαλίσεις ώστε τα πρόσωπα των οποίων τα δεδομένα υποβλήθηκαν σε επεξεργασία να διαθέτουν επαρκείς εγγυήσεις για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν από τον κίνδυνο κατάχρησης και από οποιαδήποτε παράνομη πρόσβαση ή χρήση των εν λόγω δεδομένων[33]. Η ανάγκη για τέτοιες διασφαλίσεις είναι ακόμη μεγαλύτερη όταν τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε αυτόματη επεξεργασία και όταν υπάρχει σημαντικός κίνδυνος παράνομης πρόσβασης στα δεδομένα[34]. Επιπλέον, η εσωτερική ή εξωτερική, π.χ. δικαστική, έγκριση της εγκατάστασης τεχνολογίας αναγνώρισης προσώπου μπορεί επίσης να συμβάλει ως διασφάλιση και μπορεί να αποδειχθεί αναγκαία σε ορισμένες περιπτώσεις σοβαρής παρέμβασης.[35]

53. Οι κανόνες που θεσπίζονται πρέπει να προσαρμόζονται στη συγκεκριμένη κατάσταση, π.χ. στην ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία, στη φύση των δεδομένων[36]και στον κίνδυνο παράνομης πρόσβασης στα δεδομένα. Αυτό απαιτεί κανόνες που θα χρησιμεύουν, ιδίως, για

[27] ΔΕΕ - C-594/12, σκέψη 46 με τις ακόλουθες πηγές: Υπόθεση C-343/09 Afton Chemical EU:C:2010:419, σκέψη 45· Volker und Markus Schecke και Eifert EU:C:2010:662, σκέψη 74· υποθέσεις C-581/10 και C-629/10 Nelson κ.λπ. EU:C:2012:657, σκέψη 71· υπόθεση C-283/11 Sky Österreich EU:C:2013:28, σκέψη 50· και υπόθεση C-101/12 Schaible EU:C:2013:661, σκέψη 29.

[28] ΔΕΕ - C-594/12, σκέψη 51.

[29] ΔΕΕ - C-594/12, σκέψη 52, με τις ακόλουθες πηγές: Υπόθεση C-473/12 IPI EU:C:2013:715, σκέψη 39 και την εκεί παρατιθέμενη νομολογία.

[30] ΔΕΕ - C-594/12, σκέψη 57.

[31] ΔΕΕ - C-594/12, σκέψη 56.

[32] ΔΕΕ - C-594/12, σκέψη 53.

[33] ΔΕΕ - C-594/12, σκέψη 54, με τις ακόλουθες πηγές: βλ. κατ' αναλογία, όσον αφορά το άρθρο 8 της ΕΣΔΑ, Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, Liberty κ.λπ. κατά Ηνωμένου Βασιλείου, 1 Ιουλίου 2008, προσφυγή αριθ. 58243/00, σκέψεις 62 και 63· Rotaru κατά Ρουμανίας, σκέψεις 57 έως 59, και S. και Marper κατά Ηνωμένου Βασιλείου, σκέψη 99.

[34] ΔΕΕ - C-594/12, σκέψη 55, με τις ακόλουθες πηγές: βλ., κατ' αναλογία, όσον αφορά το άρθρο 8 της ΕΣΔΑ, S. και Marper κατά Ηνωμένου Βασιλείου, σκέψη 103, και M. K. κατά Γαλλίας, 18 Απριλίου 2013, προσφυγή αριθ. 19522/09, σκέψη 35.

[35] ΕΔΔΑ, απόφαση Szabó και Vissy κατά Ουγγαρίας, σκέψεις 73-77.

[36] Βλ. επίσης τις αυξημένες απαιτήσεις για τεχνικά και οργανωτικά μέτρα κατά την επεξεργασία ειδικών κατηγοριών δεδομένων, άρθρο 29 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

τη ρύθμιση της προστασίας και της ασφάλειας των εν λόγω δεδομένων με σαφή και αυστηρό τρόπο, ώστε να διασφαλίζεται η πλήρης ακεραιότητα και εμπιστευτικότητά τους[37].

54. Όσον αφορά τη σχέση μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, δεν θα πρέπει να επιτρέπεται στους εκτελούντες την επεξεργασία να λαμβάνουν υπόψη μόνο οικονομικές παραμέτρους κατά τον καθορισμό του επιπέδου ασφάλειας που εφαρμόζουν στα δεδομένα προσωπικού χαρακτήρα· κάτι τέτοιο θα μπορούσε να θέσει σε κίνδυνο ένα επαρκώς υψηλό επίπεδο προστασίας[38].

55. Μια νομοθετική πράξη πρέπει να θεσπίζει ουσιαστικές και διαδικαστικές προϋποθέσεις και αντικειμενικά κριτήρια για τον καθορισμό των ορίων της πρόσβασης των αρμόδιων αρχών στα δεδομένα και τη μετέπειτα χρήσης τους. Για τους σκοπούς της πρόληψης, της ανίχνευσης ή της ποινικής δίωξης, τα σχετικά αδικήματα θα πρέπει να θεωρούνται αρκούντως σοβαρά ώστε να δικαιολογούν την έκταση και τη σοβαρότητα των εν λόγω παρεμβάσεων στα θεμελιώδη δικαιώματα που κατοχυρώνονται, για παράδειγμα, στα άρθρα 7 και 8 του Χάρτη[39].

56. Τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να διασφαλίζει τη δυνατότητα εφαρμογής και την ισχύ των κανόνων της ΕΕ για την προστασία των δεδομένων, ιδίως εκείνων που προβλέπονται στο άρθρο 8 του Χάρτη, το οποίο ορίζει ότι η συμμόρφωση με τις απαιτήσεις προστασίας και ασφάλειας υπόκειται στον έλεγχο ανεξάρτητης αρχής. Ο γεωγραφικός τόπος στον οποίο πραγματοποιείται η επεξεργασία μπορεί σε μια τέτοια περίπτωση να είναι σημαντικός[40].

57. Όσον αφορά τα διάφορα στάδια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, θα πρέπει να γίνεται διάκριση μεταξύ των κατηγοριών δεδομένων με βάση την πιθανή χρησιμότητά τους για τους σκοπούς του επιδιωκόμενου στόχου ή σύμφωνα με τα ενδιαφερόμενα άτομα[41]. Ο καθορισμός των προϋποθέσεων της επεξεργασίας, για παράδειγμα, ο καθορισμός της περιόδου διατήρησης, πρέπει να βασίζεται σε αντικειμενικά κριτήρια προκειμένου να διασφαλίζεται ότι η παρέμβαση περιορίζεται σε ό,τι είναι απολύτως αναγκαίο[42].

58. Με βάση κάθε κατάσταση, η αξιολόγηση της αναγκαιότητας και της αναλογικότητας πρέπει να προσδιορίζει και να εξετάζει όλες τις επιπτώσεις που εμπίπτουν στο πεδίο εφαρμογής άλλων θεμελιωδών δικαιωμάτων, όπως η ανθρώπινη αξιοπρέπεια σύμφωνα με το άρθρο 1 του Χάρτη, η ελευθερία της σκέψης, της συνείδησης και της θρησκείας σύμφωνα με το άρθρο 10 του Χάρτη, η ελευθερία της έκφρασης σύμφωνα με το άρθρο 11 του Χάρτη, καθώς και η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι σύμφωνα με το άρθρο 12 του Χάρτη.

59. Επιπλέον, πρέπει να ληφθεί υπόψη ως σοβαρό ζήτημα ότι, εάν τα δεδομένα υποβάλλονται σε συστηματική επεξεργασία χωρίς τη γνώση των υποκειμένων των δεδομένων, είναι πιθανό να δημιουργηθεί ένα γενικό αίσθημα συνεχούς παρακολούθησης[43]. Αυτό μπορεί να οδηγήσει σε αποτρεπτικά αποτελέσματα όσον αφορά ορισμένα ή όλα τα σχετικά θεμελιώδη δικαιώματα.

60. Προκειμένου να διευκολύνουν και να καταστήσουν λειτουργική την αξιολόγηση της αναγκαιότητας και της αναλογικότητας σε νομοθετικά μέτρα που σχετίζονται με την αναγνώριση προσώπου στον τομέα της επιβολής του νόμου, οι εθνικοί και ενωσιακοί νομοθέτες θα μπορούσαν να αξιοποιήσουν

[37] ΔΕΕ - C-594/12, σκέψη 66.
[38] ΔΕΕ - C-594/12, σκέψη 67.
[39] ΔΕΕ - C-594/12, σκέψεις 60 και 61.
[40] ΔΕΕ - C-594/12, σκέψη 68.
[41] ΔΕΕ - C-594/12, σκέψη 63.
[42] ΔΕΕ - C-594/12, σκέψη 64.
[43] ΔΕΕ - C-594/12, σκέψη 37.

τα διαθέσιμα πρακτικά εργαλεία που έχουν σχεδιαστεί ειδικά γι' αυτό το έργο. Ειδικότερα, θα μπορούσε να χρησιμοποιηθεί η εργαλειοθήκη για την αναγκαιότητα και την αναλογικότητα[44] που παρέχεται από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων.

3.1.3.5 Άρθρο 52 παράγραφος 3, άρθρο 53 του Χάρτη (επίπεδο προστασίας, επίσης σε σχέση με εκείνο της ΕΣΔΑ)

61. Σύμφωνα με το άρθρο 52 παράγραφος 3 και το άρθρο 53 του Χάρτη, η έννοια και εμβέλεια των δικαιωμάτων του Χάρτη που αντιστοιχούν στα δικαιώματα που εγγυάται η ΕΣΔΑ πρέπει να είναι ίδιες με εκείνες που τους αποδίδει η ΕΣΔΑ. Ενώ, ειδικότερα, για το άρθρο 7 του Χάρτη μπορεί να βρεθεί ισοδύναμο στην ΕΣΔΑ, αυτό δεν ισχύει για το άρθρο 8[45]του Χάρτη. Το άρθρο 52 παράγραφος 3 του Χάρτη δεν εμποδίζει το δίκαιο της Ένωσης να παρέχει ευρύτερη προστασία. Δεδομένου ότι η ΕΣΔΑ δεν αποτελεί νομική πράξη που έχει ενσωματωθεί επίσημα στο δίκαιο της ΕΕ, η νομοθεσία της ΕΕ πρέπει να θεσπίζεται υπό το πρίσμα των θεμελιωδών δικαιωμάτων του Χάρτη[46].

62. Σύμφωνα με το άρθρο 8 της ΕΣΔΑ, δεν επιτρέπεται παρέμβαση δημόσιας αρχής στην άσκηση αυτού του δικαιώματος σεβασμού της ιδιωτικής και οικογενειακής ζωής, εκτός εάν η εν λόγω παρέμβαση προβλέπεται από τον νόμο και αποτελεί μέτρο το οποίο, σε μια δημοκρατική κοινωνία, είναι αναγκαίο για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και ελευθεριών τρίτων.

63. Η ΕΣΔΑ καθορίζει επίσης πρότυπα όσον αφορά τον τρόπο με τον οποίο μπορούν να επιβάλλονται περιορισμοί. Μια βασική απαίτηση, εκτός από το κράτος δικαίου, είναι η προβλεψιμότητα. Προκειμένου να εκπληρωθεί η απαίτηση της προβλεψιμότητας, το δίκαιο πρέπει να είναι αρκούντως σαφές ως προς τους όρους του, ώστε να ενημερώνει καταλλήλως τα άτομα σχετικά με τις περιστάσεις και τους όρους υπό τους οποίους οι αρχές μπορούν να προβαίνουν στην εφαρμογή τέτοιων μέτρων[47]. Η εν λόγω απαίτηση αναγνωρίζεται από το ΔΕΕ και τη νομοθεσία της ΕΕ για την προστασία των δεδομένων (βλ. ενότητα 3.2.1.1).

64. Περαιτέρω, διευκρινίζοντας τα δικαιώματα του άρθρου 8 της ΕΣΔΑ, πρέπει επίσης να τηρούνται πλήρως οι διατάξεις της Σύμβασης περί προστασίας του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα[48]. Ωστόσο, πρέπει να θεωρηθεί ότι οι εν λόγω διατάξεις αντιπροσωπεύουν μόνο ένα ελάχιστο πρότυπο ενόψει του ισχύοντος δικαίου της Ένωσης.

3.2 Ειδικό νομικό πλαίσιο — η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου

65. Στην οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου προβλέπεται ένα ορισμένο πλαίσιο σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου. Καταρχάς, το

[44] Ευρωπαίος Επόπτης Προστασίας Δεδομένων, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit» (Αξιολόγηση της αναγκαιότητας των μέτρων που περιορίζουν το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα: Εργαλειοθήκη), 11.4.2017, Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ), «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» (Κατευθυντήριες γραμμές του ΕΕΠΔ για την αξιολόγηση της αναλογικότητας των μέτρων που περιορίζουν τα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα), 19.12.2019.

[45] ΔΕΕ - C-203/15 - Tele2 Sverige, σκέψη 129.

[46] ΔΕΕ – C-311/18, σκέψη 99.

[47] Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, Απόφαση, ΥΠΟΘΕΣΗ COPLAND κατά ΗΝΩΜΕΝΟΥ ΒΑΣΙΛΕΙΟΥ, 03/04/2007, Προσφυγή υπ'αρ. 62617/00, σκέψη 46.

[48] ETS αριθ. 108.

άρθρο 3 παράγραφος 13 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ορίζει τον όρο «βιομετρικά δεδομένα»[49]. Για λεπτομέρειες, βλ. ενότητα 2.1 ανωτέρω. Δεύτερον, το άρθρο 8 παράγραφος 2 διευκρινίζει ότι, προκειμένου οποιαδήποτε επεξεργασία να είναι σύννομη, πρέπει —πέραν του να είναι απαραίτητη για τους σκοπούς που αναφέρονται στο άρθρο 1 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου— να ρυθμίζεται στο εθνικό δίκαιο το οποίο καθορίζει τουλάχιστον τους στόχους της επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και τους σκοπούς της επεξεργασίας. Περαιτέρω διατάξεις ιδιαίτερης σημασίας όσον αφορά τα βιομετρικά δεδομένα είναι τα άρθρα 10 και 11 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Το άρθρο 10 πρέπει να ερμηνεύεται σε συνδυασμό με το άρθρο 8 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου[50]. Οι αρχές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, θα πρέπει πάντα να τηρούνται και κάθε αξιολόγηση της πιθανής βιομετρικής επεξεργασίας μέσω τεχνολογίας αναγνώρισης προσώπου θα πρέπει να καθοδηγείται από αυτές.

3.2.1 Επεξεργασία ειδικών κατηγοριών δεδομένων για σκοπούς επιβολής του νόμου

66. Σύμφωνα με το άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η επεξεργασία ειδικών κατηγοριών δεδομένων, όπως βιομετρικών δεδομένων, επιτρέπεται μόνο όταν είναι απολύτως αναγκαία και με την επιφύλαξη των κατάλληλων διασφαλίσεων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Επιπλέον, επιτρέπεται μόνο όταν προβλέπεται από το δίκαιο της Ένωσης ή των κρατών μελών, επιβάλλεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου ή όταν η επεξεργασία αυτή αφορά δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων. Αυτή η γενική ρήτρα υπογραμμίζει τον ευαίσθητο χαρακτήρα της επεξεργασίας ειδικών κατηγοριών δεδομένων.

3.2.1.1 Επιτρέπεται από το δίκαιο της Ένωσης ή των κρατών μελών

67. Όσον αφορά τον αναγκαίο χαρακτήρα του νομοθετικού μέτρου, στην αιτιολογική σκέψη 33 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αναφέρεται ότι «[ό]που η παρούσα οδηγία παραπέμπει στη νομοθεσία των κρατών μελών, σε νομική βάση ή νομοθετικό μέτρο, αυτό δεν προϋποθέτει απαραιτήτως νομοθετική πράξη εγκεκριμένη από κοινοβούλιο, με την επιφύλαξη των απαιτήσεων της συνταγματικής τάξης του εκάστοτε κράτους μέλους.»[51]

68. Σύμφωνα με το άρθρο 52 παράγραφος 1 του Χάρτη, κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται από τον Χάρτη «προβλέπεται από το νόμο». Αυτό απηχεί την έκφραση «προβλέπεται υπό του νόμου» του άρθρου 8 παράγραφος 2 της ΕΣΔΑ, η οποία συνεπάγεται

[49] Άρθρο 3 παράγραφος 13 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου: «Βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

[50] WP258, Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου [οδηγία (ΕΕ) 2016/680], σ. 7.

[51] Ο χαρακτήρας των εκάστοτε νομοθετικών μέτρων πρέπει να είναι σύμφωνος με το ενωσιακό ή το εθνικό δίκαιο. Ανάλογα με τον βαθμό παρέμβασης του περιορισμού, θα μπορούσε να απαιτηθεί ένα συγκεκριμένο νομοθετικό μέτρο, λαμβάνοντας υπόψη το επίπεδο του κανόνα, σε εθνικό επίπεδο.

όχι μόνο συμμόρφωση προς το εφαρμοστέο δίκαιο αλλά αφορά και την ποιότητα του εν λόγω δικαίου με την επιφύλαξη της φύσης της πράξης, μέσω της απαίτησης συμμόρφωσης προς το κράτος δικαίου.

69. Η αιτιολογική σκέψη 33 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αναφέρει περαιτέρω ότι «[ω]στόσο, η εν λόγω νομοθεσία των κρατών μελών, η νομική βάση ή το νομοθετικό μέτρο θα πρέπει να είναι διατυπωμένα με σαφήνεια και ακρίβεια και η εφαρμογή τους να είναι προβλέψιμη για όσους υπόκεινται σε αυτά, όπως απαιτείται από τη νομολογία του Δικαστηρίου και του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων. Η νομοθεσία των κρατών μελών που ρυθμίζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής της παρούσας οδηγίας θα πρέπει να καθορίζει τουλάχιστον τους στόχους, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, τους σκοπούς της επεξεργασίας και τις διαδικασίες για τη διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα και τις διαδικασίες για την καταστροφή τους».

70. Το εθνικό δίκαιο πρέπει να είναι αρκούντως σαφές στη διατύπωσή του ώστε να ενημερώνει καταλλήλως τα υποκείμενα των δεδομένων σχετικά με τις περιστάσεις και τους όρους υπό τους οποίους οι υπεύθυνοι επεξεργασίας μπορούν να προβαίνουν στην εφαρμογή τέτοιων μέτρων. Αυτό περιλαμβάνει πιθανές προϋποθέσεις για την επεξεργασία, όπως συγκεκριμένα είδη αποδεικτικών στοιχείων, καθώς και την ανάγκη δικαστικής ή εσωτερικής έγκρισης. Το εκάστοτε δίκαιο μπορεί να είναι ουδέτερο ως προς την τεχνολογία, στον βαθμό που αντιμετωπίζονται επαρκώς οι συγκεκριμένοι κίνδυνοι και τα χαρακτηριστικά της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα συστήματα τεχνολογίας αναγνώρισης προσώπου. Σύμφωνα με την οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου και τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), είναι πράγματι σημαντικό τα νομοθετικά μέτρα, τα οποία αποσκοπούν στην παροχή νομικής βάσης για ένα μέτρο αναγνώρισης προσώπου, να είναι προβλέψιμα για τα υποκείμενα των δεδομένων.

71. Ένα νομοθετικό μέτρο δεν μπορεί να επικαλεστεί ως νόμος που επιτρέπει την επεξεργασία βιομετρικών δεδομένων μέσω τεχνολογίας αναγνώρισης προσώπου για σκοπούς επιβολής του νόμου εάν αποτελεί απλή μεταφορά της γενικής ρήτρας του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

72. Εκτός από τα βιομετρικά δεδομένα, το άρθρο 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ρυθμίζει την επεξεργασία άλλων ειδικών κατηγοριών δεδομένων, όπως ο σεξουαλικός προσανατολισμός, τα πολιτικά φρονήματα και οι θρησκευτικές πεποιθήσεις, καλύπτοντας έτσι ένα ευρύ φάσμα επεξεργασίας. Επιπλέον, μια τέτοια διάταξη θα στερούνταν ειδικών απαιτήσεις που να υποδεικνύουν τις περιστάσεις και τις προϋποθέσεις υπό τις οποίες οι αρχές επιβολής του νόμου εξουσιοδοτούνται να καταφεύγουν στη χρήση τεχνολογίας αναγνώρισης προσώπου. Λόγω της αναφοράς σε άλλα είδη δεδομένων και της ρητής ανάγκης για ειδικές διασφαλίσεις χωρίς περαιτέρω προδιαγραφές, η εθνική διάταξη για τη μεταφορά του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου στο εθνικό δίκαιο — με παρόμοια γενική και αφηρημένη διατύπωση— δεν μπορεί να χρησιμοποιηθεί ως νομική βάση για την επεξεργασία βιομετρικών δεδομένων που περιλαμβάνουν αναγνώριση προσώπου, καθώς θα στερούνταν ακρίβειας και προβλεψιμότητας. Σύμφωνα με το άρθρο 28 παράγραφος 2 ή το άρθρο 46 παράγραφος 1 στοιχείο γ) της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, προτού ο νομοθέτης δημιουργήσει νέα νομική βάση για οποιαδήποτε μορφή επεξεργασίας βιομετρικών δεδομένων με τη χρήση αναγνώρισης προσώπου, θα πρέπει να συμβουλευτεί την εθνική εποπτική αρχή προστασίας δεδομένων.

3.2.1.2 Απολύτως αναγκαία

73. Η επεξεργασία μπορεί να θεωρηθεί «απολύτως αναγκαία» μόνον εάν η παρέμβαση στην προστασία των δεδομένων προσωπικού χαρακτήρα και οι περιορισμοί της περιορίζονται σε ό,τι είναι απολύτως αναγκαίο[52]. Η προσθήκη του όρου «απολύτως» σημαίνει ότι πρόθεση του νομοθέτη ήταν η επεξεργασία ειδικών κατηγοριών δεδομένων να πραγματοποιείται μόνο υπό όρους ακόμη αυστηρότερους από τους όρους αναγκαιότητας (βλ. ανωτέρω, σημείο 3.1.3.4). Η εν λόγω απαίτηση θα πρέπει να ερμηνεύεται ως απαραίτητη. Περιορίζει το περιθώριο εκτίμησης που επιτρέπεται στην αρχή επιβολής του νόμου κατά τον έλεγχο αναγκαιότητας στο απολύτως ελάχιστο. Σύμφωνα με την πάγια νομολογία του ΔΕΕ, η προϋπόθεση της «απόλυτης αναγκαιότητας» συνδέεται επίσης στενά με την απαίτηση αντικειμενικών κριτηρίων για τον καθορισμό των περιστάσεων και των προϋποθέσεων υπό τις οποίες μπορεί να πραγματοποιηθεί η επεξεργασία, αποκλείοντας έτσι κάθε επεξεργασία γενικού ή συστηματικού χαρακτήρα[53].

3.2.1.3 Προδήλως δημοσιοποιημένα

74. Κατά την αξιολόγηση του κατά πόσον η επεξεργασία αφορά δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων, θα πρέπει να υπενθυμιστεί ότι η φωτογραφία αυτή καθαυτή δεν θεωρείται συστηματικά ως βιομετρικό δεδομένο[54]. Επομένως, το γεγονός ότι μια φωτογραφία έχει προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων δεν συνεπάγεται ότι τα σχετικά βιομετρικά δεδομένα, τα οποία μπορούν να ανακτηθούν από τη φωτογραφία με συγκεκριμένα τεχνικά μέσα, θεωρείται ότι έχουν προδήλως δημοσιοποιηθεί.

75. Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα εν γένει, για να θεωρηθεί ότι τα βιομετρικά δεδομένα έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων, το υποκείμενο των δεδομένων πρέπει να έχει καταστήσει σκόπιμα το βιομετρικό υπόδειγμα (και όχι απλώς μια εικόνα προσώπου) ελεύθερα προσβάσιμο και δημόσιο μέσω μιας ανοικτής πηγής. Εάν ένας τρίτος αποκαλύψει τα βιομετρικά δεδομένα, δεν μπορεί να θεωρηθεί ότι τα δεδομένα έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

76. Επιπλέον, δεν αρκεί η ερμηνεία της συμπεριφοράς ενός υποκειμένου των δεδομένων προκειμένου να θεωρηθεί ότι τα βιομετρικά δεδομένα έχουν προδήλως δημοσιοποιηθεί. Για παράδειγμα, στην περίπτωση των κοινωνικών δικτύων ή των διαδικτυακών πλατφορμών, το ΕΣΠΔ θεωρεί ότι το γεγονός ότι το υποκείμενο των δεδομένων δεν ενεργοποίησε ή δεν έθεσε συγκεκριμένα χαρακτηριστικά προστασίας της ιδιωτικής ζωής δεν αρκεί για να θεωρηθεί ότι το εν λόγω υποκείμενο των δεδομένων έχει προδήλως δημοσιοποιήσει τα προσωπικά του δεδομένα και ότι τα δεδομένα αυτά (π.χ. φωτογραφίες) μπορούν να υποβληθούν σε επεξεργασία σε βιομετρικά υποδείγματα και να χρησιμοποιηθούν για σκοπούς ταυτοποίησης χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων. Γενικότερα, οι προεπιλεγμένες ρυθμίσεις μιας υπηρεσίας, π.χ. η δημοσιοποίηση υποδειγμάτων, ή η απουσία επιλογής, π.χ. τα υποδείγματα δημοσιοποιούνται χωρίς ο χρήστης να

[52] Συνεκτική νομολογία σχετικά με το θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής, βλ. ΔΕΕ, Υπόθεση C-73/07, σκέψη 56 (Satakunnan Markkinapörssi και Satamedia)· ΔΕΕ, Υποθέσεις C-92/09 και C-93/09 σκέψη 77 (Schecke και Eifert)· ΔΕΕ - C-594/12, σκέψη 52 (Ψηφιακά δικαιώματα)· ΔΕΕ Υπόθεση C-362/14 σκέψη 92 (Schrems).

[53] ΔΕΕ, Υπόθεση C-623/17, σκέψη 78.

[54] Βλ. αιτιολογική σκέψη 51 του ΓΚΠΔ: « η επεξεργασία φωτογραφιών δεν θα πρέπει συστηματικά να θεωρείται ότι είναι επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, καθώς αυτές καλύπτονται από τον ορισμό των βιομετρικών δεδομένων μόνο σε περίπτωση επεξεργασίας μέσω ειδικών τεχνικών μέσων που επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ή επαλήθευση της ταυτότητας ενός φυσικού προσώπου. »

είναι σε θέση να τροποποιήσει την εν λόγω ρύθμιση, σε καμία περίπτωση δεν θα πρέπει να εκλαμβάνονται ως δεδομένα που έχουν προδήλως δημοσιοποιηθεί.

3.2.2 Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

77. Το άρθρο 11 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου προβλέπει την υποχρέωση των κρατών μελών να απαγορεύουν γενικά τις αποφάσεις που βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει δυσμενή έννομα αποτελέσματα για το υποκείμενο των δεδομένων ή το θίγει σε μεγάλο βαθμό. Ως εξαίρεση από αυτή τη γενική απαγόρευση, η εν λόγω επεξεργασία μπορεί να είναι δυνατή μόνον εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή των κρατών μελών στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει κατάλληλες διασφαλίσεις υπέρ των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων, τουλάχιστον δε το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης εκ μέρους του υπεύθυνου επεξεργασίας. Μπορεί να χρησιμοποιείται μόνο περιοριστικά. Το όριο αυτό ισχύει για τις συνήθεις (και όχι τις ειδικές) κατηγορίες δεδομένων προσωπικού χαρακτήρα. Για την εξαίρεση βάσει του άρθρου 11 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ισχύει ακόμη υψηλότερο όριο και πιο περιοριστική χρήση. Τονίζει εκ νέου ότι οι αποφάσεις που αναφέρονται στο πρώτο εδάφιο δεν πρέπει να βασίζονται σε ειδικές κατηγορίες δεδομένων, δηλαδή ιδίως σε βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου. Εξαίρεση μπορεί να προβλεφθεί μόνο εάν εφαρμόζονται κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων του υποκειμένου των δεδομένων και των ελευθεριών και των έννομων συμφερόντων του εκάστοτε φυσικού προσώπου. Η εν λόγω εξαίρεση πρέπει να ερμηνεύεται επιπλέον και υπό το πρίσμα των διατάξεων του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

78. Ανάλογα με το σύστημα τεχνολογίας αναγνώρισης προσώπου, ακόμη και η ανθρώπινη παρέμβαση που αξιολογεί τα αποτελέσματα της τεχνολογίας αναγνώρισης προσώπου ενδέχεται να μην παρέχει κατ' ανάγκη από μόνη της επαρκή εγγύηση για τον σεβασμό των δικαιωμάτων των ατόμων και ιδίως του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, λαμβάνοντας υπόψη την πιθανή μεροληψία και το σφάλμα που μπορεί να προκύψει από την ίδια την επεξεργασία. Επιπλέον, η ανθρώπινη παρέμβαση μπορεί να θεωρηθεί ως εγγύηση μόνο εάν το άτομο που παρεμβαίνει μπορεί να αμφισβητήσει κριτικά τα αποτελέσματα της τεχνολογίας αναγνώρισης προσώπου κατά τη διάρκεια της ανθρώπινης παρέμβασης. Είναι ζωτικής σημασίας να δοθεί η δυνατότητα στο άτομο να κατανοήσει το σύστημα τεχνολογίας αναγνώρισης προσώπου και τα όριά του, καθώς και να ερμηνεύσει σωστά τα αποτελέσματά του. Είναι επίσης απαραίτητο να δημιουργηθεί ένας χώρος εργασίας κι ένας οργανισμός που να εξουδετερώνει τις επιπτώσεις της μεροληψίας της αυτοματοποίησης και να αποφεύγει την προώθηση της άκριτης αποδοχής των αποτελεσμάτων, π.χ. λόγω πίεσης χρόνου, επαχθών διαδικασιών, πιθανών αρνητικών επιπτώσεων στη σταδιοδρομία κ.λπ.

79. Σύμφωνα με το άρθρο 11 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η κατάρτιση προφίλ που έχει ως αποτέλεσμα διακρίσεις εις βάρος φυσικών προσώπων με βάση ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως βιομετρικά δεδομένα, απαγορεύεται σύμφωνα με το δίκαιο της Ένωσης. Σύμφωνα με το άρθρο 3 παράγραφος 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, ως «κατάρτιση προφίλ» νοείται οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη

πτυχών που αφορούν στην απόδοση στην εργασία, στην οικονομική κατάσταση, στην υγεία, στις προσωπικές προτιμήσεις, στα ενδιαφέροντα, στην αξιοπιστία, στη συμπεριφορά, στη θέση ή στις μετακινήσεις του εν λόγω φυσικού προσώπου. Κατά την εξέταση του εάν προβλέπονται κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων του υποκειμένου των δεδομένων και των ελευθεριών και των έννομων συμφερόντων του εκάστοτε φυσικού προσώπου, πρέπει να λαμβάνεται υπόψη ότι η χρήση του συστήματος τεχνολογίας αναγνώρισης προσώπου μπορεί να οδηγήσει σε κατάρτιση προφίλ, ανάλογα με τον τρόπο και τον σκοπό για τον οποίο εφαρμόζεται η τεχνολογία αναγνώρισης προσώπου. Σε κάθε περίπτωση, σύμφωνα με το δίκαιο της Ένωσης και το άρθρο 11 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η κατάρτιση προφίλ που έχει ως αποτέλεσμα διακρίσεις εις βάρος φυσικών προσώπων με βάση τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα απαγορεύεται.

3.2.3 Κατηγορίες των υποκειμένων των δεδομένων

80. Το άρθρο 6 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αφορά την αναγκαιότητα διάκρισης μεταξύ των διαφορετικών κατηγοριών υποκειμένων των δεδομένων. Η εν λόγω διάκριση πρέπει να γίνεται κατά περίπτωση και στον βαθμό του εφικτού. Πρέπει να έχει αντίκτυπο στον τρόπο επεξεργασίας των δεδομένων. Από τα παραδείγματα που παρέχονται στο άρθρο 6 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου μπορεί να συναχθεί ότι, κατά κανόνα, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πληροί τα κριτήρια της αναγκαιότητας και της αναλογικότητας όσον αφορά και την κατηγορία των υποκειμένων των δεδομένων[55]. Μπορεί επίσης να συναχθεί το συμπέρασμα ότι, όσον αφορά τα υποκείμενα των δεδομένων για τα οποία δεν υπάρχουν αποδεικτικά στοιχεία που να υποδεικνύουν ότι η συμπεριφορά τους μπορεί να συνδέεται, ακόμη και έμμεσα ή εξ αποστάσεως, με τον θεμιτό σκοπό σύμφωνα με την οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, κατά πάσα πιθανότητα η παρέμβαση δεν είναι δικαιολογημένη[56]. Εάν δεν γίνεται διάκριση, σύμφωνα με το άρθρο 6 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, κατά περίπτωση και στον βαθμό του εφικτού, η εξαίρεση από τον κανόνα του άρθρου 6 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου πρέπει να εξετάζεται αυστηρά κατά την αξιολόγηση της αναγκαιότητας και της αναλογικότητας της παρέμβασης. Η διάκριση μεταξύ των διαφόρων κατηγοριών υποκειμένων των δεδομένων φαίνεται να αποτελεί βασική απαίτηση όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα που περιλαμβάνει αναγνώριση προσώπου, λαμβάνοντας επίσης υπόψη τα πιθανά ψευδώς θετικά ή ψευδώς αρνητικά αποτελέσματα αναζήτησης, τα οποία μπορούν να έχουν σημαντικές επιπτώσεις για τα υποκείμενα των δεδομένων, καθώς και κατά τη διάρκεια μιας έρευνας.

81. Όπως προαναφέρθηκε, κατά την εφαρμογή του δικαίου της Ένωσης, πρέπει να τηρούνται οι διατάξεις του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, βλ. άρθρο 52 του Χάρτη. Ως εκ τούτου, το πλαίσιο και τα κριτήρια που προβλέπει η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου πρέπει να ερμηνεύονται υπό το πρίσμα του Χάρτη. Οι νομοθετικές πράξεις της ΕΕ και των κρατών μελών της δεν πρέπει να υπολείπονται αυτού του μέτρου και πρέπει να διασφαλίζουν την πλήρη ισχύ του Χάρτη.

[55] Βλ. επίσης ΔΕΕ - C-594/12, σκέψεις 56 - 59.
[56] Βλ. επίσης ΔΕΕ - C-594/12, σκέψη 58.

3.2.4 Δικαιώματά του υποκειμένου των δεδομένων

82. Το ΕΣΠΔ έχει ήδη παράσχει καθοδήγηση σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων στο πλαίσιο του ΓΚΠΔ σε διάφορες πτυχές[57]. Η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ορίζει παρόμοια δικαιώματα των υποκειμένων των δεδομένων και η γενική καθοδήγηση σχετικά με αυτό παρέχεται σε γνώμη της Ομάδας Εργασίας του άρθρου 29, η οποία έχει εγκριθεί από το ΕΣΠΔ[58]. Υπό ορισμένες περιστάσεις, η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου επιτρέπει ορισμένους περιορισμούς αυτών των δικαιωμάτων. Οι παράμετροι για τους εν λόγω περιορισμούς θα αναλυθούν περαιτέρω στην ενότητα 3.2.4.6. «Νόμιμοι περιορισμοί στα δικαιώματα του υποκειμένου των δεδομένων».

83. Ενώ όλα τα δικαιώματα του υποκειμένου των δεδομένων, όπως απαριθμούνται στο κεφάλαιο III της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, εφαρμόζονται φυσικά και στην επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω τεχνολογίας αναγνώρισης προσώπου, το επόμενο κεφάλαιο θα επικεντρωθεί σε ορισμένα από τα δικαιώματα και τις πτυχές που ενδέχεται να παρουσιάζουν ιδιαίτερο ενδιαφέρον για τη λήψη καθοδήγησης. Επιπλέον, το παρόν κεφάλαιο και η ανάλυσή του βασίζονται στην εν λόγω επεξεργασία με τεχνολογία αναγνώρισης προσώπου, η οποία έχει περάσει από τις νομικές απαιτήσεις που περιγράφονται στο προηγούμενο κεφάλαιο.

84. Δεδομένης της φύσης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω τεχνολογίας αναγνώρισης προσώπου (επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα συχνά χωρίς εμφανή αλληλεπίδραση με το υποκείμενο των δεδομένων), ο υπεύθυνος επεξεργασίας πρέπει να εξετάσει προσεκτικά τον τρόπο (ή εάν μπορεί) να συμμορφωθεί με τις απαιτήσεις της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου πριν από την έναρξη οποιασδήποτε επεξεργασίας με τεχνολογία αναγνώρισης προσώπου. Ειδικότερα, αναλύοντας προσεκτικά:

- ποια είναι τα υποκείμενα των δεδομένων (συχνά περισσότερα από εκείνα που αποτελούν τον κύριο στόχο για τον σκοπό της επεξεργασίας),
- τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων ενημερώνονται για την επεξεργασία με τεχνολογία αναγνώρισης προσώπου (βλ. ενότητα 3.2.4.1),
- τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους (εδώ τόσο τα δικαιώματα ενημέρωσης και πρόσβασης όσο και τα δικαιώματα διόρθωσης ή περιορισμού μπορεί να είναι ιδιαίτερα δύσκολο να υποστηριχθούν στην περίπτωση που η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται για όλες τις επαληθεύσεις εκτός από την επαλήθευση 1 προς 1 σε άμεση επαφή με το υποκείμενο των δεδομένων).

3.2.4.1 Γνωστοποίηση των δικαιωμάτων και των πληροφοριών στα υποκείμενα των δεδομένων σε συνοπτική, κατανοητή και εύκολα προσβάσιμη μορφή

85. Η τεχνολογία αναγνώρισης προσώπου ορίζει προκλήσεις όσον αφορά τη διασφάλιση της ενημέρωσης των υποκειμένων των δεδομένων σχετικά με τα βιομετρικά δεδομένα τους που υποβάλλονται σε επεξεργασία. Αποτελεί ιδιαίτερη πρόκληση εάν μια αρχή επιβολής του νόμου αναλύει μέσω

[57] Βλ. για παράδειγμα τις κατευθυντήριες γραμμές με τίτλο «1/2022 EDPB Guidelines on data subject's rights – Right of access» (1/2022 Κατευθυντήριες γραμμές του ΕΣΠΔ σχετικά με τα δικαιώματα του υποκειμένου των δεδομένων — Δικαίωμα πρόσβασης) και «Κατευθυντήριες γραμμές 3/2019 του ΕΣΠΔ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών».
[58] WP258, Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου [οδηγία (ΕΕ) 2016/680].

τεχνολογίας αναγνώρισης προσώπου υλικό βίντεο που προέρχεται από ή παρέχεται από τρίτο μέρος, δεδομένου ότι η αρχή επιβολής του νόμου έχει ελάχιστη δυνατότητα, και τις περισσότερες φορές καμία, να ενημερώσει το υποκείμενο των δεδομένων κατά τη στιγμή της συλλογής (π.χ. μέσω μιας ένδειξης επί τόπου). Οποιοδήποτε υλικό βίντεο που δεν είναι σχετικό με την έρευνα (ή τον σκοπό της επεξεργασίας) θα πρέπει πάντοτε να αφαιρείται ή να ανωνυμοποιείται (π.χ. με θόλωση χωρίς αναδρομική δυνατότητα ανάκτησης των δεδομένων) πριν από την ανάπτυξη οποιασδήποτε επεξεργασίας βιομετρικών δεδομένων, προκειμένου να αποφευχθεί ο κίνδυνος να μην εκπληρωθεί η αρχή της ελαχιστοποίησης του άρθρου 4 παράγραφος 1 στοιχείο ε) της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου και οι υποχρεώσεις ενημέρωσης του άρθρου 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Αποτελεί ευθύνη του υπευθύνου επεξεργασίας να αξιολογήσει ποιες πληροφορίες θα ήταν σημαντικές για το υποκείμενο των δεδομένων κατά την άσκηση των δικαιωμάτων του και να διασφαλίσει την παροχή των αναγκαίων πληροφοριών. Η αποτελεσματική άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων εξαρτάται από την εκπλήρωση των υποχρεώσεων ενημέρωσης του υπεύθυνου επεξεργασίας.

86. Το άρθρο 13 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ορίζει τις ελάχιστες πληροφορίες που πρέπει να παρέχονται στο υποκείμενο των δεδομένων εν γένει. Οι πληροφορίες αυτές μπορεί να παρέχονται μέσω του ιστοτόπου του υπεύθυνου επεξεργασίας, σε έντυπη μορφή (π.χ. φυλλάδιο που διατίθεται κατόπιν αιτήματος) ή μέσω άλλων πηγών εύκολα προσβάσιμων για το υποκείμενο των δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει σε κάθε περίπτωση να διασφαλίζει ότι παρέχονται αποτελεσματικά πληροφορίες τουλάχιστον όσον αφορά τα ακόλουθα στοιχεία:

- την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας, συμπεριλαμβανομένου του υπευθύνου προστασίας δεδομένων,
- τους σκοπούς της επεξεργασίας και το γεγονός ότι πραγματοποιείται επεξεργασία μέσω τεχνολογίας αναγνώρισης προσώπου,
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή και τα στοιχεία επικοινωνίας της εν λόγω αρχής,
- το δικαίωμα υποβολής αιτήματος για πρόσβαση στα δεδομένα προσωπικού χαρακτήρα, διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα και περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

87. Επιπλέον, σε ειδικές περιπτώσεις, όπως ορίζονται στο εθνικό δίκαιο, οι οποίες θα πρέπει να συνάδουν με το άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου[59], όπως για παράδειγμα η επεξεργασία με τεχνολογία αναγνώρισης προσώπου, οι ακόλουθες πληροφορίες πρέπει να παρέχονται απευθείας στο υποκείμενο των δεδομένων:

- τη νομική βάση της επεξεργασίας,
- πληροφορίες σχετικά με το πού συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα εν αγνοία του υποκειμένου των δεδομένων,

[59] Π.χ. το άρθρο 56 παράγραφος 1 του γερμανικού ομοσπονδιακού νόμου περί προστασίας δεδομένων, το οποίο, μεταξύ άλλων, ορίζει ποιες πληροφορίες πρέπει να παρέχονται στα υποκείμενα των δεδομένων σε μυστικές επιχειρήσεις.

- το χρονικό διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

- κατά περίπτωση, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα (μεταξύ άλλων σε τρίτες χώρες ή διεθνείς οργανισμούς).

88. Ενώ το άρθρο 13 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αφορά τις γενικές πληροφορίες που διατίθενται στο κοινό, το άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου αφορά τις πρόσθετες πληροφορίες που πρέπει να παρέχονται σε ένα συγκεκριμένο υποκείμενο των δεδομένων σε συγκεκριμένες περιπτώσεις, για παράδειγμα όταν τα δεδομένα συλλέγονται άμεσα από το υποκείμενο των δεδομένων ή έμμεσα εν αγνοία του υποκειμένου των δεδομένων[60]. Δεν υπάρχει σαφής ορισμός της έννοιας των «συγκεκριμένων περιπτώσεων» στο άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Ωστόσο, αναφέρεται σε καταστάσεις στις οποίες τα υποκείμενα των δεδομένων πρέπει να ενημερωθούν για την επεξεργασία που τα αφορά ειδικά και να τους παρασχεθούν οι κατάλληλες πληροφορίες για την αποτελεσματική άσκηση των δικαιωμάτων τους. Το ΕΣΠΔ θεωρεί ότι, κατά την αξιολόγηση του εάν υφίσταται «συγκεκριμένη περίπτωση», πρέπει να λαμβάνονται υπόψη διάφοροι παράγοντες, μεταξύ άλλων εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται εν αγνοία του υποκειμένου των δεδομένων, καθώς αυτός θα ήταν ο μόνος τρόπος για να μπορούν τα υποκείμενα των δεδομένων να ασκούν αποτελεσματικά τα δικαιώματά τους. Άλλα παραδείγματα «συγκεκριμένων περιπτώσεων» θα μπορούσαν να είναι όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε περαιτέρω επεξεργασία ως υποκείμενα σε διαδικασία διεθνούς ποινικής συνεργασίας ή σε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο μυστικών επιχειρήσεων, όπως ορίζεται στο εθνικό δίκαιο. Επιπλέον, από την αιτιολογική σκέψη 38 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου προκύπτει ότι, εάν η λήψη αποφάσεων πραγματοποιείται αποκλειστικά με βάση την τεχνολογία αναγνώρισης προσώπου, τότε τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τα χαρακτηριστικά της αυτοματοποιημένης λήψης αποφάσεων. Αυτό θα σήμαινε επίσης ότι πρόκειται για συγκεκριμένη περίπτωση κατά την οποία θα πρέπει να παρέχονται πρόσθετες πληροφορίες στο υποκείμενο των δεδομένων σύμφωνα με το άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου[61].

89. Τέλος, πρέπει να σημειωθεί ότι σύμφωνα με το άρθρο 13 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, τα κράτη μέλη μπορούν να θεσπίζουν νομοθετικά μέτρα που περιορίζουν την υποχρέωση παροχής πληροφοριών σε συγκεκριμένες περιπτώσεις για ορισμένους σκοπούς. Αυτό ισχύει στον βαθμό που ένα τέτοιο μέτρο είναι αναγκαίο και αναλογικό σε μια δημοκρατική κοινωνία, λαμβανομένων δεόντως υπόψη των θεμελιωδών δικαιωμάτων και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

[60] WP258, Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου [οδηγία (ΕΕ) 2016/680], σ. 21-22.

[61] Επισημαίνεται επίσης η διαφορά μεταξύ της φράσης «θέτει στη διάθεση του υποκειμένου των δεδομένων» στο άρθρο 13 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου και της φράσης «παρέχει στο υποκείμενο των δεδομένων» στο άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Στο άρθρο 13 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι οι πληροφορίες φτάνουν στο υποκείμενο των δεδομένων, όπου οι δημοσιευμένες πληροφορίες σε έναν ιστότοπο δεν επαρκούν.

3.2.4.2 Δικαίωμα πρόσβασης

90. Γενικά, το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει θετική ή αρνητική επιβεβαίωση οποιασδήποτε επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν και, εάν η απάντηση είναι θετική, την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα αυτά καθαυτά, καθώς και πρόσθετες πληροφορίες, όπως απαριθμούνται στο άρθρο 14 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Όσον αφορά την τεχνολογία αναγνώρισης προσώπου, όταν τα βιομετρικά δεδομένα αποθηκεύονται και συνδέονται με μια ταυτότητα και μέσω αλφαριθμητικών δεδομένων, αυτό θα πρέπει να επιτρέπει στην αρμόδια αρχή να επιβεβαιώνει ένα αίτημα πρόσβασης βάσει αναζήτησης από τα εν λόγω αλφαριθμητικά δεδομένα και χωρίς να προβαίνει σε περαιτέρω επεξεργασία βιομετρικών δεδομένων τρίτων (π.χ. με αναζήτηση με τεχνολογία αναγνώρισης προσώπου σε βάση δεδομένων). Πρέπει να τηρείται η αρχή της ελαχιστοποίησης των δεδομένων και δεν θα πρέπει να αποθηκεύονται περισσότερα δεδομένα από όσα είναι απαραίτητα σε σχέση με τον σκοπό της επεξεργασίας.

3.2.4.3 Δικαίωμα διόρθωσης δεδομένων προσωπικού χαρακτήρα

91. Δεδομένου ότι η τεχνολογία αναγνώρισης προσώπου δεν ορίζει απόλυτη ακρίβεια, είναι ιδιαίτερα σημαντικό οι υπεύθυνοι επεξεργασίας να επαγρυπνούν για τα αιτήματα διόρθωσης δεδομένων προσωπικού χαρακτήρα. Μπορεί επίσης να συμβεί όταν ένα υποκείμενο των δεδομένων βάσει της τεχνολογίας αναγνώρισης προσώπου έχει τοποθετηθεί σε ανακριβή κατηγορία, π.χ. να έχει τοποθετηθεί εσφαλμένα στην κατηγορία των υπόπτων με βάση την αρχική υπόθεση της δράσης σε βιντεοσκοπημένο οπτικοακουστικό υλικό. Οι κίνδυνοι για τα υποκείμενα των δεδομένων είναι ιδιαίτερα σοβαροί εάν τα εν λόγω ανακριβή δεδομένα αποθηκευτούν σε βάση δεδομένων της αστυνομίας και/ή κοινοποιηθούν σε άλλες οντότητες. Ο υπεύθυνος επεξεργασίας πρέπει να διορθώσει τα αποθηκευμένα δεδομένα και τα συστήματα τεχνολογίας αναγνώρισης προσώπου αναλόγως, βλ. αιτιολογική σκέψη 47 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

3.2.4.4 Δικαίωμα διαγραφής

92. Στις περισσότερες περιπτώσεις, η τεχνολογία αναγνώρισης προσώπου —σε περίπτωση που δεν χρησιμοποιείται για επαλήθευση 1 προς 1/έλεγχο της ταυτότητας— ισοδυναμεί με επεξεργασία μεγάλου αριθμού βιομετρικών δεδομένων των υποκειμένων των δεδομένων. Ως εκ τούτου, είναι σημαντικό ο υπεύθυνος επεξεργασίας να εξετάζει εκ των προτέρων πού βρίσκονται τα όρια του σκοπού και της αναγκαιότητάς του, ώστε ένα αίτημα διαγραφής σύμφωνα με το άρθρο 16 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου να μπορεί να διεκπεραιωθεί χωρίς άσκοπη καθυστέρηση (δεδομένου ότι ο υπεύθυνος επεξεργασίας πρέπει, μεταξύ άλλων, να διαγράψει δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία πέρα από αυτό που επιτρέπει η ισχύουσα νομοθεσία σύμφωνα με τα άρθρα 4, 8 και 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου).

3.2.4.5 Δικαίωμα περιορισμού

93. Σε περίπτωση που η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητηθεί από το υποκείμενο των δεδομένων και δεν μπορεί να διαπιστωθεί εάν αυτά είναι ακριβή ή ανακριβή (ή όταν επιβάλλεται να διατηρηθούν τα δεδομένα προσωπικού χαρακτήρα για σκοπούς μελλοντικής απόδειξης), ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να περιορίσει τα δεδομένα προσωπικού χαρακτήρα του εν λόγω υποκειμένου των δεδομένων σύμφωνα με το άρθρο 16 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Αυτό καθίσταται ιδιαίτερα σημαντικό όταν πρόκειται για τεχνολογία αναγνώρισης προσώπου (βάσει αλγορίθμου(-ων) και συνεπώς δεν παρουσιάζει ποτέ οριστικό αποτέλεσμα) σε περιπτώσεις όπου συλλέγονται μεγάλες ποσότητες δεδομένων και η ακρίβεια και η ποιότητα της ταυτοποίησης μπορεί να ποικίλλει. Όταν το

υλικό βίντεο είναι κακής ποιότητας (π.χ. από τον τόπο ενός εγκλήματος), ο κίνδυνος ψευδώς θετικών αποτελεσμάτων αυξάνεται. Επιπλέον, εάν οι εικόνες προσώπου σε έναν κατάλογο υπόπτων δεν ενημερώνονται τακτικά, αυτό θα αυξήσει επίσης τον κίνδυνο ψευδώς θετικών ή ψευδώς αρνητικών αποτελεσμάτων. Σε συγκεκριμένες περιπτώσεις, όταν τα δεδομένα δεν μπορούν να διαγραφούν λόγω του γεγονότος ότι υπάρχουν βάσιμοι λόγοι να πιστεύεται ότι η διαγραφή θα μπορούσε να επηρεάσει τα έννομα συμφέροντα του υποκειμένου των δεδομένων, τα δεδομένα θα πρέπει, αντ' αυτού, να περιορίζονται και να υποβάλλονται σε επεξεργασία μόνο για τον σκοπό που εμπόδισε τη διαγραφή τους (βλ. αιτιολογική σκέψη 47 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου).

3.2.4.6 Νόμιμοι περιορισμοί των δικαιωμάτων των υποκειμένων των δεδομένων

94. Όσον αφορά τις υποχρεώσεις ενημέρωσης του υπευθύνου επεξεργασίας και το δικαίωμα πρόσβασης των υποκειμένων των δεδομένων, περιορισμοί επιτρέπονται μόνο εφόσον προβλέπονται από τον νόμο, ο οποίος με τη σειρά του πρέπει να συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία, λαμβανομένων δεόντως υπόψη των θεμελιωδών δικαιωμάτων και των έννομων συμφερόντων του ενδιαφερόμενου φυσικού προσώπου (βλ. άρθρο 13 παράγραφος 3, άρθρο 13 παράγραφος 4, άρθρο 15 και άρθρο 16 παράγραφος 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου). Όταν η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται για σκοπούς επιβολής του νόμου, μπορεί κανείς να αναμένει ότι θα χρησιμοποιηθεί υπό περιστάσεις στις οποίες θα ήταν επιζήμια για τον επιδιωκόμενο σκοπό η ενημέρωση του υποκειμένου των δεδομένων ή η παροχή πρόσβασης στα δεδομένα. Αυτό ισχύει, για παράδειγμα, για τη διερεύνηση ενός εγκλήματος από την αστυνομία ή για την προστασία της εθνικής ασφάλειας ή της δημόσιας ασφάλειας.

95. Το δικαίωμα πρόσβασης δεν σημαίνει αυτομάτως πρόσβαση σε όλες τις πληροφορίες, π.χ. σε μια ποινική υπόθεση όπου υπάρχουν δεδομένα προσωπικού χαρακτήρα ενός ατόμου. Ένα βιώσιμο παράδειγμα του πότε μπορούν να επιτραπούν περιορισμοί του δικαιώματος θα μπορούσε να είναι κατά τη διάρκεια μια ποινικής διερεύνησης.

3.2.4.7 Άσκηση των δικαιωμάτων μέσω της εποπτικής αρχής

96. Σε περιπτώσεις στις οποίες υπάρχουν θεμιτοί περιορισμοί στην άσκηση των δικαιωμάτων σύμφωνα με το κεφάλαιο III της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, το υποκείμενο των δεδομένων μπορεί να ζητήσει από την αρχή προστασίας δεδομένων να ασκήσει τα δικαιώματά του για λογαριασμό του, ελέγχοντας τη νομιμότητα της επεξεργασίας του υπευθύνου επεξεργασίας. Εναπόκειται στον υπεύθυνο επεξεργασίας να ενημερώνει το υποκείμενο των δεδομένων για τη δυνατότητα να ασκήσει τα δικαιώματά του με τον τρόπο αυτό [βλ. άρθρο 17 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου και άρθρο 46 παράγραφος 1 στοιχείο ζ) της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου]. Όσον αφορά την τεχνολογία αναγνώρισης προσώπου, αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι εφαρμόζονται κατάλληλα μέτρα ώστε να μπορεί να διεκπεραιωθεί ένα τέτοιο αίτημα, π.χ. επιτρέποντας την αναζήτηση καταγεγραμμένου υλικού, υπό την προϋπόθεση ότι το υποκείμενο των δεδομένων παρέχει επαρκείς πληροφορίες για τον εντοπισμό των οικείων του δεδομένων προσωπικού χαρακτήρα.

3.2.5 Άλλες νομικές απαιτήσεις και διασφαλίσεις

3.2.5.1 Άρθρο 27 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

97. Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) πριν από τη χρήση της τεχνολογίας αναγνώρισης προσώπου αποτελεί υποχρεωτική απαίτηση, δεδομένου ότι ο τύπος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών, λαμβανομένων υπόψη της φύσης, του πλαισίου,

του πεδίου εφαρμογής και των σκοπών της επεξεργασίας, είναι πιθανόν να προκαλέσει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Δεδομένου ότι η χρήση της τεχνολογίας αναγνώρισης προσώπου συνεπάγεται συστηματική αυτόματη επεξεργασία ειδικών κατηγοριών δεδομένων, θα μπορούσε να θεωρηθεί ότι σε τέτοιες περιπτώσεις ο υπεύθυνος επεξεργασίας υποχρεούται, κατά κανόνα, να διενεργήσει ΕΑΠΔ. Η ΕΑΠΔ θα πρέπει να περιλαμβάνει τουλάχιστον γενική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων αυτών, διασφαλίσεις, μέτρα ασφαλείας και μηχανισμούς, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση. Το ΕΣΠΔ συνιστά τη δημοσιοποίηση των αποτελεσμάτων των εν λόγω εκτιμήσεων ή τουλάχιστον των βασικών διαπιστώσεων και συμπερασμάτων της ΕΑΠΔ, ως μέτρο ενίσχυσης της εμπιστοσύνης και της διαφάνειας[62].

3.2.5.2 Άρθρο 28 Προηγούμενη διαβούλευση με την εποπτική αρχή

98. Σύμφωνα με το άρθρο 28 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πρέπει να διαβουλεύεται με την εποπτική αρχή πριν από την επεξεργασία, εφόσον: α) από εκτίμηση των επιπτώσεων στην προστασία των δεδομένων προκύπτει ότι η επεξεργασία θα προκαλέσει μεγάλο κίνδυνο εάν ο υπεύθυνος επεξεργασίας δεν λάβει μέτρα για τον μετριασμό του κινδύνου· ή β) ο τύπος επεξεργασίας, ιδίως κατά τη χρήση νέων τεχνολογιών, μηχανισμών ή διαδικασιών, ενέχει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Όπως έχει ήδη εξηγηθεί στην ενότητα 2.3. των παρουσών κατευθυντήριων γραμμών, το ΕΣΠΔ θεωρεί ότι οι περισσότερες περιπτώσεις εγκατάστασης και χρήσης τεχνολογίας αναγνώρισης προσώπου ενέχουν εγγενή υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Ως εκ τούτου, εκτός από την ΕΑΠΔ, η αρχή που εγκαθιστά τεχνολογία αναγνώρισης προσώπου θα πρέπει να συμβουλευτεί την αρμόδια εποπτική αρχή πριν από την εγκατάσταση του συστήματος.

3.2.5.3 Άρθρο 29 Ασφάλεια επεξεργασίας

99. Ο μοναδικός χαρακτήρας των βιομετρικών δεδομένων καθιστά αδύνατη την αλλαγή των βιομετρικών δεδομένων από το υποκείμενο των δεδομένων, σε περίπτωση που αυτά διακυβεύονται, π.χ. ως αποτέλεσμα παραβίασης δεδομένων. Ως εκ τούτου, η αρμόδια αρχή που εφαρμόζει ή/και χρησιμοποιεί τεχνολογία αναγνώρισης προσώπου θα πρέπει να δώσει ιδιαίτερη προσοχή στην ασφάλεια της επεξεργασίας, σύμφωνα με το άρθρο 29 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο επιβολής του νόμου. Ειδικότερα, η αρχή επιβολής του νόμου θα πρέπει να διασφαλίζει ότι το σύστημα συμμορφώνεται με τα σχετικά πρότυπα και να εφαρμόζει μέτρα προστασίας βιομετρικών υποδειγμάτων[63]. Η εν λόγω υποχρέωση είναι ακόμη πιο σημαντική εάν η αρχή επιβολής του νόμου χρησιμοποιεί τρίτο πάροχο υπηρεσιών (εκτελών την επεξεργασία δεδομένων).

3.2.5.4 Άρθρο 20 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

100. Η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, σύμφωνα με το άρθρο 20 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, αποσκοπεί στη διασφάλιση ότι οι αρχές και οι διασφαλίσεις προστασίας των δεδομένων, όπως η ελαχιστοποίηση

[62] Για περισσότερες πληροφορίες βλ. WP 248 αναθ. 01 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του εάν η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο».

[63] Βλ. για παράδειγμα: ISO/IEC 24745 με τίτλο «Information security, cybersecurity and privacy protection — Biometric information protection» (Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής — Προστασία βιομετρικών πληροφοριών).

των δεδομένων και ο περιορισμός της αποθήκευσης, ενσωματώνονται στην τεχνολογία μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων, όπως η χρήση ψευδωνύμου, ακόμη και πριν από την έναρξη της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και θα εφαρμόζονται καθ' όλη τη διάρκεια του κύκλου ζωής της. Δεδομένου του εγγενούς υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η επιλογή των εν λόγω μέτρων δεν θα πρέπει να εξαρτάται αποκλειστικά και μόνο από οικονομικές εκτιμήσεις,[64] αλλά θα πρέπει αντ' αυτού να επιδιώκει την εφαρμογή των τεχνολογιών αιχμής στον τομέα της προστασίας των δεδομένων. Στο ίδιο πνεύμα, εάν μια αρχή επιβολής του νόμου προτίθεται να εφαρμόσει και να χρησιμοποιήσει τεχνολογία αναγνώρισης προσώπου από εξωτερικούς παρόχους, πρέπει να διασφαλίζει, για παράδειγμα μέσω της διαδικασίας σύναψης συμβάσεων, ότι χρησιμοποιούνται μόνο τεχνολογίες αναγνώρισης προσώπου που βασίζονται στις αρχές της προστασίας των δεδομένων από τον σχεδιασμό και εξ ορισμού[65]. Αυτό σημαίνει επίσης ότι η διαφάνεια σχετικά με τη λειτουργία της τεχνολογίας αναγνώρισης προσώπου δεν περιορίζεται από ισχυρισμούς περί εμπορικού απορρήτου ή δικαιωμάτων διανοητικής ιδιοκτησίας.

3.2.5.5 Άρθρο 25 Καταχωρίσεις

101. Η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου προβλέπει διάφορες μεθόδους για την απόδειξη από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία της νομιμότητας της επεξεργασίας και τη διασφάλιση της ακεραιότητας και της ασφάλειας των δεδομένων. Στο πλαίσιο αυτό, οι καταχωρίσεις συστήματος αποτελούν πολύ χρήσιμο εργαλείο και σημαντική διασφάλιση για την επαλήθευση της νομιμότητας της επεξεργασίας, τόσο εσωτερικά (δηλ. αυτοπαρακολούθηση) όσο και από εξωτερικές εποπτικές αρχές, όπως οι αρχές προστασίας δεδομένων. Σύμφωνα με το άρθρο 25 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, καταχωρίσεις τουλάχιστον για τις ακόλουθες πράξεις επεξεργασίας θα πρέπει να τηρούνται στα συστήματα αυτοματοποιημένης επεξεργασίας: συλλογή, μεταβολή, αναζήτηση πληροφοριών, κοινολόγηση, περιλαμβανομένων των διαβιβάσεων, συνδυασμό και διαγραφή. Επιπλέον, οι καταχωρίσεις της αναζήτησης πληροφοριών και της κοινολόγησης επιτρέπουν τον προσδιορισμό της αιτιολόγησης και της ημερομηνίας και της ώρας των εν λόγω πράξεων και, στο βαθμό του εφικτού, της ταυτότητας του προσώπου που αναζήτησε πληροφορίες ή κοινολόγησε δεδομένα προσωπικού χαρακτήρα, καθώς και της ταυτότητας των αποδεκτών των εν λόγω δεδομένων προσωπικού χαρακτήρα. Επιπλέον, στο πλαίσιο των συστημάτων αναγνώρισης προσώπου, συνιστώνται οι καταχωρίσεις των ακόλουθων πρόσθετων πράξεων επεξεργασίας (εν μέρει πέραν του άρθρου 25 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου):

- Αλλαγές στη βάση δεδομένων αναφοράς (προσθήκη, διαγραφή ή επικαιροποίηση). Η καταχώριση θα πρέπει να διατηρεί αντίγραφο της σχετικής εικόνας (που προστέθηκε, διαγράφηκε ή επικαιροποιήθηκε), όταν δεν είναι δυνατή με άλλον τρόπο η επαλήθευση της νομιμότητας ή του αποτελέσματος των πράξεων επεξεργασίας.

- Απόπειρες ταυτοποίησης ή επαλήθευσης, συμπεριλαμβανομένου του αποτελέσματος και της βαθμολογίας εμπιστοσύνης. Θα πρέπει να εφαρμόζεται η αρχή της αυστηρής ελαχιστοποίησης, έτσι ώστε μόνο το αναγνωριστικό στοιχείο ταυτότητας της εικόνας από τη βάση δεδομένων αναφοράς να διατηρείται στις καταχωρίσεις, αντί να αποθηκεύεται η εικόνα αναφοράς. Θα

[64] Βλ. αιτιολογική σκέψη 53 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο επιβολής του νόμου.

[65] Για περισσότερες πληροφορίες, βλ. Κατευθυντήριες γραμμές του ΕΣΠΔ σχετικά με την Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

πρέπει να αποφεύγονται οι καταχωρίσεις των βιομετρικών δεδομένων εισόδου, εκτός εάν υπάρχει ανάγκη (π.χ. μόνο σε περιπτώσεις αντιστοιχίας).

- Η ταυτότητα του χρήστη που ζήτησε την απόπειρα ταυτοποίησης ή επαλήθευσης.

- Τυχόν δεδομένα προσωπικού χαρακτήρα που αποθηκεύονται στις καταχωρίσεις των συστημάτων υπόκεινται σε αυστηρούς περιορισμούς σκοπού (π.χ. ελέγχους) και δεν θα πρέπει να χρησιμοποιούνται για άλλους σκοπούς (π.χ. για να είναι δυνατή η αναγνώριση/επαλήθευση, συμπεριλαμβανομένης μιας εικόνας που έχει διαγραφεί από τις βάσεις δεδομένων αναφοράς). Θα πρέπει να εφαρμόζονται μέτρα ασφαλείας για τη διασφάλιση της ακεραιότητας των καταχωρήσεων, ενώ συνιστάται ιδιαίτερα η ύπαρξη συστημάτων αυτόματης παρακολούθησης για τον εντοπισμό της κατάχρησης των καταχωρήσεων. Για τις καταχωρίσεις της βάσης δεδομένων αναφοράς, τα μέτρα ασφάλειας θα πρέπει να είναι ισοδύναμα με τη βάση δεδομένων αναφοράς, σε περίπτωση αποθήκευσης εικόνων προσώπου. Επίσης, θα πρέπει να εφαρμόζονται αυτόματες διαδικασίες για τη διασφάλιση της επιβολής της περιόδου διατήρησης των δεδομένων για τις καταχωρίσεις.

3.2.5.6 Άρθρο 4 παράγραφος 4 Λογοδοσία

102. Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση της επεξεργασίας με τις αρχές του άρθρου 4 παράγραφοι 1 έως 3, πρβλ. άρθρο 4 παράγραφος 4 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Η συστηματική και επικαιροποιημένη τεκμηρίωση του συστήματος (συμπεριλαμβανομένων επικαιροποιήσεων, αναβαθμίσεων και αλγοριθμικής εκπαίδευσης), των τεχνικών και οργανωτικών μέτρων (συμπεριλαμβανομένης της παρακολούθησης των επιδόσεων του συστήματος και της πιθανής ανθρώπινης παρέμβασης) και της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι ζωτικής σημασίας στο πλαίσιο αυτό. Για να αποδειχθεί η νομιμότητα της επεξεργασίας, ένα ιδιαίτερα σημαντικό στοιχείο είναι οι καταχωρίσεις σύμφωνα με το άρθρο 25 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (πρβλ. ενότητα 3.2.5.5). Η αρχή της λογοδοσίας δεν αναφέρεται μόνο στο σύστημα και στην επεξεργασία, αλλά και στην τεκμηρίωση των διαδικαστικών διασφαλίσεων, όπως οι αξιολογήσεις αναγκαιότητας και αναλογικότητας, οι ΕΑΠΔ, καθώς και οι εσωτερικές διαβουλεύσεις (π.χ. έγκριση του έργου από τη διοίκηση ή εσωτερικές αποφάσεις σχετικά με τις τιμές της βαθμολογίας εμπιστοσύνης) και οι εξωτερικές διαβουλεύσεις (π.χ. αρχή προστασίας δεδομένων). Το παράρτημα II περιλαμβάνει ορισμένα στοιχεία σχετικά με το θέμα αυτό.

3.2.5.7 Άρθρο 47 Αποτελεσματική εποπτεία

103. Η αποτελεσματική εποπτεία από τις αρμόδιες αρχές προστασίας δεδομένων αποτελεί μία από τις σημαντικότερες διασφαλίσεις για τα θεμελιώδη δικαιώματα και τις ελευθερίες των ατόμων που επηρεάζονται από τη χρήση της τεχνολογίας αναγνώρισης προσώπου. Ταυτόχρονα, η παροχή των απαραίτητων ανθρώπινων, τεχνικών και οικονομικών πόρων, των αναγκαίων εγκαταστάσεων και υποδομών σε κάθε αρχή προστασίας δεδομένων αποτελεί προϋπόθεση για την αποτελεσματική εκτέλεση των καθηκόντων και την άσκηση των εξουσιών τους[66]. Ακόμη πιο κρίσιμες από τον αριθμό του διαθέσιμου προσωπικού είναι οι δεξιότητες των εμπειρογνωμόνων, οι οποίοι θα πρέπει να καλύπτουν ένα πολύ ευρύ φάσμα θεμάτων —από τις ποινικές έρευνες και την αστυνομική συνεργασία έως την ανάλυση μαζικών δεδομένων και την τεχνητή νοημοσύνη. Ως εκ τούτου, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι πόροι των εποπτικών αρχών είναι κατάλληλοι και επαρκείς

[66] Βλ. ανακοίνωση της Επιτροπής με τίτλο «Πρώτη έκθεση σχετικά με την εφαρμογή και τη λειτουργία της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (ΕΕ) 2016/680», COM (2022) 364 final, σ. 3.4.1.

ώστε να τους επιτρέπουν να εκπληρώσουν την εντολή τους για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων και να παρακολουθούν στενά τυχόν σχετικές εξελίξεις.[67]

4 ΣΥΜΠΕΡΑΣΜΑ

104. Η χρήση τεχνολογιών αναγνώρισης προσώπου είναι άρρηκτα συνδεδεμένη με την επεξεργασία σημαντικών ποσοτήτων δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων. Το πρόσωπο και, γενικότερα, τα βιομετρικά δεδομένα συνδέονται μόνιμα και αμετάκλητα με την ταυτότητα ενός ατόμου. Ως εκ τούτου, η χρήση της αναγνώρισης προσώπου έχει άμεσο ή έμμεσο αντίκτυπο σε μια σειρά θεμελιωδών δικαιωμάτων και ελευθεριών που κατοχυρώνονται στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και μπορεί να υπερβαίνουν την προστασία της ιδιωτικής ζωής και των δεδομένων, όπως η ανθρώπινη αξιοπρέπεια, η ελευθερία της κυκλοφορίας, η ελευθερία του συνέρχεσθαι και άλλα. Αυτό είναι ιδιαίτερα σημαντικό στον τομέα της επιβολής του νόμου και της ποινικής δικαιοσύνης.

105. Το ΕΣΠΔ κατανοεί την ανάγκη των αρχών επιβολής του νόμου να έχουν στη διάθεσή τους τα βέλτιστα δυνατά μέσα για την ταχεία ταυτοποίηση των δραστών τρομοκρατικών ενεργειών και άλλων σοβαρών εγκλημάτων. Ωστόσο, τα εργαλεία αυτά θα πρέπει να χρησιμοποιούνται σε αυστηρή συμμόρφωση με το εφαρμοστέο νομικό πλαίσιο και μόνο σε περιπτώσεις που πληρούν τις απαιτήσεις της αναγκαιότητας και της αναλογικότητας, όπως ορίζονται στο άρθρο 52 παράγραφος 1 του Χάρτη. Επιπλέον, ενώ οι σύγχρονες τεχνολογίες μπορεί να αποτελούν μέρος της λύσης, σε καμία περίπτωση δεν αποτελούν πανάκεια.

106. Υπάρχουν ορισμένες περιπτώσεις χρήσης τεχνολογιών αναγνώρισης προσώπων, οι οποίες ενέχουν απαράδεκτα υψηλούς κινδύνους για τα άτομα και την κοινωνία («κόκκινες γραμμές»). Για τους λόγους αυτούς, το ΕΣΠΔ και ο ΕΕΠΔ ζήτησαν τη γενική απαγόρευσή τους[68].

107. Ειδικότερα, η εξ αποστάσεως βιομετρική ταυτοποίηση ατόμων σε δημόσια προσβάσιμους χώρους ενέχει υψηλό κίνδυνο εισβολής στην ιδιωτική ζωή των ατόμων και δεν έχει θέση σε μια δημοκρατική κοινωνία, καθώς από τη φύση της συνεπάγεται μαζική παρακολούθηση. Στο ίδιο πνεύμα, το ΕΣΠΔ θεωρεί ότι τα συστήματα αναγνώρισης προσώπου ΤΝ που κατηγοριοποιούν τα άτομα από τα βιομετρικά τους στοιχεία σε ομάδες ανάλογα με την εθνικότητα, το φύλο, καθώς και τον πολιτικό ή σεξουαλικό προσανατολισμό δεν είναι συμβατά με τον Χάρτη. Επιπλέον, το ΕΣΠΔ είναι πεπεισμένο ότι η χρήση της αναγνώρισης προσώπου ή παρόμοιων τεχνολογιών για τη διαπίστωση των συναισθημάτων ενός φυσικού προσώπου είναι άκρως ανεπιθύμητη και θα πρέπει να απαγορεύεται, ενδεχομένως με λίγες δεόντως αιτιολογημένες εξαιρέσεις. Επιπλέον, το ΕΣΠΔ θεωρεί ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα σε πλαίσιο επιβολής του νόμου που θα βασίζεται σε μια βάση δεδομένων η οποία θα εμπλουτίζεται από τη συλλογή δεδομένων προσωπικού χαρακτήρα σε μαζική κλίμακα και κατά τρόπο αδιάκριτο, π.χ. με την «εξαγωγή» φωτογραφιών και εικόνων προσώπου που είναι προσβάσιμες στο διαδίκτυο, ιδίως εκείνων που διατίθενται μέσω

[67] Βλ. «Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, para. 14» (Συμβολή του ΕΣΠΔ στην αξιολόγηση της Ευρωπαϊκής Επιτροπής σχετικά με την οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου βάσει του άρθρου 62, παράγραφος 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Βλ ΕΣΠΔ-ΕΕΠΔ Κοινή γνωμοδότηση 5/2021 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (πράξη για την τεχνητή νοημοσύνη) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

κοινωνικών δικτύων, δεν θα πληροί, ως εκ τούτου, την απαίτηση αυστηρής αναγκαιότητας που προβλέπεται από το δίκαιο της Ένωσης.

5 ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Ι: Πρότυπο υποστήριξης

Παράρτημα ΙΙ: Πρακτική καθοδήγηση για τη διαχείριση έργων με τεχνολογία αναγνώρισης προσώπου στις αρχές επιβολής του νόμου

Παράρτημα ΙΙΙ: Πρακτικά παραδείγματα

ΠΑΡΑΡΤΗΜΑ Ι — ΥΠΟΔΕΙΓΜΑ ΓΙΑ ΤΗΝ ΠΕΡΙΓΡΑΦΗ ΣΕΝΑΡΙΩΝ

(Με ενημερωτικά πλαίσια για τις πτυχές που εξετάζονται στο πλαίσιο του σεναρίου)

Περιγραφή της επεξεργασίας:

- Περιγραφή της επεξεργασίας, Πλαίσιο (σχέση με το έγκλημα), Σκοπός

Πηγή των πληροφοριών:

- Τύποι υποκειμένων των δεδομένων: ☐ όλοι οι πολίτες ☐ καταδικασθέντες ☐ ύποπτοι
  ☐ παιδιά ☐ άλλα ευάλωτα υποκείμενα των δεδομένων
- Πηγή εικόνας: ☐ δημόσια προσβάσιμοι χώροι ☐ διαδίκτυο
  ☐ ιδιωτική οντότητα ☐ άλλα φυσικά πρόσωπα ☐ άλλο
  .....
- Σύνδεση με το έγκλημα: ☐ Άμεση χρονική ☐ Μη άμεση χρονική
  ☐ Άμεση γεωγραφική ☐ Μη άμεση γεωγραφική
  ☐ Μη απαραίτητη
- Τρόπος συλλογής πληροφοριών: ☐ εξ αποστάσεως ☐ σε θάλαμο ή ελεγχόμενο περιβάλλον
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα:
  ☐ Όχι
  Ναι, συγκεκριμένα ☐ ελευθερία του συνέρχεσθαι
  ☐ Ελευθερία του λόγου
  ☐ διάφορα:.....
- Δυνατότητες για πρόσθετες πηγές πληροφόρησης σχετικά με το υποκείμενο των δεδομένων:
  ☐ έγγραφο ταυτότητας ☐ χρήση δημόσιου τηλεφώνου
  ☐ πινακίδα κυκλοφορίας οχήματος
  ☐ άλλο .....

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση: ☐ βάσεις δεδομένων γενικού σκοπού ☐ ειδικές βάσεις δεδομένων που σχετίζονται με τον τομέα του εγκλήματος
- Περιγραφή του τρόπου με τον οποίο εμπλουτίστηκαν οι εν λόγω βάσεις δεδομένων αναφοράς (και νομική βάση)
- Αλλαγή του σκοπού της βάσης δεδομένων (π.χ. η ασφάλεια της ιδιωτικής περιουσίας ήταν ο πρωταρχικός στόχος): ☐ ΝΑΙ
  ☐ ΟΧΙ

Αλγόριθμος:

- Τύπος επεξεργασίας: ☐ 1-1 επαλήθευση (έλεγχος της ταυτότητας) ☐ ταυτοποίηση 1-πολλά
- Εκτιμήσεις σχετικά με την ακρίβεια
- Τεχνικές διασφαλίσεις

Αποτέλεσμα:

- Αντίκτυπος ☐ Άμεσος (π.χ. το υποκείμενο των δεδομένων μπορεί να συλληφθεί, να ανακριθεί, να υποστεί διακρίσεις)

  ☐ Μη άμεσος (χρησιμοποιείται για στατιστικά μοντέλα, χωρίς σοβαρές νομικές ενέργειες κατά των υποκειμένων των δεδομένων)

- Αυτοματοποιημένη απόφαση: ☐ ΝΑΙ ☐ ΟΧΙ
- Διάρκεια αποθήκευσης

Νομική ανάλυση:

- Ανάλυση αναγκαιότητας και αναλογικότητας — σκοπός/σοβαρότητα του εγκλήματος/αριθμός των προσώπων που δεν εμπλέκονται αλλά επηρεάζονται από την επεξεργασία
- Τύπος προηγούμενης ενημέρωσης του υποκειμένου των δεδομένων: ☐ Κατά την είσοδο στη συγκεκριμένη περιοχή

  ☐ Γενικά στον ιστότοπο της αρχής επιβολής του νόμου

  ☐ Στον ιστότοπο της αρχής επιβολής του νόμου για τη συγκεκριμένη επεξεργασία

  ☐ Άλλο .....

- Εφαρμοστέο νομικό πλαίσιο :

  ☐ Η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου έχει ως επί το πλείστον αντιγραφεί στο εθνικό δίκαιο

  ☐ Γενικό εθνικό δίκαιο για τη χρήση βιομετρικών δεδομένων από τις αρχές επιβολής του νόμου

  ☐ Ειδικό εθνικό δίκαιο για την εν λόγω επεξεργασία (αναγνώριση προσώπου) για την εν λόγω αρμόδια αρχή

  ☐ Ειδικό εθνικό δίκαιο για την εν λόγω επεξεργασία (αυτοματοποιημένη απόφαση)

Συμπέρασμα:

Γενικές εκτιμήσεις σχετικά με το εάν η περιγραφόμενη επεξεργασία είναι πιθανώς συμβατή με το δίκαιο της ΕΕ (και ορισμένες υποδείξεις σχετικά με τις νομικές προϋποθέσεις)

ΠΑΡΑΡΤΗΜΑ ΙΙ— ΠΡΑΚΤΙΚΗ ΚΑΘΟΔΗΓΗΣΗ ΓΙΑ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΕΡΓΩΝ ΜΕ ΤΕΧΝΟΛΟΓΙΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΣΤΙΣ ΑΡΧΕΣ ΕΠΙΒΟΛΗΣ ΤΟΥ ΝΟΜΟΥ

Το παρόν παράρτημα παρέχει ορισμένη πρόσθετη πρακτική καθοδήγηση για τη διαχείριση έργων με τεχνολογία αναγνώρισης προσώπου στις αρχές επιβολής του νόμου που σχεδιάζουν να ξεκινήσουν ένα έργο που περιλαμβάνει τεχνολογία αναγνώρισης προσώπου. Παρέχει περισσότερες πληροφορίες σχετικά με τα οργανωτικά και τεχνικά μέτρα που πρέπει να λαμβάνονται υπόψη κατά την υλοποίηση του έργου και δεν θα πρέπει να θεωρείται εξαντλητικός κατάλογος των ενεργειών/μέτρων που πρέπει να ληφθούν. Θα πρέπει επίσης να εξεταστεί σε συνδυασμό με τις Κατευθυντήριες γραμμές 3/2019 του ΕΣΠΔ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών[69] και οποιονδήποτε κανονισμό της ΕΕ/του ΕΟΧ και κατευθυντήριες γραμμές του ΕΣΠΔ σχετικά με τη χρήση της τεχνητής νοημοσύνης.

Το παρόν παράρτημα παρέχει κατευθυντήριες γραμμές με βάση την παραδοχή ότι οι αρχές επιβολής του νόμου θα προμηθεύονται τεχνολογία αναγνώρισης προσώπου (ως έτοιμα προς χρήση προϊόντα). Εάν η αρχή επιβολής του νόμου σχεδιάζει να αναπτύξει (να εκπαιδεύσει περαιτέρω) την τεχνολογία αναγνώρισης προσώπου, τότε ισχύουν πρόσθετες απαιτήσεις για την επιλογή των απαραίτητων συνόλων δεδομένων εκπαίδευσης, επικύρωσης και δοκιμών που θα χρησιμοποιηθούν κατά τη διάρκεια της ανάπτυξης και των ρόλων/μέτρων για το περιβάλλον ανάπτυξης. Ομοίως, ένα έτοιμο προς χρήση προϊόν μπορεί να απαιτεί περαιτέρω προσαρμογές για την προβλεπόμενη χρήση, οπότε θα πρέπει να πληρούνται οι προαναφερθείσες απαιτήσεις για την επιλογή των συνόλων δεδομένων δοκιμών, επικύρωσης και εκπαίδευσης.

Η συμμετοχή στην ίδια αρχή επιβολής του νόμου δεν παρέχει από μόνη της πλήρη πρόσβαση σε βιομετρικά δεδομένα. Όπως συμβαίνει με οποιαδήποτε άλλη κατηγορία δεδομένων προσωπικού χαρακτήρα, τα βιομετρικά δεδομένα που συλλέγονται για συγκεκριμένο σκοπό επιβολής του νόμου στο πλαίσιο συγκεκριμένης νομικής βάσης δεν μπορούν να χρησιμοποιηθούν χωρίς κατάλληλη νομική βάση για διαφορετικό σκοπό επιβολής του νόμου [άρθρο 4 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680 για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου]. Επίσης, η ανάπτυξη/εκπαίδευση ενός εργαλείου τεχνολογίας αναγνώρισης προσώπου θεωρείται διαφορετικός σκοπός και θα πρέπει να αξιολογείται εάν η επεξεργασία βιομετρικών δεδομένων για τη μέτρηση των επιδόσεων/εκπαίδευση της τεχνολογίας ώστε να αποφεύγεται ο αντίκτυπος στα υποκείμενα των δεδομένων λόγω χαμηλών επιδόσεων είναι αναγκαία και αναλογική, λαμβανομένου υπόψη του αρχικού σκοπού της επεξεργασίας.

1. ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Όταν μια αρχή επιβολής του νόμου χρησιμοποιεί τεχνολογίες αναγνώρισης προσώπου για την εκτέλεση των καθηκόντων της που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων, κ.λπ., σύμφωνα με το άρθρο 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου), μπορεί να οριστεί υπεύθυνος επεξεργασίας για την τεχνολογία αναγνώρισης προσώπου. Ωστόσο, οι αρχές επιβολής του νόμου αποτελούνται από διάφορες

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

μονάδες/τμήματα που μπορούν να συμμετέχουν στην εν λόγω επεξεργασία, είτε με τον καθορισμό της διαδικασίας εφαρμογής τεχνολογίας αναγνώρισης προσώπου, είτε με την εφαρμογή της στην πράξη. Λόγω των εξειδικεύσεων της εν λόγω τεχνολογίας, μπορεί να χρειαστεί να εμπλακούν διαφορετικές μονάδες είτε για να υποστηρίξουν τις μετρήσεις της απόδοσής της, είτε για να την εκπαιδεύσουν περαιτέρω.

Σε ένα έργο στο οποίο εμπλέκονται αρχές επιβολής του νόμου, υπάρχουν διάφορα ενδιαφερόμενα μέρη[70] εντός των αρχών επιβολής του νόμου που μπορεί να χρειαστεί να συμμετάσχουν:

- Ανώτατη διοίκηση — για να εγκρίνει το έργο μετά την εξισορρόπηση των κινδύνων με τα πιθανά οφέλη.
- Υπεύθυνος προστασίας δεδομένων και/ή νομικό τμήμα της αρχής επιβολής του νόμου — για να συνδράμει στην αξιολόγηση της νομιμότητας της υλοποίησης ενός συγκεκριμένου έργου με τεχνολογία αναγνώρισης προσώπου· να συνδράμει στην εκτέλεση της ΕΑΠΔ· να διασφαλίζει τον σεβασμό και την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων.
- Κύριος της διαδικασίας — ενεργώντας ως ειδική μονάδα εντός της αρμόδιας αρχής επιβολής του νόμου για την ανάπτυξη του έργου, αποφασίζοντας τις λεπτομέρειες του έργου με τεχνολογία αναγνώρισης προσώπου, συμπεριλαμβανομένων των απαιτήσεων απόδοσης του συστήματος, αποφασίζοντας σχετικά με την κατάλληλη μέτρηση αμεροληψίας, καθορίζοντας τη βαθμολογία εμπιστοσύνης[71], καθορίζοντας αποδεκτά όρια μεροληψίας, προσδιορίζοντας τους πιθανούς κινδύνους που ενέχει το έργο με τεχνολογία αναγνώρισης προσώπου για τα δικαιώματα και τις ελευθερίες των ατόμων [διεξάγοντας επίσης διαβουλεύσεις με τον ΥΠΔ και το τμήμα ΤΝ ΤΠ και/ή επιστήμης δεδομένων (βλ. κατωτέρω)] και για την παρουσίασή τους στην ανώτατη διοίκηση. Ο κύριος της διαδικασίας θα συμβουλεύεται επίσης τον διαχειριστή της βάσης δεδομένων αναφοράς, πριν αποφασίσει σχετικά με τις λεπτομέρειες του έργου με τεχνολογία αναγνώρισης προσώπου, προκειμένου να κατανοήσει τόσο τον σκοπό χρήσης της βάσης δεδομένων αναφοράς όσο και τις τεχνικές λεπτομέρειες της. Σε περίπτωση επανεκπαίδευσης μιας προμηθευόμενης τεχνολογίας αναγνώρισης προσώπου, ο κύριος της διαδικασίας θα είναι επίσης υπεύθυνος για την επιλογή του συνόλου των δεδομένων εκπαίδευσης. Ως μονάδα επιφορτισμένη με την ανάπτυξη και τη λήψη αποφάσεων σχετικά με τις λεπτομέρειες του έργου, ο κύριος της διαδικασίας είναι υπεύθυνος για τη διενέργεια της ΕΑΠΔ.
- Τμήμα ΤΝ ΤΠ ή/και επιστήμης δεδομένων — να συνδράμει στη διενέργεια ΕΑΠΔ, να εξηγεί τους δείκτες μετρήσεων που είναι διαθέσιμοι για τη μέτρηση των επιδόσεων του συστήματος, της αμεροληψίας[72] και της πιθανής μεροληψίας, να εφαρμόζει την τεχνολογία και τις τεχνικές διασφαλίσεις, προκειμένου να αποτραπούν μη εξουσιοδοτημένη πρόσβαση στα συλλεχθέντα δεδομένα, κυβερνοεπιθέσεις κ.λπ. Σε περίπτωση επανεκπαίδευσης μιας προμηθευόμενης τεχνολογίας αναγνώρισης προσώπου, το τμήμα ΤΝ ΤΠ ή επιστήμης δεδομένων θα εκπαιδεύσει

[70] Οι ακόλουθοι ρόλοι είναι ενδεικτικοί των διαφορετικών ενδιαφερόμενων μερών και των αρμοδιοτήτων τους σε ένα έργο με τεχνολογία αναγνώρισης προσώπου. Ενώ η γλώσσα που χρησιμοποιείται για την περιγραφή των ρόλων στο παρόν παράρτημα δεν είναι κατηγορηματική, κάθε αρχή επιβολής του νόμου πρέπει να καθορίζει και να αναθέτει παρόμοιους ρόλους ανάλογα με την οργάνωσή της. Μπορεί να συμβαίνει μια μονάδα να συσσωρεύει περισσότερους από έναν ρόλους, για παράδειγμα κύριος της διαδικασίας και διαχειριστής βάσης δεδομένων αναφοράς, ή κύριος της διαδικασίας και τμήμα ΤΝ ΤΠ και/ή επιστήμης δεδομένων (σε περίπτωση που η μονάδα του κυρίου της διαδικασίας διαθέτει όλες τις απαραίτητες τεχνικές γνώσεις).

[71] Η βαθμολογία εμπιστοσύνης είναι το επίπεδο εμπιστοσύνης της πρόβλεψης (αντιστοίχιση), με τη μορφή πιθανότητας. Π.χ. συγκρίνοντας δύο υποδείγματα, υπάρχει 90 % εμπιστοσύνη ότι αυτά ανήκουν στο ίδιο άτομο. Η βαθμολογία εμπιστοσύνης είναι διαφορετική από την απόδοση της τεχνολογίας αναγνώρισης προσώπου, ωστόσο επηρεάζει την απόδοση. Όσο υψηλότερο είναι το όριο εμπιστοσύνης, τόσο λιγότερα ψευδώς θετικά αποτελέσματα και περισσότερα ψευδώς αρνητικά αποτελέσματα υπάρχουν στα αποτελέσματα της τεχνολογίας αναγνώρισης προσώπου.

[72] Η αμεροληψία μπορεί να οριστεί ως η έλλειψη αθέμιτων, παράνομων διακρίσεων, όπως η προκατάληψη λόγω φύλου ή φυλής.

το σύστημα, με βάση το σύνολο δεδομένων εκπαίδευσης που παρέχεται από τον κύριο της διαδικασίας. Η εν λόγω υπηρεσία θα είναι επίσης υπεύθυνη για τη θέσπιση των μέτρων για τον μετριασμό των κινδύνων που προσδιορίζονται από κοινού από τους κυρίους της διαδικασίας (π.χ. ειδικοί κίνδυνοι ΤΝ, όπως επιθέσεις συναγωγής συμπερασμάτων μοντέλου).

- Οι τελικοί χρήστες (όπως οι αστυνομικοί στο πεδίο επιχειρήσεων ή στα εγκληματολογικά εργαστήρια) — να διεξάγουν σύγκριση με τη βάση δεδομένων, να επανεξετάζουν κριτικά τα αποτελέσματα λαμβάνοντας υπόψη προηγούμενα στοιχεία και να παρέχουν ανατροφοδότηση στον κύριο της διαδικασίας για ψευδή θετικά αποτελέσματα και ενδείξεις πιθανών διακρίσεων.
- Διαχειριστής βάσης δεδομένων αναφοράς — η συγκεκριμένη μονάδα εντός της αρμόδιας αρχής επιβολής του νόμου που είναι υπεύθυνη για τη συσσώρευση και τη διαχείριση της βάσης δεδομένων αναφοράς, δηλαδή της βάσης δεδομένων με την οποία θα συγκριθούν οι εικόνες, συμπεριλαμβανομένης της διαγραφής των εικόνων προσώπου μετά την καθορισμένη περίοδο διατήρησης. Μια τέτοια βάση δεδομένων μπορεί να δημιουργηθεί ειδικά για το προβλεπόμενο έργο με τεχνολογία αναγνώρισης προσώπου ή μπορεί να προϋπάρχει, για συμβατούς σκοπούς. Ο διαχειριστής της βάσης δεδομένων αναφοράς είναι υπεύθυνος για τον καθορισμό του πότε και υπό ποιες συνθήκες μπορούν να αποθηκευτούν οι εικόνες προσώπου, καθώς και για τον καθορισμό των απαιτήσεων διατήρησης των δεδομένων τους (σύμφωνα με χρονικά ή άλλα κριτήρια).

Δεδομένου ότι οι περισσότερες περιπτώσεις εγκατάστασης και χρήσης της τεχνολογίας αναγνώρισης προσώπου ενέχουν εγγενή υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, η εποπτική αρχή προστασίας δεδομένων θα πρέπει επίσης να συμμετέχει στο πλαίσιο της προηγούμενης διαβούλευσης που απαιτείται βάσει του άρθρου 28 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

2. ΈΝΑΡΞΗ/ΠΡΙΝ ΑΠΟ ΤΗΝ ΠΡΟΜΗΘΕΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ

Ο κύριος της διαδικασίας σε μια αρχή επιβολής του νόμου θα πρέπει πρώτα να έχει σαφή κατανόηση της διαδικασίας ή των διαδικασιών που αποσκοπούν στη χρήση τεχνολογίας αναγνώρισης προσώπου (της περίπτωσης ή των περιπτώσεων χρήσης) και να διασφαλίζει ότι υπάρχει νομική βάση για την αιτιολόγηση της προβλεπόμενης περίπτωσης χρήσης. Με βάση τα ανωτέρω, πρέπει:

- Να γίνει επίσημη περιγραφή της περίπτωσης χρήσης. Πρέπει να περιγραφεί το πρόβλημα που πρέπει να επιλυθεί και ο τρόπος με τον οποίο η τεχνολογία αναγνώρισης προσώπου θα παράσχει λύση, καθώς και η επισκόπηση της διαδικασίας (έργου) στην οποία θα εφαρμοστεί. Στο πλαίσιο αυτό, οι αρχές επιβολής του νόμου θα πρέπει να τεκμηριώνουν τουλάχιστον[73]:
  - Τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που καταγράφονται στη διαδικασία
  - Τους στόχους και τους συγκεκριμένους σκοπούς για τους οποίους θα χρησιμοποιηθεί η τεχνολογία αναγνώρισης προσώπου, συμπεριλαμβανομένων των πιθανών συνεπειών για το υποκείμενο των δεδομένων μετά από αντιστοιχία.
  - Πότε και πώς θα συλλέγονται οι εικόνες προσώπου (συμπεριλαμβανομένων πληροφοριών σχετικά με το πλαίσιο της εν λόγω συλλογής, π.χ. στη θύρα του αερολιμένα, βίντεο από κάμερες ασφαλείας εκτός του καταστήματος όπου διαπράχθηκε το έγκλημα κ.λπ. και τις

[73] Στο παράρτημα Ι παρατίθεται κατάλογος των στοιχείων που βοηθούν τον υπεύθυνο επεξεργασίας να περιγράψει μια υπόθεση χρήσης τεχνολογίας αναγνώρισης προσώπου.

κατηγορίες των υποκειμένων των δεδομένων των οποίων τα βιομετρικά δεδομένα θα υποβληθούν σε επεξεργασία).

- Τη βάση δεδομένων με την οποία θα συγκριθούν οι εικόνες (βάση δεδομένων αναφοράς), καθώς και πληροφορίες σχετικά με τον τρόπο δημιουργίας της, το μέγεθός της και την ποιότητα των βιομετρικών δεδομένων που περιέχει.
- Τους φορείς της αρχής επιβολής του νόμου που θα εξουσιοδοτηθούν να χρησιμοποιούν το σύστημα τεχνολογίας αναγνώρισης προσώπου και να ενεργούν με αυτό στο πλαίσιο της επιβολής του νόμου (τα προφίλ και τα δικαιώματα πρόσβασης πρέπει να καθοριστούν από τον κύριο της διαδικασίας).
- Την προβλεπόμενη περίοδο διατήρησης των δεδομένων εισόδου, ή τη χρονική στιγμή που θα καθοριστεί η λήξη της εν λόγω περιόδου (όπως η περάτωση ή ο τερματισμός της ποινικής διαδικασίας σύμφωνα με το εθνικό δικονομικό δίκαιο για το οποίο συλλέχθηκαν αρχικά), καθώς και κάθε μεταγενέστερη ενέργεια (διαγραφή των εν λόγω δεδομένων, ανωνυμοποίηση και χρήση για στατιστικούς ή ερευνητικούς σκοπούς κ.λπ.).
- Την εφαρμογή καταχωρήσεων και την προσβασιμότητα των καταχωρίσεων και των αρχείων που τηρούνται.
- Τους δείκτες μέτρησης επιδόσεων (π.χ. ορθότητας, ακρίβεια, ανάκλησης, βαθμολογίας F1) και τα ελάχιστα αποδεκτά κατώτατα όρια.[74]
- Την εκτίμηση του αριθμού των ατόμων που θα υπόκεινται σε τεχνολογία αναγνώρισης προσώπου και σε ποια χρονική περίοδο/περίπτωση.

- Να γίνει αξιολόγηση της αναγκαιότητας και της αναλογικότητας[75]. Το γεγονός ότι υπάρχει η εν λόγω τεχνολογία δεν θα πρέπει να αποτελεί κίνητρο για την εφαρμογή της. Ο κύριος της διαδικασίας πρέπει πρώτα να αξιολογήσει κατά πόσον υπάρχει κατάλληλη νομική βάση για την προβλεπόμενη επεξεργασία. Για τον σκοπό αυτό, πρέπει να ζητηθεί η γνώμη του ΥΠΔ και της νομικής υπηρεσίας. Ο παράγοντας καθορισμού της εγκατάστασης της τεχνολογίας αναγνώρισης προσώπου θα πρέπει να είναι ότι αποτελεί αναγκαία και αναλογική λύση για ένα ειδικά καθορισμένο πρόβλημα των αρχών επιβολής του νόμου. Αυτό πρέπει να αξιολογείται ανάλογα με τον σκοπό/τη σοβαρότητα του εγκλήματος/τον αριθμό των ατόμων που δεν εμπλέκονται αλλά επηρεάζονται από το σύστημα τεχνολογίας αναγνώρισης προσώπου. Για την αξιολόγηση της νομιμότητας, θα πρέπει να λαμβάνονται υπόψη τουλάχιστον τα ακόλουθα: Η οδηγία για την

[74] Υπάρχουν διάφοροι δείκτες μέτρησης για την αξιολόγηση της απόδοσης ενός συστήματος τεχνολογίας αναγνώρισης προσώπου. Κάθε δείκτης μέτρησης παρέχει μια διαφορετική άποψη των αποτελεσμάτων του συστήματος και η επιτυχία του στην παροχή μιας επαρκούς εικόνας για το αν το σύστημα τεχνολογίας αναγνώρισης προσώπου αποδίδει καλά ή όχι εξαρτάται από την περίπτωση χρήσης τεχνολογίας αναγνώρισης προσώπου. Εάν δίνεται έμφαση στην επίτευξη υψηλών ποσοστών ορθής αντιστοίχισης ενός προσώπου, θα μπορούσαν να χρησιμοποιηθούν δείκτες μέτρησης όπως η ακρίβεια και η ανάκληση. Ωστόσο, αυτοί οι δείκτες μέτρησης δεν μετρούν πόσο καλά η τεχνολογία αναγνώρισης προσώπου χειρίζεται τα αρνητικά παραδείγματα (πόσα από αυτά αντιστοιχίστηκαν εσφαλμένα από το σύστημα). Ο κύριος της διαδικασίας, με την υποστήριξη του τμήματος ΤΝ ΤΠ και επιστήμης δεδομένων, θα πρέπει να είναι σε θέση να καθορίζει τις απαιτήσεις επιδόσεων και να τις εκφράζει στον πλέον κατάλληλο δείκτη μέτρησης σύμφωνα με την περίπτωση χρήσης τεχνολογίας αναγνώρισης προσώπου.

[75] Μπορεί να εξεταστεί το ενδεχόμενο λήψης περαιτέρω μέτρων για τη φροντίδα της αναγκαιότητας όσον αφορά την προσαρμογή και τη χρήση του συστήματος, επομένως η περιγραφή της περίπτωσης χρήσης μπορεί επίσης να αλλάξει ελαφρώς κατά την αξιολόγηση της αναγκαιότητας και της αναλογικότητας.

προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου[76], ο ΓΚΠΔ[77] [78] κάθε υφιστάμενο νομικό πλαίσιο για την ΤΝ[79] και όλες τις συνοδευτικές κατευθυντήριες γραμμές που παρέχονται από τις εποπτικές αρχές προστασίας δεδομένων (όπως οι κατευθυντήριες γραμμές 3/2019 του ΕΣΠΔ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών[80]). Οι εν λόγω πράξεις της νομοθεσίας της ΕΕ θα πρέπει πάντα να επιβεβαιώνονται με τις ισχύουσες εθνικές απαιτήσεις, ιδίως στον τομέα του ποινικού δικονομικού δικαίου. Η αξιολόγηση της αναλογικότητας θα πρέπει να προσδιορίζει τα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων που ενδέχεται να θίγονται (πέραν της προστασίας της ιδιωτικής ζωής και των δεδομένων). Θα πρέπει επίσης να περιγράφει και να εξετάζει τυχόν όρια (ή έλλειψη ορίων) που επιβάλλονται στην περίπτωση χρήσης στο σύστημα τεχνολογίας αναγνώρισης προσώπου. Για παράδειγμα, εάν το σύστημα θα λειτουργεί συνεχώς ή προσωρινά και αν θα περιορίζεται σε μια γεωγραφική περιοχή.

- Να γίνει εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) [81]. Θα πρέπει να διενεργείται ΕΑΠΔ, δεδομένου ότι η εγκατάσταση τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων[82]. Η ΕΑΠΔ θα πρέπει να περιλαμβάνει ειδικότερα: γενική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας[83], εκτίμηση των κινδύνων για τα

[76] Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

[77] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

[78] Σε περιπτώσεις κατά τις οποίες ένα επιστημονικό έργο που αποσκοπεί στην έρευνα της χρήσης τεχνολογίας αναγνώρισης προσώπου θα πρέπει να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα, αλλά η εν λόγω επεξεργασία δεν εμπίπτει στο άρθρο 4 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, σε γενικές γραμμές, εφαρμόζεται ο ΓΚΠΔ (άρθρο 9 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου). Σε περίπτωση πιλοτικών έργων που ακολουθούνται από επιχειρήσεις επιβολής του νόμου, η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου εξακολουθεί να είναι εφαρμοστέα.

[79] Για παράδειγμα, υπάρχει πρόταση ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΓΙΑ ΤΗ ΘΕΣΠΙΣΗ ΕΝΑΡΜΟΝΙΣΜΕΝΩΝ ΚΑΝΟΝΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ (ΠΡΑΞΗ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ) ΚΑΙ ΓΙΑ ΤΗΝ ΤΡΟΠΟΠΟΙΗΣΗ ΟΡΙΣΜΕΝΩΝ ΝΟΜΟΘΕΤΙΚΩΝ ΠΡΑΞΕΩΝ ΤΗΣ ΕΝΩΣΗΣ, ωστόσο αυτή δεν έχει ακόμη θεσπιστεί ως κανονισμός.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Περαιτέρω καθοδήγηση σχετικά με τις ΕΑΠΔ διατίθεται στα: Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του εάν η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, WP 248 αναθ. 01, διαθέσιμες στη διεύθυνση: https://ec.europa.eu/newsroom/article29/items/611236 και «EDPS Accountability on the ground toolkit, part II» (Εργαλειοθήκη του ΕΕΠΔ Λογοδοσία στην πράξη, μέρος ΙΙ), διαθέσιμο στη διεύθυνση: https://edps.europa.eu/node/4582_en

[82] Η τεχνολογία αναγνώρισης προσώπου, ανάλογα με την περίπτωση χρήσης, μπορεί να εμπίπτει στα ακόλουθα κριτήρια που ενεργοποιούν την επεξεργασία υψηλού κινδύνου (από τις κατευθυντήριες γραμμές για την ΕΑΠΔ, WP 248 αναθ. 01): Συστηματική παρακολούθηση, επεξεργασία δεδομένων μεγάλης κλίμακας, αντιστοίχιση ή συνδυασμός συνόλων δεδομένων, καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων.

[83] Η περιγραφή της επεξεργασίας, καθώς και η αξιολόγηση της αναγκαιότητας και της αναλογικότητας, όπως έχει ήδη περιγραφεί στα παραπάνω βήματα, αποτελούν επίσης μέρος της ΕΑΠΔ, εκτός από την εκτίμηση κινδύνου. Εάν χρειαστεί, στην ΕΑΠΔ θα παρέχεται λεπτομερέστερη περιγραφή των ροών δεδομένων προσωπικού χαρακτήρα.

δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων[84], τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων αυτών, διασφαλίσεις, μέτρα ασφαλείας και μηχανισμούς, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση. Η ΕΑΠΔ είναι μια υπό εξέλιξη διαδικασία, επομένως τυχόν νέα στοιχεία της επεξεργασίας θα πρέπει να προστίθενται και η εκτίμηση κινδύνων θα πρέπει να επικαιροποιείται σε κάθε στάδιο του έργου.

- Να ληφθεί έγκριση από την ανώτατη διοίκηση εξηγώντας τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (από την περίπτωση χρήσης και την τεχνολογία) και τα αντίστοιχα σχέδια αντιμετώπισης των κινδύνων.

3. ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ ΤΗΣ ΠΡΟΜΗΘΕΙΑΣ ΚΑΙ ΠΡΙΝ ΑΠΟ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ

- Να αποφασιστούν τα κριτήρια για την επιλογή της τεχνολογίας αναγνώρισης προσώπου (αλγορίθμου). Ο κύριος της διαδικασίας θα πρέπει να αποφασίσει τα κριτήρια για την επιλογή ενός αλγορίθμου, με τη βοήθεια του τμήματος ΤΝ ΤΠ ή/και επιστήμης δεδομένων. Στην πράξη, αυτά θα περιλαμβάνουν δείκτες μέτρησης της αμεροληψίας και των επιδόσεων που αποφασίζονται στην περιγραφή της περίπτωσης χρήσης. Τα εν λόγω κριτήρια θα πρέπει επίσης να περιλαμβάνουν πληροφορίες σχετικά με τα δεδομένα με τα οποία εκπαιδεύτηκε ο αλγόριθμος. Το σύνολο εκπαίδευσης, δοκιμών και επικύρωσης πρέπει να περιλαμβάνει επαρκώς δείγματα όλων των χαρακτηριστικών των υποκειμένων των δεδομένων που πρόκειται να υποβληθούν σε τεχνολογία αναγνώρισης προσώπου (να ληφθούν υπόψη για παράδειγμα η ηλικία, το φύλο και η φυλή) για να μειωθεί η μεροληψία. Ο πάροχος υπηρεσιών τεχνολογίας αναγνώρισης προσώπου θα πρέπει να παρέχει πληροφορίες και μετρήσεις σχετικά με τα σύνολα δεδομένων εκπαίδευσης, δοκιμών και επικύρωσης τεχνολογίας αναγνώρισης προσώπου, και να περιγράφει τα μέτρα που λαμβάνονται για τη μέτρηση και τον μετριασμό πιθανών παράνομων διακρίσεων και μεροληψιών. Ο κύριος της διαδικασίας, όπου είναι δυνατόν, πρέπει να ελέγχει κατά πόσον υπήρχε νομική βάση για τη χρήση του εν λόγω συνόλου δεδομένων από τον πάροχο για τον σκοπό της εκπαίδευσης των αλγορίθμων (με βάση τις πληροφορίες που θα διαθέσει ο πάροχος). Επίσης, ο κύριος της διαδικασίας θα πρέπει να διασφαλίζει ότι ο πάροχος υπηρεσιών τεχνολογίας αναγνώρισης προσώπου εφαρμόζει πρότυπα ασφάλειας που σχετίζονται με τα βιομετρικά δεδομένα, όπως το πρότυπο ISO/IEC 24745, το οποίο παρέχει καθοδήγηση για την προστασία των βιομετρικών πληροφοριών υπό διάφορες απαιτήσεις εμπιστευτικότητας, ακεραιότητας και δυνατότητας ανανέωσης/ανάκλησης κατά την αποθήκευση και τη διαβίβαση, καθώς και απαιτήσεις και κατευθυντήριες γραμμές για την ασφαλή και συμβατή με την προστασία της ιδιωτικής ζωής διαχείριση και επεξεργασία βιομετρικών πληροφοριών.

- Να επανεκπαιδευτεί ο αλγόριθμος (εάν είναι απαραίτητο). Ο κύριος της διαδικασίας θα πρέπει να διασφαλίζει ότι η τελειοποίηση του συστήματος τεχνολογίας αναγνώρισης προσώπου για την επίτευξη μεγαλύτερης ορθότητας πριν από τη χρήση του αποτελεί επίσης μέρος των υπηρεσιών που ανατίθενται. Σε περίπτωση που απαιτείται πρόσθετη εκπαίδευση του αποκτηθέντος συστήματος τεχνολογίας αναγνώρισης προσώπου για την τήρηση του δείκτη μέτρησης

[84] Η ανάλυση των κινδύνων για τα υποκείμενα των δεδομένων θα πρέπει να περιλαμβάνει κινδύνους που σχετίζονται με την τοποθεσία των προς σύγκριση εικόνων προσώπου (τοπικά/απομακρυσμένα), τους κινδύνους που σχετίζονται με τους εκτελούντες την επεξεργασία/υπεργολάβους επεξεργασίας, καθώς και τους κινδύνους που αφορούν ειδικά τη μηχανική μάθηση όταν αυτή εφαρμόζεται (π.χ. μόλυνση δεδομένων, αντιπαραθετικά παραδείγματα).

ορθότητας, ο κύριος της διαδικασίας, εκτός από τη λήψη της απόφασης για επανεκπαίδευση, πρέπει να αποφασίσει, με τη βοήθεια του τμήματος ΤΠ ΤΝ και/ή επιστήμης δεδομένων σχετικά με το κατάλληλο, αντιπροσωπευτικό σύνολο δεδομένων που θα χρησιμοποιηθεί και να ελέγξει τη νομιμότητα αυτής της χρήσης για τα δεδομένα.

- Να καθοριστούν οι κατάλληλες διασφαλίσεις για την αντιμετώπιση των κινδύνων που σχετίζονται με την ασφάλεια, τη μεροληψία και τις χαμηλές επιδόσεις. Αυτό περιλαμβάνει την καθιέρωση μιας διαδικασίας παρακολούθησης της τεχνολογίας αναγνώρισης προσώπου μετά τη χρήση της (καταχωρίσεις και ανατροφοδότηση για την ορθότητα και την αμεροληψία των αποτελεσμάτων). Επιπλέον, να διασφαλίζεται ότι οι κίνδυνοι που αφορούν ειδικά ορισμένα συστήματα μηχανικής μάθησης και τεχνολογίας αναγνώρισης προσώπου (π.χ. μόλυνση δεδομένων, αντιπαραθετικά παραδείγματα, αντιστροφή μοντέλου, συμπερασματολογία λευκού κουτιού) εντοπίζονται, μετρώνται και μετριάζονται. Ο κύριος της διαδικασίας θα πρέπει επίσης να ορίσει κατάλληλες διασφαλίσεις για να διασφαλίσει ότι θα τηρηθούν οι απαιτήσεις διατήρησης δεδομένων για τα βιομετρικά δεδομένα που περιλαμβάνονται στο σύνολο δεδομένων επανεκπαίδευσης.
- Να τεκμηριώνεται το σύστημα τεχνολογίας αναγνώρισης προσώπου. Αυτό θα πρέπει να περιλαμβάνει γενική περιγραφή του συστήματος τεχνολογίας αναγνώρισης προσώπου, λεπτομερή περιγραφή των στοιχείων του συστήματος τεχνολογίας αναγνώρισης προσώπου και της διαδικασίας για τη θέσπισή του, λεπτομερείς πληροφορίες σχετικά με την παρακολούθηση, τη λειτουργία και τον έλεγχο του συστήματος τεχνολογίας αναγνώρισης προσώπου και λεπτομερή περιγραφή των κινδύνων και των μέτρων μετριασμού. Τα στοιχεία που περιλαμβάνονται στην εν λόγω τεκμηρίωση θα περιλαμβάνουν τα κύρια στοιχεία της περιγραφής του συστήματος τεχνολογίας αναγνώρισης προσώπου από τις προηγούμενες φάσεις (βλ. ανωτέρω), ωστόσο αυτά θα εμπλουτίζονται με πληροφορίες σχετικά με την παρακολούθηση των επιδόσεων και την εφαρμογή αλλαγών στο σύστημα, συμπεριλαμβανομένων τυχόν ενημερώσεων εκδόσεων ή/και επανεκπαίδευσης.
- Να δημιουργούνται εγχειρίδια χρήστη, εξηγώντας την τεχνολογία και τις περιπτώσεις χρήσης. Αυτά πρέπει να εξηγούν με σαφήνεια όλα τα σενάρια και τις προϋποθέσεις υπό τις οποίες θα χρησιμοποιηθεί η τεχνολογία αναγνώρισης προσώπου.
- Να γίνεται εκπαίδευση των τελικών χρηστών σχετικά με τον τρόπο χρήσης της τεχνολογίας. Η εν λόγω εκπαίδευση πρέπει να εξηγεί τις δυνατότητες και τους περιορισμούς της τεχνολογίας, ώστε οι χρήστες να κατανοούν τις συνθήκες υπό τις οποίες είναι απαραίτητο να την εφαρμόζουν και τις περιπτώσεις στις οποίες μπορεί να είναι ανακριβής. Τα εν λόγω προγράμματα εκπαίδευσης θα συμβάλουν επίσης στον μετριασμό των κινδύνων που σχετίζονται με τη μη επαλήθευση/κριτική του αποτελέσματος του αλγορίθμου.
- Να γίνεται διαβούλευση με την εποπτική αρχή προστασίας δεδομένων, σύμφωνα με το άρθρο 28 παράγραφος 1 στοιχείο β) της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου. Να παρέχονται πληροφορίες σύμφωνα με το άρθρο 13 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου με σκοπό την ενημέρωση των υποκειμένων των δεδομένων σχετικά με την επεξεργασία και τα δικαιώματά τους. Οι εν λόγω παρατηρήσεις πρέπει να απευθύνονται στα υποκείμενα των δεδομένων σε κατάλληλη γλώσσα, ώστε αυτά να είναι σε θέση να κατανοούν την επεξεργασία και να εξηγούν τα βασικά στοιχεία της τεχνολογίας, συμπεριλαμβανομένων των ποσοστών ακρίβειας, των συνόλων δεδομένων εκπαίδευσης και των μέτρων που λαμβάνονται για την αποφυγή διακρίσεων και της χαμηλής ακρίβειας του αλγόριθμου.

4. ΣΥΣΤΑΣΕΙΣ ΜΕΤΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ

- Να διασφαλίζεται η ανθρώπινη παρέμβαση και εποπτεία των αποτελεσμάτων. Να μην λαμβάνεται κανένα μέτρο που να αφορά φυσικό πρόσωπο αποκλειστικά και μόνο βάσει της έκβασης της τεχνολογίας αναγνώρισης προσώπου (αυτό θα συνεπαγόταν παραβίαση του άρθρου 11 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου —αυτοματοποιημένη ατομική λήψη αποφάσεων με νομικές ή άλλες παρόμοιες συνέπειες για το υποκείμενο των δεδομένων). Να διασφαλίζεται ότι ένας υπάλληλος της αρχής επιβολής του νόμου επανεξετάζει τα αποτελέσματα της τεχνολογίας αναγνώρισης προσώπου. Να βεβαιώνεται επίσης ότι οι χρήστες της αρχής επιβολής του νόμου αποφεύγουν τη μεροληψία της αυτοματοποίησης, διερευνώντας αντιφατικές πληροφορίες και αμφισβητώντας κριτικά τα αποτελέσματα της τεχνολογίας. Για τον σκοπό αυτό, η συνεχής εκπαίδευση και η ευαισθητοποίηση των τελικών χρηστών είναι σημαντική, ωστόσο τα ανώτατα διοικητικά στελέχη θα πρέπει να διασφαλίζουν ότι υπάρχουν επαρκείς ανθρώπινοι πόροι για την άσκηση αποτελεσματικής εποπτείας. Αυτό συνεπάγεται την παροχή επαρκούς χρόνου σε κάθε παράγοντα για την κριτική αμφισβήτηση των αποτελεσμάτων της τεχνολογίας. Να γίνεται καταγραφή, μέτρηση και αξιολόγηση του βαθμού στον οποίο η ανθρώπινη εποπτεία αλλάζει την αρχική απόφαση της τεχνολογίας αναγνώρισης προσώπου.
- Να παρακολουθείται και να αντιμετωπίζεται η απόκλιση του μοντέλου τεχνολογίας αναγνώρισης προσώπου (υποβάθμιση των επιδόσεων) μόλις το μοντέλο τεθεί σε παραγωγική λειτουργία.
- Να καθιερώνεται μια διαδικασία για την επαναξιολόγηση των κινδύνων και των μέτρων ασφαλείας τακτικά και κάθε φορά που η τεχνολογία ή η περίπτωση χρήσης υφίσταται αλλαγές.
- Να τεκμηριώνεται κάθε αλλαγή στο σύστημα καθ' όλη τη διάρκεια του κύκλου ζωής του (π.χ. αναβαθμίσεις, επανεκπαίδευση).
- Να καθιερώνεται μια διαδικασία καθώς και οι σχετικές τεχνικές δυνατότητες για την αντιμετώπιση των αιτημάτων πρόσβασης των υποκειμένων των δεδομένων. Η τεχνική ικανότητα για την εξαγωγή δεδομένων, εάν υπάρχει ανάγκη παροχής τους στα υποκείμενα των δεδομένων, πρέπει να υπάρχει πριν από την υποβολή οποιουδήποτε αιτήματος.
- Να διασφαλίζεται ότι υπάρχουν διαδικασίες για παραβιάσεις δεδομένων. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των βιομετρικών δεδομένων, οι κίνδυνοι είναι πιθανό να είναι υψηλοί. Στην περίπτωση αυτή, όλοι οι εμπλεκόμενοι χρήστες θα πρέπει να γνωρίζουν τις σχετικές διαδικασίες που πρέπει να ακολουθήσουν, ο ΥΠΔ θα πρέπει να ενημερωθεί αμέσως και τα υποκείμενα των δεδομένων να ενημερωθούν.

ΠΑΡΑΡΤΗΜΑ III — ΠΡΑΚΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ

Υπάρχουν πολλές διαφορετικές πρακτικές ρυθμίσεις και σκοποί για τη χρήση της αναγνώρισης προσώπου, για παράδειγμα σε ελεγχόμενα περιβάλλοντα, όπως σε συνοριακές διαβάσεις, διασταύρωση με δεδομένα από αστυνομικές βάσεις δεδομένων ή από προσωπικά δεδομένα που έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων, ζωντανές ροές από κάμερες (ζωντανή αναγνώριση προσώπου) κ.λπ. Κατά συνέπεια, οι κίνδυνοι για την προστασία των δεδομένων προσωπικού χαρακτήρα και άλλων θεμελιωδών δικαιωμάτων και ελευθεριών διαφέρουν σημαντικά στις διάφορες περιπτώσεις χρήσης. Προκειμένου να διευκολυνθεί η αξιολόγηση της αναγκαιότητας και της αναλογικότητας, η οποία θα πρέπει να προηγείται της απόφασης σχετικά με την πιθανή εγκατάσταση της αναγνώρισης προσώπου, οι τρέχουσες κατευθυντήριες γραμμές παρέχουν μη εξαντλητικό κατάλογο πιθανών εφαρμογών της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου.

Τα σενάρια που παρουσιάζονται και αξιολογούνται βασίζονται σε **υποθετικές** καταστάσεις και αποσκοπούν στην απεικόνιση ορισμένων συγκεκριμένων χρήσεων της τεχνολογίας αναγνώρισης προσώπου και στην παροχή βοήθειας για κατά περίπτωση εκτιμήσεις, καθώς και στον καθορισμό ενός συνολικού πλαισίου. Δεν φιλοδοξούν να είναι εξαντλητικές και δεν θίγουν τυχόν τρέχουσες ή μελλοντικές διαδικασίες που αναλαμβάνονται από εθνική εποπτική αρχή όσον αφορά τον σχεδιασμό, τον πειραματισμό ή την εφαρμογή τεχνολογιών αναγνώρισης προσώπου. Η παρουσίαση αυτών των σεναρίων θα πρέπει να εξυπηρετεί μόνο τον σκοπό του αντιπροσωπευτικού δείγματος της καθοδήγησης προς τους υπεύθυνους χάραξης πολιτικής, τους νομοθέτες και τις αρχές επιβολής του νόμου, που παρέχεται ήδη στο παρόν έγγραφο, κατά τον σχεδιασμό και την εξέταση της εφαρμογής τεχνολογιών αναγνώρισης προσώπων, προκειμένου να διασφαλιστεί η πλήρης συμμόρφωση με το κεκτημένο της ΕΕ στον τομέα της προστασίας των δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, θα πρέπει να ληφθεί υπόψη ότι, ακόμη και σε παρόμοιες καταστάσεις χρήσης τεχνολογίας αναγνώρισης προσώπου, η παρουσία ή η απουσία ορισμένων στοιχείων μπορεί να οδηγήσει σε διαφορετικό αποτέλεσμα της αξιολόγησης της αναγκαιότητας και της αναλογικότητας.

1 ΣΕΝΑΡΙΟ 1

1.1. Περιγραφή

Ένα σύστημα αυτοματοποιημένου συνοριακού ελέγχου που επιτρέπει την αυτοματοποιημένη διέλευση των συνόρων με τον έλεγχο της ταυτότητας της βιομετρικής εικόνας που είναι αποθηκευμένη στο ηλεκτρονικό ταξιδιωτικό έγγραφο των πολιτών της ΕΕ και άλλων ταξιδιωτών που διέρχονται από τη συνοριακή διάβαση και την εξακρίβωση ότι ο επιβάτης είναι ο νόμιμος κάτοχος του εγγράφου.

Η εν λόγω επαλήθευση/έλεγχος της ταυτότητας περιλαμβάνει αναγνώριση προσώπου μόνο ένα προς ένα και διενεργείται σε ελεγχόμενο περιβάλλον (π.χ. σε ηλεκτρονικές θύρες αερολιμένων). Τα βιομετρικά δεδομένα του ταξιδιώτη που διέρχεται από τη συνοριακή διάβαση καταγράφονται όταν αυτός/αυτή καλείται ρητά να κοιτάξει την κάμερα στην ηλεκτρονική θύρα και συγκρίνονται με εκείνα του προσκομιζόμενου εγγράφου (διαβατήριο, ταυτότητα κ.λπ.) το οποίο εκδίδεται σύμφωνα με συγκεκριμένες τεχνικές απαιτήσεις.

Ταυτόχρονα, ενώ η επεξεργασία σε τέτοιες περιπτώσεις δεν εμπίπτει κατ' αρχήν στο πεδίο εφαρμογής της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, το αποτέλεσμα της επαλήθευσης μπορεί επίσης να χρησιμοποιηθεί για την αντιστοίχιση

(αλφαριθμητικά) δεδομένων του προσώπου με τις βάσεις δεδομένων επιβολής του νόμου στο πλαίσιο του συνοριακού ελέγχου και, ως εκ τούτου, μπορεί να συνεπάγεται ενέργειες με σημαντική νομική ισχύ για το υποκείμενο των δεδομένων, π.χ. σύλληψη λόγω καταχώρισης στο SIS. Υπό ειδικές συνθήκες, τα βιομετρικά δεδομένα μπορούν επίσης να χρησιμοποιηθούν για την αναζήτηση αντιστοιχιών σε βάσεις δεδομένων επιβολής του νόμου (σε μια τέτοια περίπτωση, θα εκτελείται ταυτοποίηση 1 προς πολλά σε αυτό το βήμα).

Το αποτέλεσμα της επεξεργασίας βιομετρικών εικόνων έχει άμεσο αντίκτυπο στο υποκείμενο των δεδομένων: μόνο σε περίπτωση επιτυχούς επαλήθευσης επιτρέπει τη διέλευση των συνόρων. Σε περίπτωση ανεπιτυχούς ταυτοποίησης, οι συνοριοφύλακες πρέπει να πραγματοποιήσουν έναν δεύτερο έλεγχο για να διασφαλίσουν ότι το υποκείμενο των δεδομένων είναι διαφορετικό από εκείνο που απεικονίζεται στο έγγραφο ταυτοποίησης.

Σε περίπτωση εντοπισμού συναγερμικής ειδοποίησης στο SIS ή εθνικής συναγερμικής ειδοποίησης, οι συνοριοφύλακες πρέπει να διενεργήσουν δεύτερη επαλήθευση και τους αναγκαίους περαιτέρω ελέγχους και στη συνέχεια να προβούν σε κάθε αναγκαία ενέργεια, π.χ. σύλληψη του προσώπου, ενημέρωση των ενδιαφερόμενων αρχών.

Πηγή των πληροφοριών:
- Είδη υποκειμένων των δεδομένων: ☒ όλα τα άτομα που διέρχονται τα σύνορα
- Πηγή της εικόνας: ☒ άλλο (έγγραφο ταυτότητας)
- Σύνδεση με το έγκλημα: ☒ Δεν είναι απαραίτητο
- Τρόπος συλλογής πληροφοριών: ☒ σε θάλαμο ή ελεγχόμενο περιβάλλον
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα: Ναι, συγκεκριμένα: ☒ δικαίωμα ελεύθερης κυκλοφορίας ☒ δικαίωμα ασύλου

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):
- Εξειδίκευση ☒ ειδικές βάσεις δεδομένων που σχετίζονται με τον έλεγχο των συνόρων

Αλγόριθμος:
- Τύπος επαλήθευσης: ☒ 1-1 επαλήθευση (έλεγχος της ταυτότητας)

Αποτέλεσμα:
- Αντίκτυπος ☒ Άμεσος (επιτρέπεται ή απαγορεύεται η είσοδος στο υποκείμενο των δεδομένων)
- Αυτοματοποιημένη απόφαση: ☒ Ναι

1.2. Εφαρμοστέο νομικό πλαίσιο

Από το 2004, σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 2252/2004 του Συμβουλίου[85], τα διαβατήρια και άλλα ταξιδιωτικά έγγραφα που εκδίδονται από τα κράτη μέλη πρέπει να περιέχουν βιομετρική εικόνα προσώπου αποθηκευμένη σε ηλεκτρονικό τσιπ ενσωματωμένο στο έγγραφο.

Ο κώδικας συνόρων του Σένγκεν (ΚΣΣ)[86] καθορίζει τις απαιτήσεις για τους συνοριακούς ελέγχους προσώπων στα εξωτερικά σύνορα. Για τους πολίτες της ΕΕ και άλλα πρόσωπα που απολαύουν του δικαιώματος της ελεύθερης κυκλοφορίας σύμφωνα με το δίκαιο της Ένωσης, οι ελάχιστοι έλεγχοι θα πρέπει να συνίστανται στην επαλήθευση των ταξιδιωτικών τους εγγράφων, κατά περίπτωση με τη

[85] ΚΑΝΟΝΙΣΜΟΣ (ΕΚ) αριθ. 2252/2004 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Δεκεμβρίου 2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών.

[86] ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/399 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ της 9ης Μαρτίου 2016 περί κώδικα της Ένωσης σχετικά με το καθεστώς διέλευσης προσώπων από τα σύνορα (κώδικας συνόρων του Σένγκεν).

χρήση τεχνικών συσκευών. Ο ΚΣΣ τροποποιήθηκε στη συνέχεια με τον κανονισμό (ΕΕ) 2017/2225[87], ο οποίος εισήγαγε, μεταξύ άλλων, ορισμούς για τις «ηλεκτρονικές θύρες», το «αυτοματοποιημένο σύστημα συνοριακού ελέγχου» και το «σύστημα αυτοεξυπηρέτησης», καθώς και τη δυνατότητα επεξεργασίας βιομετρικών δεδομένων για τη διενέργεια συνοριακών ελέγχων.

Ως εκ τούτου, θα μπορούσε να θεωρηθεί ότι υπάρχει σαφής και προβλέψιμη νομική βάση που επιτρέπει αυτή τη μορφή επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Επιπλέον, το νομικό πλαίσιο θεσπίζεται σε επίπεδο Ένωσης και εφαρμόζεται άμεσα στα κράτη μέλη.

1.3. Αναγκαιότητα και αναλογικότητα — σκοπός/σοβαρότητα του εγκλήματος

Η επαλήθευση της ταυτότητας των πολιτών της ΕΕ στο πλαίσιο αυτοματοποιημένου συνοριακού ελέγχου, με τη χρήση της βιομετρικής εικόνας τους, αποτελεί στοιχείο των συνοριακών ελέγχων στα εξωτερικά σύνορα της ΕΕ. Κατά συνέπεια, συνδέεται άμεσα με την ασφάλεια των συνόρων και εξυπηρετεί έναν στόχο γενικού συμφέροντος που αναγνωρίζεται από την Ένωση. Επιπλέον, οι θύρες ΑΣΣΕ συμβάλλουν στην επιτάχυνση της διεκπεραίωσης των επιβατών και μειώνουν τον κίνδυνο ανθρώπινων σφαλμάτων. Επιπροσθέτως, το πεδίο εφαρμογής, η έκταση και η ένταση της παρέμβασης σε αυτό το σενάριο είναι πολύ πιο περιορισμένα σε σύγκριση με άλλες μορφές αναγνώρισης προσώπου. Ωστόσο, η επεξεργασία βιομετρικών δεδομένων δημιουργεί πρόσθετους κινδύνους για τα υποκείμενα των δεδομένων, οι οποίοι πρέπει να αντιμετωπιστούν και να μετριαστούν καταλλήλως από την αρμόδια αρχή που εγκαθιστά και λειτουργεί το σύστημα τεχνολογίας αναγνώρισης προσώπου.

1.4. Συμπέρασμα

Η επαλήθευση της ταυτότητας των πολιτών της ΕΕ στο πλαίσιο ενός αυτοματοποιημένου συνοριακού ελέγχου αποτελεί αναγκαίο και αναλογικό μέτρο, εφόσον υπάρχουν οι κατάλληλες διασφαλίσεις, ιδίως η εφαρμογή των αρχών του περιορισμού του σκοπού, της ποιότητας των δεδομένων, της διαφάνειας και του υψηλού επιπέδου ασφάλειας.

2 ΣΕΝΑΡΙΟ 2

2.1. Περιγραφή

Οι αρχές επιβολής του νόμου ορίζουν ένα σύστημα ταυτοποίησης των θυμάτων απαγωγής παιδιών. Εξουσιοδοτημένος αστυνομικός μπορεί να προβεί σε σύγκριση των βιομετρικών δεδομένων ενός παιδιού, για το οποίο υπάρχουν υποψίες ότι έχει απαχθεί, με βάση δεδομένων για τα θύματα απαγωγής παιδιών υπό αυστηρές προϋποθέσεις, με αποκλειστικό σκοπό τον εντοπισμό ανηλίκων που ενδέχεται να ανταποκρίνονται στην περιγραφή του εξαφανισμένου παιδιού για το οποίο έχει κινηθεί έρευνα και έχει εκδοθεί η συναγερμική ειδοποίηση.

Η επίμαχη επεξεργασία θα αποτελείται από τη σύγκριση του προσώπου ή της εικόνας ενός ατόμου, που μπορεί να αντιστοιχεί στην περιγραφή ενός παιδιού που αγνοείται, με τις εικόνες που είναι αποθηκευμένες στη βάση δεδομένων. Η εν λόγω επεξεργασία θα πραγματοποιείται σε συγκεκριμένες περιπτώσεις και όχι σε συστηματική βάση.

Η βάση δεδομένων με την οποία θα εφαρμοστεί η σύγκριση εμπλουτίζεται με φωτογραφίες εξαφανισμένων παιδιών για τα οποία έχει αναφερθεί υποψία απαγωγής παιδιών, απειλή για τη ζωή ή τη σωματική ακεραιότητα του παιδιού, και έχει κινηθεί ποινική έρευνα υπό δικαστική αρχή, και για τα οποία έχει εκδοθεί συναγερμική ειδοποίηση για απαγωγή παιδιών. Τα δεδομένα συλλέγονται στο

[87] Κανονισμός (ΕΕ) 2017/2225 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Νοεμβρίου 2017, για την τροποποίηση του κανονισμού (ΕΕ) 2016/399 όσον αφορά τη χρήση του συστήματος εισόδου/εξόδου.

πλαίσιο των διαδικασιών που καθορίζονται από την αρμόδια αρχή επιβολής του νόμου, δηλαδή από αστυνομικούς που είναι εξουσιοδοτημένοι να εκτελούν δικαστικές αστυνομικές αποστολές. Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που καταγράφονται είναι οι εξής:

- ταυτότητα, προσωνυμία, άλλο όνομα, γονική σχέση, ιθαγένεια, διευθύνσεις, διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμοί τηλεφώνου·
- ημερομηνία και τόπος γέννησης·
- πληροφορίες σχετικά με τη γονική συγγένεια·
- φωτογραφία με τεχνικά χαρακτηριστικά που επιτρέπουν τη χρήση συσκευής αναγνώρισης προσώπου και άλλες φωτογραφίες.

Τα αποτελέσματα της σύγκρισης πρέπει επίσης να επανεξετάζονται και να επαληθεύονται από εξουσιοδοτημένο υπάλληλο, προκειμένου να επιβεβαιώνονται τα προηγούμενα αποδεικτικά στοιχεία με το αποτέλεσμα της σύγκρισης και να αποκλείονται τυχόν ψευδώς θετικά αποτελέσματα.

Οι εικόνες παιδιών και τα δεδομένα προσωπικού χαρακτήρα μπορούν να διατηρούνται μόνο καθ' όλη τη διάρκεια της συναγερμικής ειδοποίησης και πρέπει να διαγράφονται αμέσως μετά την περάτωση ή τον τερματισμό της ποινικής διαδικασίας, σύμφωνα με τις εθνικές διαδικασίες για τις οποίες έχουν εισαχθεί στη βάση δεδομένων.

Ενώ η περίοδος διατήρησης των βιομετρικών δεδομένων στη βάση δεδομένων μπορεί να προβλέπεται για σχετικά μεγάλο χρονικό διάστημα και να ορίζεται σύμφωνα με το εθνικό δίκαιο, η άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων και ιδίως το δικαίωμα διόρθωσης και διαγραφής προβλέπει πρόσθετη εγγύηση για τον περιορισμό της παρέμβασης στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα των οικείων υποκειμένων των δεδομένων.

Πηγή των πληροφοριών:

- Τύποι υποκειμένων των δεδομένων: ☒ Παιδιά
- Πηγή της εικόνας ☒ άλλο: μη προκαθορισμένο, ύποπτο θύμα απαγωγής παιδιών
- Σύνδεση με το έγκλημα ☒ Μη άμεση χρονική ☒ Μη άμεση γεωγραφική
- Τρόπος συλλογής πληροφοριών: ☒ σε θάλαμο ή ελεγχόμενο περιβάλλον
- Πλαίσιο: επηρεάζει άλλα θεμελιώδη δικαιώματα ☒ Ναι, συγκεκριμένα: ☒ διάφορα

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση ☒ ειδική βάση δεδομένων

Αλγόριθμος:

- Τύπος επαλήθευσης: ☒ ταυτοποίηση 1-πολλά

Αποτέλεσμα:

- Αντίκτυπος ☒ Άμεσος
- Αυτοματοποιημένη απόφαση: ☒ ΟΧΙ, υποχρεωτική επανεξέταση από εξουσιοδοτημένο υπάλληλο

Νομική ανάλυση:

- Εφαρμοστέο νομικό πλαίσιο: ☒ Ειδικό εθνικό δίκαιο για την εν λόγω επεξεργασία (αναγνώριση προσώπου)

2.2. Ισχύον νομικό πλαίσιο

Το εθνικό δίκαιο προβλέπει ειδικό νομικό πλαίσιο για τη δημιουργία της βάσης δεδομένων, το οποίο καθορίζει τους σκοπούς της επεξεργασίας, καθώς και τα κριτήρια για τον εμπλουτισμό, την πρόσβαση και τη χρήση της βάσης δεδομένων. Τα νομοθετικά μέτρα που απαιτούνται για την εφαρμογή της προβλέπουν επίσης τον καθορισμό μιας περιόδου διατήρησης, καθώς και την αναφορά στις εφαρμοστέες αρχές της ακεραιότητας και της εμπιστευτικότητας. Τα νομοθετικά μέτρα προβλέπουν επίσης τους τρόπους παροχής πληροφοριών στο υποκείμενο των δεδομένων και, στην περίπτωση αυτή, στον/στους δικαιούχο/-ους της γονικής μέριμνας, καθώς και την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τον πιθανό περιορισμό τους, κατά περίπτωση. Κατά την προετοιμασία της πρότασης για το αντίστοιχο νομοθετικό μέτρο, έπρεπε να ζητηθεί η γνώμη της εθνικής εποπτικής αρχής.

2.3. Αναγκαιότητα και αναλογικότητα — σκοπός/σοβαρότητα του εγκλήματος/αριθμός των προσώπων που δεν εμπλέκονται αλλά επηρεάζονται από την επεξεργασία

Προϋποθέσεις και διασφαλίσεις για την επεξεργασία

Η σύγκριση αναγνώρισης προσώπου μπορεί να πραγματοποιηθεί μόνο από εξουσιοδοτημένο υπάλληλο ως έσχατη λύση, εάν δεν υπάρχουν άλλα λιγότερο παρεμβατικά μέσα και όπου είναι απολύτως αναγκαίο, για παράδειγμα, σε περίπτωση αμφιβολίας σχετικά με τη γνησιότητα του ταξιδιωτικού εγγράφου ταυτότητας ανηλίκου και/ή μετά την εξέταση προηγούμενων αποδεικτικών στοιχείων και υλικού που έχουν συλλεχθεί, τα οποία υποδεικνύουν πιθανή αντιστοιχία με την περιγραφή εξαφανισθέντος παιδιού για το οποίο διεξάγεται ποινική έρευνα.

Παρέχεται επίσης πρόσθετη διασφάλιση με την υποχρεωτική επανεξέταση και επαλήθευση της σύγκρισης της αναγνώρισης προσώπου από εξουσιοδοτημένο υπάλληλο, προκειμένου να επιβεβαιώνονται τα προηγούμενα αποδεικτικά στοιχεία με το αποτέλεσμα της σύγκρισης και να αποκλείονται τυχόν ψευδώς θετικά αποτελέσματα.

Επιδιωκόμενος στόχος

Η δημιουργία της βάσης δεδομένων εξυπηρετεί σημαντικούς στόχους γενικού δημόσιου συμφέροντος, ιδίως την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων και την προστασία των δικαιωμάτων και ελευθεριών των άλλων. Η δημιουργία της βάσης δεδομένων και η προβλεπόμενη επεξεργασία φαίνεται να συμβάλλει στην ταυτοποίηση των παιδιών που έχουν πέσει θύματα απαγωγής και, επομένως, μπορεί να θεωρηθεί ως μέτρο κατάλληλο για την υποστήριξη του νόμιμου στόχου της διερεύνησης και της δίωξης τέτοιων εγκλημάτων.

Σκοπός και πληθυσμός της βάσης δεδομένων

Οι σκοποί της επεξεργασίας καθορίζονται σαφώς από τη νομοθεσία και η βάση δεδομένων χρησιμοποιείται μόνο για τον σκοπό της ταυτοποίησης εξαφανισθέντων παιδιών για τα οποία έχει αναφερθεί υποψία απαγωγής παιδιών και έχει κινηθεί ποινική έρευνα υπό την εποπτεία δικαστικής αρχής και για τα οποία έχει εκδοθεί συναγερμική ειδοποίηση για αρπαγή ανηλίκου. Οι προϋποθέσεις που προβλέπονται από τον νόμο για τον πληθυσμό της βάσης δεδομένων αποσκοπούν στον αυστηρό περιορισμό του αριθμού των υποκειμένων των δεδομένων και των δεδομένων προσωπικού χαρακτήρα που πρέπει να περιλαμβάνονται στη βάση δεδομένων. Ο κάτοχος της γονικής μέριμνας έναντι του παιδιού πρέπει να ενημερώνεται σχετικά με την επεξεργασία που πραγματοποιείται και

τους όρους άσκησης των δικαιωμάτων του παιδιού σε σχέση με τη βιομετρική επεξεργασία που προβλέπεται για τον σκοπό της ταυτοποίησης ή με τα δεδομένα προσωπικού χαρακτήρα του παιδιού που αποθηκεύονται στη βάση δεδομένων.

2.4. Συμπέρασμα

Λαμβάνοντας υπόψη την αναγκαιότητα και την αναλογικότητα της προβλεπόμενης επεξεργασίας, καθώς και το βέλτιστο συμφέρον του παιδιού κατά τη διενέργεια της εν λόγω επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και υπό την προϋπόθεση ότι υπάρχουν επαρκείς εγγυήσεις που διασφαλίζουν ιδίως την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων — λαμβάνοντας ιδίως υπόψη το γεγονός ότι πρόκειται να υποβληθούν σε επεξεργασία δεδομένα παιδιών, η εν λόγω εφαρμογή της επεξεργασίας αναγνώρισης προσώπου μπορεί να θεωρηθεί πιθανώς συμβατή με το δίκαιο της ΕΕ.

Επιπλέον, δεδομένου του είδους της επεξεργασίας και της χρησιμοποιούμενης τεχνολογίας, η οποία συνεπάγεται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του οικείου υποκειμένου των δεδομένων, το ΕΣΠΔ θεωρεί ότι η εκπόνηση προτάσεων νομοθετικών μέτρων που πρόκειται να εγκριθούν από εθνικά κοινοβούλια ή κανονιστικών μέτρων που βασίζονται σε τέτοια νομοθετικά μέτρα και τα οποία συνδέονται με την προβλεπόμενη επεξεργασία, πρέπει να περιλαμβάνει προηγούμενη διαβούλευση με την εποπτική αρχή, προκειμένου να διασφαλιστεί η συνέπεια και η συμμόρφωση με το εφαρμοστέο νομικό πλαίσιο, πρβλ. άρθρο 28 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

3 ΣΕΝΑΡΙΟ 3:

3.1. Περιγραφή

Κατά τη διάρκεια αστυνομικών επεμβάσεων σε ταραχές και ερευνών που ακολούθησαν, ορισμένα άτομα αναγνωρίστηκαν ως ύποπτοι, π.χ. από προηγούμενες έρευνες με χρήση υλικού από κάμερες κλειστού κυκλώματος παρακολούθησης ή μαρτύρων. Οι εικόνες αυτών των υπόπτων συγκρίνονται με φωτογραφίες ατόμων που καταγράφηκαν σε κάμερες κλειστού κυκλώματος παρακολούθησης ή σε κινητές συσκευές σε τόπο εγκλήματος ή σε γύρω περιοχές.

Για την απόκτηση λεπτομερέστερων αποδεικτικών στοιχείων σχετικά με τα άτομα που είναι ύποπτα ότι έχουν συμμετάσχει σε ταραχές που περιβάλλουν διαδήλωση, η αστυνομία δημιουργεί μια βάση δεδομένων η οποία αποτελείται από υλικό εικόνων με χαλαρή τοπική και χρονική σύνδεση με τις ταραχές. Η βάση δεδομένων περιλαμβάνει ιδιωτικές καταγραφές που μεταφορτώνονται στην αστυνομία από πολίτες, υλικό από τις κάμερες κλειστού κυκλώματος παρακολούθησης δημόσιων συγκοινωνιών, υλικό βιντεοεπιτήρησης που ανήκει στην αστυνομία και υλικό που δημοσιεύεται από τα μέσα μαζικής ενημέρωσης χωρίς κανένα συγκεκριμένο περιορισμό ή διασφάλιση. Η επίδειξη σοβαρής εγκληματικής συμπεριφοράς δεν αποτελεί προϋπόθεση για τη συλλογή των αρχείων στη βάση δεδομένων. Ως εκ τούτου, στη βάση δεδομένων αποθηκεύονται άτομα που δεν συμμετείχαν στις ταραχές —ένα σημαντικό ποσοστό του τοπικού πληθυσμού που έτυχε να περάσει από εκεί τη στιγμή της διαδήλωσης ή συμμετείχε στη διαδήλωση αλλά όχι στις ταραχές. Ανέρχεται σε χιλιάδες αρχεία βίντεο και εικόνων.

Χρησιμοποιώντας ένα λογισμικό αναγνώρισης προσώπου, όλα τα πρόσωπα που εμφανίζονται στα εν λόγω αρχεία αντιστοιχίζονται σε μοναδικά αναγνωριστικά προσώπου. Τα πρόσωπα των μεμονωμένων υπόπτων συγκρίνονται στη συνέχεια αυτόματα με αυτά τα αναγνωριστικά προσώπου. Η βάση δεδομένων που αποτελείται από όλα τα βιομετρικά υποδείγματα στα χιλιάδες αρχεία βίντεο και εικόνων αποθηκεύεται έως ότου περατωθούν όλες οι πιθανές έρευνες. Οι θετικές αντιστοιχίσεις

εξετάζονται από τους αρμόδιους υπαλλήλους, οι οποίοι στη συνέχεια αποφασίζουν για περαιτέρω ενέργειες. Αυτό μπορεί να περιλαμβάνει την απόδοση του αρχείου που βρέθηκε στη βάση δεδομένων στο ποινικό αρχείο του αντίστοιχου ατόμου, καθώς και περαιτέρω μέτρα, όπως ανάκριση ή σύλληψη του εν λόγω ατόμου.

Η εθνική νομοθεσία προβλέπει μια γενική διάταξη, σύμφωνα με την οποία η επεξεργασία βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση ενός φυσικού προσώπου είναι επιτρεπτή εφόσον είναι απολύτως αναγκαία και υπόκειται σε κατάλληλες διασφαλίσεις για τα δικαιώματα και τις ελευθερίες του ενδιαφερόμενου ατόμου.

Πηγή των πληροφοριών:

- Τύποι υποκειμένων των δεδομένων: ☒ όλα τα άτομα
- Πηγή εικόνας: ☒ χώροι προσβάσιμοι στο κοινό ☒ ιδιωτικές οντότητες ☒ άλλα άτομα ☒ άλλο: μέσα μαζικής ενημέρωσης
- Σύνδεση με το έγκλημα: ☒ Όχι απαραίτητα άμεση γεωγραφική ή χρονική σύνδεση
- Τρόπος συλλογής πληροφοριών: ☒ εξ αποστάσεως
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα: Ναι, συγκεκριμένα ☒ το πλαίσιο της ελευθερίας του συνέρχεσθαι
- Διαθέσιμες πρόσθετες πηγές πληροφόρησης σχετικά με το υποκείμενο των δεδομένων: ☒ άλλες: δεν αποκλείονται (όπως η χρήση μηχανημάτων ATM ή η είσοδος σε καταστήματα), καθώς δεν μπορεί να ασκηθεί έλεγχος επί των κινήτρων στις εικόνες.

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση: ☒ ειδικές βάσεις δεδομένων που σχετίζονται με τον τομέα του εγκλήματος

Αλγόριθμος:

- Τύπος επεξεργασίας: ☒ ταυτοποίηση 1-πολλά

Αποτέλεσμα:

- Αντίκτυπος: ☒ Άμεσος (π.χ. το υποκείμενο των δεδομένων μπορεί να συλληφθεί, να ανακριθεί)
- Αυτοματοποιημένη απόφαση: ☒ ΟΧΙ
- Διάρκεια αποθήκευσης: μέχρι να περατωθούν όλες οι πιθανές έρευνες

Νομική ανάλυση:

- Είδος προηγούμενης ενημέρωσης του υποκειμένου των δεδομένων: ☒ Γενικά στον ιστότοπο της αρχής επιβολής του νόμου
- Εφαρμοστέο νομικό πλαίσιο : ☒ η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου έχει ως επί το πλείστον αντιγραφεί στο εθνικό δίκαιο ☒ Γενικό εθνικό δίκαιο για τη χρήση βιομετρικών δεδομένων από τις αρχές επιβολής του νόμου

3.2. Ισχύον νομικό πλαίσιο

Όπως διευκρινίστηκε ανωτέρω, οι νομικές βάσεις που απλώς επαναλαμβάνουν τη γενική ρήτρα του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου δεν είναι επαρκώς σαφείς ως προς τους όρους τους, ώστε να παρέχουν στα άτομα επαρκή ένδειξη των όρων και των περιστάσεων υπό τις οποίες οι αρχές επιβολής του νόμου έχουν την εξουσία να χρησιμοποιούν καταγραφές καμερών κλειστού κυκλώματος παρακολούθησης από δημόσιους χώρους για τη δημιουργία βιομετρικού υποδείγματος του προσώπου τους και να το συγκρίνουν με αστυνομικές βάσεις δεδομένων, άλλες διαθέσιμες καταγραφές καμερών κλειστού κυκλώματος

παρακολούθησης ή ιδιωτικές καταγραφές κ.λπ. Συνεπώς, το νομικό πλαίσιο που θεσπίζεται στο παρόν σενάριο δεν πληροί τις ελάχιστες απαιτήσεις για να χρησιμεύσει ως νομική βάση.

3.3. Αναγκαιότητα και αναλογικότητα

Στο παράδειγμα αυτό, η επεξεργασία εγείρει διάφορες ανησυχίες στο πλαίσιο των αρχών της αναγκαιότητας και της αναλογικότητας για διάφορους λόγους:

Τα άτομα δεν είναι ύποπτα για σοβαρό έγκλημα. Η επίδειξη σοβαρής εγκληματικής συμπεριφοράς δεν αποτελεί προϋπόθεση για τη χρήση των αρχείων της βάσης δεδομένων που περιέχουν το υλικό εικόνας. Επίσης, η άμεση χρονική και γεωγραφική σύνδεση με το έγκλημα δεν αποτελεί προϋπόθεση για τη χρήση των αρχείων που περιέχονται στη βάση δεδομένων. Αυτό έχει ως αποτέλεσμα ένα σημαντικό ποσοστό του τοπικού πληθυσμού να αποθηκεύεται σε μια βιομετρική βάση δεδομένων για διάστημα ενδεχομένως αρκετών ετών, έως ότου περατωθούν όλες οι έρευνες.

Η βάση δεδομένων για τον τόπο ενός εγκλήματος δεν περιορίζεται σε εικόνες που πληρούν τις απαιτήσεις αναλογικότητας, οδηγώντας έτσι σε απεριόριστο αριθμό εικόνων προς σύγκριση. Αυτό έρχεται σε αντίθεση με την αρχή της ελαχιστοποίησης των δεδομένων. Ένας μικρότερος αριθμός εικόνων θα επέτρεπε επίσης να ληφθούν υπόψη μη αλγοριθμικά και λιγότερο παρεμβατικά μέσα, π.χ. υπερ-αναγνωριστές.[88]

Καθώς το παράδειγμα προέρχεται από το περιβάλλον μιας διαδήλωσης, είναι επίσης πιθανό οι εικόνες να αποκαλύπτουν τις πολιτικές απόψεις των συμμετεχόντων στη διαδήλωση, αποτελώντας τη δεύτερη ειδική κατηγορία δεδομένων που ενδέχεται να επηρεαστεί σε αυτό το σενάριο. Σε αυτό το σενάριο, δεν είναι σαφές πώς μπορεί να αποτραπεί η συλλογή αυτών των δεδομένων και με ποιες διασφαλίσεις. Επιπλέον, όταν τα υποκείμενα των δεδομένων μάθουν ότι η συμμετοχή τους σε μια διαδήλωση είχε ως αποτέλεσμα την καταχώρισή τους σε μια βιομετρική βάση δεδομένων της αστυνομίας, αυτό μπορεί να έχει σοβαρά ανασταλτικά αποτελέσματα για τη μελλοντική άσκηση του δικαιώματος του συνέρχεσθαι.

Τα βιομετρικά υποδείγματα στη βάση δεδομένων μπορούν επίσης να συγκριθούν μεταξύ τους. Αυτό επιτρέπει στην αστυνομία όχι μόνο να αναζητήσει ένα συγκεκριμένο άτομο σε όλο το υλικό της, αλλά και να αναδημιουργήσει το πρότυπο συμπεριφοράς ενός ατόμου για μια περίοδο αρκετών ημερών. Μπορεί επίσης να συγκεντρώσει πρόσθετες πληροφορίες σχετικά με τα άτομα, όπως κοινωνικές επαφές και συμμετοχή στην πολιτική ζωή.

Η παρέμβαση εντείνεται περαιτέρω από το γεγονός ότι τα δεδομένα υποβάλλονται σε επεξεργασία εν αγνοία των υποκειμένων των δεδομένων.

Λαμβάνοντας υπόψη ότι φωτογραφίες και βίντεο καταγράφονται συνεχώς από άτομα και ότι ακόμη και η πανταχού παρούσα κάλυψη με κάμερες κλειστού κυκλώματος παρακολούθησης μπορεί να αναλυθεί βιομετρικά, αυτό μπορεί να οδηγήσει σε σοβαρό αποτρεπτικό αντίκτυπο.

Η εκτεταμένη χρήση ιδιωτικών φωτογραφιών και βίντεο, συμπεριλαμβανομένης της πιθανής κατάχρησης, όπως η καταγγελία, αποτελεί ένα ακόμη σημείο ανησυχίας. Δεδομένου ότι η κατάχρηση όπως η καταγγελία είναι επίσης ένας κίνδυνος που ενυπάρχει στις ποινικές διαδικασίες εν γένει, ο

[88] Δηλαδή, άτομα με εξαιρετική ικανότητα αναγνώρισης προσώπου. Πρβλ. επίσης: «Face Recognition by Metropolitan Police Super-Recognisers» (Αναγνώριση προσώπου από τους Υπερ-αναγνωριστές της Μητροπολιτικής αστυνομίας), της 26ης Φεβρουαρίου 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

κίνδυνος είναι σημαντικά υψηλότερος όσον αφορά την επεκτασιμότητα των δεδομένων που υποβάλλονται σε επεξεργασία και τον αριθμό των εμπλεκόμενων ατόμων, καθώς τα άτομα ενδέχεται να μεταφορτώσουν επίσης υλικό που σχετίζεται με ένα συγκεκριμένο άτομο ή ομάδα ατόμων που δεν τους αρέσει. Τα αιτήματα της αστυνομίας για μεταφόρτωση φωτογραφιών και βίντεο ενδέχεται να οδηγήσουν σε πολύ χαμηλά κατώτατα όρια για την παροχή υλικού από άτομα, ιδίως δεδομένου ότι αυτό θα μπορούσε να γίνει ανώνυμα ή τουλάχιστον χωρίς να χρειάζεται να παρουσιαστούν και να ταυτοποιηθούν σε αστυνομικό τμήμα.

3.4. Συμπέρασμα

Στο παράδειγμα, δεν υπάρχει συγκεκριμένη διάταξη που θα μπορούσε να χρησιμεύσει ως νομική βάση. Ωστόσο, ακόμη και αν υπήρχε επαρκής νομική βάση, δεν θα πληρούνταν οι απαιτήσεις αναγκαιότητας και αναλογικότητας, με αποτέλεσμα να προκληθεί δυσανάλογη παρέμβαση στα δικαιώματα του υποκειμένου των δεδομένων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα δυνάμει του Χάρτη.

4 ΣΕΝΑΡΙΟ 4

4.1. Περιγραφή

Η αστυνομία εφαρμόζει έναν τρόπο ταυτοποίησης υπόπτων που διαπράττουν σοβαρό έγκλημα και έχουν καταγραφεί σε κάμερες κλειστού κυκλώματος παρακολούθησης με αναδρομική τεχνολογία αναγνώρισης προσώπου. Ο υπάλληλος επιλέγει χειροκίνητα την εικόνα ή τις εικόνες υπόπτων στο υλικό βίντεο που έχει συλλεχθεί από τον τόπο του εγκλήματος ή αλλού στο πλαίσιο προκαταρκτικής έρευνας και στη συνέχεια αποστέλλει την εικόνα ή τις εικόνες στην εγκληματολογική υπηρεσία. Η εγκληματολογική υπηρεσία χρησιμοποιεί την τεχνολογία αναγνώρισης προσώπου για την αντιστοίχιση της/των εν λόγω εικόνας/εικόνων με εικόνες ατόμων που έχουν συλλεχθεί στο παρελθόν από την αστυνομία σε βάση δεδομένων (μια αποκαλούμενη βάση δεδομένων περιγραφής η οποία αποτελείται από υπόπτους και πρώην κρατουμένους). Η βάση δεδομένων περιγραφής αναλύεται γι' αυτή τη διαδικασία —προσωρινά και σε απομονωμένο περιβάλλον— με τεχνολογία αναγνώρισης προσώπου προκειμένου να είναι σε θέση να εκτελέσει τη διαδικασία αντιστοίχισης. Για να ελαχιστοποιηθεί η παρέμβαση στα δικαιώματα και τα συμφέροντα των ατόμων που αντιστοιχίζονται, ένας πολύ περιορισμένος αριθμός υπαλλήλων της εγκληματολογικής υπηρεσίας έχει την άδεια να διεξάγει την πραγματική διαδικασία αντιστοίχισης, η πρόσβαση στα δεδομένα περιορίζεται στους υπαλλήλους στους οποίους έχει ανατεθεί ο συγκεκριμένος φάκελος και πραγματοποιείται χειροκίνητος έλεγχος των αποτελεσμάτων πριν από τη διαβίβαση οποιουδήποτε αποτελέσματος στον ανακριτικό υπάλληλο. Τα βιομετρικά δεδομένα δεν διαβιβάζονται εκτός του ελεγχόμενου, απομονωμένου περιβάλλοντος. Μόνο το αποτέλεσμα και η εικόνα (όχι το βιομετρικό υπόδειγμα) χρησιμοποιούνται περαιτέρω στην έρευνα. Οι εργαζόμενοι λαμβάνουν ειδική εκπαίδευση σχετικά με τους κανόνες και τις διαδικασίες για την εν λόγω επεξεργασία και κάθε επεξεργασία προσωπικών και βιομετρικών δεδομένων προσδιορίζεται επαρκώς στο εθνικό δίκαιο.

Πηγή των πληροφοριών:

- Είδη υποκειμένων των δεδομένων: ☒ ύποπτοι που εντοπίζονται από τις καταγραφές καμερών κλειστού κυκλώματος παρακολούθησης
- Πηγή εικόνας: ☒ χώροι προσβάσιμοι στο κοινό ☒ διαδίκτυο
- Σύνδεση με το έγκλημα:☒ Άμεση χρονική
  ☒ Άμεση γεωγραφική

- Τρόπος συλλογής πληροφοριών: ☒ εξ αποστάσεως
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα: Ναι, συγκεκριμένα: ☒ Ελευθερία του συνέρχεσθαι ☒ Ελευθερία του λόγου ☒ διάφορα: __

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση: ☒ ειδικές βάσεις δεδομένων που σχετίζονται με τον τομέα του εγκλήματος

Αλγόριθμος:

- Τύπος επεξεργασίας: ☒ ταυτοποίηση 1-πολλά

Αποτέλεσμα:

- Αντίκτυπος: ☒ Άμεσος (π.χ. το υποκείμενο των δεδομένων συλλαμβάνεται, ανακρίνεται)
- Αυτοματοποιημένη απόφαση: ☒ ΟΧΙ

Νομική ανάλυση:

- Ισχύον νομικό πλαίσιο : ☒ Ειδικό εθνικό δίκαιο για την εν λόγω επεξεργασία (αναγνώριση προσώπου) για την εν λόγω αρμόδια αρχή

4.2. Ισχύον νομικό πλαίσιο

Σε αυτό το σενάριο, ορίζεται στο εθνικό δίκαιο ότι βιομετρικά δεδομένα μπορούν να χρησιμοποιηθούν για τη διενέργεια εγκληματολογικής ανάλυσης όταν αυτό είναι απολύτως αναγκαίο για την επίτευξη του σκοπού της ταυτοποίησης υπόπτων που διαπράττουν σοβαρό έγκλημα μέσω της αντιστοίχισης των εικόνων στη βάση δεδομένων περιγραφής. Η εθνική νομοθεσία καθορίζει τα δεδομένα που μπορούν να υποβληθούν σε επεξεργασία, καθώς και τις διαδικασίες για τη διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα και τις διαδικασίες για την καταστροφή τους, παρέχοντας έτσι επαρκείς εγγυήσεις κατά του κινδύνου κατάχρησης και αυθαιρεσίας.

4.3. Αναγκαιότητα και αναλογικότητα

Η χρήση της αναγνώρισης προσώπου είναι σαφώς πιο αποδοτική ως προς τον χρόνο από τη χειροκίνητη αντιστοίχιση σε εγκληματολογικό επίπεδο. Η χειροκίνητη επιλογή των εικόνων εκ των προτέρων περιορίζει την παρεμβολή σε σύγκριση με την αντιπαραβολή όλου του υλικού βίντεο με μια βάση δεδομένων και, ως εκ τούτου, διαφοροποιεί και στοχεύει μόνο τα άτομα εκείνα που καλύπτονται από τον στόχο, δηλαδή την καταπολέμηση του σοβαρού εγκλήματος. Ωστόσο, εξακολουθεί να είναι σημαντικό να εξεταστεί εάν η αντιστοίχιση μπορεί να γίνει χειροκίνητα σε εύλογο χρονικό διάστημα, ανάλογα με την εκάστοτε περίπτωση. Ο περιορισμός των προσώπων που έχουν πρόσβαση στην τεχνολογία και τα δεδομένα προσωπικού χαρακτήρα μειώνει τον αντίκτυπο στα δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων, καθώς και τα βιομετρικά υποδείγματα που δεν αποθηκεύονται ή δεν χρησιμοποιούνται αργότερα κατά την έρευνα. Ο χειροκίνητος έλεγχος του αποτελέσματος σημαίνει επίσης μειωμένο κίνδυνο ψευδώς θετικών αποτελεσμάτων.

4.4. Συμπέρασμα

Είναι σημαντικό η εθνική νομοθεσία να παρέχει κατάλληλη νομική βάση για την επεξεργασία βιομετρικών δεδομένων, καθώς και για την εθνική βάση δεδομένων με την οποία πραγματοποιείται η αντιστοίχιση. Σε αυτό το σενάριο έχουν θεσπιστεί διάφορα μέτρα για τον περιορισμό της παρέμβασης στα δικαιώματα προστασίας των δεδομένων, όπως οι όροι για τη χρήση της τεχνολογίας αναγνώρισης προσώπου που καθορίζονται στη νομική βάση, ο αριθμός των ατόμων που έχουν πρόσβαση στην τεχνολογία και τα βιομετρικά δεδομένα, οι χειροκίνητοι έλεγχοι κ.λπ. Η τεχνολογία

αναγνώρισης προσώπου βελτιώνει σημαντικά την αποτελεσματικότητα του ερευνητικού έργου της εγκληματολογικής υπηρεσίας της αστυνομίας, βασίζεται σε νόμο που επιτρέπει στην αστυνομία να επεξεργάζεται βιομετρικά δεδομένα όταν είναι απολύτως αναγκαίο και, ως εκ τούτου, εντός αυτών των πλαισίων μπορεί να θεωρηθεί νόμιμη παρέμβαση στα δικαιώματα του ατόμου.

5 ΣΕΝΑΡΙΟ 5

5.1. Περιγραφή

Ως απομακρυσμένη βιομετρική ταυτοποίηση νοείται όταν οι ταυτότητες των ατόμων διαπιστώνονται με τη βοήθεια βιομετρικών αναγνωριστικών στοιχείων (εικόνας προσώπου, βάδισης, ίριδας, κ.λπ.) από απόσταση, σε δημόσιο χώρο και με συνεχή ή διαρκή τρόπο, ελέγχοντάς τα με (βιομετρικά) δεδομένα που είναι αποθηκευμένα σε μια βάση δεδομένων[89]. Η απομακρυσμένη βιομετρική ταυτοποίηση πραγματοποιείται σε πραγματικό χρόνο, εάν η συλλογή του υλικού εικόνας, η σύγκριση και η ταυτοποίηση πραγματοποιούνται χωρίς σημαντική καθυστέρηση.

Πριν από κάθε ανάπτυξη βιομετρικής αναγνώρισης από απόσταση σε πραγματικό χρόνο, η αστυνομία καταρτίζει έναν κατάλογο υπόπτων με τα άτομα που παρουσιάζουν ενδιαφέρον στο πλαίσιο μιας έρευνας. Αυτός εμπλουτίζεται με εικόνες προσώπου των ατόμων. Με βάση πληροφορίες που υποδεικνύουν ότι τα άτομα θα βρίσκονται σε συγκεκριμένη περιοχή, όπως ένα εμπορικό κέντρο ή μια δημόσια πλατεία, η αστυνομία αποφασίζει πότε, πού και για πόσο χρονικό διάστημα θα αναπτύξει την εξ αποστάσεως βιομετρική ταυτοποίηση.

Την ημέρα της δράσης, τοποθετούν ένα αστυνομικό ημιφορτηγό επιτόπου ως κέντρο ελέγχου, με έναν ανώτερο αστυνομικό να επιβαίνει σε αυτό. Το ημιφορτηγό περιέχει οθόνες που απεικονίζουν οπτικοακουστικό υλικό από κάμερες κλειστού κυκλώματος παρακολούθησης τοποθετημένες σε κοντινή απόσταση, είτε τοποθετούμενες σε ad hoc βάση είτε μέσω σύνδεσης με τις ροές βίντεο των ήδη εγκατεστημένων καμερών. Καθώς οι πεζοί περνούν μπροστά από τις κάμερες, η τεχνολογία απομονώνει εικόνες προσώπου, τις μετατρέπει σε βιομετρικό υπόδειγμα και τις συγκρίνει με τα βιομετρικά υποδείγματα των ατόμων που περιλαμβάνονται στον κατάλογο υπόπτων.

Εάν εντοπιστεί πιθανή αντιστοίχιση μεταξύ του καταλόγου υπόπτων και των ατόμων που περνούν από τις κάμερες, αποστέλλεται συναγερμική ειδοποίηση στους αστυνομικούς στο ημιφορτηγό, οι οποίοι στη συνέχεια ενημερώνουν τους αστυνομικούς επιτόπου εάν η συναγερμική ειδοποίηση είναι θετική, π.χ. μέσω ασύρματης συσκευής. Στη συνέχεια, ο υπάλληλος επιτόπου θα αποφασίσει εάν θα παρέμβει, θα προσεγγίσει ή θα συλλάβει τελικά το άτομο. Τα μέτρα που λαμβάνει ο υπάλληλος επιτόπου καταγράφονται. Σε περίπτωση διακριτικού ελέγχου, οι πληροφορίες που συλλέγονται (όπως με ποιον είναι το άτομο, τι φοράει και πού πηγαίνει) αποθηκεύονται.

Η αναφερόμενη εθνική νομοθεσία προβλέπει μια γενική διάταξη, σύμφωνα με την οποία η επεξεργασία βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση ενός φυσικού προσώπου είναι επιτρεπτή εφόσον είναι απολύτως αναγκαία και υπόκειται σε κατάλληλες διασφαλίσεις για τα δικαιώματα και τις ελευθερίες του ενδιαφερόμενου ατόμου.

Πηγή των πληροφοριών:

- Τύποι υποκειμένων των δεδομένων: ☒ όλα τα άτομα
- Πηγή εικόνας: ☒ δημόσια προσβάσιμοι χώροι
- Σύνδεση με το έγκλημα: ☒ Όχι απαραίτητα άμεση γεωγραφική ή χρονική σύνδεση

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

- Τρόπος συλλογής πληροφοριών: ☒ εξ αποστάσεως
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα: Ναι, συγκεκριμένα:☒ Ελευθερία του συνέρχεσθαι☒ Ελευθερία του λόγου☒ διάφορα
- Διαθέσιμες πρόσθετες πηγές πληροφόρησης σχετικά με το υποκείμενο των δεδομένων: ☒ άλλες: δεν αποκλείονται (όπως η χρήση μηχανημάτων ATM ή η είσοδος σε καταστήματα)

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση: ☒ ειδικές βάσεις δεδομένων που σχετίζονται με τον τομέα του εγκλήματος

Αλγόριθμος:

- Τύπος επεξεργασίας: ☒ ταυτοποίηση 1-πολλά

Αποτέλεσμα:

- Αντίκτυπος: ☒ Άμεσος (π.χ. το υποκείμενο των δεδομένων συλλαμβάνεται, ανακρίνεται)
- Αυτοματοποιημένη απόφαση: ☒ ΟΧΙ
- Διάρκεια αποθήκευσης: μέχρι να περατωθούν όλες οι πιθανές έρευνες

Νομική ανάλυση:

- Είδος προηγούμενης ενημέρωσης του υποκειμένου των δεδομένων: ☒ Γενικά στον ιστότοπο της αρχής επιβολής του νόμου
- Ισχύον νομικό πλαίσιο: ☒ η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου έχει ως επί το πλείστον αντιγραφεί στο εθνικό δίκαιο ☒ Γενικό εθνικό δίκαιο για τη χρήση βιομετρικών δεδομένων από τις αρχές επιβολής του νόμου

5.2. Ισχύον νομικό πλαίσιο

Οι νομικές βάσεις που απλώς επαναλαμβάνουν τη γενική ρήτρα του άρθρου 10 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου δεν είναι επαρκώς σαφείς ως προς τους όρους τους, ώστε να παρέχουν στα άτομα επαρκή ένδειξη των όρων και των περιστάσεων υπό τις οποίες οι αρχές επιβολής του νόμου έχουν την εξουσία να χρησιμοποιούν καταγραφές καμερών κλειστού κυκλώματος παρακολούθησης από δημόσιους χώρους για τη δημιουργία βιομετρικού υποδείγματος του προσώπου τους και να το συγκρίνουν με αστυνομικές βάσεις δεδομένων. Ως εκ τούτου, το νομικό πλαίσιο που θεσπίζεται στο παρόν σενάριο δεν πληροί τις ελάχιστες απαιτήσεις για να χρησιμεύσει ως νομική βάση.[90]

5.3. Αναγκαιότητα και αναλογικότητα

Ο πήχης της αναγκαιότητας και της αναλογικότητας γίνεται υψηλότερος όσο βαθύτερη είναι η παρέμβαση. Η εξ αποστάσεως βιομετρική ταυτοποίηση σε δημόσιους χώρους έχει διάφορες επιπτώσεις στα θεμελιώδη δικαιώματα:

Τα σενάρια συνεπάγονται την παρακολούθηση όλων των περαστικών στον αντίστοιχο δημόσιο χώρο. Επομένως, επηρεάζει σοβαρά την εύλογη προσδοκία των πληθυσμών να παραμένουν ανώνυμοι σε

[90] Σε περιπτώσεις κατά τις οποίες ένα επιστημονικό έργο που αποσκοπεί στην έρευνα της χρήσης τεχνολογίας αναγνώρισης προσώπου θα πρέπει να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα, αλλά η εν λόγω επεξεργασία δεν εμπίπτει στο άρθρο 4 παράγραφος 3 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου ή εκτός του πεδίου εφαρμογής του δικαίου της Ένωσης, εφαρμόζεται ο ΓΚΠΔ. Σε περίπτωση πιλοτικών έργων που ακολουθούνται από επιχειρήσεις επιβολής του νόμου, η οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου εξακολουθεί να είναι εφαρμοστέα.

δημόσιους χώρους[91]. Αυτό αποτελεί προϋπόθεση για πολλές πτυχές της δημοκρατικής διαδικασίας, όπως η απόφαση συμμετοχής σε μια ένωση πολιτών, οι επισκέψεις σε συγκεντρώσεις και οι συναντήσεις με ανθρώπους από κάθε κοινωνικό και πολιτισμικό υπόβαθρο, η συμμετοχή σε μια πολιτική διαμαρτυρία και η επίσκεψη σε τόπους κάθε είδους. Η έννοια της ανωνυμίας σε δημόσιους χώρους είναι απαραίτητη για την ελεύθερη συλλογή και ανταλλαγή πληροφοριών και ιδεών. Διαφυλάσσει την πολυφωνία, την ελευθερία του συνέρχεσθαι ειρηνικώς και την ελευθερία του συνεταιρίζεσθαι, καθώς και την προστασία των μειονοτήτων, και υποστηρίζει τις αρχές της διάκρισης των εξουσιών και των ελέγχων και ισορροπιών. Η υπονόμευση της έννοιας της ανωνυμίας στους δημόσιους χώρους μπορεί να οδηγήσει σε σοβαρό αποτρεπτικό αποτέλεσμα για τους πολίτες. Ενδέχεται να απέχουν από ορισμένες συμπεριφορές που εμπίπτουν στα πλαίσια μιας ελεύθερης και ανοικτής κοινωνίας. Κάτι τέτοιο θα επηρέαζε το δημόσιο συμφέρον, καθώς μια δημοκρατική κοινωνία απαιτεί την αυτοδιάθεση και τη συμμετοχή των πολιτών της στη δημοκρατική διαδικασία.

Εάν εφαρμοστεί μια τέτοια τεχνολογία, η απλή βόλτα στο δρόμο, στο μετρό ή στον φούρνο στην περιοχή εφαρμογής θα οδηγήσει στη συλλογή προσωπικών, συμπεριλαμβανομένων των βιομετρικών, δεδομένων από τις υπηρεσίες επιβολής του νόμου και, στο πρώτο σενάριο, στην αντιστοίχιση με τις βάσεις δεδομένων της αστυνομίας. Μια κατάσταση, στην οποία το ίδιο επιτυγχάνεται με τη λήψη δακτυλικών αποτυπωμάτων, είναι σαφώς δυσανάλογη.

Ο αριθμός των υποκειμένων των δεδομένων που θίγονται είναι εξαιρετικά υψηλός, δεδομένου ότι κάθε άτομο που περνάει μπροστά από την αντίστοιχη δημόσια περιοχή θίγεται. Επιπλέον, τα σενάρια συνεπάγονται την αυτοματοποιημένη μαζική επεξεργασία βιομετρικών δεδομένων, καθώς και τη μαζική αντιστοίχιση βιομετρικών δεδομένων με τις αστυνομικές βάσεις δεδομένων.

Σε όλη την ευρωπαϊκή νομολογία, η μαζική παρακολούθηση απαγορεύεται (π.χ. το ΕΔΔΑ στην υπόθεση S. και Marper κατά Ηνωμένου Βασιλείου έκρινε την αδιάκριτη διατήρηση βιομετρικών δεδομένων ως «δυσανάλογη παρέμβαση» στο δικαίωμα στην ιδιωτική ζωή, καθώς δεν μπορεί να θεωρηθεί «αναγκαία σε μια δημοκρατική κοινωνία»).

Η απομακρυσμένη βιομετρική ταυτοποίηση είναι τόσο επιρρεπής στη μαζική παρακολούθηση που δεν υπάρχουν αξιόπιστα μέσα περιορισμού. Διαφέρει ουσιαστικά από τη βιντεοεπιτήρηση αυτή καθαυτή, καθώς η πιθανή χρήση βιντεοσκοπημένου οπτικοακουστικού υλικού χωρίς βιομετρική ταυτοποίηση αποτελεί ήδη ισχυρή παρέμβαση, αλλά ταυτόχρονα είναι περιορισμένη, ενώ εάν εφαρμοστεί η τεχνολογία αναγνώρισης προσώπου, η ποιότητα του ήδη ευρέως διαδεδομένου συστήματος βιντεοεπιτήρησης ως κύριας πηγής των δεδομένων θα μεταβληθεί. Επιπλέον, ιδίως όσον αφορά τα συνεπαγόμενα αποτρεπτικά αποτελέσματα, οι πιθανοί περιορισμοί στην εφαρμογή των ήδη υφιστάμενων εγκαταστάσεων βιντεοεπιτήρησης δεν θα είναι ορατοί και, ως εκ τούτου, δεν θα είναι αξιόπιστοι για το κοινό.

Η απομακρυσμένη βιομετρική ταυτοποίηση από τις αστυνομικές αρχές αντιμετωπίζει τον καθένα ως πιθανό ύποπτο. Σε ένα κράτος δικαίου, ωστόσο, οι πολίτες τεκμαίρεται ότι είναι ενάρετοι μέχρι να αποδειχθεί η παραβατική συμπεριφορά τους. Η εν λόγω αρχή αντικατοπτρίζεται επίσης εν μέρει στην οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η οποία υπογραμμίζει την ανάγκη για διάκριση, στο μέτρο του δυνατού, μεταξύ της μεταχείρισης των καταδικασθέντων ή των υπόπτων στην οποία περίπτωση επιβολής του νόμου πρέπει να υπάρχουν «*σοβαροί λόγοι να πιστεύεται ότι έχουν διαπράξει ή πρόκειται να διαπράξουν ποινικό αδίκημα» [άρθρο 6 στοιχείο α) της*

[91] Απάντηση του ΕΣΠΔ στους βουλευτές του Ευρωπαϊκού Κοινοβουλίου, σχετικά με την εφαρμογή αναγνώρισης προσώπου που αναπτύχθηκε από την Clearview AI, στις 10 Ιουνίου 2020, αριθ. αναφ.: OUT2020-0052.

*οδηγίας*για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου] σε σύγκριση με εκείνους που δεν έχουν καταδικαστεί ή δεν είναι ύποπτοι για εγκληματική δραστηριότητα.

Εφαρμόζεται σε κομβικά σημεία μεταφορών ή σε δημόσιους χώρους, με τις υπηρεσίες επιβολής του νόμου να χρησιμοποιούν μια τεχνολογία ικανή να ταυτοποιεί μοναδικά ένα άτομο, να εντοπίζει και να αναλύει την τοποθεσία και τις κινήσεις του και να αποκαλύπτει μέχρι και τις πιο ευαίσθητες πληροφορίες για ένα άτομο (ακόμη και σεξουαλικές προτιμήσεις, θρησκεία, προβλήματα υγείας). Με τον τρόπο αυτό προκύπτει ο τεράστιος κίνδυνος παράνομης πρόσβασης και χρήσης των δεδομένων.

Η εγκατάσταση ενός συστήματος που επιτρέπει την αποκάλυψη του πυρήνα της συμπεριφοράς και των χαρακτηριστικών του ατόμου οδηγεί σε ισχυρά αποτρεπτικά αποτελέσματα. Κάνει τους ανθρώπους να αναρωτιούνται αν πρέπει να συμμετέχουν σε μια συγκεκριμένη εκδήλωση, βλάπτοντας έτσι τη δημοκρατική διαδικασία. Επίσης, η συνάντηση και η δημόσια εμφάνιση με έναν συγκεκριμένο φίλο που είναι γνωστό ότι έχει προβλήματα με την αστυνομία ή συμπεριφέρεται με έναν μοναδικό τρόπο μπορεί να θεωρηθεί κρίσιμη, καθώς όλα αυτά θα οδηγούσαν στην προσέλκυση του αλγορίθμου του συστήματος και, κατά συνέπεια, των αρχών επιβολής του νόμου.

Είναι αδύνατη η προστασία ευάλωτων υποκειμένων των δεδομένων, όπως τα παιδιά. Επιπλέον, επηρεάζονται τα άτομα που έχουν επαγγελματικό συμφέρον —και συχνά αντίστοιχη νομική υποχρέωση— να διατηρούν τις επαφές τους εμπιστευτικές, όπως οι δημοσιογράφοι, οι δικηγόροι και ο κλήρος. Αυτό θα μπορούσε π.χ. να οδηγήσει στην αποκάλυψη της πηγής και του δημοσιογράφου, ή του γεγονότος ότι ένα άτομο συμβουλεύεται δικηγόρο υπεράσπισης ποινικού δικαίου. Το πρόβλημα δεν ισχύει μόνο για τυχαίους δημόσιους χώρους, στους οποίους π.χ. συναντώνται δημοσιογράφοι και οι πηγές τους, αλλά φυσικά και για τους δημόσιους χώρους που είναι απαραίτητοι για την προσέγγιση και την πρόσβαση σε ιδρύματα ή επαγγελματίες στο πλαίσιο αυτό.

Επιπλέον, η δυσφορία των ανθρώπων για την τεχνολογία αναγνώρισης προσώπου μπορεί να τους οδηγήσει σε αλλαγή της συμπεριφοράς τους, αποφεύγοντας τους χώρους όπου αναπτύσσεται η τεχνολογία αναγνώρισης προσώπου και αποσύροντας τους έτσι από την κοινωνική ζωή και τις πολιτιστικές εκδηλώσεις. Ανάλογα με την έκταση της ανάπτυξης της τεχνολογίας αναγνώρισης προσώπου, ο αντίκτυπος στους ανθρώπους μπορεί να είναι τόσο σημαντικός ώστε να επηρεάσει την ικανότητά τους να ζουν μια αξιοπρεπή ζωή[92].

Ως εκ τούτου, υπάρχει μεγάλη πιθανότητα να επηρεαστεί η ουσία —ο αδιαμφισβήτητος πυρήνας— του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα. Ισχυρές ενδείξεις (βλ. ενότητα 3.1.3.2 των κατευθυντήριων γραμμών) είναι ιδίως οι ακόλουθες: σε μεγάλη κλίμακα, τα μοναδικά βιολογικά χαρακτηριστικά των ανθρώπων υποβάλλονται σε αυτόματη επεξεργασία από τις αρχές επιβολής του νόμου με αλγορίθμους που βασίζονται στην αληθοφάνεια με περιορισμένη μόνο εξηγησιμότητα των αποτελεσμάτων. Οι περιορισμοί των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων επιβάλλονται ανεξαρτήτως της ατομικής συμπεριφοράς του ατόμου ή των περιστάσεων που το αφορούν. Από στατιστική άποψη, σχεδόν όλα τα υποκείμενα των δεδομένων που επηρεάζονται από την εν λόγω παρέμβαση είναι νομοταγή φυσικά πρόσωπα. Οι δυνατότητες παροχής πληροφοριών στο υποκείμενο των δεδομένων είναι περιορισμένες. Στις περισσότερες περιπτώσεις, η δικαστική προσφυγή θα είναι δυνατή μόνο σε μεταγενέστερο στάδιο.

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, σ. 20.

Η εξάρτηση από ένα σύστημα που βασίζεται στην αληθοφάνεια και με περιορισμένη εξηγησιμότητα μπορεί να οδηγήσει σε διάχυση της ευθύνης και έλλειψη στον τομέα της επανόρθωσης και μπορεί να αποτελέσει κίνητρο για αμέλεια.

Μόλις εφαρμοστεί ένα τέτοιο σύστημα, το οποίο μπορεί να εφαρμοστεί και στις υπάρχουσες κάμερες κλειστού κυκλώματος παρακολούθησης, με ελάχιστη προσπάθεια και χωρίς να είναι ορατό από τα άτομα, μπορεί να χρησιμοποιηθεί καταχρηστικά και να συμβάλει στη συστηματική και ταχεία κατάρτιση καταλόγων ατόμων με βάση την εθνοτική καταγωγή, το φύλο, τη θρησκεία κ.λπ. Η αρχή της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα με βάση προκαθορισμένα κριτήρια, όπως η τοποθεσία στην οποία βρίσκεται ένα άτομο και η διαδρομή που διανύει εφαρμόζεται ήδη[93] και είναι επιρρεπής σε διακρίσεις.

Ανάλογα με την ευαισθησία, την εκφραστικότητα και την ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία, τα συστήματα για την εξ αποστάσεως αναγνώριση προσώπου σε δημόσια προσβάσιμους χώρους είναι επιρρεπή σε κατάχρηση με δυσμενή αντίκτυπο για τα ενδιαφερόμενα άτομα. Τέτοια δεδομένα μπορούν επίσης εύκολα να συλλεχθούν και να χρησιμοποιηθούν καταχρηστικά για την άσκηση πίεσης σε βασικούς παράγοντες της αρχής των ελέγχων και ισορροπιών, όπως η πολιτική αντιπολίτευση, οι αξιωματικοί και οι δημοσιογράφοι.

Τέλος, τα συστήματα τεχνολογίας αναγνώρισης προσώπου τείνουν να ενσωματώνουν ισχυρές επιπτώσεις μεροληψίας όσον αφορά τη φυλή και το φύλο: τα ψευδώς θετικά αποτελέσματα πλήττουν δυσανάλογα τα έγχρωμα άτομα και τις γυναίκες[94], έχοντας ως αποτέλεσμα διακρίσεις. Τα αστυνομικά μέτρα μετά από ένα ψευδώς θετικό αποτέλεσμα, όπως οι έρευνες και οι συλλήψεις, στιγματίζουν περαιτέρω τις εν λόγω ομάδες.

5.4. Συμπέρασμα

Τα προαναφερθέντα σενάρια σχετικά με την εξ αποστάσεως επεξεργασία βιομετρικών δεδομένων σε δημόσιους χώρους για σκοπούς ταυτοποίησης δεν επιτυγχάνουν δίκαιη ισορροπία μεταξύ των αντικρουόμενων ιδιωτικών και δημόσιων συμφερόντων και, ως εκ τούτου, συνιστούν δυσανάλογη παρέμβαση στα δικαιώματα του υποκειμένου των δεδομένων σύμφωνα με τα άρθρα 7 και 8 του Χάρτη.

6 ΣΕΝΑΡΙΟ 6

6.1. Περιγραφή

Μια ιδιωτική οντότητα παρέχει μια εφαρμογή όπου εικόνες προσώπου συλλέγονται από το διαδίκτυο για τη δημιουργία μιας βάσης δεδομένων. Ο χρήστης, π.χ. η αστυνομία, μπορεί στη συνέχεια να μεταφορτώσει μια φωτογραφία και με τη χρήση βιομετρικής ταυτοποίησης η εφαρμογή θα προσπαθήσει να την αντιστοιχίσει με τις εικόνες προσώπου ή τα βιομετρικά υποδείγματα στη βάση δεδομένων της.

[93] Πρβλ. Άρθρο 6 της οδηγίας (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων και άρθρο 33 του κανονισμού (ΕΕ) 2018/1240 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Σεπτεμβρίου 2018 για τη θέσπιση Ευρωπαϊκού Συστήματος Πληροφοριών και Αδειοδότησης Ταξιδιού (ETIAS), καθώς και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1077/2011, (ΕΕ) αριθ. 515/2014, (ΕΕ) 2016/399, (ΕΕ) 2016/1624 και (ΕΕ) 2017/2226.

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Ένα τοπικό αστυνομικό τμήμα διεξάγει έρευνα για ένα έγκλημα που έχει καταγραφεί σε βίντεο, όπου ένας αριθμός πιθανών μαρτύρων και υπόπτων δεν μπορεί να ταυτοποιηθεί μέσω της αντιστοίχισης των συλλεχθέντων πληροφοριών με εσωτερικές βάσεις δεδομένων ή πληροφορίες. Τα άτομα, με βάση τις συλλεγόμενες πληροφορίες, δεν είναι καταχωρισμένα σε καμία υπάρχουσα αστυνομική βάση δεδομένων. Η αστυνομία αποφασίζει να χρησιμοποιήσει ένα εργαλείο όπως περιγράφεται ανωτέρω, το οποίο παρέχεται από ιδιωτική εταιρεία, για την ταυτοποίηση των ατόμων μέσω βιομετρικής ταυτοποίησης.

Πηγή των πληροφοριών:

- Τύποι υποκειμένων των δεδομένων: ☒ όλοι οι πολίτες (μάρτυρες) ☒ καταδικασθέντες ☒ ύποπτοι
- Πηγή της εικόνας: ☒ Βιντεοσκοπημένο οπτικοακουστικό υλικό από δημόσιο χώρο ή συλλεχθέν αλλού στο πλαίσιο προκαταρκτικής έρευνας
- Σύνδεση με το έγκλημα: ☒ Δεν είναι απαραίτητο
- Τρόπος συλλογής πληροφοριών: ☒ εξ αποστάσεως
- Πλαίσιο — επηρεάζει άλλα θεμελιώδη δικαιώματα: Ναι, συγκεκριμένα: ☒ Ελευθερία του συνέρχεσθαι ☒ Ελευθερία του λόγου ☒ διάφορα: __

Βάση δεδομένων αναφοράς (με την οποία συγκρίνονται οι συλλεχθείσες πληροφορίες):

- Εξειδίκευση: ☒ βάσεις δεδομένων γενικού σκοπού που εμπλουτίζονται από το διαδίκτυο

Αλγόριθμος:

- Τύπος επεξεργασίας: ☒ ταυτοποίηση 1-πολλά

Αποτέλεσμα:

- Αντίκτυπος ☒ Άμεσος (π.χ. το υποκείμενο των δεδομένων συλλαμβάνεται, ανακρίνεται, υφίσταται διακρίσεις)
- Αυτοματοποιημένη απόφαση: ☒ ΟΧΙ

Νομική ανάλυση:

- Τύπος προηγούμενης ενημέρωσης του υποκειμένου των δεδομένων: ☒ Όχι

6.2. Ισχύον νομικό πλαίσιο

Όταν μια ιδιωτική οντότητα παρέχει μια υπηρεσία η οποία περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την οποία καθορίζει τον σκοπό και τα μέσα (εν προκειμένω, εξαγωγή εικόνων από το διαδίκτυο για τη δημιουργία βάσης δεδομένων), η εν λόγω ιδιωτική οντότητα πρέπει να διαθέτει νομική βάση για τη συγκεκριμένη επεξεργασία. Επιπλέον, η αρχή επιβολής του νόμου που αποφασίζει να χρησιμοποιήσει την εν λόγω υπηρεσία για τους σκοπούς της πρέπει να διαθέτει νομική βάση για την επεξεργασία για την οποία καθορίζει τους σκοπούς και τα μέσα. Για να μπορεί η αρχή επιβολής του νόμου να επεξεργάζεται βιομετρικά δεδομένα, πρέπει να υπάρχει νομικό πλαίσιο που να καθορίζει τον στόχο, τα προς επεξεργασία δεδομένα προσωπικού χαρακτήρα, τους σκοπούς της επεξεργασίας και τις διαδικασίες για τη διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα, καθώς και τις διαδικασίες για την καταστροφή τους.

Το σενάριο αυτό συνεπάγεται μαζική συλλογή δεδομένων προσωπικού χαρακτήρα από άτομα που δεν γνωρίζουν ότι τα δεδομένα τους συλλέγονται. Μια τέτοια επεξεργασία θα μπορούσε να είναι νόμιμη μόνο σε πολύ εξαιρετικές περιστάσεις. Ανάλογα με το πού βρίσκεται η βάση δεδομένων, η χρήση μιας τέτοιας υπηρεσίας μπορεί να συνεπάγεται τη διαβίβαση δεδομένων προσωπικού χαρακτήρα ή/και ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής

Ένωσης (από την αστυνομία, π.χ. «στέλνοντας» την εικόνα του προσώπου στο βίντεο παρακολούθησης ή συλλεχθείσα με άλλο τρόπο), απαιτώντας έτσι ειδικές προϋποθέσεις για τη διαβίβαση αυτή, βλ. άρθρο 39 της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου.

Δεν υπάρχουν ειδικοί κανόνες σε αυτό το σενάριο που να επιτρέπουν την εν λόγω επεξεργασία από την αρχή επιβολής του νόμου.

6.3. Αναγκαιότητα και αναλογικότητα

Η χρήση της υπηρεσίας από την αρχή επιβολής του νόμου σημαίνει ότι τα δεδομένα προσωπικού χαρακτήρα κοινοποιούνται σε ιδιωτική οντότητα που χρησιμοποιεί βάση δεδομένων στην οποία τα δεδομένα προσωπικού χαρακτήρα συλλέγονται κατά τρόπο απεριόριστο, σε μαζική κλίμακα. Δεν υπάρχει σύνδεση μεταξύ των δεδομένων προσωπικού χαρακτήρα που συλλέγονται και του επιδιωκόμενου στόχου από την αρχή επιβολής του νόμου. Η κοινοποίηση δεδομένων από την αρχή επιβολής του νόμου στην ιδιωτική οντότητα σημαίνει επίσης έλλειψη ελέγχου για την αρχή όσον αφορά τα δεδομένα που υποβάλλονται σε επεξεργασία από την ιδιωτική οντότητα και μεγάλη δυσκολία για τα υποκείμενα των δεδομένων να ασκήσουν τα δικαιώματά τους, καθώς δεν θα γνωρίζουν ότι τα δεδομένα τους υποβάλλονται σε επεξεργασία με αυτόν τον τρόπο. Αυτό θέτει πολύ υψηλά τον πήχη για τις περιπτώσεις στις οποίες η επεξεργασία αυτή θα μπορούσε ακόμα και να πραγματοποιηθεί. Είναι αμφίβολο αν οποιοσδήποτε στόχος θα πληρούσε τις απαιτήσεις που ορίζονται στην οδηγία, δεδομένου ότι τυχόν παρεκκλίσεις από τα δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων και περιορισμοί τους εφαρμόζονται μόνο όταν είναι απολύτως αναγκαίο. Το γενικό συμφέρον της αποτελεσματικότητας στην καταπολέμηση σοβαρών εγκλημάτων δεν μπορεί από μόνο του να δικαιολογήσει την επεξεργασία όταν συλλέγονται αδιακρίτως τόσο τεράστιες ποσότητες δεδομένων. Ως εκ τούτου, η εν λόγω επεξεργασία δεν πληροί τις απαιτήσεις της αναγκαιότητας και της αναλογικότητας.

6.4. Συμπέρασμα

Η έλλειψη σαφών, επακριβών και προβλέψιμων κανόνων που να πληρούν τις απαιτήσεις των άρθρων 4 και 10 της οδηγίας, καθώς και η έλλειψη αποδεικτικών στοιχείων ότι η εν λόγω επεξεργασία είναι απολύτως αναγκαία για την επίτευξη των επιδιωκόμενων στόχων, οδηγούν στο συμπέρασμα ότι η χρήση της εν λόγω εφαρμογής δεν πληροί τις απαιτήσεις της αναγκαιότητας και της αναλογικότητας και θα σήμαινε δυσανάλογη παρέμβαση στα δικαιώματα των υποκειμένων των δεδομένων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα δυνάμει του Χάρτη.