ΥΠΟΒΟΛΗ ΚΑΤΑΓΓΕΛΙΑΣ ΕΝΩΠΙΟΝ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

–

ΑΙΤΗΜΑ ΕΞΕΤΑΣΗΣ ΤΩΝ ΠΡΑΚΤΙΚΩΝ ΤΗΣ ΕΤΑΙΡΙΑΣ CLEARVIEW AI, INC.

I. Εισαγωγή και Σκοπός της Αναφοράς

1. Μέσω της αναφοράς αυτής, η Αστική Μη Κερδοσκοπική Εταιρία Homo Di italis μετά από σχετική ανάθεση του υποκειμένου των δεδομένων [redacted] παρέχει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ("**ΑΠΔΠΧ**") αποδεικτικά στοιχεία και ανάλυση, ώστε να ερευνήσει πιθανή παραβίαση της νομοθεσίας για την προστασία των προσωπικών δεδομένων από την εταιρία Clearview AI, Inc. ("**Clearview**").

2. Οι πρακτικές της Clearview σχετικά με τα προσωπικά δεδομένα και οι χρήσεις της πλατφόρμα της οδηγούν σε ουσιαστικές και διαρκείς παραβάσεις του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679 (ΓΚΠΔ - GDPR) και του ν.4624/2019. Μετά τις εισαγωγικές ενότητες, η αναφορά αυτή δομείται γύρω από δύο κύρια σκέλη της επίδρασης της Clearview στο υποκείμενο των δεδομένων (και εν δυνάμει σε κάθε υποκείμενο δεδομένων που βρίσκεται στην Ελλάδα): (1) Την αρχική επεξεργασία προσωπικών δεδομένων εκ μέρους της Clearview μέσω της συλλογής, αποθήκευσης και ταυτοποίησης (ενότητα V), και (2) τη χρήση των υπηρεσιών της Clearview από τις αρχές επιβολής του νόμου (ενότητα VI).

II. Οι καταγγέλλοντες

3. [redacted] αναθέτει στην Αστική Μη Κερδοσκοπική Εταιρία Homo Digitalis με έδρα στην Αθήνα, οδός Αχνιάδων 17-19 & Παράλου 12, να υποβάλει την καταγγελία για λογαριασμό της. Η Homo Digitalis διαθέτει καταστατικούς σκοπούς που είναι γενικού συμφέροντος και δραστηριοποιείται στον τομέα της προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων (Συνοδευτικό Έγγραφο 2). Επομένως σύμφωνα με το άρθρο 80, παρ. 1 του GDPR και το άρθρο 41 του ν.4624/2019 μπορεί να υποβάλει την καταγγελία για λογαριασμό του υποκειμένου των δεδομένων και να ασκήσει τα δικαιώματα του μετά από ανάθεση. Είναι σημαντικό να σημειώσουμε ότι παράλληλα με την καταγγελία αυτή, σήμερα κατατέθηκαν άλλες τέσσερις (4) συναφείς καταγγελίες ενώπιον των αρχών προστασίας προσωπικών δεδομένων της Αυστρίας, της Γαλλίας, της Ιταλίας και του Ηνωμένου Βασιλείου από τις οργανώσεις της κοινωνίας των πολιτών Privacy International, noyb και Hermes Center με σκοπό την επιδίωξη

μιας συντονισμένης απάντησης στις πρακτικές της εταιρίας Clearview AI από τους αρμόδιους εποπτικούς φορείς.

III. Ο Υπεύθυνος Επεξεργασίας – Clearview AI, Inc.

4. Η Clearview AI, Inc. είναι μία εταιρεία που εδρεύει στις ΗΠΑ, ιδρυθείσα το 2017. Το μοναδικό της προϊόν είναι μία πλατφόρμα αναγνώρισης προσώπου, η οποία επιτρέπει στους χρήστες να αντιστοιχίσουν φωτογραφίες ατόμων με φωτογραφίες τους που υπάρχουν στο διαδίκτυο. Η πλατφόρμα της «περιλαμβάνει τη μεγαλύτερη γνωστή βάση δεδομένων που περιέχει περισσότερες από 3 δισεκατομμύρια εικόνες προσώπων, οι οποίες προέρχονται από δημόσιες διαδικτυακές πηγές, περιλαμβανομένων ειδήσεων, ιστοσελίδων φωτογραφιών σήμανσης, δημόσιων μέσων κοινωνικής δικτύωσης και άλλων δημόσιων πηγών.»[1]

5. Το 2020, η Clearview είχε περίπου 2,900 ενεργούς χρήστες. Παρότι κατευθύνει όλα τα δημοσίως διαθέσιμα διαφημιστικά υλικά της προς αρχές επιβολής του νόμου, οι πελάτες της Clearview λέγεται πως ποικίλουν μεταξύ «τμημάτων ασφαλείας κολλεγίων και εισαγγελικών γραφείων» και περιλαμβάνουν «έναν ανησυχητικό αριθμό ιδιωτικών εταιρειών σε βιομηχανίες όπως η διασκέδαση (Madison Square Garden και Eventbrite), τα τυχερά παίγνια (Las Vegas Sands και Pechanga Resort Casino), ο αθλητισμός (το NBA), η βιομηχανία φυσικής κατάστασης (Equinox), ακόμα και τα κρυπτονομίσματα (Coinbase).»[2] Πηγές επίσης ενδεικνύουν πως την πλαφόρμα της Clearview έχουν χρησιμοποιήσει φυσικά πρόσωπα, τα οποία σύμφωνα με αναφορές χρησιμοποίησαν «την εφαρμογή σε ραντεβού και σε πάρτυ – και για να κατασκοπεύσουν το κοινό».[3]

Τεχνική περιγραφή της βάσης δεδομένων εικόνας και του προϊόντος της Clearview

6. Σύμφωνα με την έρευνά μας και την ανάλυση δημοσίως διαθέσιμων πηγών,[4] και σύμφωνα με την τεχνογνωσία μας, αντιλαμβανόμαστε πως η βάση δεδομένων εικόνας που δημιουργήθηκε από την Clearview για την πλατφόρμα αναγνώρισης προσώπου της περιλαμβάνει τέσσερα στάδια:

    1) **Αυτοματοποιημένος συλλέκτης εικόνων** – ένα αυτοματοποιημένο εργαλείο το οποίο ερευνά δημόσιες ιστοσελίδες και συλλέγει όσες εικόνες εντοπίζει που περιέχουν ανθρώπινα πρόσωπα. Μαζί με τις εικόνες αυτές, ο συλλέκτης επίσης συλλέγει μεταδεδομένα που συνδέονται με τις εικόνες αυτές, όπως η εικόνα ή ο τίτλος της ιστοσελίδας και ο σύνδεσμος πηγής της.

---

[1] 'Overview' (Clearview AI). https://clearview.ai/overview.
[2] BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA' (27 Φεβρουαρίου 2020). https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[3] Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich' (The New York Times, 5 March 2020). https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.
[4] Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001 (2 February 2021). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Clearview AI, 'Law Enforcement' (Clearview AI Website). https://clearview.ai/law-enforcement; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR (27 Ιανουάριος 2021). https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.

2) **Αποθήκευση εικόνας και μεταδεδομένων** – οι εικόνες και τα μεταδεδομένα που συλλέγονται μέσω της διαδικασίας συλλογής αποθηκεύονται στους διακομιστές της Clearview. Αυτά τα προσωπικά δεδομένα αποθηκεύονται επ' αόριστον, δηλ. ακόμα και αφού αφαιρεθεί ή καταστεί μη δημόσια μία εικόνα ή μία ιστοσελίδα που φιλοξενεί εικόνες.

3) **Αφαίρεση χαρακτηριστικών προσώπου μέσω νευρικών δικτύων επεξεργασίας εικόνων** – για κάθε εικόνα που συλλέγεται, κάθε πρόσωπο που περιλαμβάνεται στην εικόνα σκανάρεται και υφίσταται επεξεργασία, ώστε να αφαιρεθούν τα μοναδικά χαρακτηριστικά προσώπου του. Τα πρόσωπα μεταφράζονται σε αριθμητικές ακολουθίες, τις οποίες αναφέρουμε ως «διανύσματα». Τα διανύσματα αυτά αποτελούνται από 512 σημεία δεδομένων που αντιπροσωπεύουν τις διάφορες μοναδικές γραμμές που συναποτελούν ένα πρόσωπο. Κατά το στάδιο αυτό, τα πρόσωπα μετατρέπονται από εικόνες σε μοναδικά βιομετρικά αριθμητικά αναγνωριστικά στοιχεία, τα οποία είναι αναγνωρίσιμα από μηχανές.

4) **Αποθήκευση και καταλογοποίηση/κατακερματισμός χαρακτηριστικών προσώπου** – Η Clearview αποθηκεύει όλα αυτά τα αναγνωριστικά στοιχεία σε μία βάση δεδομένων, όπου αυτά συσχετίζονται με τις εικόνες και άλλες αλιευμένες πληροφορίες που αποθηκεύονται στο διακομιστή της Clearview. Τα διανύσματα αυτά στη συνέχεια κατακερματίζονται (ο κατακερματισμός συνίσταται στη μετατροπή ενός διανύσματος, μέσω μίας μαθηματικής συνάρτησης, σε μία συντομότερη τιμή ή κλειδί καθορισμένου μεγέθους που αντιπροσωπεύει το αρχικό διάνυσμα), για δύο σχετικούς σκοπούς της, την καταλογοποίηση της βάσης δεδομένων, και τη μελλοντική αναγνώριση προσώπων. Κάθε ένα διαφορετικό πρόσωπο στη βάση δεδομένων διαθέτει ένα ξεχωριστό διάνυσμα και αντιστοίχως μία κατακερματισμένη τιμή που σχετίζεται με αυτό, ώστε να καθίσταται δυνατή η αναγνώριση και η ταυτοποίηση.

7. Το πέμπτο και τελευταίο στάδιο στον κύκλο ζωής του προϊόντος της Clearview είναι η **ταυτοποίηση**. Αυτή πραγματοποιείται όταν ένας χρήστης της Clearview επιθυμεί να αναγνωρίσει ένα άτομο, και για το λόγο αυτό αναρτά μία εικόνα του ατόμου-στόχου του και διενεργεί μία αναζήτηση. Η Clearview στη συνέχεια αναλύει την εικόνα και εξάγει ένα διάνυσμα από το υπό στόχευση πρόσωπο, το οποίο στη συνέχεια κατακερματίζεται και συγκρίνεται έναντι όλων των κατακερματισμένων διανυσμάτων που έχουν αποθηκευτεί στην πλατφόρμα της. Τέλος, το εργαλείο της Clearview εξάγει κάθε ταυτοποιημένη εικόνα από τη βάση δεδομένων διανυσμάτων και τις παρουσιάζει στο χρήστη ως αποτελέσματα αναζήτησης, μαζί με τυχόν σχετικά μεταδεδομένα, επιτρέποντας στο χρήστη να δει την αρχική σελίδα των ταυτοποιημένων εικόνων.

IV. <u>Υπόβαθρο</u>

A. Οι «αποκαλύψεις» σχετικά με την Clearview και το συνακόλουθο ενδιαφέρον των ρυθμιστικών αρχών

8. Στις 18 Ιανουαρίου 2020, ένα άρθρο των New York Times με τίτλο «Η Μυστικοπαθής Εταιρεία Που Μπορεί Να Λήξει Την Ιδιωτικότητα Όπως Την

Ξέρουμε» αποκάλυψε την ύπαρξη της Clearview στον κόσμο.[5] Πριν το άρθρο αυτό, η Clearview δρούσε με σκόπιμη μυστικότητα, την ώρα που παρείχε το προϊόν της σε «περισσότερες από 600 αρχές επιβολής του νόμου» και «σε τουλάχιστον μερικές εταιρείες για σκοπούς ασφαλείας». Μετά τις «αποκαλύψεις» αυτές, οργανισμοί και ρυθμιστικές αρχές στις Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) και στο εξωτερικό ξεκίνησαν να ερευνούν τις πρακτικές της Clearview.

9. Στις ΗΠΑ, «φέρεται πως οκτώ προσφυγές υποβλήθηκαν εντός ημερών μετά τη δημοσίευση του άρθρου των Times, ενώ ακολούθησαν περισσότερες».[6] Λόγω της έλλειψης ομοσπονδιακής νομοθεσίας σχετικά με τα προσωπικά δεδομένα στις ΗΠΑ, οι προσφυγές αυτές εξετάζονται σε διαφορετικές πολιτείες σύμφωνα με την πολιτειακή νομοθεσία. Μία από αυτές υποβλήθηκε το Μάιο του 2020 από το ACLU στο Ιλινόις,[7] σύμφωνα με το Νόμο Ιδιωτικότητας Βιομετρικών Πληροφοριών (ΝΙΒΠ) της πολιτείας, ο οποίος ρυθμίζει τη συλλογή και χρήση βιομετρικών πληροφοριών. Μία ακόμα προσφυγή υποβλήθηκε το Φεβρουάριο του 2021 στην Καλιφόρνια από ακτιβιστικές ομάδες ανθρωπίνων δικαιωμάτων και δικαιωμάτων των μεταναστών, με τον ισχυρισμό ότι οι πρακτικές της Clearview παραβιάζουν διάφορες τοπικές απαγορεύσεις της χρήσης τεχνολογίας αναγνώρισης προσώπου από την κυβέρνηση.[8]

10. Στον Καναδά, το Γραφείο του Επιτρόπου Ιδιωτικότητας Καναδά («**ΓΕΙΚ**»), μαζί με επαρχιακές ρυθμιστικές αρχές ιδιωτικότητας, εκκίνησαν έρευνα σχετικά με τις πρακτικές της Clearview το Φεβρουάριο του 2020. Η αναφορά ευρημάτων του δημοσιεύτηκε στις 2 Φεβρουαρίου 2021, προτείνοντας την παύση παροχής υπηρεσιών εκ μέρους της Clearview στον Καναδά, την παύση της συλλογής, χρήσης και δημοσιοποίησης εικόνων και βιομετρικών ιστών προσώπου που συλλέχθηκαν από φυσικά πρόσωπα στον Καναδά, και τη διαγραφή των εικόνων και των βιομετρικών ιστών προσώπου Καναδών που βρίσκονται στην κατοχή της.[9]

11. Στο Ηνωμένο Βασίλειο και την Αυστραλία, οι ρυθμιστικές αρχές προσωπικών δεδομένων εκκίνησαν κοινή έρευνα επί των «πρακτικών χειρισμού προσωπικών πληροφοριών» της Clearview τον Ιούλιο του 2020.[10]

12. Στην ΕΕ, δυσανάλογες ενέργειες έχουν ληφθεί σε διαφορετικές χώρες. Στη Γερμανία, ένα άτομο πέτυχε τη λήψη διαταγής από την Αρχή Προστασίας Προσωπικών Δεδομένων του Αμβούργου, σύμφωνα με την οποία επιβλήθηκε στην Clearview να διαγράψει την τιμή κατακερματισμού που συνδέεται με τις φωτογραφίες προσώπου του.[11] Η διαταγή περιοριζόταν στην ένδικη ατομική

[5] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' (The New York Times, 18 Ιανουάριος 2020). https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[6] Sam Jungyun Choi et al, 'Clearview AI revelations spark action on use of facial recognition', Privacy Laws & Business International Report (Αύγοστοςτ 2020). https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf.
[7] ACLU, 'ACLU sues Clearview AI. https://www.aclu.org/press-releases/aclu-sues-clearview-ai.
[8] CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists' https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.
[9] OPCC (n 4).
[10] Information Commissioner's Office, 'The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.' https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc.
[11] noyb, 'Clearview AI's biometric photo database deemed illegal in the EU, but only partial deletion https://noyb.eu/en/clearview-ai-deemed-illegal-eu.

περίπτωση και δεν πέτυχε να διατάξει την παύση των δραστηριοτήτων της Clearview στη δικαιοδοσία αυτή. Στη Σουηδία, η Σουηδική Αρχή Προστασίας Ιδιωτικότητας ανακάλυψε το Φεβρουάριο 2021 ότι η Σουηδική Αστυνομία χρησιμοποιούσε παράνομα τις υπηρεσίες της Clearview και επεξεργαζόταν προσωπικά δεδομένα παραβιάζοντας το Σουηδικό Νόμο Εγκληματικών Δεδομένων και την εφαρμοστική νομοθεσία της Οδηγίας 2016/680.[12] Διάφορες άλλες χώρες εκκίνησαν έρευνα επί των πρακτικών της Clearview, όπως η Ιταλία.[13] Στην Ελλάδα, η Homo Digitalis απηύθυνε ανοιχτή επιστολή προς τον Υπουργό Προστασίας του Πολίτη κ. Μ. Χρυσοχοΐδη τον Φεβρουάριο του 2020. Με την επιστολή μας στοχεύαμε να πληροφορηθούμε αναφορικά με τη πιθανή χρήση της εφαρμογής Clearview AI από αρχές επιβολής του νόμου στην Ελληνική Επικράτεια. Μόνο η Ελληνική Αστυνομία ανταποκρίθηκε στην επιστολή αυτή και με απάντησή της τον Μάιο του 2020 μας γνωστοποίησε ότι δεν χρησιμοποιείται από τις υπηρεσίες της η εφαρμογή της εταιρίας.[14]

13. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων ("**ΕΣΠΔ**"), κατόπιν ερωτήσεων από Μέλη του Ευρωπαϊκού Κοινοβουλίου που εξέθεταν προβληματισμούς σχετικά με την Clearview, εξέδωσε μία προκαταρκτική αξιολόγηση στις 10 Ιουνίου 2020.[15] Η αξιολόγηση αυτή επικεντρώθηκε στη «συμμόρφωση και νομιμότητα της επεξεργασίας που απορρέει από την πιθανή χρήση από Ευρωπαϊκές αρχές επιβολής του νόμου μίας υπηρεσίας όπως αυτή που παρέχεται από την Clearview AI», εκφράζοντας σοβαρές αμφιβολίες.

14. Ο αριθμός των διαφορετικών υποθέσεων που εγέρθηκαν στην Ευρώπη και αλλού υποδεικνύει έντονη και μαζική ανησυχία ατόμων και ρυθμιστικών αρχών σχετικά με τις πρακτικές της Clearview. Παρόλα αυτά μέχρι σήμερα δεν έχουν γίνει προσπάθειες ώστε να υιοθετηθεί συντονισμένη προσέγγιση σε αυτό το εγγενώς παγκόσμιο ζήτημα. Μία συντονισμένη προσέγγιση έχει καθυστερήσει από καιρό στην Ευρώπη, η οποία διαθέτει ένα από τα δυνατότερα νομικά συστήματα ιδιωτικότητας και προστασίας προσωπικών δεδομένων στον κόσμο. Μία κατακερματισμένη προσέγγιση θα μείωνε την αξία και την ισχύ του GDPR και της Οδηγίας 2016/680 που είναι άρρηκτα συνδεδεμένη με την παροχή του ίδιου επιπέδου προστασίας της ιδιωτικότητας σε όλους τους Ευρωπαίους πολίτες.

Β. Η εκ μέρους της Clearview επεξεργασία υπόκειται στον GDPR και τον ν.4624/2019

15. Η Homo Digitalis ισχυρίζεται ότι η συμπεριφορά του υπευθύνου επεξεργασίας εμπίπτει στο Άρθρο 3(2) του GDPR, καθώς η Clearview έχει αναφερθεί, σε διάφορες περιπτώσεις, να παρέχει τις υπηρεσίες της τόσο σε ιδιωτικές οντότητες όσο και σε αρχές επιβολής του νόμου στην ΕΕ, και έχει εμπλακεί στην

[12] Integritetsskydds myndigheten, 'Police unlawfully used facial recognition app' https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/.
[13] Wired, 'Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo' (15 April 2021). https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/?refresh_ce=.
[14] Homo Digitalis, Η ΕΛ.ΑΣ. απαντάει για τις φήμες συνεργασίας με την CLEARVIEW AI, https://www.homodigitalis.gr/posts/6765
[15] EDPB, Letter to Members of the European Parliament (Ref: OUT2020-0052) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en.

παρακολούθηση της συμπεριφοράς υποκειμένων των δεδομένων στην ΕΕ μέσω της συλλογής των προσωπικών τους δεδομένων. Επιπλέον, η ιστοσελίδα της εταιρείας και η συμπεριφορά της σχετικά με την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων επιβεβαιώνουν ότι η εταιρεία δρα σαν να υπόκειται στις υποχρεώσεις που επιβάλλονται από τον GDPR.

16. Επίσης, όπως προκύπτει από την αναλυτική επικοινωνία του υποκειμένου των δεδομένων με την Clearview AI (Συνοδευτικό Έγγραφο 3), το ΥΔ υπέβαλε αίτημα πρόσβασης στα προσωπικά της δεδομένα με βάση το άρθρο 15 GDPR στις 24 Μαρτίου 2021 χρησιμοποιώντας την διαθέσιμη πλατφόρμα που βρίσκεται στην ιστοσελίδα της εταιρίας παραχωρώντας τα απαραίτητα προσωπικά δεδομένα που της ζητήθηκαν για την ταυτοποίησή της. Το αίτημά της έλαβε αριθμό πρωτοκόλλου ενώ το ΥΔ παρέλαβε και επιβεβαιωτικό μήνυμα ορθής λήψης του αιτήματος πρόσβασης από την εταιρία. Ωστόσο, μετά την πάροδο ενός μήνα από την υποβολή του αιτήματος η Clearview AI δεν ανταποκρίθηκε στις υποχρεώσεις της και δεν ενημέρωσε το ΥΔ για την πορεία του αιτήματός της. Το ΥΔ στις 26 Απριλίου 2021 έστειλε νέα επικοινωνία στην εταιρία προκειμένου αυτή να συμμορφωθεί με τις υποχρεώσεις της. Τότε η εταιρία ενημέρωσε το ΥΔ ότι αδυνατεί να εντοπίσει το αίτημα πρόσβασής του και της ζήτησε να παραχωρήσει εκ νέου - μέσω email αυτή τη φορά - τα σημαντικά προσωπικά δεδομένα που απαιτούνται για την ταυτοποίησή της, υποσχόμενη ότι το αίτημά της θα έχει άμεση προτεραιότητα. Το ΥΔ απάντησε στην εταιρία ότι έχει λάβει αριθμό πρωτοκόλλου για το αίτημά της και αυτό έχει καταχωρηθεί ορθώς και κάλεσε την εταιρία να συμμορφωθεί με τις υποχρεώσεις της, όπως αυτές πηγάζουν από το άρθρο 12 παρ. 3 GDPR. Ωστόσο η εταιρία Clearview AI δεν έχει απαντήσει μέχρι και την ημέρα της κατάθεσης της παρούσας αναφοράς στο ΥΔ παραβιάζοντας τις υποχρεώσεις της.

Η εκ μέρους της Clearview επεξεργασία προσωπικών δεδομένων θέτει σε εφαρμογή το Άρθρο 3(2)(β) GDPR

17. Η εκ μέρους του υπευθύνου επεξεργασίας επεξεργασία των προσωπικών δεδομένων υποκειμένων των δεδομένων που βρίσκονται στην ΕΕ χαρακτηρίζεται από τα ακόλουθα στοιχεία από την ιστοσελίδα/διαδικτυακή πλατφόρμα του υπεύθυνου επεξεργασίας: (α) γίνεται αναφορά σε διεθνείς διαβιβάσεις σε πρόσφατη έκδοση της πολιτικής ιδιωτικότητας του υπεύθυνου επεξεργασίας: «Όταν προσωπικά δεδομένα διαβιβάζονται εκτός του ΕΟΧ, θα θέσουμε σε εφαρμογή κατάλληλα μέτρα προστασίας ώστε να διασφαλίσουμε ότι τέτοια διαβίβαση εκτελείται σε συμμόρφωση με τους εφαρμοστέους κανόνες προστασίας προσωπικών δεδομένων»,[16] και (β) σαφείς αναφορές στο «Γενικό Κανονισμό Προσωπικών Δεδομένων» στους Όρους Παροχής Υπηρεσίας και την Πολιτική Ιδιωτικότητας του υπευθύνου επεξεργασίας.[17]

18. Η Clearview συστηματικά συλλέγει και επεξεργάζεται, μέσω του αλγορίθμου αναγνώρισης προσώπου της, τα προσωπικά δεδομένα υποκειμένων των δεδομένων που βρίσκονται στην ΕΕ. Αυτή η πρακτική ανέρχεται σε

[16] Clearview AI, Inc. Privacy Policy (version 1, τελευταία ενημερωμένη στις 29 Ιανουαρίου 2020). https://clearview.ai/privacy/privacy_policy.
[17] Clearview AI, Inc. Terms of Service. https://clearview.ai/help/tos.

παρακολούθηση της συμπεριφοράς υποκειμένων των δεδομένων στην ΕΕ – εμπίπτει ξεκάθαρα στην απαίτηση του Προοιμίου 24 GDPR ότι «για τον καθορισμό του κατά πόσον μια δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί ότι παρακολουθεί τη συμπεριφορά υποκειμένου των δεδομένων, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής μετέπειτα χρήσης τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες συνίστανται στη διαμόρφωση του «προφίλ» ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του».

19. Ακόμη, μετά την υποβολή μίας προσφυγής από ένα υποκείμενο των δεδομένων που διέμενε στο Αμβούργο, ο Επίτροπος Προστασίας Προσωπικών Δεδομένων και Ελευθερίας της Πληροφορίας του Αμβούργου («**ΕΠΠΔΕΠΑ**») στις 27 Ιανουαρίου 2021 επικοινώνησε την πρόθεσή του να διατάξει την Clearview να λάβει συγκεκριμένες ενέργειες ώστε να διαγράψει τα δεδομένα του υποκειμένου των δεδομένων. Ο ΕΠΠΔΕΠΑ ισχυρίστηκε πως έχει δικαιοδοσία και πως εφαρμόζεται ο GDPR αφού συμπέρανε ότι η Clearview πράγματι παρακολουθεί τη συμπεριφορά υποκειμένων των δεδομένων στην Ένωση, σημειώνοντας ειδικότερα ότι «σκοπός της εταιρείας είναι να δύναται να ταυτοποιεί υποκείμενα. Τέτοια ταυτοποίηση καθίσταται δυνατή μέσω αποθήκευσης δημοσιεύσεων/προφίλ/λογαριασμών χρηστών που συνδέονται με μία φωτογραφία, όπως συγκεκριμένα σε μέσα κοινωνικής δικτύωσης, φόρουμ ή ιστολόγια, σε ένα προφίλ, ή τουλάχιστον να δύναται να δημιουργήσει ένα προφίλ ενός ατόμου ανά πάσα στιγμή. Αυτή η μετέπειτα χρήση τεχνικών επεξεργασίας προσωπικών δεδομένων που στοχεύει στην κατάρτιση προφίλ είναι αποφασιστικός ενδείκτης».[18] Θεωρούμε ότι και η ΑΠΔΠΧ θα καταλήξει στο ίδιο συμπέρασμα με τον ΕΠΠΔΕΠΑ ως προς την εφαρμογή του GDPR.

20. Τέλος, μία προηγούμενη έκδοση της πολιτικής ιδιωτικότητας της Clearview δείχνει ότι αυτή δημοσίως υποβάλλει εαυτόν στην αρμοδιότητα Αρχών Προστασίας Προσωπικών Δεδομένων του ΕΟΧ: «Κάτοικοι του Ευρωπαϊκού Οικονομικού Χώρου ή της Ελβετίας που επιθυμούν να υποβάλουν προσφυγή ή επιθυμούν την επίλυση διαφοράς που σχετίζεται με την επεξεργασία προσωπικών δεδομένων εκ μέρους της Clearview AI μπορούν να προσφύγουν αρμοδίως και δωρεάν στην αρμόδια Αρχή Προστασίας Δεδομένων (ΑΠΔ) της χώρας τους.»[19] Αυτή η πολιτική ιδιωτικότητας αντικαταστάθηκε το Μάρτιο του 2021 από μία έκδοση που φροντίζει να μην αναφέρεται σε κατοίκους του ΕΟΧ ή στην Ευρωπαϊκή νομοθεσία,[20] προφανώς ώστε να αποφευχθεί το παρόν επιχείρημα υπαγωγής. Όμως, καθώς δεν υπάρχουν αποδείξεις ότι η Clearview άλλαξε τις πρακτικές της και έπαψε να επεξεργάζεται προσωπικά δεδομένα κατοίκων της ΕΕ, δε βλέπουμε λόγο να θεωρήσουμε ότι η δικαιοδοσία επί των πρακτικών της έχει αλλάξει με κάποιο τρόπο.

[18] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (n 4).
[19] Clearview AI, Inc. Privacy Policy (version 1) (n 16).
[20] Clearview AI, Inc. Privacy Policy (version 2, τελευταία ενημερωμένη στις 20 Μαρτίου 2021). https://clearview.ai/privacy-policy.

21. Για τους λόγους που αναπτύχθηκαν ανωτέρω, η Homo Digitalis ισχυρίζεται ότι η ΑΠΔΠΧ πρέπει να θεωρήσει πως η συμπεριφορά του υπεύθυνου επεξεργασίας εμπίπτει στο πεδίο εφαρμογής του Άρθρου 3(2) του GDPR.

22. Επιπροσθέτως, ενόψει των ισχυουσών προτάσεων για τη ρύθμιση της μαζικής βιομετρικής παρακολούθησης,[21] η Homo Digitalis ισχυρίζεται ότι οι ισχύοντες νόμοι και νομοθεσία προστασίας προσωπικών δεδομένων είναι πλήρως επαρκή για να κριθούν παράνομες οι πρακτικές της Clearview. Μία νομοθεσία για τη μαζική βιομετρική παρακολούθηση θα ήταν πράγματι αναγκαία για να παρασχεθεί νομική σαφήνεια σχετικά με τη χρήση τεχνολογίας αναγνώρισης προσώπου σε δημόσιους χώρους σε περιορισμένες, ατομικές περιπτώσεις – όμως η μαζική παρακολούθηση βιομετρικών δεδομένων από μία ιδιωτική εταιρεία εμπίπτει καταφανώς εντός του πεδίου εφαρμογής της υπάρχουσας νομοθεσίας, η οποία σχεδιάστηκε για να προστατεύει τους Ευρωπαίους πολίτες από ακριβώς τέτοιου είδους πρακτικές.

Γ. Γιατί η ΑΠΔΠΧ πρέπει να λάβει υπόψη του την αναφορά αυτή

23. Η Homo Digitalis ανησυχεί ότι το να επιτραπεί σε εταιρείες όπως η Clearview να χρησιμοποιούν, πωλούν ή παρέχουν λογισμικά αναγνώρισης προσώπου σε ιδιώτες πελάτες και αρχές επιβολής του νόμου μπορεί να υποβαθμίσει θεμελιωδώς τα δικαιώματα των υποκειμένων των δεδομένων, αποτυγχάνοντας να τηρηθούν οι αρχές επεξεργασίας προσωπικών δεδομένων και τα αυστηρά πρότυπα επεξεργασίας που επιβάλλονται από τον GDPR και τον ν.4624/2019. Ο τρόπος που λειτουργεί και χρησιμοποιείται πλέον η τεχνολογία αυτή συγκρούεται με τις βλάβες που αποσκοπεί να αποκαταστήσει η νομοθεσία. Αν αφεθούν ατιμώρητες, τέτοιες πρακτικές μπορεί να έχουν σοβαρές επιπτώσεις για την κοινωνία μας εν συνόλω. Στην ψηφιακή εποχή, τέτοιες περιλαμβάνουν τον περιορισμό της συμμετοχής των ατόμων σε δημοκρατικές διαδικασίες μέσω του διαδικτύου, περιορισμούς στην ανάπτυξη των κοινωνικοπολιτικών ταυτοτήτων τους και «πραγματικές» βλάβες η ανικανότητα διενέργειας καθημερινών δραστηριοτήτων χωρίς το φόβο της παρακολούθησης.

24. Επιπροσθέτως, η Homo Digitalis ισχυρίζεται ότι θα είχε μεγάλη αξία για την ΑΠΔΠΧ να αξιοποιήσει τους μηχανισμούς συνεργασίας και συνεκτικότητας που προβλέπονται στα Άρθρα 60 έως 62 του GDPR. Η πρόσφατη αξιολόγηση εκ μέρους της Ευρωπαϊκής Επιτροπής σχετικά με τον GDPR[22] παρατηρεί πως «οι αρχές προστασίας προσωπικών δεδομένων δεν έχουν μέχρι τώρα κάνει πλήρη χρήση των εργαλείων που παρέχει ο GDPR, όπως κοινές ενέργειες που θα μπορούσαν να οδηγήσουν σε κοινές έρευνες». Η Homo Digitalis ισχυρίζεται ότι έρευνες σχετικά με την Clearview AI θα επωφελούνταν σημαντικά από μία διασυνοριακή συνεργασία, και πως η αποτελεσματική εφαρμογή απαιτεί συνεκτική διασυνοριακή προσέγγιση. Όπως θα εξηγηθεί περαιτέρω στη συνέχεια, οι πρακτικές της Clearview απειλούν τον ανοιχτό χαρακτήρα του Διαδικτύου και τις πολυάριθμες ελευθερίες που το χαρακτηρίζουν. Λόγω της

[21] European Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', COM(2021) 206 final

[22] European Commission, 'Communication From the Commission to the European Parliament and the Council – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' (COM(2020)0264) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

παγκόσμιας φύσης του Διαδικτύου, η διατήρηση αυτών των ουσιωδών χαρακτηριστικών απαιτεί μία παγκόσμια προσέγγιση που θα αναπτύσσει αποτελέσματα στο μέγιστο δυνατό βαθμό.

V. Νομοθετικό Πλαίσιο και Προβληματισμοί: Επεξεργασία εκ μέρους της Clearview AI, Inc. (GDPR)

25. Η ενότητα αυτή της αναφοράς εκθέτει τους προβληματισμούς της Homo Digitalis σχετικά με το πρώτο στάδιο της αλληλεπίδρασης της Clearview με υποκείμενα των δεδομένων στην ΕΕ, δηλαδή την αρχική επεξεργασία προσωπικών δεδομένων μέσω της συλλογής, της αποθήκευσης και της εξαγωγής χαρακτηριστικών προσώπου. Η νομική ανάλυσή μας και οι προβληματισμοί μας βασίζονται στις έρευνες της Homo Digitalis σε δημοσίως διαθέσιμες πηγές σχετικά με την τεχνολογία της Clearview, υποστηριζόμενες από την τεχνολογική και νομική εξειδίκευση της Homo Digitalis και των συνεργατών της. Οι πρωταρχικοί προβληματισμοί είναι ότι (i) η Clearview επεξεργάζεται τόσο μη-ευαίσθητα προσωπικά δεδομένα όσο και ειδικές κατηγορίες προσωπικών δεδομένων, χωρίς έγκυρη νομική βάση, και (ii) η επεξεργασία αυτή παραβιάζει διάφορες αρχές επεξεργασίας δεδομένων.

26. Αφού αναφέραμε ότι η Clearview επεξεργάζεται προσωπικά δεδομένα και ευαίσθητα προσωπικά δεδομένα (ενότητα Α), αυτή η ενότητα της αναφοράς θα εκθέσει τις διάφορες παραβάσεις του GDPR από τις εκ μέρους της Clearview πρακτικές συλλογής, αποθήκευσης και ταυτοποίησης, οι οποίες αποτυγχάνουν να σεβαστούν τις ακόλουθες αρχές προστασίας δεδομένων που προβλέπονται στο Άρθρο 5 του GDPR:

(α) Αρχή 1 – Νομιμότητα, Αντικειμενικότητα και Διαφάνεια
   i. Διαφάνεια (ενότητα Β)
   ii. Αντικειμενικότητα (ενότητα Γ)
   iii. Νομιμότητα και Νόμιμη Βάση σύμφωνα με τα Άρθρα 6 και 9 του GDPR (έννομα συμφέροντα και ειδικές κατηγορίες προσωπικών δεδομένων) (ενότητα Δ)

(β) Αρχή 2 – Περιορισμός του Σκοπού (ενότητα **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**)

Α. Η Clearview επεξεργάζεται προσωπικά δεδομένα και ειδικές κατηγορίες προσωπικών δεδομένων

Η Clearview επεξεργάζεται προσωπικά δεδομένα όπως αυτά ορίζονται στο Άρθρο 4(1) GDPR

27. Λαμβάνοντας υπόψη την τεχνική περιγραφή του προϊόντος της Clearview στην ενότητα ΙΙΙ παραπάνω, η Homo Digitalis ισχυρίζεται ότι η Clearview πραγματοποιεί «επεξεργασία προσωπικών δεδομένων με εν όλω ή εν μέρει αυτοματοποιημένα μέσα» όπως προβλέπεται από το Άρθρο 2(1) GDPR.

28. Κατά πρώτον, οι εικόνες που συλλέγει η Clearview από δημοσίως διαθέσιμες διαδικτυακές πηγές είναι προσωπικά δεδομένα. Οι φωτογραφίες εμπίπτουν προφανώς εντός του ορισμού των προσωπικών δεδομένων του Άρθρου 4(1)

GDPR, ειδικά όπως αυτός ερμηνεύεται με τη βοήθεια του Προοιμίου 26 GDPR: «Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. […] Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου.» Λόγω της μοναδικότητας ενός προσώπου, μία φωτογραφία ενός προσώπου κατ' ανάγκη καθιστά δυνατή, μέσω της «ανθρώπινης» αναγνώρισης, την εξακρίβωση της ταυτότητας ενός υποκειμένου. Όπως καθίσταται σαφές από την τεχνολογία της Clearview, επίσης κατ' ανάγκη καθιστά δυνατή την ταυτοποίηση ενός προσώπου μέσω της μηχανικής αναγνώρισης.

29. Ένα τέτοιο συμπέρασμα εναρμονίζεται επίσης με τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης («**ΔΕΕ**»). Το τελευταίο έχει κρίνει ότι «η εικόνα ενός προσώπου που καταγράφεται από μία κάμερα αποτελεί προσωπικό δεδομένο κατά την έννοια του Άρθρου 2(α) της Οδηγίας 95/46 στο βαθμό που καθιστά δυνατή την ταυτοποίηση του εν λόγω ατόμου».[23] Ο ορισμός των προσωπικών δεδομένων στην Οδηγία 95/46 είναι, ουσιωδώς, ο ίδιος με αυτόν που περιλαμβάνεται στο Άρθρο 4(1) του GDPR.

30. Κατά δεύτερον, τα μεταδεδομένα που επίσης συλλέγει, αποθηκεύει και συνδυάζει με τις εικόνες η Clearview ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα. Αυτό επίσης επιβεβαιώνει ότι οι φωτογραφίες που συλλέχθηκαν από την Clearview είναι προσωπικά δεδομένα, καθώς ενδέχεται «εμμέσως» να καθιστούν δυνατή την ταυτοποίηση ενός υποκειμένου των δεδομένων, καθώς ο υπεύθυνος επεξεργασίας διαθέτει «τα μέσα, τα οποία ενδέχεται να χρησιμοποιηθούν ώστε να ταυτοποιηθεί το υποκείμενο των δεδομένων», γεγονός που καθιστά το άτομο έμμεσα ταυτοποιήσιμο, όπως κρίθηκε από το ΔΕΕ στην υπόθεση *Breyer*.[24]

31. Κατά τρίτον, αυτά τα προσωπικά δεδομένα συλλέγονται, αποθηκεύονται, δομούνται μέσω καταλογοποίησης δια διανυσμάτων και ανακτώνται όταν ένας χρήστης πραγματοποιεί μία έρευνα. Αυτές είναι όλες διεργασίες που εμπίπτουν στον ορισμό της «επεξεργασίας» σύμφωνα με το Άρθρο 4(2) GDPR.

Η Clearview επεξεργάζεται βιομετρικά δεδομένα όπως ορίζονται στο Άρθρο 4(14) GDPR

32. Σύμφωνα με το Άρθρο 4(14) GDPR, ως «βιομετρικά δεδομένα» ορίζονται τα «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**».

[23] Υπόθεση C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, παρ. 22.
[24] Υπόθεση C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, παρ. 48.

33. Η Clearview επομένως επεξεργάζεται βιομετρικά δεδομένα υπό τουλάχιστον δύο έννοιες:

(α) Οι εικόνες προσώπου που συλλέγει από διαδικτυακές πηγές είναι βιομετρικά δεδομένα, και
(β) Άπαξ και δημιουργηθούν διανύσματα, αυτά καθ' αυτά καθίστανται βιομετρικά δεδομένα, καθώς είναι δεδομένα που απορρέουν από «ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά [...] χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου».

Η Clearview επεξεργάζεται ειδικές κατηγορίες δεδομένων σύμφωνα με το Άρθρο 9(1) GDPR

34. Η Clearview συστηματικά επεξεργάζεται ειδικές κατηγορίες δεδομένων όπως ορίζονται από το Άρθρο 9(1) GDPR. Σύμφωνα με το Άρθρο 9(1), οι ειδικές κατηγορίες προσωπικών δεδομένων περιλαμβάνουν «βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου». Σύμφωνα με το Προοίμιο 51 του GDPR, «[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. Αν και αυτός ο ορισμός προβλέπει ότι οι φωτογραφίες προσώπων που η Clearview συλλέγει από δημόσιες πηγές δεν αποτελούν κατ' ανάγκη ειδικές κατηγορίες δεδομένων, καθιστά επίσης σαφές ότι οι φωτογραφίες αυτές καθίστανται τέτοια όταν υφίστανται επεξεργασία στα πλαίσια του σταδίου 3 της δομής της βάσης δεδομένων της Clearview. Το σκανάρισμα κάθε προσώπου, η εξαγωγή των μοναδικών ταυτοποιητικών χαρακτηριστικών προσώπου του και η μετατροπή των χαρακτηριστικών αυτών σε διανύσματα αποτελούν «ειδική τεχνική επεξεργασία η οποία επιτρέπει την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου.»

35. Επιπρόσθετα, τα μεταδεδομένα που συλλέγονται, αποθηκεύονται και συσχετίζονται με εικόνες προσώπων ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα που αποκαλύπτουν «τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση», που αποτελούν ειδικές κατηγορίες δεδομένων. Για παράδειγμα, εικόνες προσώπου μπορούν να εντοπιστούν σε ιστοσελίδα ένωσης μελών ενορίας, ή σε ιστοσελίδα μελών σωματείου, συνδέοντας με τον τρόπο αυτό ταυτοποιήσιμα άτομα με τέτοια χαρακτηριστικά.

36. Πρέπει επίσης να σημειωθεί ότι η Clearview επεξεργάζεται τα προσωπικά δεδομένα παιδιών, των οποίων οι εικόνες προσώπου είναι διαθέσιμες στο

διαδίκτυο,[25] και η επεξεργασία των οποίων υπόκειται σε ακόμα αυστηρότερους περιορισμούς βάσει του συνόλου των διατάξεων του GDPR.[26]

Β. Διαφάνεια και το δικαίωμα πληροφόρησης

37. Η διαφάνεια είναι κύριο συστατικό της πρώτης αρχής προστασίας δεδομένων, όπως προβλέπεται στο Άρθρο 5(1)(α) GDPR και υποστηρίζεται από το δικαίωμα ενημέρωσης των Άρθρων 13 και 14. Το Προοίμιο 60 του GDPR προβλέπει ότι «[ο]ι αρχές της δίκαιης και διαφανούς επεξεργασίας απαιτούν να ενημερώνεται το υποκείμενο των δεδομένων για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της.» Σύμφωνα με το Άρθρο 14(3)(α), όταν τα προσωπικά δεδομένα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων, όπως εν προκειμένω συμβαίνει με την εκ μέρους της Clearview επεξεργασία, ο υπεύθυνος επεξεργασίας οφείλει να παρέχει στο υποκείμενο των δεδομένων πληροφόρηση «εντός εύλογης προθεσμίας από τη συλλογή των δεδομένων προσωπικού χαρακτήρα, αλλά το αργότερο εντός ενός μηνός».

38. Η Clearview έχει αναρτήσει στην ιστοσελίδα της Πολιτική Ιδιωτικότητας (η «**Πολιτική**»)[27], η οποία ανανεώθηκε το Μάρτιο 2021 από προηγούμενη έκδοση που απευθυνόταν σε ένα παγκόσμιο κοινό.[28] Η νέα έκδοση αφαίρεσε αναφορές σε κατοίκους του Ευρωπαϊκού Οικονομικού Χώρου ή της Ελβετίας. Ωστόσο, ρητώς εφαρμόζεται σε «φωτογραφίες που είναι δημοσίως διαθέσιμες στο διαδίκτυο» και στην εξαγωγή «γεωεντοπισμού και μετρήσεων χαρακτηριστικών προσώπων ατόμων στις φωτογραφίες» - πράγμα που σημαίνει ότι κατ' ανάγκη εφαρμόζεται σε όλα τα άτομα του κόσμου των οποίων τα πρόσωπα, εν γνώσει ή εν αγνοία τους, είναι αναρτημένα σε δημοσίως διαθέσιμα σημεία του Διαδικτύου, και επομένως και σε κατοίκους της ΕΕ, συμπεριλαμβανομένης της Ελλάδας.

39. Η Clearview δεν έχει καταφέρει να παράσχει την απαιτούμενη διαφάνεια υπό τουλάχιστον δύο έννοιες. Κατά πρώτον, η Clearview ουδέποτε ειδοποιεί άτομα ότι επεξεργάζεται τα προσωπικά τους δεδομένα, με αποτέλεσμα τα πληττόμενα άτομα να μην καταφέρνουν ποτέ να διαβάσουν την πολιτική ιδιωτικότητας της Clearview πριν ή μετά την επεξεργασία των προσωπικών τους δεδομένων. Σύμφωνα με τις Οδηγίες της Ομάδας Εργασίας του Αρθ. 29 σχετικά με τη διαφάνεια,[29] «ένα κεντρικό ζήτημα της αρχής της διαφάνειας […] είναι ότι το υποκείμενο των δεδομένων πρέπει να δύναται να καθορίσει εξ αρχής το εύρος και τις συνέπειες που συνεπάγεται η επεξεργασία και ότι θα πρέπει αυτό να μην καταλαμβάνεται εξ απροόπτου σε μεταγενέστερο σημείο σχετικά με τους τρόπους, με τους οποίους χρησιμοποιούνται τα προσωπικά του δεδομένα». Το απρόοπτο στην περίπτωση της Clearview είναι πλήρες – ο μόνος τρόπος για να γνωρίζει ένα υποκείμενο των δεδομένων ότι τα δεδομένα του υφίστανται

[25] Βλέπετε letter from Edward J. Markey (United States Senator) to Mr. Hoan Ton-That, σελ. 2,: https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, citing Kashmir Hill and Gabriel J.X. Dance, 'Clearview's Facial Recognition App Is Identifying Child Victims of Abuse', https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.
[26] Για παράδειγμα, Αρθρα 8, 12(1), και 17(1)(f), και Recital 38.
[27] Clearview Privacy Policy (version 2) (n 20).
[28] Clearview Privacy Policy (version 1) (n 16).
[29] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

επεξεργασία είναι να διαβάσει τις διάφορες δημοσιεύσεις σχετικά με τις πρακτικές της.

40. Κατά δεύτερον, ακόμα και αν κάποιος μπορούσε να αποκτήσει πρόσβαση στην Πολιτική την κατάλληλη στιγμή πριν ή λίγο μετά την επεξεργασία των δεδομένων του, η Clearview παρέχει ατελή και παραπλανητική πληροφόρηση. Στην ενότητα «Τι δεδομένα συλλέγουμε;», σημειώνει ότι «συλλέγει φωτογραφίες που είναι δημοσίως διαθέσιμες στο Διαδίκτυο» και ότι «ενδέχεται να εξάγει πληροφορίες από τις φωτογραφίες αυτές, περιλαμβανομένου του γεωεντοπισμού και των μετρήσεων χαρακτηριστικών προσώπου ατόμων στις φωτογραφίες». Αυτή η δήλωση είναι ατελής και παραπλανητική με δύο τρόπους: (1) παρουσιάζει την εξαγωγή πληροφοριών και μετρήσεων χαρακτηριστικών προσώπου ως απλή πιθανότητα (χρησιμοποιώντας τη λέξη «ενδέχεται», η οποία πρέπει να αποφεύγεται σε πολιτικές ιδιωτικότητας[30]), την ώρα που στην πραγματικότητα αυτή είναι μία αυτοματοποιημένη διαδικασία, και (2) παραλείπει διάφορους άλλους τύπους προσωπικών δεδομένων που η Clearview συλλέγει αυτόματα, όπως ονόματα και άλλες πληροφορίες που περιλαμβάνονται σε URLs, φωτογραφίες και τίτλους ιστοσελίδων που συλλέγονται.

41. Επιπροσθέτως, η νέα αυτή έκδοση της πολιτικής της Clearview έχει αφαιρέσει πληροφορίες σχετικά με τις νομικές βάσεις, στις οποίες βασίζεται η Clearview για την επεξεργασία των προσωπικών δεδομένων. Η προηγούμενη έκδοση της πολιτικής ιδιωτικότητας της Clearview αναφερόταν σε νόμιμες βάσεις συγκεκριμενοποιημένες σύμφωνα με τον GDPR, όπως τα έννομα συμφέροντα ή η ρητή συγκατάθεση.[31] Και πάλι, σε κάτι που πρέπει να γίνει αντιληπτό ως μία μάλλον απόπειρα να αποφύγει την εφαρμογή του GDPR, η Clearview αφαίρεσε ουσιώδεις πληροφορίες που πρέπει να παρέχονται όταν γίνεται επεξεργασία προσωπικών δεδομένων κατοίκων της ΕΕ, συμπεριλαμβανομένης της Ελλάδας.

42. Σε διάφορες δημόσιες δηλώσεις,[32] η Clearview φαίνεται να υποθέτει ότι κάθε δικαίωμα πληροφόρησης καταργείται από το γεγονός ότι τα προσωπικά δεδομένα που συλλέγονται είναι δημοσίως διαθέσιμα, και ότι επομένως τα υποκείμενα των δεδομένων θα είχαν «παραιτηθεί» από το δικαίωμα αυτό συναινώντας σιωπηρά στη δημοσίευση των εικόνων τους στο διαδίκτυο. Ωστόσο, όπως η αναφορά αυτή θα αναλύσει περαιτέρω και θα εξηγήσει κατωτέρω, αυτή η πρακτική είναι λάθος για διάφορους λόγους. Είναι επομένως απαράδεκτο να λαμβάνει η Clearview πλήρεις πληροφορίες και συναίνεση από άτομα στην κατ' αυτόν τον τρόπο επεξεργασία των εικόνων προσώπου τους.

43. Αυτή η έλλειψη διαφάνειας, που καθ' αυτή αποτελεί παραβίαση του GDPR, υπονοεί επίσης ότι μία μεγάλη πλειοψηφία των υποκειμένων των δεδομένων δε γνωρίζουν την εκ μέρους της Clearview επεξεργασία των προσωπικών δεδομένων τους και επομένως δεν μπορούν με κανένα τρόπο να ασκήσουν κανένα από τα δικαιώματά τους σχετικά με την επεξεργασία αυτή.

[30] Art 29 WP Guidelines on transparency παρ.13.
[31] Clearview Privacy Policy (version 1)
[32] Όπως για παράδειγμα CNN Business YouTube channel, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' https://www.youtube.com/watch?v=q-1bR3P9RAw.

Γ. Αντικειμενικότητα και εύλογες προσδοκίες των υποκειμένων των δεδομένων

44. Η αντικειμενικότητα είναι άλλο ένα συστατικό της πρώτης αρχής επεξεργασίας δεδομένων του Άρθρου 5(1)(α) GDPR. Πυρήνας της αντικειμενικότητας είναι ότι η κρίσιμη επεξεργασία δεδομένων πρέπει να είναι σύμφωνη με τις εύλογες προσδοκίες των ατόμων: «διαφάνεια σημαίνει ότι πρέπει να επεξεργάζεσαι προσωπικά δεδομένα με τρόπους που μπορούν τα υποκείμενα των δεδομένων να προσδοκούν ευλόγως και να μην τα χρησιμοποιείς με τρόπους που θα έχουν αδικαιολόγητα αρνητικές συνέπειες σε αυτούς.»[33]

45. Οι εύλογες προσδοκίες ιδιωτικότητας είναι επίσης μία βασική αρχή της νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου («**ΕΔΔΑ**»), η οποία χρησιμοποιείται ώστε να αξιολογηθεί αν υπάρχει παρέμβαση με την ιδιωτική ζωή ενός ατόμου σύμφωνα με το Άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου («**ΕΣΔΑ**»). Το ΕΔΔΑ σε πολλές περιπτώσεις ερεύνησε αν τα άτομα «είχαν εύλογη προσδοκία ότι η ιδιωτικότητά τους θα γίνει σεβαστή και θα προστατευτεί».[34] Στη νομολογία του, το Δικαστήριο έχει υπογραμμίσει ότι κανένα άτομο δεν μπορεί ευλόγως να αναμένει ότι υλικό που αποτυπώνει ευαίσθητες πλευρές της ιδιωτικής του ζωής μπορεί να δημοσιευθεί αργότερα στα ΜΜΕ, ακόμα και αν οι ενέργειές του είναι «ήδη στη δημόσια σφαίρα»[35] και πως η χρήση φωτογραφικού εξοπλισμού για τη λήψη και επεξεργασία βιομετρικών δεδομένων ατόμων για σκοπούς διάφορους από αυτούς που εξαρχής αναμένονταν από εκείνα δεν μπορεί να εμπίπτει εντός της έννοιας των ευλόγων προσδοκιών ιδιωτικότητας.[36]

46. Η Homo Digitalis ισχυρίζεται ότι οι εύλογες προσδοκίες των υποκειμένων των δεδομένων καταπατώνται εμφανώς από τις πρακτικές της Clearview. Στην πρόσφατη απόφασή του, το ΓΕΙΚ έκρινε ότι «άτομα που δημοσίευσαν τις φωτογραφίες τους στο διαδίκτυο, ή των οποίων οι φωτογραφίες δημοσιεύτηκαν από τρίτους, δεν είχαν εύλογες προσδοκίες ότι η Clearview θα συνέλεγε, χρησιμοποιούσε και δημοσιοποιούσε τις φωτογραφίες τους για σκοπούς ταυτοποίησης».[37] Αυτό υποστηρίζεται περαιτέρω από μία έρευνα που πραγματοποιήθηκε από τον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (FRA), σύμφωνα με την οποία Ευρωπαίοι πολίτες ερωτήθηκαν σχετικά με την προθυμία τους να μοιραστούν διαφορετικά είδη προσωπικών δεδομένων τους με κυβερνητικούς οργανισμούς και ιδιωτικές εταιρείες.[38] Σε 27 χώρες της ΕΕ, το 94% των ερωτώμενων ρητώς δήλωσαν ότι δεν ήταν πρόθυμοι να μοιραστούν τις εικόνες προσώπου τους με ιδιωτικές εταιρείες για σκοπούς ταυτοποίησης.

---

[33] ICO, 'Guide to the General Data Protection Regulation (GDPR) – Principle (a): Lawfulness, fairness and transparency'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness.
[34] *Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, Σεπτεμβρίου 2017), παρ 73.
[35] *Peck v. United Kingdom* App No 44647/98 (ECtHR, 28 Ιανουαρίου 2003), παρα 61-62.
[36] *Perry v. United Kingdom* App No 63737/00 (ECtHR, 17 Ιουλίου 2003), para 41.
[37] OPCC (n 4), Overview.
[38] European Union Agency for Fundamental Rights, 'Your rights matter: Data protection and privacy - Fundamental Rights Survey' https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1.

47. Η πρακτική συλλογής και επεξεργασίας δημοσίως διαθέσιμων δεδομένων από πλατφόρμες μέσων κοινωνικής δικτύωσης, που ορίζεται ως «κατασκοπεία μέσων κοινωνικής δικτύωσης» («**ΚΜΚΔ**») ή «παρακολούθηση μέσων κοινωνικής δικτύωσης», επικρίθηκε τα τελευταία χρόνια λόγω ανησυχίας σχετικά με τη συμβατότητά της με τις εύλογες προσδοκίες ιδιωτικότητας. Στα πλαίσια μίας διαβούλευσης για τη χρήση της παρακολούθησης μέσων κοινωνικής δικτύωσης από την Ευρωπαϊκή Υπηρεσία Υποστήριξης για το Άσυλο, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων («**ΕΕΠΔ**») έκρινε πως η παρακολούθηση μέσων κοινωνικής δικτύωσης «περιλαμβάνει χρήσεις προσωπικών δεδομένων που συγκρούονται ή υπερβαίνουν τις εύλογες προσδοκίες των ατόμων. Τέτοιες χρήσεις συχνά συντελούν στη χρήση προσωπικών δεδομένων για σκοπούς και σε πλαίσια πέραν των αρχικών, και με τρόπους που το άτομο δεν μπορεί ευλόγως να προσδοκά.»[39]

48. Η εκ μέρους της Clearview επεξεργασία είναι ένας ιδιαιτέρως αδιάκριτος τρόπος παρακολούθησης μέσων κοινωνικής δικτύωσης, ο οποίος υπερβαίνει τις δημόσιες πληροφορίες κατά περίπτωση. Η εκ μέρους της Clearview αυτόματη συλλογή, αποθήκευση και επεξεργασία για την εξαγωγή βιομετρικών ταυτοποιητών την απομακρύνουν ακόμα περισσότερο από κάθε εύλογες προσδοκίες των υποκειμένων των δεδομένων, και γι' αυτό με κανένα τρόπο δεν είναι συμβατή με την αρχή της αντικειμενικότητας. Η εφαρμογή αναγνώρισης προσώπου στη συλλογή συνθέσεων δεδομένων είναι το ζήτημα: στην επιστολή του προς το Ευρωπαϊκό Κοινοβούλιο, γνωμοδοτώντας προκαταρκτικά επί της χρήσης της Clearview από τις αρχές επιβολής του νόμου, το ΕΣΔΠ τόνισε ότι η τεχνολογία αναγνώρισης προσώπου ενδέχεται να «επηρεάσει τις εύλογες προσδοκίες των ατόμων για ανωνυμία σε δημόσιους χώρους».[40] Συνδυάζοντας ΚΜΚΔ και τεχνολογία αναγνώρισης προσώπου, η υπηρεσία που παρέχει η Clearview ουσιαστικά εκμηδενίζει την προσδοκία των ατόμων ότι οι ζωές και οι ταυτότητές τους στη φυσική ιδιωτική τους ζωή δεν είναι δυνατόν να συνδεθούν αμέσως με τις ζωές και τις ταυτότητές τους στο διαδίκτυο.

Σύγκριση με τη μηχανή αναζήτησης της Google

49. Η Clearview, σε διάφορες δημόσιες αναφορές, έχει συχνά συγκρίνει την υπηρεσία της με τη μηχανή αναζήτησης της Google, υποστηρίζοντας ότι η υπηρεσία της είναι απλώς μία «μηχανή αναζήτησης προσώπων» και όχι μία μηχανή αναζήτησης ιστοσελίδων, η οποία χρησιμοποιεί πρόσωπα αντί για λέξεις ως όρους αναζήτησης.[41] Η σύγκριση αυτή φαίνεται πως δείχνει ότι το εργαλείο της Clearview θα ενέπιπτε εντός της εύλογης προσδοκίας των υποκειμένων σχετικά με την ιδιωτικότητα, καθώς ο καθένας γνωρίζει ότι τα δεδομένα του συλλέγονται από μηχανές αναζήτησης. Ωστόσο, η Homo Digitalis επιθυμεί να παρέχει κάποιες διευκρινίσεις σχετικά με τις τεχνολογικές διαδικασίες που εφαρμόζονται από τις πλατφόρμες της Google και της Clearview, οι οποίες θα καταδείξουν ότι αυτές διαφέρουν θεμελιωδώς.

[39] EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961). https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.
[40] EDPB letter to the European Parliament.
[41] Πχ CNN Business, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]'.

50. Οι «μηχανές αναζήτησης» της Google και της Clearview πραγματοποιούν τρεις διακριτές ενέργειες:

(α) Κύλιση (Crawling) – αυτοματοποιημένη πρόσβαση σε μία ιστοσελίδα και συλλογή δεδομένων από την ιστοσελίδα,
(β) Καταλογοποίηση – λήψη περιεχομένου από μία ιστοσελίδα σε ένα διακομιστή της μηχανής αναζήτησης, και με τον τρόπο αυτό προσθήκη περιεχομένου στον «κατάλογό» της, και
(γ) Καταχώριση – προβολή ταυτοποιημένου περιεχομένου στις σελίδες αποτελεσμάτων αναζήτησης.

51. Στο στάδιο κύλισης, ο ιδιοκτήτης μιας ιστοσελίδας μπορεί να χρησιμοποιήσει ένα αρχείο robots.txt που καθοδηγεί τα διαδικτυακά ρομπότ ως προς τον τρόπο, με τον οποίο θα κινηθούν μέσα στην ιστοσελίδα του. Αυτό είναι ένα αρχείο κειμένου που επιτρέπει στους διαχειριστές ιστοσελίδων να δώσουν εντολή σε μία μηχανή αναζήτησης ότι δεν επιθυμούν τα αποτελέσματα των σελίδων τους να καταλογοποιηθούν, για παράδειγμα. Η συμμόρφωση με το αρχείο robots.txt είναι προαιρετική, και πιθανώς μπορεί να αγνοηθεί από τους κυλιστές. Πλατφόρμες όπως το LinkedIn ή το Facebook έχουν περιλάβει τέτοια αρχεία στις ιστοσελίδες τους, και ρητά απαγορεύουν κυλιστές στους όρους και τις προϋποθέσεις των ιστοσελίδων τους.

52. Η Google παρέχει στους διαχειριστές πλατφόρμας έλεγχο ως προς ποιες πληροφορίες από τη σελίδα τους μπορούν να καταλογοποιηθούν και να καταχωρηθούν στα αποτελέσματα αναζήτησής της, περιλαμβάνοντας την επιλογή να αποκλειστούν πλήρως. Η Clearview έχει δηλώσει ότι ο κυλιστής εικόνων της έχει διαμορφωθεί ώστε να σέβεται τυχόν οδηγίες υπάρχουν στα αρχεία robots.txt.[42] Ωστόσο, η Clearview έχει καταλογοποιήσει περιεχόμενο από το YouTube, το Facebook, το Twitter και το Instagram.[43] Το YouTube ρητά απαγορεύει αυτόματη συλλογή από κάθε πληροφορία που μπορεί να ταυτοποιήσει ένα άτομο, καθώς και τη συλλογή κάθε δεδομένων με εξαίρεση τις «δημόσιες μηχανές αναζήτησης», όπως της Google.[44]

53. Επομένως, η Clearview δε σέβεται τις οδηγίες να μην συλλέγει περιεχόμενο από συγκεκριμένες ιστοσελίδες, και για το λόγο αυτό έχει εναχθεί από διάφορες μεγάλες πλατφόρμες για παραβίαση των πολιτικών τους.[45] Ένας λόγος για τον οποίο η κύλιση εκ μέρους της Google είναι αποδεκτή, ενώ η συλλογή εκ μέρους της Clearview δεν είναι, είναι ότι η Google έχει αναπτύξει παρουσία από τις πρώτες μέρες του Web 2.0. Οι χρήστες του Web 2.0 έχουν αναπτύξει περιεχόμενο και χρησιμοποίησαν το διαδίκτυο γνωρίζοντας ότι η Google υπήρχε, και ότι αυτή θα συνέλεγε και θα καταλογοποιούσε το περιεχόμενό τους. Η Clearview, από την άλλη, εμφανίστηκε περισσότερο από μία δεκαετία μετά την έκρηξη των μέσων κοινωνικής δικτύωσης, απαιτώντας νομιμότητα στη συλλογή οποιωνδήποτε δεδομένων δημοσιεύονταν στο διαδίκτυο από χρήστες τη δεκαετία αυτή, και επεξεργαζόμενη αυτά μέσω τεχνολογίας αναγνώρισης

[42] OPCC (n 4), παρ. 17.
[43] Hill (v 5).
[44] YouTube GB, 'Terms of Service'. https://www.youtube.com/static?template=terms.
[45] Alfred Ng and Steven Musil, 'Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection' https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

προσώπου, η οποία δεν υπήρχε λίγα χρόνια πριν. Αυτό θεμελιωδώς συγκρούεται με τις αρχές της προβλεψιμότητας και της εύλογης προσδοκίας.

54. Η συστηματική και χωρίς διακρίσεις συλλογή εικόνων προσώπων ατόμων από το Διαδίκτυο επομένως δεν εμπίπτει εντός των εύλογων προσδοκιών των ατόμων και παραβιάζει την αρχή της αντικειμενικότητας. Το ζήτημα της αντικειμενικότητας επιδεινώνεται από την απουσία διαφάνειας και από την έλλειψη σεβασμού για το δικαίωμα ενημέρωσης των ατόμων, καθώς και από διάφορες άλλες παραβιάσεις των αρχών προστασίας δεδομένων που εκτίθενται στην παρούσα αναφορά.

Δ. Νομιμότητα και Νόμιμη Βάση

55. Το τρίτο συστατικό της πρώτης αρχής προστασίας δεδομένων του Άρθρου 5(1)(α) του GDPR είναι η νομιμότητα, που απαιτεί τα προσωπικά δεδομένα να υφίστανται νόμιμη επεξεργασία. Το Άρθρο 6 εκθέτει έναν εξαντλητικό κατάλογο νόμιμων βάσεων, στα πλαίσια των οποίων είναι δυνατή η επεξεργασία προσωπικών δεδομένων.

56. Εκτός από την απαίτηση ύπαρξης νόμιμης βάσης σύμφωνα με το Άρθρο 6, η επεξεργασία «ειδικών κατηγοριών» προσωπικών δεδομένων απαγορεύεται, εκτός αν πληρούται μία από τις προϋποθέσεις του εξαντλητικού καταλόγου του Άρθρου 9(2) GDPR. Καθώς η Clearview επεξεργάζεται βιομετρικά δεδομένα που αποτελούν «ειδικές κατηγορίες» δεδομένων, οφείλει να βασίζεται σε μία νόμιμη βάση σύμφωνα τόσο με το Άρθρο 6 όσο και με το Άρθρο 9 – και όχι σύμφωνα με ένα μόνο από τα δύο.[46] Είναι σχετικά σαφές από την προηγούμενη έκδοση της πολιτικής ιδιωτικότητας της Clearview[47] ότι αυτή η διττή απαίτηση δεν είχε γίνει πλήρως αντιληπτή: στην ενότητα «Νόμιμη βάση επεξεργασίας», παρείχε νόμιμους λόγους για την επεξεργασία προσωπικών δεδομένων (βάσει του Άρθρου 6) διακριτά προς λόγους επεξεργασίας ειδικών κατηγοριών δεδομένων (βάσει του Άρθρου 9). Επιπροσθέτως, σε δημόσιες αναφορές η Clearview φαίνεται να θεωρεί ότι το επιχείρημα «αποκτούμε δεδομένα μόνο από δημοσίως διαθέσιμες πηγές» από μόνο του αιτιολογεί όλη την επεξεργασία που αυτή πραγματοποιεί.

57. Η αναφορά αυτή θα αναλύσει τώρα το κατά πόσο εφαρμόζονται οι πιο σχετικές νόμιμες βάσεις στην εκ μέρους της Clearview επεξεργασία σύμφωνα με το Άρθρο 6 και το Άρθρο 9.

<u>Έννομα Συμφέροντα – Άρθρο 6(1)(στ) GDPR</u>

58. Η κύρια νόμιμη βάση, επί της οποίας θα μπορούσε να βασίζεται η Clearview, και στην οποία φαίνεται να βασίζεται, σύμφωνα με το Άρθρο 6 είναι τα «έννομα συμφέροντα» (Άρθρο 6(1)(στ)). Αυτό καθίσταται σαφές από την προφανή αδυναμία εφαρμογής των λοιπών νόμιμων βάσεων, και από το γεγονός ότι στην

[46] Βλέπετε Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (844/14/EN WP217)..14. Επίσης, Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2.
[47] Clearview Privacy Policy (version 1)

προηγούμενη έκδοση της πολιτικής ιδιωτικότητάς της,[48] η Clearview ρητά βασιζόταν στη βάση αυτή: «η επεξεργασία είναι αναγκαία βάσει των εννόμων συμφερόντων της Clearview, και δεν επηρεάζει δυσανάλογα τα συμφέροντα ή τα θεμελιώδη δικαιώματα και ελευθερίες σας». Οι λοιπές βάσεις στις οποίες επεδίωκε να βασιστεί εφαρμόζονταν μόνο σε δεδομένα των χρηστών των υπηρεσιών της. Για παράδειγμα, η νόμιμη βάση «η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου» (Άρθρο 6(1)(δ)) θα μπορούσε πιθανώς να εφαρμοστεί μόνο στο τελευταίο στάδιο της επεξεργασίας στον κύκλο ζωής του εργαλείου της Clearview, δηλ. όταν αξιοποιείται αυτό από μία αρχή εφαρμογής του νόμου στα πλαίσια έρευνας ενός ταυτοποιημένου εγκλήματος – δεν μπορεί να αιτιολογήσει όλη την προηγούμενη επεξεργασία.

59. Το Προοίμιο 47 του GDPR προβλέπει ότι τα έννομα συμφέροντα ενός υπεύθυνου επεξεργασίας:

> *μπορεί να παρέχουν τη νομική βάση για την επεξεργασία, υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων,* ***λαμβάνοντας υπόψη τις θεμιτές προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας.*** *Τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν* ***υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας****, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας ή βρίσκεται στην υπηρεσία του. Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων* ***ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο*** *της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία.* (η υπογράμμιση δική μας)

60. Αν και η νόμιμη βάση «έννομων συμφερόντων» επιτρέπει κάποια ευελιξία, αυτό δεν υπονοεί ότι είναι χωρίς όρια ή ότι μπορεί να διαπλαστεί ακριβώς ώστε να προσαρμοστεί ή να δικαιολογήσει οποιαδήποτε δραστηριότητα επεξεργασίας.[49] Όμως, διαρκώς γίνεται κατάχρηση αυτής της νομικής βάσης: μία πρόσφατη απόφαση του Ευρωπαϊκού Κοινοβουλίου προειδοποιεί ότι η βάση των εννόμων συμφερόντων «αναφέρεται πολύ συχνά με καταχρηστικό τρόπο ως νόμιμος λόγος επεξεργασίας».[50] Και συνεχίζει:

> *Το Ευρωπαϊκό Κοινοβούλιο […] επισημαίνει ότι οι υπεύθυνοι επεξεργασίας εξακολουθούν να βασίζονται στο έννομο συμφέρον χωρίς να διεξάγουν τον απαιτούμενο έλεγχο της ισορροπίας των συμφερόντων, ο οποίος περιλαμβάνει αξιολόγηση των θεμελιωδών δικαιωμάτων· εκφράζει ιδιαίτερη ανησυχία για το γεγονός ότι ορισμένα κράτη μέλη θεσπίζουν εθνική νομοθεσία*

[48] Ibid.
[49] ICO, 'Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
[50] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), παρ. 7.

για τον καθορισμό των όρων επεξεργασίας βάσει του έννομου συμφέροντος, προβλέποντας την εξισορρόπηση των αντίστοιχων συμφερόντων του υπευθύνου επεξεργασίας και των οικείων ατόμων, ενώ ο ΓΚΠΔ υποχρεώνει όλους τους υπεύθυνους επεξεργασίας να πραγματοποιούν αυτόν τον έλεγχο εξισορρόπησης μεμονωμένα και να αξιοποιούν αυτή τη νομική βάση· […]

Εκτίμηση Εννόμων Συμφερόντων

61. Ένας υπεύθυνος επεξεργασίας που επιδιώκει να βασιστεί στη βάση των εννόμων συμφερόντων οφείλει να πραγματοποιήσει μία αξιολόγηση, και να καταστήσει την αξιολόγηση αυτή διαθέσιμη στα επηρεαζόμενα υποκείμενα των δεδομένων.[51] Η Clearview δεν έχει καταστήσει καμία αξιολόγηση εννόμων συμφερόντων δημοσίως διαθέσιμη.

62. Τέτοια αξιολόγηση εννόμων συμφερόντων πρέπει να πραγματοποιηθεί λαμβάνοντας υπόψη τις τρεις προϋποθέσεις που προβλέπονται από το Άρθρο 6(1)(στ) και αναλύονται περαιτέρω στις αποφάσεις του ΔΕΕ *Rigas Satiksme*[52] και *Fashion ID*[53]:

(1) **Η επιδίωξη ενός εννόμου συμφέροντος από τον υπεύθυνο επεξεργασίας ή από το(υς) τρίτο(υς) στο(υς) οποίο(υς) παρέχονται τα δεδομένα («σκοπός»)**: Στην περίπτωση της Clearview, τέτοιο θα ήταν ένα εμπορικό συμφέρον, δηλ. η παροχή μίας υπηρεσίας σε τρίτους με οικονομικό αντάλλαγμα. Είναι αυταπόδεικτο ότι οι εταιρείες δεν μπορούν να αξιοποιούν απλά και μόνο την επιδίωξη των εμπορικών τους μοντέλων ή του κέρδους ως «έννομα συμφέροντα». Το έννομο συμφέρον των τρίτων προς τους οποίους παρέχονται τα δεδομένα μπορεί να θεωρηθεί ως η ταυτοποίηση ατόμων. Στην περίπτωση του πιο συχνού πελάτη της Clearview, μίας αρχής επιβολής του νόμου, το Άρθρο 6(1) του GDPR ρητώς προβλέπει ότι η νόμιμη βάση εννόμων συμφερόντων «δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την εκτέλεση των καθηκόντων τους». Στην περίπτωση οποιουδήποτε άλλου πελάτη της Clearview, δηλ. ιδιωτικών εταιρειών και ατόμων, η νομιμότητα των συμφερόντων τους είναι μόνο υποθετική. Σε κάθε περίπτωση, ένα μελλοντικό και αόριστο συμφέρον κάποιου τρίτου μέρους δεν μπορεί να δικαιολογήσει τις αρχικές δραστηριότητες επεξεργασίας. Στην περίπτωση αυτή, η συλλογή, η βιομετρική επεξεργασία και η αποθήκευση των εικόνων ατόμων διενεργείται πριν χρησιμοποιήσει κάποιος πελάτης τα δεδομένα, και πριν κάποιος μπορεί ακόμα και να διανοηθεί τη συγκεκριμένη χρήση που θα πραγματοποιήσουν με αυτά οι πελάτες της Clearview. Όπως περιγράφηκε από το ΓΕΙΚ του Καναδά, οι δραστηριότητες της Clearview δεν είναι τίποτα περισσότερο από «μία μαζική ταυτοποίηση και παρακολούθηση ατόμων από μία ιδιωτική εταιρεία στα πλαίσια μίας εμπορικής δραστηριότητας».[54]

(2) **Η αναγκαιότητα επεξεργασίας προσωπικών δεδομένων για τους σκοπούς των επιδιωκόμενων εννόμων συμφερόντων**

[51] ICO (n 49).
[52] Υπόθεση 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, παρ. 28-31.
[53] Υπόθεση C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, παρ. 95.
[54] OPCC (n 4), παρ. 72.

(«αναγκαιότητα») – αν η Clearview είχε έννομο συμφέρον σχετικό με την αξιολόγηση αυτή, αυτή η προϋπόθεση θα απαιτούσε να αξιολογηθεί αν το εμπορικό όφελος της Clearview θα μπορούσε να επιτευχθεί με μέσα λιγότερο διεισδυτικά στα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, σύμφωνα με την αρχή ότι οι εξαιρέσεις και οι περιορισμοί σε σχέση με την προστασία προσωπικών δεδομένων πρέπει να εφαρμόζονται μόνο στο βαθμό που αυτό είναι αυστηρά αναγκαίο.[55] Έχοντας αποδείξει ότι τα συμφέροντα μίας αρχής εφαρμογής του νόμου δεν μπορούν να ληφθούν υπόψη σε αυτή τη συγκεκριμένη αξιολόγηση, δεν μπορεί να υποστηριχθεί ότι ιδιώτες πελάτες της Clearview *έχουν ανάγκη* να αξιοποιήσουν το εργαλείο αυτό για τα συμφέροντά τους. Η ύπαρξη λιγότερο διεισδυτικών εναλλακτικών είναι κρίσιμη, λαμβάνοντας υπόψη την αρχή της ελαχιστοποίησης των δεδομένων, σύμφωνα με την οποία τα δεδομένα θα είναι «είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία».[56] Για παράδειγμα, η Clearview αναφέρει ότι τράπεζες μπορούν να αξιοποιήσουν το εργαλείο της για ασφάλεια και ελέγχους ιστορικού, όμως οι τράπεζες διενεργούν τέτοιους ελέγχους χωρίς ένα τέτοιο εργαλείο εδώ και δεκαετίες. Είναι εξίσου δύσκολο να γίνει αντιληπτό γιατί τέτοιοι έλεγχοι μπορούν μόνο να διενεργηθούν στη βάση μίας εικόνας προσώπου, και όχι επί τη βάση άλλων ταυτοποιητών.

(3) **Ότι τα θεμελιώδη δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων, των οποίων τα δεδομένα επιβάλλουν την προστασία, δεν υπερισχύουν («στάθμιση»)** – αυτό απαιτεί στάθμιση μεταξύ των συμφερόντων του υπευθύνου επεξεργασίας και των αποτελεσμάτων της επεξεργασίας σε ένα υποκείμενο δεδομένων. Στη θεμελιώδη υπόθεση *Google Spain*, το ΔΕΕ έκρινε ότι η επεξεργασία προσωπικών δεδομένων

> *την οποία πραγματοποιεί ο φορέας εκμετάλλευσης μηχανής αναζήτησης, ενδέχεται να θίγει σημαντικά τα θεμελιώδη δικαιώματα στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, όταν η αναζήτηση μέσω της μηχανής αυτής πραγματοποιείται με βάση το ονοματεπώνυμο φυσικού προσώπου, εφόσον η εν λόγω επεξεργασία παρέχει τη δυνατότητα σε οποιονδήποτε χρήστη του διαδικτύου να αποκτά, μέσω του καταλόγου αποτελεσμάτων, μια συστηματική επισκόπηση των διαθέσιμων στο διαδίκτυο πληροφοριών σχετικά με το εν λόγω πρόσωπο, οι οποίες αφορούν δυνητικά διάφορες πτυχές της ιδιωτικής του ζωής και θα ήταν αδύνατο ή εξαιρετικά δυσχερές να διασταυρωθούν χωρίς τη μηχανή αναζήτησης, και κατά τον τρόπο αυτό, να σχηματίζει ένα, κατά το μάλλον ή ήττον, λεπτομερές προφίλ του προσώπου αυτού.*[57]

Το ΔΕΕ έκρινε επίσης ότι «η επέμβαση αυτή, λόγω της ενδεχόμενης σοβαρότητάς της, δεν μπορεί να δικαιολογείται μόνο με βάση το οικονομικό

[55] Υποθέσεις C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] EU:C:2010:662, παρ 86; Υποθεση C-473/12 *IPI* [2013] EU:C:2013:715, παρ. 39; Υποθεση C-212/13 *Ryneš* [2014] EU:C:2014:2428, παρ. 28.

[56] C/Jorge Juan 6 28001 – Madrid. https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf.

[57] Υπόθεση C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, παρ 80.

συμφέρον του φορέα εκμετάλλευσης της μηχανής αναζήτησης στην ως άνω επεξεργασία».[58]

Αυτό που το ΔΕΕ περιέγραψε εδώ ως σημαντική επέμβαση με τα θεμελιώδη δικαιώματα των ατόμων είναι ακριβώς αυτό που πραγματοποιεί η Clearview, με παράγοντες που μόνο να ενδυναμώσουν μπορούν τη σοβαρότητα αυτής της επέμβασης: (α) στην περίπτωση της Clearview, δεν απαιτείται η γνώση του ονόματος ενός ατόμου για να παραχθούν αποτελέσματα αναζήτησης, παρά μόνο το πρόσωπό του, το οποίο μπορεί να αποκτηθεί απλά και μόνο με το πέρασμα ενός ατόμου στο δρόμο και τη λήψη της φωτογραφίας του, και (β) στην περίπτωση της Clearview, ένα άτομο δεν μπορεί, χωρίς να χρησιμοποιήσει το ίδιο το εργαλείο της Clearview, να γνωρίζει τι πληροφορίες σχετικά με αυτό υπάρχουν διαθέσιμες εκεί έξω (ενώ μπορεί να πραγματοποιήσει έρευνα του ονόματός του και άλλων εγγράφων ταυτοποιητών μέσω της Google).

Η Γνωμοδότηση της Ομάδας Εργασίας του Άρθρου 29 για τα Έννομα Συμφέροντα[59] εκθέτει επιπλέον κάποιους από τους παράγοντες που πρέπει να ληφθούν υπόψη όταν διενεργείται τέτοιος έλεγχος στάθμισης:

i. **Η φύση και η πηγή του εννόμου συμφέροντος** – όπως αναλύθηκε στην παράγραφο (1) ανωτέρω, το συμφέρον της Clearview επί της επεξεργασίας είναι ένα αμιγώς εμπορικό συμφέρον.

ii. **Η επίπτωση στα υποκείμενα των δεδομένων,** περιλαμβανομένων:

- της φύσης των δεδομένων, όπως αν η επεξεργασία περιλαμβάνει δεδομένα που μπορούν να θεωρηθούν ευαίσθητα ή έχουν αποκτηθεί από δημοσίως διαθέσιμες πηγές – η Clearview επεξεργάζεται βιομετρικά δεδομένα, τα οποία είναι ιδιαίτερα ευαίσθητα, όπως θα αναπτυχθεί κατωτέρω, το γεγονός ότι τα δεδομένα αποκτήθηκαν από δημοσίως διαθέσιμες πηγές δεν επηρεάζει την ευαίσθητη φύση τους και την ανάγκη προστασίας της ιδιωτικότητας. Η Ομάδα Εργασίας του Άρθρου 29 σημείωσε ότι:

  > *είναι σημαντικό να τονιστεί ότι τα προσωπικά δεδομένα, ακόμα και αν έχουν καταστεί δημοσίως διαθέσιμα, συνεχίζουν να θεωρούνται προσωπικά δεδομένα, και η επεξεργασία τους επομένως εξακολουθεί να απαιτεί κατάλληλες εγγυήσεις. Δεν υφίσταται γενική άδεια περαιτέρω χρήσης και επεξεργασίας δημοσίως διαθέσιμων προσωπικών δεδομένων στα πλαίσια του Άρθρου 7(στ).*[60]

  Αν και γίνεται δεκτό ότι το γεγονός πως τα προσωπικά δεδομένα είναι δημοσίως διαθέσιμα μπορεί να είναι ένας σχετικός παράγοντας υπέρ

[58] Ibid, παρ. 81.
[59] Art 29 WP Opinion on Legitimate Interests, pp. 36-43. **Η Homo Digitalis υπογραμμίζει ότι το ΕΣΠΔ βρίσκεται σε διαδικασία αναθεώρησης αυτής της Γνωμοδότησης με βάση το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου που αναφέρουμε στην υποσημείωση ν.50.**
[60] Ibid, σελ. 39.

της ύπαρξης εννόμων συμφερόντων, εφιστάται στη συνέχεια η προσοχή ότι αυτό θα μπορούσε να ισχύει μόνο «αν η δημοσίευση πραγματοποιήθηκε με την εύλογη προσδοκία της περαιτέρω χρήσης των δεδομένων για συγκεκριμένους σκοπούς (π.χ. για σκοπούς έρευνας ή για σκοπούς που συνδέονται με τη διαφάνεια και τη λογοδοσία).» Όπως αναπτύχθηκε ανωτέρω στην ενότητα Γ, σε καμία περίπτωση δεν εμπίπτει η εκ μέρους της Clearview επεξεργασία εντός αυτής της εύλογης προσδοκίας περαιτέρω χρήσης.

- του τρόπου επεξεργασίας των προσωπικών δεδομένων (περιλαμβανομένου του αν τα δεδομένα κοινοποιούνται δημοσίως ή καθίστανται με άλλο τρόπο διαθέσιμα σε ένα μεγάλο αριθμό ατόμων, ή αν μεγάλος αριθμός προσωπικών δεδομένων υφίστανται επεξεργασία ή συνδυάζονται με άλλα δεδομένα, π.χ. στην περίπτωση της κατάρτισης προφίλ για εμπορικούς σκοπούς, για σκοπούς εφαρμογής του νόμου ή για άλλους σκοπούς) – τα δεδομένα που επεξεργάζεται η Clearview υφίστανται διέλευση μέσα από τον αλγόριθμο αναγνώρισης προσώπου της, πράγμα που αποτελεί ιδιαίτερα διεισδυτικό τρόπο επεξεργασίας. Κάθε ένας από τους πελάτες της Clearview μπορεί να αποκτήσει πρόσβαση στα δεδομένα που επεξεργάζεται η Clearview. Αυτή αποτελεί μία ευρεία, απροσδιόριστη και απεριόριστη ομάδα ατόμων. Επιπροσθέτως, ο συνδυασμός τμημάτων πληροφοριών σχετικά με την ιδιωτική ζωή ενός ατόμου, που δημοσιεύθηκαν στο Διαδίκτυο εκούσια ή ακούσια, μπορεί να οδηγήσει στη δημιουργία μίας πολύ διεισδυτικής και ευαίσθητης οπτικής επί της ζωής τους, η οποία δεν θα μπορούσε ποτέ να επιτευχθεί μέσω χειροκίνητης διαδικτυακής έρευνας ή μέσω της χρήσης μηχανών αναζήτησης που λειτουργούν με όρους-κλειδιά. Λαμβάνοντας υπόψη ότι τέτοια τεχνογνωσία μπορεί να χρησιμοποιηθεί για να ληφθούν αποφάσεις σχετικά με συλλήψεις και ποινικές καταδίκες, η επίδραση μπορεί να θεωρηθεί μόνο του υψηλότερου επιπέδου.

- των εύλογων προσδοκιών, ειδικά σε σχέση με τη χρήση και αποκάλυψη των δεδομένων στο σχετικό πλαίσιο, η εκ μέρους της Clearview επεξεργασία δεν μπορεί να εμπίπτει εντός των ευλόγων προσδοκιών σχετικά με τη χρήση και αποκάλυψη των δεδομένων.

- των ιδιοτήτων του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων, περιλαμβανομένης της ισορροπίας δυνάμεων μεταξύ του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων, ή του αν το υποκείμενο των δεδομένων είναι παιδί ή κατ' άλλο τρόπο ανήκει σε μία πιο ευάλωτη μερίδα του πληθυσμού – οι συνθήκες της εκ μέρους της Clearview επεξεργασίας καθιστούν την επίδραση στα υποκείμενα των δεδομένων ιδιαίτερα έντονη. Όπως το Προοίμιο 47 του GDPR καθιστά σαφές, κάτι το έννομο θα πρέπει τουλάχιστον εν μέρει να εξαρτάται από το αν ένα έννομο συμφέρον εξυπηρετείται λόγω της σχέσης μεταξύ του υπεύθυνου και του υποκειμένου. Όχι μόνο δεν έχει η Clearview καμία σχέση με τα πληττόμενα άτομα, αλλά και η ύπαρξη και οι δραστηριότητές της είναι εντελώς άγνωστες στα

περισσότερα υποκείμενα των δεδομένων. Σε συνδυασμό με την απρόβλεπτη χρήση του εργαλείου της από αρχές επιβολής του νόμου και ιδιωτικές οντότητες ανά τον κόσμο, οι συνθήκες αυτές καθιστούν την ισορροπία δυνάμεων ιδιαίτερα δυσμενή προς τα υποκείμενα των δεδομένων. Επιπροσθέτως, λόγω των χωρίς διακρίσεις πρακτικών της, η Clearview κατ' ανάγκη επεξεργάζεται προσωπικά δεδομένα παιδιών και ευάλωτων μερίδων του πληθυσμού. Αυτή ευαλωτότητα συχνά επιδεινώνεται από την έλλειψη ελέγχου αυτών των πληθυσμών επί των διαδικτυακών ταυτοτήτων τους.

Η Γνωμοδότηση της Ομάδας Εργασίας του Άρθρου 29 επί των Εννόμων Συμφερόντων θεωρεί πως σε περιπτώσεις όπου η προεξόφληση ή η θεμελίωση βλάβης ή ζημίας σε υποκείμενα των δεδομένων είναι ιδιαίτερα δύσκολη, «είναι έτι περισσότερο σημαντικό να εστιάζει κανείς στην πρόληψη και να διασφαλίζει ότι δραστηριότητες επεξεργασίας μπορούν μόνο να εκτελεστούν, εφόσον δεν επιφέρουν κίνδυνο ή επιφέρουν μόνο χαμηλό κίνδυνο αναίτιας αρνητικής επίδρασης στα συμφέροντα ή τις θεμελιώδη δικαιώματα και ελευθερίες των υποκειμένων των δεδομένων».[61] Λαμβάνοντας υπόψη τη μη αμελητέα επίδραση που ενδέχεται να έχει η εκ μέρους της Clearview επεξεργασία επί των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων, η Homo Digitalis ισχυρίζεται ότι η ΑΠΔΠΧ οφείλει να υιοθετήσει μία ιδιαιτέρως προσεκτική προσέγγιση και να αποτρέψει τέτοιου είδους επικίνδυνη επεξεργασία.

iii. **Επιπρόσθετα μέτρα προστασίας για την πρόληψη αναιτιώδους επίδρασης στα υποκείμενα των δεδομένων**, περιλαμβανομένων:

- της ελαχιστοποίησης των δεδομένων – το μοντέλο λειτουργίας της Clearview βασίζεται σε αρχές αντίθετες με την ελαχιστοποίηση των δεδομένων. Με το να συλλέγει και να επεξεργάζεται αδιακρίτως προσωπικά δεδομένα μέσω των αλγορίθμων αναγνώρισης προσώπου της, προσομοιάζει πολύ στη μαζική συλλογή ομάδων δεδομένων και τη μαζική παρακολούθηση.

- των τεχνικών και οργανωτικών μέτρων που διασφαλίζουν ότι τα δεδομένα δεν μπορούν να χρησιμοποιηθούν για να ληφθούν αποφάσεις ή άλλα μέτρα σε σχέση με τα άτομα («λειτουργικός διαχωρισμός») – ο τελικός σκοπός του προϊόντος της Clearview είναι να λαμβάνονται αποφάσεις και ενέργειες σε σχέση με άτομα, οι οποίες ενδέχεται να έχουν μία ουσιωδώς αρνητική επίδραση στις ζωές τους.

- της εκτενούς χρήσης τεχνικών ανωνυμοποίησης, συγκέντρωσης δεδομένων, τεχνολογιών βελτίωσης της ιδιωτικότητας, ιδιωτικότητας εκ του σχεδιασμού, μελετών εκτίμησης αντικτύπου ιδιωτικότητας και προστασίας δεδομένων. Εξ όσων γνωρίζουμε, δεν έχουν

[61] Ibid, σελ.51.

ενσωματωθεί στο προϊόν της Clearview τεχνολογίες ή σχεδιασμοί βελτίωσης της ιδιωτικότητας. Σε κάθε περίπτωση, ο σκοπός καθ' αυτός του προϊόντος της είναι να αφαιρέσει από κάθε άτομο με κάποια (εκούσια ή ακούσια) διαδικτυακή παρουσία την προστασία της ταυτότητάς του που ευλόγως μπορούν να αναμένει.

- της αυξημένης διαφάνειας, του γενικού και απροϋπόθετου δικαιώματος αντίταξης, της φορητότητας των δεδομένων και σχετιζόμενων μέτρων ενδυνάμωσης των υποκειμένων των δεδομένων (ζητήματα που παίζουν «ένα κρίσιμο ρόλο στα πλαίσια του Άρθρου 6(στ)»[62]) – αυτό απαιτεί από τον υπεύθυνο να διενεργήσει «μία προσεκτική και αποτελεσματική εκ των προτέρων αξιολόγηση, επί τη βάση των συγκεκριμένων γεγονότων της ένδικης περίπτωσης και όχι αφαιρετικά, λαμβάνοντας επίσης υπόψη τις εύλογες προσδοκίες των υποκειμένων των δεδομένων». Παρά τις πολλαπλές ευκαιρίες, όπως η πολιτική ιδιωτικότητάς της, ή τα πολλά αιτήματα πρόσβασης υποκειμένων των δεδομένων που λαμβάνει, στο βαθμό που η Homo Digitalis γνωρίζει, η Clearview ποτέ δεν εκπόνησε ή δεν απέδειξε την εκπόνηση του κριτηρίου εξισορρόπησης. Όπως αναπτύσσεται ανωτέρω στην ενότητα Β, οι δραστηριότητες της Clearview ενδεικνύουν μία πλήρη έλλειψη διαφάνειας και λογοδοσίας προς τα υποκείμενα των δεδομένων. Η Clearview παρέχει περιορισμένα το δικαίωμα αντίταξης στην επεξεργασία, παρότι είναι ασαφές τι θα περιελάμβανε η αντίταξη στην επεξεργασία. Λόγω της φύσης της τεχνολογίας της Clearview, είναι πιθανό ότι κάθε αντίταξη θα επιδρούσε μόνο στην επιστροφή αποτελεσμάτων όταν διενεργείται μία έρευνα, και δεν θα περιόριζε την περαιτέρω συλλογή προσωπικών δεδομένων μέσω την αλγορίθμων αναγνώρισης προσώπου της.

63. Αξιοποιώντας το ανωτέρω πλαίσιο για να αναλυθεί το αν εφαρμόζεται η νόμιμη βάση των εννόμων συμφερόντων στις δραστηριότητες επεξεργασίας της Clearview, είναι σαφές ότι σε κάθε έναν παράγοντα, η Clearview εμπίπτει στην κατηγορία υψηλού ρίσκου και ιδιαιτέρως αρνητικής επίδρασης. Επιπροσθέτως, οι διάφοροι «ελαφρυντικοί» παράγοντες στη διάθεσή της που θα μπορούσαν να αμβλύνουν αυτή την επίδραση είναι απλώς απόντες από τις δραστηριότητές της. Και δεδομένου ότι κάθε έννομο συμφέρον είναι στην καλύτερη περίπτωση ένα εμπορικό συμφέρον, η εξισορρόπηση οδηγεί στο συμπέρασμα ότι η εκ μέρους της επεξεργασία δεν πρέπει να γίνει αποδεκτή και δεν πρέπει να της αναγνωριστεί νόμιμη βάση κατ' Άρθρο 6(1)(στ).

64. Έχουν πραγματοποιηθεί κάποιες αξιολογήσεις εννόμων συμφερόντων από αρχές προστασίας δεδομένων ανά την Ευρώπη, και αυτές ενδεικνύουν πολύ στενή ερμηνεία των εννόμων συμφερόντων που σε καμία περίπτωση δεν μπορεί να επεκταθεί σε αυτόν τον τρόπο συστηματικής και αδιάκριτης επεξεργασίας που εκτελεί η Clearview. Για παράδειγμα, στην υπ' αριθμ. 35/2020 απόφασή του,[63]

[62] Ibid, σελ.43.
[63] Autorité de Protection des Données, Chambre Contentieuse, 'Décision quant au fond 35/2020 du 30 juin 2020' (Numéro de dossier : DOS-2019-01240). https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf.

το Τμήμα Δικαστικών Διαφορών της Βελγικής Αρχής Προστασίας Δεδομένων αξιολόγησε αν η επανάχρηση μίας δημοσίως διαθέσιμης εικόνας προφίλ στο Facebook ενός ατόμου από μία Βελγική δικαστική αρχή ώστε να εκτελεστεί μία «απαγόρευση παρουσίας» εμπίπτει στα έννομα συμφέροντα της αρχής. Σημείωσε ότι:

> *Ο GDPR θεσπίζει ένα σημαντικό περιορισμό στην ελευθερία επανάχρησης δημοσίως διαθέσιμων προσωπικών δεδομένων. Το Τμήμα Δικαστικών Διαφορών σημειώνει ότι η εφαρμοστέα αρχή προβλέπει τα ακόλουθα: το γεγονός ότι η εικόνα προφίλ ενός ατόμου είναι ελεύθερα διαθέσιμη στο κοινό δε σημαίνει ότι τρίτοι μπορούν να τη χρησιμοποιούν ελεύθερα. Η χρήση της εικόνας αυτής είναι δυνατή μόνο εάν υπάρχει μία βάσιμη νόμιμη βάση.*

Κρίθηκε ότι η επανάχρηση της εικόνας προφίλ του ατόμου ενέπιπτε στη νόμιμη βάση εννόμων συμφερόντων, γιατί η αρχή είχε ένα έννομο συμφέρον (την εκτέλεση της απόφασής της), για την πραγματοποίηση του οποίου ήταν αναγκαία η επεξεργασία (δεν μπορούσε να επιτευχθεί με άλλα μέσα, και η αρχή φρόντισε να «θολώσει» τα πρόσωπα άλλων ατόμων της εικόνας). Αυτή η νόμιμη βάση εφαρμόστηκε συγκεκριμένα επί της προσφυγής του ατόμου και δεν μπορεί να επεκταθεί αδιακρίτως. Η εκ μέρους της Βελγικής Αρχής Προστασίας Δεδομένων μελέτη ώστε να επιτρέψει τη συγκεκριμένη και περιορισμένη επανάχρηση της εικόνας προφίλ του προσφεύγοντος καταδεικνύει το ότι το να επιτραπεί στην Clearview να συλλέγει και να επαναχρησιμοποιεί συστηματικά κάθε μία εικόνα προσώπου που είναι διαθέσιμη στο Διαδίκτυο χαρακτηρίζεται από έλλειψη αναλογικότητας και δεν μπορεί να γίνει αποδεκτό.

65. Ομοίως, το ΓΕΙΚ του Καναδά πραγματοποίησε μία αξιολόγηση σχετικά με τα έννομα συμφέροντα αντίστοιχη σύμφωνα με την εφαρμοστέα νομοθεσία και έκρινε πως:

> *Θεωρούμε ότι η Clearview δεν διαθέτει, στην περίπτωση αυτή, έναν επιτρεπόμενο σκοπό, για:*
>
> *i. τη μαζική και αδιάκριτη συλλογή εικόνων εκατομμυρίων ατόμων ανά τον Καναδά, περιλαμβανομένων και παιδιών, μεταξύ των 3 δισεκατομμυρίων εικόνων που έχει συλλέξει παγκοσμίως,*
> *ii. την ανάπτυξη αρχείων βιομετρικής αναγνώρισης προσώπου επί τη βάση των εικόνων αυτών, και τη διατήρηση των πληροφοριών αυτών ακόμα και μετά την αφαίρεση από το Διαδίκτυο της εικόνας ή του συνδέσμου πηγής, ή*
> *iii. τη μετέπειτα χρήση και διαβίβαση των πληροφοριών αυτών για τους δικούς της εμπορικούς σκοπούς,*
>
> *όταν τέτοιοι σκοποί:*
>
> *iv. δε σχετίζονται με τους σκοπούς για τους οποίους δημοσιεύθηκαν εξαρχής οι εικόνες (για παράδειγμα, κοινωνική ή επαγγελματική δικτύωση),*
> *v. συχνά βλάπτουν το άτομο (για παράδειγμα, έρευνες, πιθανή σύλληψη, γελοιοποίηση, κλπ.), και*
> *vi. δημιουργούν τον κίνδυνο σημαντικής βλάβης στα άτομα, των οποίων οι εικόνες αποκτώνται από την Clearview (περιλαμβανομένων βλαβών που συνδέονται με την εσφαλμένη ταυτοποίηση ή την έκθεση σε πιθανές*

παραβάσεις προσωπικών δεδομένων), δεδομένου ότι η μεγάλη πλειοψηφία των ατόμων αυτών δεν έχουν και δε θα έχουν ποτέ εμπλακεί σε ένα έγκλημα, ή δεν έχουν ταυτοποιηθεί με τρόπο που υποβοηθά τη διαλεύκανση ενός σοβαρού εγκλήματος.[64]

66. Εξισορροπώντας και συμπληρώνοντας την ανωτέρω αξιολόγηση τυχόν βλάβης στα υποκείμενα των δεδομένων, οι ακόλουθες ενότητες τονίζουν τρεις σημαντικούς παράγοντες της βλάβης που προκαλείται από το εργαλείο της Clearview στα υποκείμενα των δεδομένων: (α) οι γνωστοί κίνδυνοι της επεξεργασίας βιομετρικών δεδομένων, (β) το αναπόφευκτο αποτέλεσμα αποθάρρυνσης των θεμελιωδών δικαιωμάτων, και (γ) οι συγκεκριμένες βλάβες που μπορούν να προβλεφθούν για ευάλωτες κοινότητες.

Κίνδυνοι επεξεργασίας βιομετρικών δεδομένων

67. Τα βιομετρικά δεδομένα θεωρούνται ειδικές κατηγορίες δεδομένων λόγω της μοναδικής τους φύσης, η οποία παράγεται από ανθρώπινα χαρακτηριστικά, όπως τα δακτυλικά αποτυπώματα, η φωνή, το πρόσωπο, τα μοτίβα αμφιβληστροειδούς χιτώνα και ίριδας, η γεωμετρία χεριού, το βάδισμα ή τα προφίλ γονιδιώματος. Αποτελούν καθ' αυτά ευαίσθητα δεδομένα, ανεξαρτήτως της πηγής ή του τρόπου συλλογής τους.[65] Και η ΑΠΔΠΧ έχει κρίνει αντιστοίχως για ειδικές κατηγορίες προσωπικών δεδομένων, όπως τα γενετικά αποτυπώματα.[66] Όπως έκρινε το ΓΕΙΚ του Καναδά:

Οι βιομετρικές πληροφορίες είναι χαρακτηριστικές, μάλλον απίθανο να τροποποιηθούν στο μέλλον, δύσκολο να αλλάξουν και εν πολλοίς μοναδικές για το κάθε άτομο. Τα βιομετρικά δεδομένα προσώπου είναι ιδιαιτέρως ευαίσθητα, λαμβάνοντας υπόψη ότι αποτελούν χαρακτηριστικά της ταυτότητας ενός ατόμου, γεγονός που υποβοηθά την ικανότητα ταυτοποίησης και παρακολούθησης των ατόμων.[67]

68. Όταν υιοθετούνται εν τη απουσία στέρεων νομικών συστημάτων και αυστηρών μέτρων προστασίας, οι βιομετρικές τεχνολογίες απειλούν την ιδιωτικότητα και την προσωπική ασφάλεια, καθώς η εφαρμογή τους μπορεί να διευρυνθεί ώστε να διευκολύνει τις διακρίσεις, την κατάρτιση προφίλ και τη μαζική παρακολούθηση.[68] Ως έχει, με ένα εργαλείο σαν αυτό της Clearview, το αποτύπωμα προσώπου ενός ατόμου μπορεί να αξιοποιηθεί ώστε να εντοπιστεί το όνομά του και οι λογαριασμοί του στα μέσα κοινωνικής δικτύωσης, και ώστε να συνδυαστούν οι πληροφορίες αυτές με τη φυσική του παρουσία στο δρόμο, τα μαγαζιά που επισκέπτεται και οι φωτογραφίες που αυτό ή οι φίλοι του δημοσιεύουν στο διαδίκτυο – μία μαζική επέκταση των κατά βάση περιορισμένων τρόπων, με τους οποίους χρησιμοποιούνταν μέχρι τώρα η βιομετρία.

---

[64] OPCC (n 4),παρ. 76.
[65] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 Απριλίου 2008).
[66] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γνωμοδότηση 2/2019 https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=&field_year_to=&field_category=All&field_thematic=All&field_protocol_number=&field_keywords=%CE%B1%CF%80%CE%BF%CF%84%CF%85%CF%80%CF%8E%CE%BC%CE%B1%CF%84%CE%B1
[67] OPCC (n 4), παρ. 74.
[68] Privacy International, 'Biometrics'. https://privacyinternational.org/learn/biometrics.

69. Καθώς είναι έμφυτα δύσκολο ή αδύνατο να μεταβληθούν, τα βιομετρικά δεδομένα μπορούν να ταυτοποιήσουν ένα άτομο για ολόκληρη τη ζωή του. Αυτό καθιστά προβληματική τη δημιουργία βάσεων βιομετρικών δεδομένων, καθώς αναμένονται κίνδυνοι στο απώτερο μέλλον – είτε σε περίπτωση αλλαγής πολιτικής κατάστασης ή καθεστώτος, είτε σε περίπτωση μελλοντικής παράβασης δεδομένων, είτε στην περίπτωση της ανάπτυξης τεχνολογίας, μέσω της οποίας η βιομετρία μπορεί να αξιοποιηθεί για νέους σκοπούς και να αποκαλύψει περισσότερες πληροφορίες για τα άτομα από όσες δύναται να αποκαλύψει επί του παρόντος. Ως εκ τούτου, η συλλογή και αποθήκευση βιομετρικών δεδομένων δύναται να υποστεί σοβαρή κατάχρηση.[69]

70. Η Ομάδα Εργασίας του Άρθρου 29 της Οδηγίας 95/46 ήδη αναγνώρισε πριν από κάποια χρόνια τη σημασία της επεξεργασίας βιομετρικών δεδομένων: «Τα βιομετρικά δεδομένα αλλάζουν μη αναστρέψιμα τη σχέση μεταξύ σώματος και ταυτότητας, καθώς αυτά καθιστούν τα χαρακτηριστικά του ανθρώπινου σώματος «αναγνώσιμα από μηχανές» και υποκείμενα σε περαιτέρω χρήση.»[70] Ήδη προέβλεψε τη βλάβη που μπορεί να προκληθεί μέσω της εξαγωγής βιομετρικών χαρακτηριστικών από δημοσίως διαθέσιμες πληροφορίες, και ακριβώς προκατέβαλε τις δραστηριότητες επεξεργασίας της Clearview:

> *Φωτογραφίες στο διαδίκτυο, στα μέσα κοινωνικής δικτύωσης, σε διαδικτυακή οργάνωση φωτογραφιών ή σε εφαρμογές διαμοιρασμού δεν επιτρέπεται να υφίστανται περαιτέρω επεξεργασία ώστε να εξάγονται βιομετρικά πρότυπα ή να εισάγονται σε ένα βιομετρικό σύστημα αναγνώρισης των προσώπων στις φωτογραφίες με τρόπο αυτόματο (αναγνώριση προσώπου) χωρίς συγκεκριμένη νόμιμη βάση (π.χ. συγκατάθεση) για το νέο αυτό σκοπό.*[71]

71. Οι βλάβες που προκαλούνται από την επεξεργασία βιομετρικών δεδομένων είναι ακόμα μεγαλύτερες και ανησυχητικές για τα θεμελιώδη δικαιώματα όταν ληφθούν υπόψη στα πλαίσια της χρήσης που πραγματοποιείται κατά την επιβολή του νόμου. Επί του παρόντος, η Homo Digitalis ισχυρίζεται ότι οι κίνδυνοι είναι υψηλοί αν επιτραπεί σε μία ιδιωτική οντότητα να πραγματοποιεί μαζική και αδιάκριτη επεξεργασία βιομετρικών δεδομένων.

Αποθάρρυνση θεμελιωδών δικαιωμάτων

72. Η Ομάδα Εργασίας του Άρθρου 29 ισχυρίζεται ότι κατά την αξιολόγηση της επίδρασης της επεξεργασίας, «η αποθάρρυνση της προστατευόμενης συμπεριφοράς, όπως η ελευθερία έρευνας ή έκφρασης, η οποία μπορεί να προκληθεί από τη διαρκή παρακολούθηση/εντοπισμό, πρέπει επίσης να μελετηθεί.»[72] Η Homo Digitalis επιθυμεί να επιστήσει την προσοχή στη νομολογία των Γερμανικών δικαστηρίων και αρχών, που έχουν εκτελέσει εκτενείς μελέτες της επίδρασης της βιντεοεπιτήρησης επί των θεμελιωδών δικαιωμάτων στα πλαίσια αξιολογήσεων εννόμων συμφερόντων. Πιο συγκεκριμένα, ο

[69] UN High Commissioner for Human Rights, 'The right to privacy in the digital age' (Doc.A/HRC/39/29) https://undocs.org/A/HRC/39/29.
[70] Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies'. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
[71] Ibid.
[72] Art 29 WP Opinion on Legitimate Interests.

Επίτροπος Προστασίας Δεδομένων του Baden-Württemberg τόνισε τη σημασία του δικαιώματος ελεύθερης ανάπτυξης της προσωπικότητας κατά την αξιολόγηση της έντασης της παρακολούθησης μέσω βιντεοεπιτήρησης:[73] έκρινε ότι εντός εστιατορίων, πάρκων ψυχαγωγίας και γενικά σε μέρη όπου οι άνθρωποι συγκεντρώνονται για να φάνε, να πιούνε, να συζητήσουν και να χαλαρώσουν, το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας θα υπερισχύει των εννόμων συμφερόντων του υπεύθυνου επεξεργασίας. Καθώς το Διαδίκτυο έχει καταστεί ένα μέρος κοινωνικοποίησης αντίστοιχο με τέτοιους δημόσιους χώρους, πρέπει να εφαρμοστεί η ίδια αρχή. Επιπροσθέτως, οι κίνδυνοι της βιντεοεπιτήρησης που εντοπίζονται επιδεινώνονται με την μαζική πραγματική ταυτοποίηση που καθίσταται δυνατή από την τεχνολογία της Clearview.

73. Ο ΕΕΠΔ ρητά θεωρεί ότι η ΚΜΚΔ, η οποία αποτελεί ακριβώς την πρακτική εκείνη που καθιστά δυνατή και είναι σχεδιασμένη να διευκολύνει η τεχνολογία της Clearview, συντελεί σημαντικά στην αποθάρρυνση διάφορων δικαιωμάτων και ελευθεριών:

> *Η παρακολούθηση των χρηστών μέσων κοινωνικής δικτύωσης είναι μία δραστηριότητα επεξεργασίας προσωπικών δεδομένων που δημιουργεί υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων. Ο επανακαθορισμός του σκοπού των δεδομένων πιθανώς θα επηρεάσει τον αυτοκαθορισμό των πληροφοριών ενός ατόμου, θα μειώσει περαιτέρω τον έλεγχο των υποκειμένων των δεδομένων επί των δεδομένων τους... Πράγματι, ο περιορισμός του ιδιωτικού χώρου που είναι διαθέσιμος στους ανθρώπους, ως αποτέλεσμα της αναπόφευκτης παρακολούθησης από εταιρείες και από την κυβέρνηση, αποθαρρύνει τη δυνατότητα και την επιθυμία των ατόμων να εκφράζονται και να σχηματίζουν ελεύθερα σχέσεις, περιλαμβανομένης της αστικής σφαίρας, με τρόπο ιδιαίτερα σημαντικό για την υγεία της δημοκρατίας.*[74]

74. Το Διαδίκτυο και οι πλατφόρμες των μέσων κοινωνικής δικτύωσης παίζουν πλέον ζωτικό ρόλο στην ανάπτυξη της ιδιωτικής κοινωνικής και πολιτικής ζωής των ατόμων, καθώς και της διαδικτυακής τους ταυτότητας. Αποτελούν το ψηφιακό περιβάλλον ζωής των σύγχρονων αστικών τοπίων, όπου οι άνθρωποι αποκτούν πρόσβαση σε πληροφορίες, διαμορφώνουν και συζητούν ιδέες, εγείρουν αντιθετικές απόψεις, επεξεργάζονται πιθανές μεταρρυθμίσεις, εκθέτουν τη μεροληψία και τη διαφθορά και οργανώνονται ώστε να υποστηρίξουν πολιτικές, οικονομικές, κοινωνικές, περιβαλλοντικές και πολιτιστικές αλλαγές.[75]

75. Είναι κρίσιμο για ένα υγιές, αγωνιζόμενο και ανοικτό Διαδίκτυο τα άτομα να νιώθουν ελεύθερα να μοιραστούν προσωπικές πληροφορίες και φωτογραφίες όπως επιθυμούν χωρίς το φόβο ότι οι πληροφορίες αυτές θα υπεξαιρεθούν αμέσως και θα αποθηκευτούν για απροσδιόριστους σκοπούς. Η πληροφορία αυτοπροσδιορισμού όπως ο καθένας θεωρεί αρμόζον στα διάφορα Διαδικτυακά

---

[73] Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen', p. 9.
[74] EDPS (n 39).
[75] Privacy International, 'Protecting civic spaces' https://privacyinternational.org/sites/ default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf.

fora, έχοντας έλεγχο επί της διαβίβασης των διαφορετικών τμημάτων των πληροφοριών στα διάφορα μέρη, αφαιρείται από τον επαπειλούμενο κίνδυνο ότι όλες αυτές οι ξεχωριστές πληροφορίες είναι εντοπίσιμες και ενοποιήσιμες με το πάτημα ενός κουμπιού.

Βλάβες για ευάλωτες κοινότητες

76. Το εργαλείο της Clearview μπορεί επίσης να προκαλέσει ιδιαίτερη βλάβη σε ευάλωτα άτομα. Για την ενότητα αυτή ενημερωθήκαμε σημαντικά από, και θα θέλαμε να επιστήσουμε την προσοχή σε, τις εργασίες της Αμερικανικής Ένωσης Αστικών Ελευθεριών (ΑΕΑΕ) κατά τις αναφορές της ενάντια στην Clearview στην πολιτεία του Ιλινόις σύμφωνα με το ΝΙΒΠ.[76]

77. Οι ευάλωτες ομάδες βρίσκονται σε αυξημένο κίνδυνο αν ταυτοποιούνται όταν βιώνουν τις ζωές τους. Οι επιζώντες σεξουαλικής κακοποίησης ή εμπορικής σεξουαλικής εκμετάλλευσης, για παράδειγμα, ή οι μετανάστες, επανειλημμένως στοχοποιούνται με παρενοχλητικά ή ρατσιστικά κίνητρα από ιδιώτες και αστυνομικούς υπαλλήλους αντιστοίχως. «Στερώντας τα άτομα αυτά από τον έλεγχο επί και την ασφάλεια των ευαίσθητων βιομετρικών ταυτοποιητών τους και απειλώντας ότι μπορεί να καταστεί επουσιωδώς εύκολο να ταυτοποιηθούν και να εντοπιστούν τόσο στο διαδίκτυο όσο και στην πραγματική ζωή, το σύστημα της Clearview τα εκθέτει σε παρενοχλητική παρακολούθηση, παρενόχληση και βία.»[77] Ο φόβος ταυτοποίησης μπορεί επίσης να οδηγήσει αυτά τα άτομα να αποφεύγουν ορισμένα μέρη και συναντήσεις για να λάβουν τις υποστηρικτικές υπηρεσίες που χρειάζονται.

78. Επιπροσθέτως, ο κατακερματισμός διανυσμάτων που πραγματοποιείται όταν η Clearview εξάγει βιομετρικά χαρακτηριστικά από εικόνες προσώπου πιθανώς επιτρέπει την κατηγοριοποίηση των προσώπων των ατόμων με βάση βαθμούς ομοιότητας. Αυτό εγείρει την πιθανότητα οι πελάτες της Clearview να πραγματοποιούν αυτοματοποιημένες ομαδοποιήσεις ατόμων επί τη βάση της εθνικότητας, του δέρματός τους ή άλλης κατηγοριοποίησης – και ανοίγει την πόρτα σε διακριτικό εντοπισμό και παρακολούθηση, ή σε πρακτικές όπως η αστυνόμευση με βάση την πρόβλεψη.

79. Έχοντας εκθέσει τους πολλαπλούς και σοβαρούς κινδύνους και βλάβες που προκαλούνται από τις δραστηριότητες της Clearview για τα δικαιώματα και τις ελευθερίες των ατόμων, η Homo Digitalis ισχυρίζεται ότι η αξιολόγηση της στάθμισης των εννόμων συμφερόντων πρέπει να καταλήξει πως δεν υπάρχει έγκυρη νόμιμη βάση στα πλαίσια του Άρθρου 6(1)(στ) του GDPR. Η έλλειψη νόμιμης βάσης στα πλαίσια του Άρθρου 6 του GDPR αρκεί για να κριθεί παράνομη η επεξεργασία, ωστόσο σε περίπτωση που η ΑΠΔΠΧ διαφωνούσε, η επόμενη ενότητα αξιολογεί το αν εφαρμόζεται κάποια νόμιμη βάση για την επεξεργασία ειδικών κατηγοριών δεδομένων.

<u>Έχουν προδήλως δημοσιοποιηθεί – Άρθρο 9(2)(ε) GDPR</u>

[76] Complaint, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353. https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.
[77] Plaintiff's response to defendant's motion to dismiss, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353.

80. Καθώς η Clearview επεξεργάζεται ειδικές κατηγορίες δεδομένων, πέραν μίας νόμιμης βάσης στα πλαίσια του Άρθρου 6 (η οποία απουσιάζει, όπως αποδείχθηκε στην προηγούμενη ενότητα), πρέπει επίσης να ικανοποιεί τουλάχιστον μία από τις προϋποθέσεις του Άρθρου 9(2). Η μόνη σχετική προϋπόθεση στην περίπτωση της Clearview είναι «η επεξεργασία [να] αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων», σύμφωνα με το Άρθρο 9(2)(ε) του GDPR. Η Homo Digitalis σημειώνει ότι ακόμα και αν εφαρμοζόταν η προϋπόθεση αυτή, θα εφαρμοζόταν μόνο στις εικόνες προσώπου (οι οποίες αποτελούν βιομετρικά δεδομένα, βλέπε ενότητα V.A ανωτέρω) που η Clearview συλλέγει διαδικτυακά – τα βιομετρικά δεδομένα που η Clearview δημιουργεί μέσω της εξαγωγής διανυσμάτων δεν είναι δυνατόν να πληρούν αυτή την προϋπόθεση.

81. Το γεγονός ότι οι πληροφορίες είναι διαδικτυακά διαθέσιμες δεν αποτελεί αυτόματη νόμιμη βάση επεξεργασίας σύμφωνα με το Άρθρο 9. Όπως επίσημα αναγνωρίζεται από κάποια (έστω και περιορισμένη) καθοδήγηση από αρχές προστασίας δεδομένων και το σχετικό ακαδημαϊκό σχολιασμό,[78] η εξαίρεση σύμφωνα με το Άρθρο 9(2)(ε) πρέπει να ερμηνεύεται στενά. Ιδιαιτέρως, οι όροι «προδήλως» και «από το υποκείμενο των δεδομένων» εφαρμόζονται σε πολύ ιδιαίτερες περιπτώσεις δημοσιοποίησης προσωπικών δεδομένων.

82. Κατά πρώτον, η ιδιωτικότητα των δημοσίως διαθέσιμων πληροφοριών πρέπει να εξακολουθεί να προστατεύεται σε σημαντικό βαθμό. Αυτό είναι κρίσιμο για ένα υγιές και ανοιχτό Διαδίκτυο όπου τα άτομα μπορούν να ασκήσουν τα θεμελιώδη δικαιώματα και τις ελευθερίες τους. Το εργαλείο αναγνώρισης προσώπου της Clearview είναι το αρχέτυπο μίας φαινομενικά αθώας νέας τεχνολογίας που, αν επιτραπεί να χρησιμοποιηθεί και να αξιοποιηθεί σε μεγάλο βαθμό, θα μπορούσε να αλλάξει θεμελιωδώς το Διαδίκτυο όπως το γνωρίζουμε και τη διαδικτυακή συμπεριφορά των ατόμων. Λειτουργεί με την εσφαλμένη υπόθεση πως ό,τι είναι δημοσίως διαθέσιμο στο Διαδίκτυο αυτομάτως ανήκει σε ολόκληρη τη δημόσια σφαίρα και έχει προσφερθεί γενναιόδωρα σε ολόκληρο τον κόσμο, ώστε να το δει αμέσως και να το επαναχρησιμοποιήσει κατά βούληση. Ωστόσο, μία αυστηρή διάκριση μεταξύ της δημόσιας και της ιδιωτικής σφαίρας έχει μικρή σχέση με τις σύγχρονες κοινωνίες, όπου μεγάλα τμήματα των οικονομικών, κοινωνικών και δημοκρατικών ζωών μας διάγονται διαδικτυακά. Η θεώρηση του Διαδικτύου ως ένα ομογενοποιημένο, πλήρως δημόσιο και απόλυτα προσβάσιμο φόρουμ, στο οποίο ο καθένας συναινεί οι προσωπικές του πληροφορίες να μπορούν να αρπαχθούν από τον καθέναν με το που εντάσσονται σε ένα δημόσιο τμήμα του Διαδικτύου, αποτελεί παρανόηση.

83. Οι κίνδυνοι της αυστηρής αυτής διάκρισης είναι επίσης ιδιαίτερα αληθινοί στο μη διαδικτυακό κόσμο, όπως κρίθηκε στο παρελθόν από το ΕΔΔΑ. Όπως έκρινε το Δικαστήριο στην υπόθεση *Peck κατά UK*[79], η αποκάλυψη στα μέσα με σκοπό δημοσιοποίησης ενός υλικού βιντεοσκόπησης ενός υποψηφίου, του οποίου η απόπειρα αυτοκτονία καταγράφηκε σε κλειστό σύστημα τηλεόρασης,

[78] Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2. https://doi.org/10.1093/idpl/ipab005.
[79] App no 44647/98 (ECtHR, 28 Ιανουάριος 2003), παρα. 53, 61-62.

αποτελούσε σοβαρή ανάμιξη με την ιδιωτική ζωή του υποψηφίου, παρά το γεγονός ότι βρισκόταν σε δημόσιο χώρο κατά το χρόνο αυτό. Στην υπόθεση αυτή, η κρίση του ΕΔΔΑ περιορίστηκε στην υπόθεση ότι κανένα άτομο δεν μπορεί να αναμένει ευλόγως ότι βιντεοσκοπικό υλικό που απεικονίζει ευαίσθητα τμήματα της ιδιωτικής του ζωής μπορεί να κυκλοφορήσει αργότερα στα μέσα, ακόμα και αν οι πράξεις του ήταν «ήδη στο δημόσιο τομέα».[80]

84. Κατά δεύτερον, είναι κοινή γνώση για όλους όσους είναι έστω και λίγο εξοικειωμένοι με τη χρήση του Διαδικτύου και των μέσων κοινωνικής δικτύωσης, ότι πολλές διαδικτυακές φωτογραφίες ατόμων δεν θα δημοσιοποιούνταν *από* τα ίδια τα *υποκείμενα των δεδομένων*. Τα μέσα κοινωνικής δικτύωσης επιτρέπουν σε ένα χρήστη να αναρτά φωτογραφίες του ιδίου, καθώς και οποιουδήποτε άλλου ατόμου. Αυτά τα άλλα άτομα (που ενδέχεται να είναι φίλοι του αναρτώντος ή άγνωστοι περαστικοί σε δημόσιους χώρους) ενδέχεται να μην αναρτούσαν τα ίδια τις εικόνες προσώπου τους διαδικτυακά, ενώ μπορεί να μη γνωρίζουν καν ότι φωτογραφίες που περιλαμβάνουν τα πρόσωπά τους έχουν αναρτηθεί και είναι παρούσες στο δημόσιο Διαδίκτυο.

85. Το ΓΕΙΚ κατέληξε στο ίδιο συμπέρασμα κατά την αξιολόγηση του αν τα προσωπικά δεδομένα που συλλέγει η Clearview εμπίπτουν συνολικά εντός της Καναδικής εξαίρεσης «δημοσιοποίησης», η οποία εφαρμόζεται μόνο «όταν το άτομο προσέφερε τις πληροφορίες» ή όταν «είναι εύλογο να θεωρηθεί ότι το άτομο που αφορούν οι πληροφορίες προσέφερε τις πληροφορίες»: «Καθώς η Clearview πραγματοποιεί μαζική συλλογή εικόνων μέσω αυτοματοποιημένων εργαλείων, είναι αναπόφευκτο σε πολλές περιπτώσεις να έχουν αναρτηθεί οι εικόνες από ένα τρίτο μέρος.»[81]

86. Κατά τρίτον, όπως εξηγήθηκε στην ενότητα ΙΙΙ, άπαξ και συλλεχθούν, οι φωτογραφίες διατηρούνται στη βάση δεδομένων της Clearview επ' αόριστον, ασχέτως του αν οι φωτογραφίες αυτές εξακολουθούν να είναι δημοσίως διαθέσιμες ανά πάσα στιγμή. Όπως ορθά παρατηρήθηκε σε ένα άρθρο των New York Times σχετικά με την Clearview, «αν το προφίλ σας συλλέχθηκε ήδη, είναι πλέον αργά. Η εταιρεία διατηρεί όλες τις εικόνες που συνέλεξε, ακόμα και αν αργότερα διαγραφούν ή κατέβουν».[82] Σημειώνει στη συνέχεια, «αν και ο κος. Ton-That δήλωσε ότι η εταιρεία εργάζεται στη δημιουργία ενός εργαλείου που θα επιτρέπει στα άτομα να ζητήσουν την αφαίρεση των εικόνων τους, αν αυτές αφαιρέθηκαν από την ιστοσελίδα πηγής.» Ως προς αυτή την τελευταία «δικαιολογία», εν πρώτοις είναι απαράδεκτο ότι η Clearview εφάρμοσε την τεχνολογία της χωρίς να υπάρχει ήδη αυτό το εργαλείο, και κατά δεύτερον, ένα τέτοιο εργαλείο θα μπορούσε σε κάθε περίπτωση μόνο να προσφέρει εξαιρετικά περιορισμένη διέξοδο για τα άτομα – θα υπονοούσε ότι τα άτομα (1) γνωρίζουν κατ' αρχάς ότι η Clearview συλλέγει τις εικόνες προσώπου τους, (2) υποβάλλουν συστηματικά αιτήματα πρόσβασης, ώστε να πληροφορηθούν ποιες εικόνες συλλέχθηκαν από την Clearview, (3) ελέγχουν τα αποτελέσματα αυτών των αιτημάτων με όσα δημοσιοποιούν στο διαδίκτυο, και (4) υποβάλλουν ατομικά αιτήματα διαγραφής. Αυτό είναι πλήρως παράλογο και αποτελεί ωμή προσβολή του δικαιώματος των ατόμων να ελέγχουν τις διαδικτυακές ταυτότητές τους,

[80] Ibid.
[81] OPCC (n 4), παρ. 66.
[82] Hill (v 5).

εμποδίζοντας κάθε αποτελεσματικό έλεγχο των δικαιωμάτων των υποκειμένων των δεδομένων που προβλέπονται από τον GDPR.

87. Τέλος, οι ρυθμίσεις ιδιωτικότητας ως γνωστόν δύσκολα ρυθμίζονται και προσαρμόζονται σωστά ώστε οι πληροφορίες που κάποιος επιθυμεί να παραμείνουν εντός ιδιωτικών διαδικτυακών κύκλων να βρίσκονται πράγματι και να παραμένουν εκεί. Έρευνα της Privacy International επανειλημμένα έχει δείξει πόσο περίπλοκο είναι για τα άτομα να προσαρμόσουν τις ρυθμίσεις τους ώστε να είναι φιλικές προς την ιδιωτικότητα, με αποτέλεσμα οι νόμιμες προϋποθέσεις της συγκατάθεσης συχνά να μην πληρούνται.[83] «Σκοτεινά μοτίβα», όπως αποκαλούνται από το Νορβηγικό Συμβούλιο Καταναλωτή, σημαίνουν πως τα υποκείμενα των δεδομένων δεν έχουν πάντα έλεγχο της διαδικτυακής προσωπικής τους ζωής.[84]

88. Συνεπώς, η Homo Digitalis ισχυρίζεται ότι η Clearview δεν πληροί καμία προϋπόθεση της επεξεργασίας ειδικών κατηγοριών δεδομένων σύμφωνα με το Άρθρο 9(2)(ε) GDPR.

C. Περιορισμός του Σκοπού

89. Μία άλλη θεμελιώδης αρχή της προστασίας δεδομένων που παραβιάζεται απροκάλυπτα από την εκ μέρους της Clearview επεξεργασία είναι αυτή του περιορισμού του σκοπού, σύμφωνα με το Άρθρο 5(1)(β) του GDPR. Η εφαρμογή της αρχής αυτής πρέπει να λαμβάνει υπόψη τους παράγοντες που παρατίθενται στο Άρθρο 6(4), οι οποίοι στην περίπτωση αυτή σαφώς ενδεικνύουν ότι η επεξεργασία της Clearview δεν είναι συμβατή με το σκοπό, για τον οποίον αρχικά αποκαλύφθηκαν τα προσωπικά δεδομένα.

90. Το ζήτημα του περιορισμού του σκοπού εγγενώς συνδέεται με το τι μπορεί κάποιος να αναμένει ότι θα συμβεί με τα δημοσίως διαθέσιμα προσωπικά του δεδομένα, όπως αναπτύχθηκε στις παραγράφους 44 με 54 παραπάνω. Η Homo Digitalis απέδειξε ότι η επανάχρηση για σκοπούς επεξεργασίας στα πλαίσια βιομετρικής βάσης δεδομένων σαφέστατα δεν εμπίπτει εντός τέτοιων προσδοκιών. Όπως δήλωσε το ΕΣΠΔ, χρήσεις των προσωπικών δεδομένων στα πλαίσια της παρακολούθησης μέσων κοινωνικής δικτύωσης «συχνά καταλήγουν στο να χρησιμοποιούνται τα προσωπικά δεδομένα πέραν του αρχικού τους σκοπού, του αρχικού τους πλαισίου και με τρόπους που το άτομο δεν μπορεί ευλόγως να αναμένει.»[85]

91. Η ακόλουθη δήλωση της γνωμοδότησης της Ομάδας του Άρθρου 29 για τη βιομετρία είναι επίσης διαφωτιστική:

---

[83] Privacy International, 'Most cookie banners are annoying and deceptive. This is not consent. https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. και Privacy International, 'Facebook - Profile Settings' https://privacyinternational.org/guide-step/3959/facebook-profile-settings.

[84] Norwegian Consumer Council, 'Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy' https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[85] EDPS.

Φωτογραφίες στο διαδίκτυο, στα μέσα κοινωνικής δικτύωσης, σε διαδικτυακή οργάνωση φωτογραφιών ή σε εφαρμογές διαμοιρασμού δεν επιτρέπεται να υφίστανται περαιτέρω επεξεργασία ώστε να εξάγονται βιομετρικά πρότυπα ή να εισάγονται σε ένα βιομετρικό σύστημα αναγνώρισης των προσώπων στις φωτογραφίες με τρόπο αυτόματο (αναγνώριση προσώπου) χωρίς συγκεκριμένη νόμιμη βάση (π.χ. συγκατάθεση) για το νέο αυτό σκοπό. Αν δεν υπάρχει νόμιμη βάση για αυτόν τον δευτερεύοντα σκοπό, η επεξεργασία πρέπει επίσης να είναι επαρκής, σχετική και όχι υπερβολική σε σχέση με το σκοπό αυτό. Αν ένα υποκείμενο των δεδομένων έχει συγκατατεθεί στην επεξεργασία φωτογραφιών, στις οποίες εμφανίζεται, ώστε να προστίθεται αυτόματα ετικέτα του σε ένα διαδικτυακό φωτογραφικό άλμπουμ μέσω ενός αλγορίθμου αναγνώρισης προσώπου, αυτή η επεξεργασία πρέπει να επιτυγχάνεται με τρόπο φιλικό προς την προστασία δεδομένων: τα βιομετρικά δεδομένα δεν είναι πλέον αναγκαία μετά την προσθήκη ετικέτας στις φωτογραφίες και το όνομα, το ψευδώνυμο ή άλλο κείμενο που καθορίζεται από το υποκείμενο των δεδομένων πρέπει να διαγράφεται. Η δημιουργία μίας μόνιμης βιομετρικής βάσης δεδομένων είναι εκ των προτέρων μη αναγκαία για το σκοπό αυτό.[86]

92. Λαμβάνοντας υπόψη αυτή τη δήλωση, η εκ μέρους της Clearview επεξεργασία συνιστά έναν εντελώς νέο σκοπό σε σχέση με την αρχική δημοσιοποίηση, για τον οποίο οφείλει να έχει μία διακριτή, έγκυρη νόμιμη βάση. Όπως αναπτύχθηκε στην ενότητα V.0 ανωτέρω, κάτι τέτοιο δεν υπάρχει, και επομένως η Clearview παραβιάζει την αρχή περιορισμού του σκοπού.

93. Η Homo Digitalis συμπεραίνει ότι οι πρακτικές της Clearview αποτελούν παραβάσεις των αρχών της διαφάνειας, της αντικειμενικότητας και του περιορισμού του σκοπού, καθώς και της απαίτησης ύπαρξης νόμιμης βάσης. Η Homo Digitalis δεν θα αξιολογήσει τη συμμόρφωση με τον GDPR της χρήσης του εργαλείου της Clearview εκ μέρους των πελατών της πέραν των αρχών επιβολής του νόμου, καθώς αυτοί είναι οι μόνοι πελάτες στους οποίους η Clearview διαφημίζεται ανοιχτά. Ωστόσο, θα θέλαμε να επιστήσουμε την προσοχή της ΑΠΔΠΧ σε δημοσιευμένες προβλέψεις από «αστυνομικούς υπαλλήλους και επενδυτές της Clearview» ότι το εργαλείο «θα καταστεί τελικά διαθέσιμο στο κοινό».[87]

VI. Νομικό Πλαίσιο και Προβληματισμοί: Επεξεργασία από τις Αρχές Επιβολής του Νόμου (Οδηγία 2016/680 όπως μεταφέρθηκε στην ελληνική έννομη τάκη με τις διατάξεις του ν.4624/2019)

94. Οι αποκλίσεις από τα θεμελιώδη ατομικά δικαιώματα πρέπει να πραγματοποιούνται μέσω νομοθετικών μέτρων σε ζητήματα τέτοιας σημασίας όπως η κρατική ασφάλεια, η άμυνα, η πρόληψη, η έρευνα, ο εντοπισμός ή η δίωξη εγκλημάτων, κτλ. Αν και τέτοιες περιορισμένες αποκλίσεις μπορεί να εφαρμόζονται σε επεξεργασία εκ μέρους αρχών επιβολής του νόμου, μέσω του ν.4624/2019, δεν είναι δυνατό με κανένα τρόπο να εφαρμόζονται σε μία ιδιωτική οντότητα που συλλέγει αδιακρίτως προσωπικά δεδομένα, με τον πιθανό τελικό σκοπό να πωλεί τη χρήση της βάσης δεδομένων αυτής σε αυστηρά

[86] Art 29 WP σελ.7.
[87] Hill (v 5).

ρυθμιζόμενες αρχές. Όπως επανειλημμένα παρατηρήθηκε από την έρευνα της Privacy International,[88] η χρήση ιδιωτικών εργαλείων για την εφαρμογή του νόμου συχνά οδηγεί στην παράκαμψη των απαιτητικών μέτρων προστασίας των θεμελιωδών δικαιωμάτων που επιβάλλονται στις δημόσιες αρχές.

95. Αν και η Homo Digitalis θεωρεί πως οι παραβάσεις του GDPR που αναπτύχθηκαν στην ενότητα V επαρκούν για να εκδοθεί διαταγή κατά της συλλογής προσωπικών δεδομένων υποκειμένων των δεδομένων που βρίσκονται στο UK από την Clearview, οι παραβάσεις αυτές καθίστανται έτι σαφέστερες όταν ληφθούν υπόψη σε συνδυασμό με την τελική επιδιωκόμενη χρήση των προσωπικών δεδομένων που συλλέγει και επεξεργάζεται η Clearview. Σε περίπτωση που Η ΑΠΔΠΧ επιτρέψει τις πρακτικές συλλογής της Clearview στην Ελλάδα, η Homo Digitalis ισχυρίζεται ότι πρέπει να απαγορευτεί η χρήση των προσωπικών δεδομένων που συλλέγονται από αρχές επιβολής του νόμου, ώστε να περιοριστεί η βλάβη που προκαλείται στα υποκείμενα των δεδομένων. Κάτι τέτοιο γεννά σοβαρούς προβληματισμούς και παραβιάζει τον ν.4624/2019.

96. Αυτή η ενότητα της αίτησης κατά πρώτον εκθέτει τους προβληματισμούς της Homo Digitalis ως προς τη χρήση τεχνολογίας αναγνώρισης προσώπου και ΚΜΚΔ από τις αρχές επιβολής του νόμου, προβληματισμούς που επιδεινώνονται όταν αυτές οι τεχνολογίες χρησιμοποιούνται συνδυαστικά, όπως συμβαίνει στην περίπτωση της. Στη συνέχεια, πραγματοποιείται ανάλυση του πώς τέτοιοι προβληματισμοί μεταφράζονται σε διάφορες παραβάσεις της DPA 2018, ιδίως δε της πρώτης αρχής προστασίας δεδομένων (αρ.35) και της απαίτησής της για νομιμότητα.

Α. Προβληματισμοί ως προς τη χρήση τεχνολογίας αναγνώρισης προσώπου και ΚΜΚΔ από την αστυνομία

97. Η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία έχει θεμελιώδη επίδραση στον τρόπο που η κοινωνία μας παρακολουθείται και αστυνομεύεται. Η εισαγωγή τέτοιας διεισδυτικής τεχνολογίας δεν δημιουργεί μόνο σημαντικές ερωτήσεις ως προς την ιδιωτικότητα και την προστασία των δεδομένων, αλλά επίσης και ηθικά ερωτήματα ως προς το αν οι σύγχρονες δημοκρατίες θα επέτρεπαν ποτέ τη χρήση της. Με το εργαλείο της Clearview, η αστυνομία μπορεί να αναγνωρίσει αποτελεσματικά κάθε ένα άτομο που καταγράφεται σε κάμερα (ή τουλάχιστον να συνδυάσει τη φυσική του ταυτότητα με τη διαδικτυακή του παρουσία). Μία αστυνομική δύναμη θα μπορούσε πολύ ρεαλιστικά να αποφασίσει να ταυτοποιεί κάθε ένα άτομο ενός πλήθους διαδηλωτών και να δημιουργήσει προφίλ γι' αυτά από πληροφορίες που αλιεύονται από το διαδίκτυο. Αυτή είναι μία εντελώς δυστοπική προοπτική που αποκτά πολύ ρεαλιστικές πιθανότητες με το εργαλείο της Clearview.

98. Η τεχνολογία αναγνώρισης προσώπου, όπως αναπτύσσεται στους δημόσιους χώρους για το σκοπό αστυνόμευσης, δεν παρεμβαίνει μόνο στην ιδιωτικότητα και στα δικαιώματα προστασίας δεδομένων των ατόμων, αλλά επίσης μπορεί να

[88] See for example: Privacy International, 'Public-Private surveillance partnerships'. Available at https://privacyinternational.org/campaigns/unmasking-policing-inc; Privacy International, 'One Ring to watch them all' (25 June 2020). Available at https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.

επηρεάσει σημαντικά την άσκηση των δικαιωμάτων της ελευθερίας της σκέψης, της συνείδησης και της θρησκείας, της ελευθερίας της έκφρασης και της ελευθερίας του συνέρχεσθαι και συνεταιρίζεσθαι. Το ΕΣΠΔ έχει τονίσει ότι η χρήση τεχνολογίας αναγνώρισης προσώπου «είναι ουσιαστικά ένα ηθικό ζήτημα για μία δημοκρατική κοινωνία» καθώς μπορεί «προφανώς να παρακωλύσει την ατομική ελευθερία έκφρασης και την ελευθερία του συνέρχεσθαι».[89]

99. Στην αναφορά της επί του Άρθρου 21 του Διεθνούς Συμφώνου Ατομικών και Πολιτικών Δικαιωμάτων προς την Επιτροπή Ανθρωπίνων Δικαιωμάτων του ΟΗΕ, η Privacy International τόνισε πώς οι νέες τεχνολογίες παρακολούθησης μπορούν να επηρεάσουν την άσκηση του δικαιώματος ειρηνικής διαδήλωσης, έχοντας *«ως αποτέλεσμα την παρακώλυση των ατόμων»*.[90] Λόγω του αποτελέσματος αυτού, είναι εξαιρετικά δύσκολο έως αδύνατο για τις αρχές που επιθυμούν να κάνουν χρήση αυτής της τεχνολογίας να αξιολογήσουν επαρκώς τα αρνητικά αποτελέσματα επί της άσκησης των ανωτέρω δικαιωμάτων, και κατά συνέπεια να αιτιολογήσουν τη χρήση του.[91]

100. Η Homo Digitalis έχει ήδη με αναφορά της ενημερώσει την ΑΠΔΠΧ για τις σχετικές προκλήσεις που ανακύπτουν από τη σύμβαση έξυπνης αστυνόμευσης που έχει υπογράψει η ΕΛ.ΑΣ. και με βάση την οποία η τελευταία θα προμηθευτεί εντός των επόμενων μηνών συσκευές που θα χρησιμοποιούν λογισμικό αναγνώρισης προσώπου, ενώ αναμένει με ιδιαίτερο ενδιαφέρον την απόφαση της ΑΠΔΠ επί του ζητήματος αυτού.[92]

101. Η παρακολούθηση των μέσων κοινωνικής δικτύωσης παρουσιάζει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα των ατόμων. Νομοθέτες και όργανα του ΟΗΕ έχουν τονίσει την ανάγκη να τηρούνται αυστηρά μέτρα προστασίας για τέτοιες πρακτικές. Στη νομολογία του, το ΕΔΔΑ έχει τονίσει ότι «το εφαρμοστέο δίκαιο πρέπει να προβλέπει κατάλληλα μέτρα προστασίας για να αποτρέπει κάθε τέτοια χρήση προσωπικών δεδομένων που μπορεί να είναι ασύμβατη με τις εγγυήσεις του Άρθρου 8 της Διεθνούς Σύμβασης».[93] Τέτοια μέτρα προστασίας πρέπει να εφαρμόζονται επί όλων των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων που πραγματοποιούνται από δημόσιες αρχές, περιλαμβανομένης της συλλογής, διατήρησης ή αποθήκευσής τους, της ανάλυσης, της διαβίβασης ή της αποκάλυψης, ή κάθε άλλου τρόπου επεξεργασίας. Όπως τόνισε το Δικαστήριο στην υπόθεση *Marper*:

> *Η ανάγκη τέτοιων μέτρων προστασίας καθίσταται ακόμα μεγαλύτερη στην περίπτωση της προστασίας προσωπικών δεδομένων που υφίστανται αυτοματοποιημένη επεξεργασία, ιδίως όταν τέτοια δεδομένα χρησιμοποιούνται για σκοπούς αστυνόμευσης. Το εφαρμοστέο δίκαιο πρέπει ιδιαιτέρως να φροντίζει ότι τα δεδομένα αυτά είναι σχετικά και όχι υπέρμετρα*

[89] EDPS, 'Facial Recognition: A solution in search of a problem?' https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en
[90] Privacy International, 'Submission on Article 21 of the International Covenant on Civil and Political Rights' (https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf.
[91] Privacy International, 'Protecting Civic Spaces' https://privacyinternational.org/long-read/2852/protecting-civic-spaces.
[92] Homo Digitalis, Η ΑΠΔΠΧ ερευνά την ΕΛ.ΑΣ. μετά από αίτημα της Homo Digitalis, https://www.homodigitalis.gr/posts/7290
[93] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 Απριλίου 2008), παρ 103.

σε σχέση με τους σκοπούς για τους οποίους αποθηκεύονται, και πως αυτά διατηρούνται σε μία μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων για όχι μεγαλύτερο χρονικό διάστημα από αυτό που απαιτείται για το σκοπό που αποθηκεύτηκαν τα δεδομένα αυτά […]. Το εφαρμοστέο δίκαιο πρέπει επίσης να προβλέπει επαρκείς εγγυήσεις ότι τα τηρούμενα προσωπικά δεδομένα προστατεύονται αποτελεσματικά από την κακή χρήση και την κατάχρηση […]. Οι ανωτέρω σκέψεις είναι ιδίως κρίσιμες σε σχέση με την προστασία ειδικών κατηγοριών ή πιο ευαίσθητων δεδομένων.[94]

102. Σε γενικές γραμμές, η μαζική παρακολούθηση ενδέχεται να παρέμβει στο δικαίωμα των ατόμων να εκφράζονται ανώνυμα, να διαμορφώνουν και να μοιράζονται τις σκέψεις τους, να συμμετέχουν σε αμφιλεγόμενες συζητήσεις, να παρίστανται σε δημόσιες συναθροίσεις και να προσφεύγουν εναντίον της κυβέρνησης. Μακροπρόθεσμα, αυτή μπορεί να οδηγήσει σε αυτολογοκρισία: τα άτομα ενδέχεται να αποφεύγουν να επισκέπτονται συγκεκριμένα προφίλ μέσων κοινωνικής δικτύωσης, να πατούν like, να μοιράζονται, να κάνουν re-tweet σε αμφιλεγόμενες δημοσιεύσεις, να συμμετέχουν σε συγκεκριμένες ομάδες συζήτησης ή ακόμα και να χρησιμοποιούν συγκεκριμένες λέξεις. Τελικά, αυτή η αυτολογοκρισία ενδέχεται να αλλάξει τον τρόπο με τον οποίο τα άτομα αναζητούν νέες πληροφορίες, αναπτύσσουν και συζητούν ιδέες, και οργανώνονται γύρω από αυτές.[95]

103. Επιπροσθέτως, η συχνή συλλογή και επεξεργασία δημοσίως διαθέσιμων πληροφοριών και σκοπούς συλλογής στοιχείων ενδέχεται να οδηγήσει σε τέτοιες καταχρήσεις που παρατηρούμε σε άλλα είδη μυστικής παρακολούθησης ή άλλες αστυνομικές πρακτικές. Κάτι τέτοιο μπορεί να περιλαμβάνει συστηματική στοχοποίηση συγκεκριμένων εθνοτικών και θρησκευτικών ομάδων από αρχές επιβολής του νόμου. Είναι αδύνατο να υπάρξουν εγγυήσεις ότι δεν υφίσταται ρατσιστική ή θρησκευτική προκατάληψη στη διαδικτυακή παρακολούθηση, αν δεν υπάρχει ενημέρωση, διαφάνεια και επίβλεψη. Και όπως οι αρχές επιβολής του νόμου είναι συχνά μυστικοπαθείς σχετικά με τη χρήση των μέσων κοινωνικής δικτύωσης και τις πηγές των πληροφοριών τους, μπορεί να γίνει ιδιαίτερα δύσκολο για τα άτομα να αμφισβητήσουν την πιθανή παράβαση του νόμου λόγω της χρήσης τέτοιων δεδομένων.[96]

104. Κάθε δραστηριότητα επεξεργασίας που εκτελείται από τις αρχές επί προσωπικών δεδομένων ατόμων που δημοσιοποιούνται σε μέσα κοινωνικής δικτύωσης για σκοπούς που υπερβαίνουν αυτά που ευλόγως μπορούν να αναμένουν ή να προβλέψουν τα άτομα θα πρέπει να θεωρείται ως σοβαρή επέμβαση στο δικαίωμα στο σεβασμό της ιδιωτικής ζωής, ιδίως όταν τέτοια επεξεργασία περιλαμβάνει τη χρήση τεχνολογίας αναγνώρισης προσώπου για να συνδεθούν και να συνδυαστούν οι πηγές των πληροφοριών. Διαφορετικά, θα απαρνούνταν κανείς την αναγκαία προστασία που προβλέπει το ΕΔΔΑ για την ιδιωτική ζωή των ατόμων στο διαδικτυακό περιβάλλον, ένα πεδίο «όπου η

[94] Ibid.
[95] Privacy International, 'Protecting Civic Spaces'.
[96] Privacy International, 'Is your Local Authority looking at your Facebook likes?' https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf.

κατάχρηση είναι δυνητικά τόσο εύκολη σε ατομικές περιπτώσεις και μπορεί να έχει τόσο βλαπτικές συνέπειες για την κοινωνία εν συνόλω».[97]

Β. Παράβαση της Πρώτης Αρχής Προστασίας Δεδομένων: Νομιμότητα

105. Σύμφωνα με το αρ. 45 του ν.4624/2019, τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε σύννομη και δίκαιη επεξεργασία, ενώ όπως ορίζει το άρ. 46. η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν είναι απολύτως αναγκαία για την ενάσκηση των καθηκόντων του υπεύθυνου επεξεργασίας.

106. Αυτό το τμήμα της αναφοράς θα εκθέσει στη συνέχεια γιατί η χρήση του εργαλείου της Clearview από τις αρχές επιβολής του νόμου δεν μπορεί να πληροί τις προϋποθέσεις των άρθρων 45 και 46.

Δε βασίζεται στο νόμο

107. Δεν υπάρχει στην Ελληνική Έννομη τάξη διάταξη νόμου με την οποία να ορίζεται η χρήση τέτοιου είδους παρεμβατικών πρακτικών από την Ελληνική Αστυνομία στο πλαίσιο της άσκησης των καθηκόντων της.

Δεν είναι αναγκαία εν στενή εννοία

108. Η έννοια της αναγκαιότητας απαιτεί η αστυνομία να αποδεικνύει την ύπαρξη μίας συγκεκριμένης, σαφούς και άμεσης απειλής της εθνικής ή της δημόσιας ασφάλειας που θα δικαιολογούσε την ανάγκη χρήσης τέτοιου είδους τεχνολογίας. Το ΕΔΔΑ εφάρμοσε μία αξιολόγηση της εν στενή εννοία αναγκαιότητας σχετικά με επεμβάσεις στο δικαίωμα της ιδιωτικότητας στα πλαίσια της παρακολούθησης. Στην υπόθεση *Szabó και Vissy κατά Ουγγαρίας*, το ΕΔΔΑ υπέδειξε ότι δοθείσης της «δυνατότητας της προηγμένης τεχνολογίας να εισβάλλει στην ιδιωτικότητα των πολιτών»,

> *[ένα] μέτρο μυστικής παρακολούθησης μπορεί να κριθεί ως σύμφωνο με τη Σύμβαση μόνο αν είναι εν στενή εννοία αναγκαίο, ως γενικό ζητούμενο για την προστασία [των] δημοκρατικών θεσμών και, επιπλέον, εάν είναι εν στενή εννοία αναγκαίο, ως ειδικό ζητούμενο για την κτήση της ζωτικής πληροφόρησης στα πλαίσια μία ατομικής έρευνας. Σύμφωνα με την κρίση του Δικαστηρίου, κάθε μέτρο μυστικής παρακολούθησης που δεν ανταποκρίνεται στα κριτήρια αυτά θα είναι ευάλωτο σε καταχρήσεις εκ μέρους των αρχών, οι οποίες διαθέτουν εξαιρετικές τεχνολογίες. Το Δικαστήριο σημειώνει ότι τόσο το Δικαστήριο της Ευρωπαϊκής Ένωσης όσο και ο Ειδικός Ανταποκριτής των Ηνωμένων Εθνών απαιτούν τα μέτρα μυστικής παρακολούθησης να ανταποκρίνονται σε ειδικές ανάγκες – μία προσέγγιση που θεωρεί σημαντικό να υποστηρίξει.*[98]

109. Ο ICO θεωρεί ότι η εν στενή εννοία αναγκαιότητα στα πλαίσια ευαίσθητης επεξεργασίας προσωπικών δεδομένων μέσω ζωντανής αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου απαιτεί ο υπεύθυνος

[97] *Klass v. Germany*, App no 5029/71 (ECtHR, 6 Σεπτέμβριος 1978), παρ. 56.
[98] App no 37138/14 (ECtHR, 13 October 2015), para 73.

επεξεργασίας «να εκτιμά την αναλογικότητα της ευαίσθητης επεξεργασίας και της διαθεσιμότητας βιώσιμων εναλλακτικών της ζωντανής αναγνώρισης προσώπου».[99] Η Homo Digitalis θεωρεί πως το εργαλείο της Clearview δεν θα μπορούσε ποτέ να κριθεί ως εν στενή εννοία αναγκαίο, καθώς η χρήση του αποτελεί ενέργεια με μικρές πιθανότητες επιτυχίας και η αστυνομία ποτέ δε θα μπορούσε να είναι σίγουρη ότι η χρήση του θα μπορούσε έστω και πιθανώς να παράξει μία θετική ταυτοποίηση, σε αντίθεση με τη χρήση «παραδοσιακών» καταλόγων παρακολούθησης που αποκλειστικά περιλαμβάνουν άτομα που είναι εύλογα ύποπτοι.

110. Στα πλαίσια των μέτρων περιορισμού του χρόνου διατήρησης, το ΔΕΕ έχει κρίνει ότι για να περιοριστούν σε αυτά που είναι απολύτως αναγκαία, τα μέτρα αυτά πρέπει να υπόκεινται σε περιορισμούς που «πρακτικά οριοθετούν το εύρος του μέτρου αυτού και, επομένως, τα πληττόμενα άτομα».[100] Τα πληττόμενα άτομα, στην περίπτωση της Clearview, είναι κατ' ουσίαν ολόκληρος ο πληθυσμός – με αποτέλεσμα ο καθένας να τίθεται σε ένα κατάλογο παρακολούθησης. Παρά το γεγονός ότι η διατήρηση δεδομένων στην περίπτωση της Clearview πραγματοποιείται από μία ιδιωτική εταιρεία και όχι από την αστυνομία, πρέπει να εφαρμοστεί η ίδια αξιολόγηση: οι βλάβες που εντοπίζονται από τα δικαστήρια και τις αρχές στην περίπτωση της αδιάκριτης και επ' αόριστον διατήρησης παραμένουν οι ίδιες όταν οι αρχές επιβολής του νόμου αποκτούν ελεύθερη πρόσβαση στη βάση δεδομένων της Clearview. Η Homo Digitalis παρακινεί την ΑΠΔΠΧ να αποτρέψει την αποφυγή των εκ του νόμου υποχρεώσεων που σχετίζονται με τα ανθρώπινα δικαιώματα και την προστασία δεδομένων εκ μέρους των δημόσιων αρχών και να αποτρέψει την εφαρμογή ενός ιδιωτικού εργαλείου επιχειρήσεων παρακολούθησης χωρίς να εφαρμόζονται επί του εργαλείου αυτού οι ίδιες υποχρεώσεις.

111. Επιπλέον, η αδιάκριτη συλλογή, αποθήκευση και επεξεργασία φωτογραφιών από την Clearview μπορεί εύκολα να συγκριθεί με κάθε μαζική συλλογή δεδομένων, η οποία έχει κριθεί παράνομη.[101] Ο κίνδυνος κατάχρησης των μαζικών βάσεων δεδομένων είναι σημαντικός, και για το λόγο αυτό το ΔΕΕ έχει κρίνει ότι «γενική πρόσβαση σε όλα τα δεδομένα που τηρούνται, ανεξαρτήτως της ύπαρξης σύνδεσης, έστω και έμμεσης, με τον επιδιωκόμενο σκοπό, δεν μπορεί να θεωρηθεί ως περιορισμένη στο απολύτως αναγκαίο»[102].

112. Ως τμήμα της αξιολόγησης αναγκαιότητας, η αρχή της αναλογικότητας πρέπει να ληφθεί υπόψη – στην πραγματικότητα, η αναγκαιότητα υπόκειται στην αναλογικότητα, σύμφωνα με την εργαλειοθήκη αξιολόγησης αναγκαιότητας του ΕΣΠΔ, και ως εκ τούτου ακόμα και ένα εν στενή εννοία αναγκαίο μέτρο οφείλει να είναι αναλογικό.[103] Στην υπόθεση *S. και Marper κατά UK*,[104] το ΕΔΔΑ αναμετρήθηκε με ένα ακόμα μέτρο που περιελάμβανε την αδιάκριτη διατήρηση

[99] ICO σελ. 14.
[100] Συνεκδικασθείσες Υποθέσεις C–203/15 and C–698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson* [2016] ECR I–970, παρ. 110.
[101] Υπόθεση C-623/17 *Privacy International v SSFCA and Ors* [2020] ECLI:EU:C:2020:790.
[102] Ibid, para 78.
[103] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" (11 April 2017), σελ. 5. https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[104] App nos 30562/04 and 30566/04 (ECtHR, 12 Απρίλιος 2008).

βιομετρικών, δηλ. δακτυλικών αποτυπωμάτων, γονιδιώματος και κυτταρικών δειγμάτων, για σκοπούς εντοπισμού και δίωξης του εγκλήματος. Έκρινε πως:

> *η προστασία που προβλέπεται στο Άρθρο 8 της Σύμβασης θα αποδυναμωνόταν με απαράδεκτο τρόπο αν η χρήση σύγχρονων επιστημονικών τεχνικών του συστήματος της ποινικής δικαιοσύνης επιτρεπόταν με κάθε κόστος και χωρίς προσεκτική αξιολόγηση των πιθανών πλεονεκτημάτων της εκτενούς χρήσης τέτοιων τεχνικών έναντι σημαντικών συμφερόντων της ιδιωτικής ζωής. Σύμφωνα με την κρίση του Δικαστηρίου, η στιβαρή συναίνεση που υφίσταται μεταξύ των Συμβαλλόμενων Μελών σε σχέση με το ζήτημα αυτό έχει μεγάλη σημασία και περιορίζει το περιθώριο εκτίμησης που διαθέτει το εναγόμενο Κράτος κατά την αξιολόγηση των επιτρεπόμενων ορίων παρέμβασης με την ιδιωτική ζωή σε αυτή τη σφαίρα. Το Δικαστήριο θεωρεί πως κάθε Κράτος που ισχυρίζεται πως διαθέτει πρωτοπόρο ρόλο στην ανάπτυξη νέων τεχνολογιών φέρει ειδική ευθύνη εντοπισμού της σωστής ισορροπίας σε σχέση με το ζήτημα αυτό.*[105]

113. Οι προβληματισμοί που αναπτύχθηκαν ανωτέρω στην ενότητα VI.A καταδεικνύουν τη σοβαρή επέμβαση στην ιδιωτικότητα, την προστασία των δεδομένων και τα λοιπά θεμελιώδη δικαιώματα που προκαλείται από το εργαλείο της Clearview. Αυτή η σοβαρή επέμβαση βαρύνει ιδιαίτερα κατά την στάθμιση έναντι τυχόν πλεονεκτημάτων της τεχνολογίας. Επιπλέον, στα πλαίσια της αναγνώρισης προσώπου, κάθε στάθμιση μεταξύ των πλεονεκτημάτων αυτής της τεχνολογίας παρακολούθησης και των βλαβών στα ανθρώπινα δικαιώματα θα είναι πολύ δύσκολη, λαμβάνοντας υπόψη τις προκλήσεις κατάλληλης ενσωμάτωσης των αποτελεσμάτων της τελευταίας, δεδομένων των επιπτώσεων αποθάρρυνσης της τεχνολογίας αναγνώρισης προσώπου. Για παράδειγμα, οι αρχές μάλλον δε θα είναι σε θέση να αξιολογήσουν τον ακριβή αριθμό των ατόμων που θα επέλεγαν να μην παραστούν σε μία δημόσια εκδήλωση, θυσιάζοντας την ελευθερία έκφρασης και την ελευθερία του συνέρχεσθαι λόγω των εύλογων προβληματισμών σχετικά με την κατάχρηση των βιομετρικών δεδομένων τους από την αστυνομία. Δεδομένης της μαζικής και αδιάκριτης φύσης των δεδομένων που συλλέγει και επεξεργάζεται η Clearview, καθώς και των σημαντικών προβληματισμών σε σχέση με τα ανθρώπινα δικαιώματα που εγείρονται λόγω της χρήσης τους για τη διευκόλυνση της εφαρμογής της τεχνολογίας αναγνώρισης προσώπου, η Homo Digitalis θεωρεί πως η εφαρμογή της Clearview από τις αρχές επιβολής του νόμου δεν μπορεί ποτέ να είναι αναλογική.

VII. Αιτήματα που επιδιώκει η παρούσα καταγγελία - αναφορά

114. Λαμβάνοντας υπόψη τα ως άνω και προκειμένου να υπάρξει συμμόρφωση με τις διατάξεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και να προστατευτεί το υποκείμενο των δεδομένων αλλά και το σύνολο των υποκειμένων δεδομένων που διαμένουν στην ελληνική επικράτεια από παράνομες πρακτικές επεξεργασίας της εταιρίας Clearview AI, αιτούμαστε από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα την πλήρη άσκηση των ερευνητικών, διορθωτικών και συμβουλευτικών της εξουσιών της όπως

[105] Ibid, παρ. 112.

αυτές πηγάζουν από τα άρθρα 57-58 GDPR και το άρθρο 15 του ν.4624/2019 που μεταφέρει στην Ελληνική έννομη τάξη τις διατάξεις των άρθρων 47-48 της Οδηγίας 2016/680.

115. Καλούμε την ΑΠΔΠΧ να ανταποκριθεί στο αίτημά μας και να αναλάβει τις εξουσίες αυτές.

116. Συνοπτικά, η Homo Digitalis καλεί την ΑΠΔΠΧ να ερευνήσει τα ακόλουθα:

(α) Τη μη συμμόρφωση της Clearview AI με τις υποχρεώσεις του άρθρου 12 παρ. 3 GDPR στο πλαίσιο της άσκησης του δικαιώματος πρόσβασης από το υποκείμενο των δεδομένων,

(β) Τη συλλογή από την Clearview εικόνων από το διαδίκτυο και την επεξεργασία βιομετρικών δεδομένων, και συγκεκριμένα:

i. Την τήρηση των αρχών της σύννομης διαφανούς και δίκαιης επεξεργασίας, κυρίως αναφορικά με την εύλογη προσδοκία των υποκειμένων των δεδομένων σχετικά με τον σεβασμό της ιδιωτικής τους ζωής και την προστασία των προσωπικών δεδομένων τους,
ii. Την ύπαρξη νόμιμης βάσης επεξεργασίας σύμφωνα με τις διατάξεις των άρθρων 6 και 9 του GDPR, και την εξέταση εάν πληρούνται τα κριτήρια για να θεωρηθεί ότι η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή ότι η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων, αντίστοιχα, και
iii. Την προστασία της αρχής της ελαχιστοποίησης των δεδομένων.

(γ) Τη χρήση των υπηρεσιών της Clearview AI από αρχές επιβολής του νόμου, και τα κριτήρια που καθιστούν αυτή την επεξεργασία σύννομη.

117. Τέλος, όπως αναφέρουμε στην αρχή της παρούσας καταγγελίας-αναφοράς και συγκεκριμένα στην παράγραφο 3, άλλες τέσσερις παρόμοιες καταγγελίες κατά των πρακτικών της Clearview AI έχουν κατατεθεί σήμερα ενώπιον των αρμόδιων εποπτικών αρχών στην Αυστρία, την Γαλλία, την Ιταλία και το Ηνωμένο Βασίλειο. Επομένως σύμφωνα με τη διαδικασία που προβλέπεται στο Κεφάλαιο VIII του GDPR και τις διατάξεις των άρθρων 62 επόμενα καλούμε την ΑΠΔΠΧ να συνεργαστεί με τις εθνικές αρχές προστασίας προσωπικών δεδομένων άλλων κρατών με σκοπό την επιδίωξη μιας συντονισμένης έρευνας για τις πρακτικές της εταιρίας Clearview AI από τους αρμόδιους εποπτικούς φορείς. Μαζί με τις άλλες οργανώσεις της κοινωνίας των πολιτών που συμμετέχουν στις κοινές αυτές δράσεις θα κοινοποιήσουμε τα ζητήματα που ανακύπτουν ενώπιον του Ευρωπαίου Επόπτη Προστασίας Δεδομένων και του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

Το Δ.Σ. της
Homo Digitalis Αστική Μη Κερδοσκοπική Εταιρία
27.5.2021