ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
του Γκόλνα Ιωάννη-Νικόλαου (Α.Μ. ΜΔΙ2012)

[Η ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΗΝ ΑΝΙΧΝΕΥΣΗ ΕΓΚΛΗΜΑΤΩΝ/ ΕΠΙΒΟΛΗ ΤΟΥ ΝΟΜΟΥ/ ΠΡΟΛΗΠΤΙΚΗ ΑΣΤΥΝΟΜΕΥΣΗ]

Επιβλέπουσα:

Καθηγήτρια Λίλιαν Μήτρου

Πειραιάς, Μάιος 2022

Στους γονείς μου, διότι χωρίς τη στήριξή τους

δεν θα είχα καταφέρει τίποτα

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Διανύοντας τη δεύτερη δεκαετία του 21ου αιώνα είναι ευκόλως αντιληπτό ότι η ανθρώπινη κοινωνία έχει μετεξελιχθεί και έχει λάβει μία νέα, μία ηλεκτρονική/ ψηφιακή μορφή. Θα μπορούσε κάποιος να πει ότι πλέον το μεγαλύτερο μέρος των καθημερινών δραστηριοτήτων πραγματοποιείται με τη βοήθεια του διαδικτύου ή και αποκλειστικά από αυτό. Ενδεικτικά αναφέρεται ότι οι πιο δημοφιλείς πλατφόρμες παγκοσμίως είναι οι ιστοσελίδες κοινωνικής δικτύωσης, καθώς το Facebook μετρά 2,85 δισεκατομμύρια ενεργούς χρήστες μηνιαίως, σύμφωνα με στοιχεία του 2021[1], το Instagram, το οποίο αγοράστηκε από το Facebook κατά το έτος 2012, μετρά παραπάνω από 1 δισεκατομμύριο χρήστες, με βάση την έρευνα του 2020[2], ενώ το Twitter απαριθμεί 353 εκατομμύρια χρήστες (2020)[3]. Βέβαια η γέννηση της ηλεκτρονικής κοινωνίας δεν αποδεικνύεται μόνο από τα μέσα κοινωνικής δικτύωσης. Αντιθέτως η ραγδαία τεχνολογική ανάπτυξη, αποκύημα της 4ης βιομηχανικής επανάστασης, έχει αμέτρητες εκφάνσεις. Πλέον οι περισσότερες χρηματικές συναλλαγές πραγματοποιούνται ψηφιακά μέσω συστημάτων όπως το «blockchain» και το «bitcoin», ταυτόχρονα η έννοια της τηλεργασίας δεν αποτελεί σενάριο επιστημονικής φαντασίας, αλλά στηρίζεται στιβαρά στο σήμερα. Παρατηρείται λοιπόν μία τάση ψηφιοποίησης και αυτοματοποίησης του όλου συστήματος με απώτερο σκοπό τη διευκόλυνση της ανθρώπινης ζωής. Αυτός ακριβώς είναι ένας, απλός μεν, ακριβής δε ορισμός της τεχνητής νοημοσύνης (artificial intelligence/ AI), η οποία έχει διεισδύσει στην καθημερινότητά μας σαν κάτι το αυτονόητο.

Αναπόσπαστο, και αναγκαίο, κομμάτι της καθημερινότητας μας όμως είναι και η εύρυθμη λειτουργία του Δικαιϊκού Συστήματος, καθώς η απουσία της δικαιοσύνης δημιουργεί την ανομία και την καταπάτηση των ελευθεριών. Φυσικό επακόλουθο λοιπόν είναι να ξεκινήσει η αξιοποίηση των νέων τεχνολογικών δυνατοτήτων για τη βέλτιστη και αποτελεσματικότερη απονομή της δικαιοσύνης[4]. Η χρήση της τεχνητής νοημοσύνης πραγματοποιείται είτε προληπτικά, δηλαδή πριν καν εκδηλωθεί η αξιόποινη συμπεριφορά με τη μορφή της προληπτικής αστυνόμευσης (predictive policing), είτε κατασταλτικά, αφού

[1] Menlo Park (2021), *Facebook Reports First Quarter 2021 Results*, διαθέσιμο στο https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results/default.aspx

[2] https://el.wikipedia.org/wiki/Instagram

[3] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/?fbclid=IwAR08yhtuhoWLQo26hgwnmi1ZB3S3Q5SlhKIZo5Y8o3nyRTs28Ka6h4DKpww

[4] Λ. Κανέλλος (2021), *ΕΦΑΡΜΟΓΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ στο δίκαιο και στη δικαστική πρακτική*, εκδόσεις Νομική Βιβλιοθήκη

υποπέσουν στην αντίληψη των αστυνομικών ή δικαστικών αρχών (intelligence led policing/ ILP). Παράλληλα, λόγω της πανδημίας του κορωνοϊού που ξεκίνησε τον Μάρτιο του 2020 και οδήγησε μεγάλο μέρος του δυτικού κόσμου σε καραντίνα[5], οι υγειονομικές αρχές ανά τον κόσμο ξεκίνησαν να χρησιμοποιούν παρόμοιες μεθόδους ILP για την ιχνηλάτηση των κρουσμάτων, με απώτερο σκοπό την εξάλειψη της διασποράς του ιού. Συνολικά όλες αυτές οι εξελίξεις συνέβαλαν στη δημιουργία μηχανισμών αυτοματοποιημένου κοινωνικού ελέγχου που παρακολουθούν ολόκληρες πόλεις ή ακόμη και χώρες εγκαινιάζοντας μία περίοδο «αλγοριθμικής διακυβέρνησης»[6] και ψηφιακού ολοκληρωτισμού, που πολλές φορές λειτουργούν εις βάρος των ατομικών ελευθεριών των πολιτών, στην προσπάθεια να ενισχύσουν το αίσθημα της κρατικής ασφάλειας. Αφού αναλυθούν οι προαναφερθείσες τεχνικές ηλεκτρονικής αστυνόμευσης, εν συνεχεία θα διερευνηθεί το σχετικό Ευρωπαϊκό νομοθετικό πλαίσιο, δίνοντας ιδιαίτερη έμφαση στα νομικά ζητήματα που είναι ασαφή ή δεν ορίζονται επαρκώς, δημιουργώντας σύγχυση στον νομικό χώρο. Ακολούθως, θα εξεταστούν οι κίνδυνοι που ενδέχεται να προκύψουν από τη χρήση της τεχνητής νοημοσύνης, τόσο στις ατομικές ελευθερίες, όπως στην προστασία της ιδιωτικότητας, όσο και στις συλλογικές ελευθερίες, όπως στην ισότητα Τέλος θα προταθούν ορισμένες λύσεις που έχουν ως στόχο σε πρώτο βαθμό την εύρυθμη λειτουργία των συστημάτων τεχνητής νοημοσύνης στον τομέα της αστυνόμευσης, προστατεύοντας παράλληλα τις ατομικές ελευθερίες, και σε δεύτερο βαθμό τη δημιουργία ενός κλίματος εμπιστοσύνης ανάμεσα στα υποκείμενα της επεξεργασίας και στις νέες τεχνολογίες.

1. ΕΙΣΑΓΩΓΗ

Από την αρχή της δημιουργίας του ο άνθρωπος προσπαθεί συνεχώς να βρει τρόπους για να διευκολύνει τη ζωή του. Όλες οι εφευρέσεις, είτε πρόκειται για τον τροχό που ανακαλύφθηκε πριν από χιλιάδες χρόνια είτε για το κινητό τηλέφωνο που ανακαλύφθηκε πριν μερικές δεκαετίες, έχουν σαν κοινή αφετηρία την ανθρώπινη τάση για μείωση (ή και εκμηδενισμό θα τολμούσαμε να πούμε) των «περιττών ενεργειών». Αυτή η τάση της ανθρώπινης φύσεως αποτέλεσε και τον αιτιώδη παράγοντα για την ταχύτατη εξέλιξη της τεχνητής νοημοσύνης, που ξεκίνησε από τα μέσα του 20ου αιώνα. Από τη στιγμή που έγινε αντιληπτό από τους

[5] CBC, (2020), Coronavirus: *WHO calls COVID-19 outbreak a pandemic as Italy orders most stores to close*, διαθέσιμο στο https://www.cbc.ca/news/world/coronavirus-pandemic-1.5493411

[6] Christian Katzenbach, Lena Ulbricht, (2019), *Algorithmic governance*, διαθέσιμο στο https://policyreview.info/concepts/algorithmic-governance

ανθρώπους ότι υπάρχουν όρια στις γνωστικές λειτουργίες τους, ξεκίνησαν οι προσπάθειες για τη δημιουργία συστημάτων που θα μπορούσαν να αντιγράψουν την ανθρώπινη σκέψη, χωρίς όμως να έχουν όρια στην αποθήκευση και επεξεργασία των γνώσεων[7]. Για να καταστεί κάτι τέτοιο εφικτό θα πρέπει οι μηχανές να συλλέγουν δεδομένα (data) να τα επεξεργάζονται και να οδηγούνται σε κάποιο συμπέρασμα, μέσω της μίμησης της ανθρώπινης συμπεριφοράς και δη της σκέψης[8]. Συνεπώς για την ανάπτυξη της τεχνητής νοημοσύνης απαιτούνται οι κατάλληλες υποδομές που ευνοούν τη συνεχή ροή της πληροφορίας. Για το λόγο αυτό δεν είναι τυχαίο που, όπως όλοι οι τεχνολογικοί τομείς, η τεχνητή νοημοσύνη βιώνει σημαντικότατη ανάπτυξη τις τελευταίες δεκαετίες.

Η δημιουργία του διαδικτύου, των μέσων κοινωνικής δικτύωσης και των μηχανών αναζήτησης επέφεραν ως αποτέλεσμα την εκθετική αύξηση των ηλεκτρονικών δεδομένων, γνωστά και ως big data[9]. Ανάλογες εξελίξεις παρατηρήθηκαν και στην επεξεργασία αυτού του τεράστιου όγκου δεδομένων (data mining)[10]. Δημιουργήθηκε έτσι το κατάλληλο τεχνολογικό υπόβαθρο για την κωδικοποίηση της ανθρώπινης σκέψης με τη χρήση αλγορίθμων από υπολογιστικά συστήματα. Από εκείνη τη στιγμή και έπειτα η τεχνητή νοημοσύνη εισήλθε απότομα σε πολλαπλούς τομείς της καθημερινότητας, όπως για παράδειγμα στις ηλεκτρονικές αγορές και στη δυνατότητα τηλεργασίας[11]. Έτσι λοιπόν η Τεχνητή Νοημοσύνη εγκαθίδρυσε την περιβόητη ψηφιακή διακυβέρνηση, δημιουργώντας την «κοινωνία της πληροφορίας» η οποία είναι ελεύθερα προσβάσιμη. Μάλιστα η Ελλάδα στην προσπάθειά της να συμβαδίσει με τις εξελίξεις της εποχής τροποποίησε το Σύνταγμα της προσθέτοντας το άρθρο 5[A] που ορίζει ότι «Καθένας έχει δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας».

Αναπόφευκτο ήταν η τεχνητή νοημοσύνη να εισέλθει και στο χώρο της αστυνόμευσης. Αξιοσημείωτη είναι η έκθεση της οργάνωσης προστασίας ανθρωπίνων δικαιωμάτων Carnegie[12], σύμφωνα με την οποία κατά το 2019 πάνω από 70 χώρες σε όλο τον κόσμο

---

[7] Nilsson, N. (2010), *The Quest for Artificial Intelligence*, United Kingdom: Stanford University

[8] Ρεφανίδης Γ. (2005), *Τεχνητή Νοημοσύνη: Μια σύγχρονη προσέγγιση*, εκδόσεις Κλειδάριθμος

[9] Λίντα Γαλάζιου (2016), *Τι είναι πράγματι τα Big Data;*, διαθέσιμο στο https://www.epixeiro.gr/article/2728

[10] SAS, *Data Mining What it is & why it matters*, διαθέσιμο στο https://www.sas.com/en_us/insights/analytics/data-mining.html#dmtechnical

[11] Sarah Brayne and Angele Christin (2020), *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal courts*, Oxford University Press

[12] Ολόκληρη η έκθεση είναι διαθέσιμη στο https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

χρησιμοποιούν τεχνολογίες AI για παρακολούθηση των υπηκόων τους. Αυτό δεν σημαίνει απαραίτητα ότι όλες οι χώρες χρησιμοποιούν τις ίδιες εφαρμογές τεχνητής νοημοσύνης ή ότι τις χρησιμοποιούν όλες με τον ίδιο «ολοκληρωτικό» τρόπο. Αντιθέτως, η έρευνα αυτή μας δείχνει ότι οι εγχώριες αρχές πλέον χρησιμοποιούν διάφορες σύγχρονες τεχνολογικές πρακτικές για τη διευκόλυνσή τους στον αέναο αγώνα κατά της εγκληματικότητας. Αυτές οι δυνατότητες εντάσσονται συνοπτικά σε δύο κατηγορίες, στις εφαρμογές που λειτουργούν προληπτικά, δηλαδή πριν πραγματοποιηθεί το έγκλημα, και δεύτερον στις εφαρμογές που λειτουργούν κατασταλτικά, αφού δηλαδή εκδηλωθεί η παραβατική συμπεριφορά. Ιδιαίτερη μνεία αξίζουν οι εφαρμογές ιχνηλάτησης του κορωνοϊού, διότι το λογισμικό τους παρουσιάζει έντονες, ή και τρομακτικές θα μπορούσε να πει κανείς, ομοιότητες με αυτό της αλγοριθμικής αστυνόμευσης. Συνδυαστικά αυτές οι καινοτομίες έδωσαν τη δυνατότητα στις κρατικές αρχές να δημιουργήσουν ένα νέο δυστοπικό καθεστώς συνεχούς παρακολούθησης και κοινωνικού ελέγχου καταπατώντας πλήρως κάθε μορφή δικαιώματος και ατομικών ελευθεριών των πολιτών. Όλες αυτές οι σύγχρονες μορφές τεχνολογικής αστυνόμευσης μέσω της AI θα εξεταστούν αναλυτικά, εστιάζοντας παράλληλα στο σχετικό νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης μαζί με τα νομικά κενά που ενυπάρχουν σε αυτό. Σε δεύτερο στάδιο θα διερευνηθούν οι κίνδυνοι που ενδέχεται να ανακύψουν καθώς και τα δικαιώματα που θίγονται από αυτές τις πρακτικές. Τέλος θα παρουσιαστούν ορισμένες προτεινόμενες λύσεις για την αντιμετώπιση των αρνητικών επιπτώσεων της χρήσης της AI στο πλαίσιο επιβολής του νόμου.

2. ΠΡΟΛΗΠΤΙΚΗ ΑΣΤΥΝΟΜΕΥΣΗ

Για να γίνει πλήρως αντιληπτός ο θεσμός της προληπτικής αστυνόμευσης, κρίνεται ορθό σε πρώτο βαθμό να αναλυθούν οι δύο έννοιες που την απαρτίζουν, η πρόληψη και η αστυνόμευση. Μιας και η πρόληψη αποτελεί μία έκφανση της αστυνόμευσης, είναι πρέπον η ανάλυση να ξεκινήσει από τον ορισμό της τελευταίας.

Η αστυνόμευση, περιγράφει το σύνολο των αρμοδιοτήτων ορισμένων κρατικών οργάνων και μηχανισμών που έχουν ως στόχο την επιβολή του νόμου, τη διατήρηση της δημόσιας τάξης και τη διαχείριση της δημόσιας ασφάλειας[13]. Για την εύρυθμη λειτουργία της κοινωνίας δεν αρκεί μονάχα η θέσπιση νόμων, αλλά και η άμεση και αποτελεσματική εφαρμογή τους.

[13] BJS (2021), *Law Enforcement*, διαθέσιμο στο https://bjs.ojp.gov/topics/law-enforcement

Αυτή η αναγκαιότητα είναι που αποτέλεσε γενεσιουργό αιτία για τη δημιουργία αυτού του θεσμού. Στο πλαίσιο της ορθής εφαρμογής του νόμου, οι αστυνομικές αρχές είναι αρμόδιες για τη διερεύνηση, την σύλληψη και την επιβολή ποινής στους πολίτες που παραβίασαν τον νόμο[14]. Επομένως ο όρος αστυνόμευση περικλείει τόσο το αστυνομικό σώμα, όσο και το δικαστικό.

Συνεπώς ο βασικός στόχος της αστυνόμευσης είναι ο εντοπισμός των αξιόποινων πράξεων και η καταστολή τους. Μάλιστα, αυτές οι ενέργειες πρέπει να γίνουν όσο το δυνατόν πιο γρήγορα, ώστε να μη βρεθούν σε κίνδυνο περισσότεροι πολίτες και παράλληλα να μην πληγεί η κρατική ασφάλεια. Γενικότερα η αντίδραση στην είδηση ότι είχε διαπραχθεί κάποιο έγκλημα αποτελούσε βασικό άξονα στην αξιολόγηση της λειτουργίας των αστυνομικών αρχών[15]. Με την πάροδο των χρόνων όμως, παρατηρήθηκε ότι η φιλοσοφία της αστυνόμευσης άρχισε να αλλάζει, να εξελίσσεται. Πηγή προβληματισμών αποτέλεσε η άποψη ότι, ακόμη και αν εντοπιστεί ταχύτατα μια εγκληματική ενέργεια και κατασταλεί, η δημόσια βλάβη έχει ήδη επέλθει. Πρέπει λοιπόν οι αστυνομικές αρχές να προλάβουν αυτή τη δημόσια βλάβη. Κατ᾽ αυτόν τον τρόπο γεννήθηκε η έννοια της πρόληψης σύμφωνα με την οποία, ο στόχος της αστυνόμευσης είναι να ανιχνεύσει και να αντιμετωπίσει το έγκλημα πριν αυτό εξωτερικευτεί, και όχι να περιμένει την εκδήλωση του, διότι η πρόληψη έχει μεγαλύτερη κοινωνική αξία από την καταστολή[16]. Αυτή η αλλαγή φιλοσοφίας έδωσε το έναυσμα για την ανάπτυξη τεχνικών πρόληψης του εγκλήματος.

2.1 Ο ρόλος των δεδομένων και ο ορισμός της προληπτικής αστυνόμευσης

Κρίσιμος παράγοντας για τις εφαρμογές πρόληψης αποδείχθηκε η μαζική παραγωγή δεδομένων που δημιούργησε τον κόσμο των big data και της ψηφιακής κοινωνίας. Σε αυτή την νέα πραγματικότητα όλες οι πτυχές της κοινωνίας έχουν λάβει τη μορφή δεδομένων. Αντλώντας πληροφορίες από όλα αυτά τα δεδομένα οι κρατικές αρχές με τη βοήθεια

[14] New Law Journal, Volume 123, Part 1 - Page 358, 1974

[15] Ishmael Mugari and Emeka Obioha (2021), Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing, διαθέσιμο στο https://www.mdpi.com/2076-0760/10/6/234/htm

[16] Pascal Martens (2016), PREDICTIVE POLICING TENSION BETWEEN ANALYTICS AND INTUITION A Literature Review in accordance with the requirements for the degree of Master of Science in Policing, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/346400071_PREDICTIVE_POLICING_TENSION_BETWEEN_ANALYTICS_AND_INTUITION_A_Literature_Review_in_accordance_with_the_requirements_for_the_degree_of_Master_of_Science_in_Policing

υπολογιστικών συστημάτων άρχισαν να τα επεξεργάζονται, να τα ομαδοποιούν και να βρίσκουν κοινά μοτίβα. Τα μοτίβα αυτά έδωσαν την δυνατότητα στους αναλυτές να καταλάβουν ότι το έγκλημα δεν είναι μία τυχαία ή συγκυριακή πράξη. Αντιθέτως είναι άμεσο αποτέλεσμα πολλών παραγόντων, όπως οι περιβαλλοντικές συνθήκες η περιστασιακή λήψη αποφάσεων αλλά και το κοινωνικό υπόβαθρο του δράστη[17]. Η ανακάλυψη αυτή λειτούργησε σαν έναυσμα για την ανάπτυξη αλγορίθμων οι οποίοι, με τη δημιουργία μοτίβων, θα ήταν σε θέση ,σύμφωνα με τις πιθανότητες, να υπολογίζουν κατά πόσο είναι πιθανό να διαπραχθεί ένα έγκλημα, σε ποιο μέρος και από ποιον. Εφαρμόζοντας τη μεθοδολογία αυτή, άρχισαν να αναδύονται στην επιφάνεια οι πρώτες εφαρμογές προληπτικής αστυνόμευσης.

Η αλήθεια είναι ότι πολλοί έχουν αποπειραθεί να δώσουν έναν απλό και ταυτόχρονα ακριβή ορισμό της προληπτικής αστυνόμευσης, λίγοι όμως είναι αυτοί που το κατάφεραν. Μία από τις πρώτες απόπειρες σημειώθηκε το 2010 από την Beth Pearsall, σύμφωνα με την οποία προληπτική αστυνόμευση είναι η συλλογή δεδομένων από πολλές διαφορετικές πηγές, η ανάλυσή τους και η αξιοποίηση των αποτελεσμάτων τους για την πρόβλεψη, πρόληψη και αποτελεσματικότερη ανταπόκριση στα μελλοντικά εγκλήματα[18]. Φαινομενικά αυτός ο ορισμός φαίνεται πολύ εύστοχος, όμως δεν είναι γιατί δεν αναφέρει τη σημασία της τεχνολογίας και των υπολογιστικών συστημάτων στην επεξεργασία αυτή. Για να προκύψει ένας ορθός ορισμός πρέπει να επισημανθούν τα βασικά χαρακτηριστικά της προληπτικής αστυνόμευσης που είναι η χρήση νέων τεχνολογιών και αλγορίθμων, η πιθανολόγηση μελλοντικών εγκλημάτων και η βελτίωση της λήψης αποφάσεων για την αντιμετώπιση της εγκληματικότητας. Συνεπώς με βάση τα ανωτέρω προληπτική αστυνόμευση είναι η χρήση αλγορίθμων και άλλων τεχνολογιών τεχνητής νοημοσύνης για τον εντοπισμό πιθανών εγκληματικών δραστηριοτήτων, βελτιώνοντας έτσι την ικανότητα λήψεως αποφάσεων (decision-making) σχετικά με την αντιμετώπιση της εγκληματικότητας[19].

---

[17] βλ. Sarah Brayne and Angele Christin υποσημείωση 11

[18] "the taking of data from disparate sources, analysing them and then using the result to anticipate, prevent and respond more effectively to future crime", Beth Pearsall (2010) *Predictive Policing: The Future of Law Enforcement?*, διαθέσιμο στο https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement

[19] Fernando Miro-Llinares (2020), *Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/339638731_Predictive_policing_utopia_or_dystopia_On_attitudes_towards_the_use_of_big_data_algorithms_for_law_enforcement

Όπως θα αναλυθεί εκτενώς στη συνέχεια, ένα αποτελεσματικό σύστημα προληπτικής αστυνόμευσης αντλεί και επεξεργάζεται πολλών ειδών δεδομένα από πολλές διαφορετικές πηγές. Δηλαδή δεν επεξεργάζεται μόνο στοιχεία που σχετίζονται με ποινικά αδικήματα, αντιθέτως εστιάζει και σε άλλους άξονες όπως τα κοινωνικά κριτήρια. Ακόμη τα δεδομένα που συλλέγονται προέρχονται από διαφορετικές πηγές (όπως για παράδειγμα κάμερες ασφαλείας, μέσα κοινωνικής δικτύωσης, drones κ.α.). Αξιολογώντας όλα αυτά τα στοιχεία τα «έξυπνα» υπολογιστικά συστήματα που τα επεξεργάζονται δημιουργούν γραφήματα και πίνακες όπου περιλαμβάνουν τις τοποθεσίες που είναι το πιθανότερο να αποτελέσουν εστίες εγκληματικών πράξεων (π.χ. κακόφημες περιοχές, δρόμοι με χαμηλό φωτισμό), αλλά και καταλόγους ατόμων τα οποία είτε είναι πιθανό να αποτελέσουν θύματα αξιόποινων πράξεων (π.χ. ηλικιωμένοι άνθρωποι, κάτοικοι κακόφημων γειτονιών) είτε, επειδή συντρέχουν επιβαρυντικοί παράγοντες, είναι ενδεχόμενο να διαπράξουν κάποιο έγκλημα (π.χ. χρήστες ουσιών, άνεργοι, άνθρωποι που ζουν κάτω από το όριο της φτώχιας). Με βάση αυτά γίνεται αντιληπτό ότι τα μοντέλα προβλεπτικής αστυνόμευσης χωρίζονται σε δύο μεγάλες κατηγορίες. Σε μοντέλα που προβλέπουν τον τόπο που μπορεί να πραγματοποιηθεί έγκλημα και σε μοντέλα που προβλέπουν τα άτομα που μπορεί να εμπλακούν σε ένα έγκλημα[20] είτε ως θύτες είτε ως θύματα. Πρόκειται για συστήματα που λειτουργούν τελείως διαφορετικά, οπότε και χρήζουν ξεχωριστής ανάλυσης.

2.2 Γεωγραφικά συστήματα αστυνόμευσης

Τα γεωγραφικά μοντέλα προβλεπτικής αστυνόμευσης (γνωστά και ως placed-based predictive policing), έχουν σαν κύριο έργο τη συλλογή και επεξεργασία δεδομένων προς εντοπισμό περιοχών και σημείων έντονης εγκληματικότητας (crime hotspots). Οι αστυνομικές αρχές εξετάζοντας αυτά τα δεδομένα, αξιολογούν τον κίνδυνο και οργανώνουν τις καθημερινές περιπολίες τους[21]. Με τη σωστή οργάνωση των περιπολιών, τόσο χωροταξικά όσο και χρονικά, οι αρχές έχουν τη δυνατότητα να επέμβουν την καταλληλότερη στιγμή σε επικείμενα hotspots, εξαλείφοντας κατ' αυτόν τον τρόπο την εγκληματικότητα και διασφαλίζοντας τη σωματική ακεραιότητα των πολιτών. Για να

[20] Orla Lynskey (2019), *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, διαθέσιμο σε pdf στο https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/criminal-justice-profiling-and-eu-data-protection-law-precarious-protection-from-predictive-policing/10FD4B64364191B619FBCB864CD40A7F

[21] Βλ. Λ. Κανέλλος, υποσημείωση 4

μπορέσει να είναι λειτουργικός ο αλγόριθμος επεξεργασίας δεδομένων, κάθε εφαρμογή έχει ως βάση της, μία ή περισσότερες, εγκληματολογικές θεωρίες σχετικά με την πιθανότητα επανάληψης των εγκληματικών πράξεων. Από αυτές τις θεωρίες, δύο είναι που χρειάζονται περαιτέρω ανάλυση, μιας και η συντριπτική πλειοψηφία των placed-based εφαρμογών βασίστηκαν σε μία εκ των δύο ή και στις δύο. Η πρώτη θεωρία είναι η θεωρία της «πιθανής επανάληψης» (πιο σωστός είναι ο αμερικάνικος ορισμός «near-repeat theory»), και η δεύτερη η θεωρία του «επικίνδυνου σημείου» («risk terrain modelling», συνοπτικά RTM).

2.2.1 Near-repeat theory και σχετικές εφαρμογές

Η θεωρία της «πιθανής επανάληψης», είναι ένας όρος εμπνευσμένος από την επιστήμη της σεισμολογίας[22]. Όπως λοιπόν, όταν γίνεται σεισμός είναι πολύ πιθανό να υπάρξουν μετασεισμοί τα επόμενα εικοσιτετράωρα, αντίστοιχα όταν γίνεται ένα έγκλημα είναι πιθανό να επαναληφθεί η εγκληματική πράξη στην ίδια περιοχή. Σύμφωνα με μελέτες[23], ορισμένα εγκλήματα μπορούν να επαναληφθούν σε κοντινό χρονικό διάστημα, στην γύρω περιοχή που εκδηλώθηκε το αρχικό έγκλημα. Βέβαια είναι πολύ περιορισμένος ο τύπος των εγκλημάτων που έχει όντως βάση αυτή η θεωρία. Τα σημαντικότερα ποινικά αδικήματα είναι τα αδικήματα περιουσιακής φύσεως, με χαρακτηριστικότερη περίπτωση τις διαρρήξεις.

Εμπνευσμένοι από την ανωτέρω θεωρία, ερευνητές του Πανεπιστημίου της Καλιφόρνια δημιούργησαν το 2011 την εφαρμογή PredPol[24]. Η εφαρμογή αυτή αναγνωρίζει τοποθεσίες που είναι πιθανό να λειτουργήσουν σαν hotspots για παράνομες πράξεις εντός ενός συγκεκριμένου χρονικού πλαισίου. Πρόκειται για ένα πολύ απλό λογισμικό στη δομή και τη λειτουργία του, καθώς βασίζεται μόνο σε 3 είδη δεδομένων, το είδος του εγκλήματος, την τοποθεσία και το χρόνο που διαπράχθηκε. Ουσιαστικά χρησιμοποιεί τον ελάχιστο όγκο δεδομένων για να κάνει τις απαραίτητες προβλέψεις. Αφού αναλυθούν τα δεδομένα σχηματίζονται χάρτες που δείχνουν ποιες περιοχές ενδεχομένως να είναι ευάλωτες σε εγκληματικές πράξεις στο άμεσο μέλλον. Οι χάρτες αυτοί στέλνονται στα αστυνομικά τμήματα έτσι ώστε με γνώμονα αυτούς να οργανώσουν τις περιπολίες τους[25]. Το σκεπτικό

---

[22] Βλ. Orla Lynskey, υποσημείωση 17

[23] Degeling M and Berendt B (2018), *What is wrong with Robocops as consultants? A technology-centric critique of predictive policing*, AI and Society 33, 347-356

[24] Πληροφορίες για τη λειτουργία του προγράμματος είναι διαθέσιμες στο σχετικό site https://www.predpol.com/how-predictive-policing-works/

[25] Andrew Ferguson (2017), *Policing Predictive Policing*, Washington University Law Review, διαθέσιμο σε pdf στο https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6306&context=law_lawreview

πίσω από αυτές τις ενέργειες είναι ότι η παρουσία περιπόλων σε αυτές τις περιοχές θα αποτελέσει τροχοπέδη για τις εγκληματικές πράξεις που επίκειται να συμβούν. Απ' ότι φαίνεται, σε πρώτο στάδιο τουλάχιστον, η τακτική αυτή απέδωσε καρπούς καθώς κατά τον πρώτο χρόνο λειτουργίας του προγράμματος οι διαρρήξεις μειώθηκαν κατά 30%[26]. Αυτή η επιτυχία αποτέλεσε κίνητρο για να αρχίσει να αξιοποιείται το πρόγραμμα και σε εγκλήματα άλλου τύπου. Πιο συγκεκριμένα το πρόγραμμα PredPol άρχισε να χρησιμοποιείται και για την πρόληψη εγκλημάτων που σχετίζονταν με όπλα. Συλλέγοντας δεδομένα από εγκλήματα που πραγματοποιήθηκαν στο Σικάγο κατά τη διετία 2009-2011 το πρόγραμμα παρατήρησε ότι ένα μεγάλο μέρος των εγκλημάτων που σχετίζονται με όπλα, συνδέονται με ανθρωποκτονίες. Έχοντας το μοτίβο αυτό σαν βάση το PredPol στάθηκε ικανό να προβλέψει την τοποθεσία των 50% μελλοντικών ανθρωποκτονιών[27]. Κατ' αυτόν τον τρόπο η χρήση του προγράμματος αυτού όχι μόνο συνεχίστηκε, αλλά επεκτάθηκε και σε άλλα εγκλήματα.

Βασισμένη στην ίδια θεωρία στην Ευρώπη αναπτύχθηκε η εφαρμογή Precobs. Πρόκειται για ένα από τα πρώτα προγράμματα προληπτικής αστυνόμευσης που αναπτύχθηκαν στην Ευρώπη, όντας μάλιστα ένα από τα πιο δημοφιλή. Από τις αρχές του 21ου αιώνα στη Γερμανία οι διαρρήξεις βρίσκονταν σε έξαρση, ενώ παράλληλα τα ποσοστά διαλεύκανσης των εγκλημάτων από τις τοπικές αστυνομικές αρχές ήταν ιδιαίτερα χαμηλά, λόγω του ότι πολλές εγκληματολογικές αναλύσεις ήταν αρκετά πρόχειρες και βεβιασμένες δημιουργώντας σύγχυση στην επίλυση των εγκλημάτων. Αυτό σε συνδυασμό με τους μειωμένους πόρους των τοπικών τμημάτων αποτέλεσαν επιτακτική ανάγκη για την ενίσχυση του έργου τους μέσω των νέων τεχνολογιών. Έτσι το 2015, έχοντας υπόψιν τις εξελίξεις στην αντίπερα όχθη του Ατλαντικού, δημιουργήθηκε στην Γερμανία η εφαρμογή Precobs (Pre Crime Observation System)[28]. Ακολουθώντας πιστά τη μεθοδολογία του PredPol, το πρόγραμμα αυτό εφαρμόζοντας τη θεωρία near-repeat, λειτουργεί με το σκεπτικό ότι όταν

[26] Jennifer Bachner (2017), *Predictive Policing: Preventing Crime with Data and Analytics* διαθέσιμο σε pdf στο
https://www.businessofgovernment.org/sites/default/files/Management%20Predictive%20Policing.pdf
[27] Βλ. Andrew Ferguson, υποσημείωση 25
[28] Πολύ λεπτομερής ανάλυση του τρόπου λειτουργίας του προγράμματος Precobs παρατηρείται στην ακαδημαϊκή έρευνα των Simon Egbert και Matthias Leese του 2020, βλ. Simon Egbert and Matthias Leese (2020), *Criminal Futures: Predictive Policing and Everyday Police Work*, Routledge Studies in Policing and society

πραγματοποιείται μία διάρρηξη, είναι πιθανό να επαναληφθεί σε στενό γεωγραφικό και χρονικό πλαίσιο.

Το λογισμικό της εφαρμογής βασίζεται σε δεδομένα διαρρήξεων που είχαν γίνει στο παρελθόν. Πιο συγκεκριμένα, αναλύει και επεξεργάζεται δεδομένα σχετικά με τον τόπο και τον χρόνο του εγκλήματος, το πώς τελέστηκε το έγκλημα (modus operandi) και άλλα επιμέρους χαρακτηριστικά όπως η αξία των κλοπιμαίων. Όλα αυτά τα δεδομένα τα ταξινομεί σε δύο μεγάλες κατηγορίες, στα κριτήρια ενεργοποίησης (trigger criteria) και στα κριτήρια μη ενεργοποίησης (anti-trigger criteria). Αν τα περισσότερα δεδομένα εμπίπτουν στην πρώτη κατηγορία, τότε συνάγεται το συμπέρασμα ότι είναι πιθανό να επαναληφθεί σύντομα διάρρηξη στην περιοχή σε σύντομο χρονικό διάστημα. Εν συνεχεία σχηματίζεται ο χάρτης της περιοχής όπου έγινε η ανάλυση, τονίζοντας τα σημεία όπου είναι πιο ευάλωτα στον κίνδυνο near-repeat εγκλήματος. Ο χάρτης αυτός μαζί με τα αποτελέσματα της επεξεργασίας στέλνονται από τις αρχές στα αρμόδια αστυνομικά τμήματα, τα οποία τον εξετάζουν και προγραμματίζουν τις περιπολίες στην περιοχή. Η σωστή διανομή των περιπολιών έχει ως αποτέλεσμα την πρόληψη του εγκλήματος[29]. Το Precobs πέρα από τη Γερμανία εφαρμόζεται και σε ορισμένες πόλεις της Ελβετίας με μεγάλη επιτυχία καθώς παρατηρήθηκε ότι στη Ζυρίχη οι διαρρήξεις μειώθηκαν κατά 30%.

2.2.2 Το μοντέλο risk terrain και η καινοτομία του HunchLab

Την ίδια χρονική περίοδο που εμφανίστηκε στο προσκήνιο η θεωρία near-repeat, άρχισε να αναπτύσσεται και μία άλλη θεωρία επίσης στις ΗΠΑ, τη «μητέρα» της προληπτικής αστυνόμευσης. Κατά τη συλλογή και την επεξεργασία δεδομένων από προηγούμενα εγκλήματα, παρατηρήθηκε ότι υπάρχουν ορισμένοι γεωγραφικοί και πολεοδομικοί παράγοντες που ευνοούν την διάπραξη εγκλημάτων. Για παράδειγμα πολλά εγκλήματα έχουν πραγματοποιηθεί σε δρόμους με χαμηλό φωτισμό ή σε πάρκα που υπάρχουν πολλοί ναρκομανείς. Τα στοιχεία αυτά δεν θεωρήθηκαν συμπτώσεις και αποτέλεσαν την σπίθα για να δημιουργηθεί το μοντέλο risk terrain (Risk Terrain Modelling, RTM). Το μοντέλο αυτό εξετάζει το έγκλημα από γεωχωρική άποψη, εντοπίζοντας και αναλύοντας περιβαλλοντικούς παράγοντες κινδύνου που συνδέονται με την αξιόποινη πράξη, με σκοπό τον εντοπισμό των σημείων αυτών που η διαμόρφωσή τους τις καθιστά πιθανές για έδρα

[29] Deutschland Land der Ideen, https://land-der-ideen.de/en/project/Precobs-software-for-predicting-crimes-355

εγκληματικών δραστηριοτήτων και πράξεων[30]. Σε αντίθεση με τη θεωρία near-repeat που εστιάζει κυρίως σε ενδογενείς παράγοντες, όπως η επαναλαμβανόμενη παραβατική συμπεριφορά, το RTM εστιάζει σχεδόν αποκλειστικά σε εξωτερικούς παράγοντες για την αξιολόγηση μίας περιοχής ως επικίνδυνη[31]. Το μοντέλο εξετάζει τη φυσική πραγματικότητα της πόλης και αναζητά χαρακτηριστικά που καθιστούν μία περιοχή πιο επικίνδυνη από μία άλλη. Για παράδειγμα εξετάζεται το αν ένας δρόμος είναι πολυσύχναστος ή αν υπάρχει αστυνομικό τμήμα σε μία γειτονιά. Η πρώτη εφαρμογή που αξιοποίησε το μοντέλο risk terrain ήταν η RTMDx[32], ένα λογισμικό που δημιουργήθηκε από το Πανεπιστήμιο Rutgers.

Μπορεί η RTMDx να ήταν η πρώτη εφαρμογή που αναπτύχθηκε σύμφωνα με το RTM, ωστόσο η εφαρμογή που πραγματικά χρήζει αναφοράς είναι η εφαρμογή HunchLab. Η εφαρμογή αυτή αποτέλεσε σημαντικότατη καινοτομία καθώς ήταν το πρώτο πρόγραμμα που συνδύασε τη θεωρία near repeat και το μοντέλο risk terrain. Πρόκειται για μία αρκετά πιο περίπλοκη, στο λογισμικό της, εφαρμογή σε σχέση με τις προαναφερθείσες καθώς επεξεργάζεται πολύ μεγαλύτερο όγκο δεδομένων από περισσότερες πηγές και στηρίζεται σε τεχνικές machine learning[33]. Το HunchLab λαμβάνει πάρα πολλούς παράγοντες υπόψιν[34] όπως τα ποσοστά εγκληματικότητας, τα μοτίβα near repeat, διάφορους κοινωνικοοικονομικούς παράγοντες και φυσικά τη χωρική διάρθρωση της πόλης. Όπως είναι λογικό οι προβλέψεις αυτές λειτουργούν συμβουλευτικά για την οργάνωση των τοπικών αστυνομικών περιπόλων. Μάλιστα για τη διευκόλυνση του έργου της αστυνομίας το HunchLab διατίθεται σαν εφαρμογή και σε κινητές συσκευές, ώστε να μπορούν ζωντανά να βλέπουν τις περιοχές που ενδέχεται να αποτελέσουν εστίες εγκλημάτων. Ως προς την

---

[30] Ο ακριβής ορισμός που διατυπώθηκε από τους Caplan, Joel, Leslie Kennedy, Jeremy Barnum και Eric Piza είναι ο εξής: «Risk Terrain Modelling is a geospatial crime analysis tool that is designed to examine environmental risk factors associated with crime and to identify the areas where their spatial influence is linked with vulnerability to criminal behaviour», Caplan Joel, Leslie Kennedy, Jeremy Barnum and Eric Piza (2017), *Crime in Context: Utilising Risk. Terrain Modelling and Conjunctive Analysis of Case Configuations to Explore the Dynamics of Criminogenic Behaviour Settings*, Journal of Contemporary Criminal Justice

[31] Βλ. Orla Lynskey, υποσημείωση 17

[32] Βλ. Ishmael Mugari, υποσημείωση 15

[33] Ο όρος machine learning αναφέρεται σε μία υποκατηγορία τεχνητής νοημοσύνης. Πρόκειται για αλγορίθμους, οι οποίοι με την επεξεργασία των δεδομένων και την εμπειρία που αποκτούν από αυτό, μπορούν αυτομάτως να βελτιωθούν και να κάνουν πιο ακριβείς προβλέψεις, χωρίς να χρειάζεται να προγραμματιστούν από τον άνθρωπο. Eleni Kosta (2020), *Algorithmic state surveillance: Challenging the notion of agency in human rights*, διαθέσιμο στο https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12331

[34] Βλ. Andrew Ferguson, υποσημείωση 25

αποτελεσματικότητα της εφαρμογής, οι πρώτες μελέτες ήταν αρκετά ενθαρρυντικές, καθώς τόσο στο Σικάγο όσο και στην Καλιφόρνια[35] παρατηρήθηκε μείωση της εγκληματικότητας.

Η λειτουργία του HunchLab, σε συνδυασμό με τα επιτυχή αποτελέσματά του έδωσε ώθηση στη δημιουργία πολλών εφαρμογών προληπτικής αστυνόμευσης που συνδυάζουν περισσότερες θεωρίες ανίχνευσης εγκλημάτων και στηρίζονται στο machine learning. Ταυτόχρονα άλλα προγράμματα που προϋπήρχαν ξεκίνησαν να τροποποιούνται ώστε να μπορούν να εφαρμόζουν συνδυαστικά το near repeat με το RTM. Χαρακτηριστική περίπτωση είναι το Precobs όπου κατά τη διαδικασία διαμόρφωσης του προληπτικού χάρτη λαμβάνονται υπόψη και γεωγραφικοί παράγοντες, όπως ο φωτισμός στους δρόμους. Βέβαια αυτό έχει σαν μειονέκτημα ότι οι αστυνομικές αρχές και οι αναλυτές θα πρέπει συνεχώς να ενημερώνουν τις βάσεις δεδομένων τους[36] και τους σχετικούς αλγόριθμους, για όποια αλλαγή σημειώνεται στο εξωτερικό περιβάλλον, έτσι ώστε να εξακολουθεί να λειτουργεί σωστά η εφαρμογή.

2.3 Ανθρωποκεντρικά συστήματα προληπτικής αστυνόμευσης

Ανθρωποκεντρικά συστήματα προληπτικής αστυνόμευσης χαρακτηρίζονται τα προγράμματα που έχουν σχεδιαστεί για να αξιολογούν τις πιθανότητες ενός ατόμου να διαπράξει ένα έγκλημα ή να είναι το θύμα μίας μελλοντικής εγκληματικής πράξης[37]. Η αξιολόγηση αυτή δεν βασίζεται σε γεωγραφικά στοιχεία, όπως συμβαίνει στα γεωγραφικά συστήματα, αλλά εστιάζει στον προσωπικό βίο και στο κοινωνικό υπόβαθρο του υποκειμένου, τα οποία περιλαμβάνουν πληροφορίες για την οικογενειακή του κατάσταση, το ποινικό μητρώο του και γενικότερα ερευνά το κοινωνικό δίκτυο (social media) στο οποίο εντάσσεται. Αξιολογώντας τα ανωτέρω στοιχεία προκύπτει μία αξιολόγηση επικινδυνότητας (risk score) του κάθε ατόμου που υποδεικνύει το κατά πόσο είναι πιθανό το συγκεκριμένο άτομο να εμπλακεί σε ένα έγκλημα.

---

[35] Andrew Ferguson (2020), Predictive Policing Theory, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=527000067124025069089116075074096108039003024042071075093075112088116121097095010067114102007027106035006118101122070002026084005082039040022094024066121104030086084045079095094027068065114126090080114084000092023070097004116118087010071028007111101&EXT=pdf&INDEX=TRUE

[36] Βλ. Degeling M and Berendt B υποσημείωση 20

[37] Kate Robertson, Cynthia Koo and Yolanda Song (2020), *TO SURVEIL AND PREDICT a human rights analysis of algorithmic policing in Canada*, University of Toronto

Κατά τη μαζική συλλογή και επεξεργασία των big data από τις αστυνομικές αρχές, παρατηρήθηκε ότι μοτίβα παραβατικότητας δεν υπάρχουν μόνο σε άξονα με τον τόπο του εγκλήματος, αλλά και σε άξονα με τα πρόσωπα που εμπλέκονται σε αυτά. Δηλαδή όπως ακριβώς υπάρχουν ορισμένα μέρη στην πόλη που στατιστικά είναι πιο πιθανό να διαπραχθεί κάποιο αδίκημα, έτσι ακριβώς υπάρχουν κατηγορίες ανθρώπων που είναι πιο πιθανό να εμπλακούν σε κάποιο έγκλημα, είτε ως δράστες είτε ως θύματα. Σημαντικότατο ρόλο στον καθορισμό της επικινδυνότητας κατέχει το κοινωνικό υπόβαθρο του κάθε ανθρώπου, όπως για παράδειγμα η οικονομική του κατάσταση, το μορφωτικό του επίπεδο ή το ποινικό μητρώο του. Η όλη αυτή φιλοσοφία αποτελεί προϊόν αρκετών ερευνών που πραγματοποιήθηκαν σε πολιτείες των ΗΠΑ τα τελευταία χρόνια[38]. Με αφορμή τις μελέτες για την καταπολέμηση της ένοπλης βίας, φαινόμενο που βρισκόταν σε έξαρση στις ΗΠΑ, παρατηρήθηκε ότι ένα μεγάλο ποσοστό των εμπλεκομένων προέρχονταν από τα ίδια κοινωνικά στρώματα. Ενώ δηλαδή η ένοπλη βία ήταν ένα πρόβλημα που βασάνιζε όλη τη χώρα, οι άμεσα εμπλεκόμενοι αποτελούσαν ένα πολύ μικρό ποσοστό του πληθυσμού[39]. Όπως διατυπώθηκε από ερευνητές στο Σικάγο, «ένας πολύ μικρός αριθμός συνοικιών της πόλης είναι υπεύθυνες για τα περισσότερα περιστατικά βίας. Το εγκληματολογικό πρόβλημα όλης της πόλης είναι στην πραγματικότητα γεωγραφικά και κοινωνικά συμπυκνωμένο σε λιγοστές ξεπεσμένες και κοινωνικά απομονωμένες γειτονιές. Επίσης τα δεδομένα αποκάλυψαν ότι τα περισσότερα θύματα (και δράστες) ένοπλης βίας στο Σικάγο τείνουν να είναι νεαροί αφροαμερικανοί πολίτες που μένουν σε γειτονιές στη δυτική ή νότια πλευρά της πόλης»[40]. Αυτές οι διαπιστώσεις είναι που γέννησαν την ιδέα ότι πέρα από τον τόπο μπορεί να πιθανολογηθεί και το πρόσωπο που θα εμπλακεί σε έγκλημα. Ευθύς αμέσως ξεκίνησαν τα πρώτα βήματα για την ανάπτυξη αποδοτικών ανθρωποκεντρικών συστημάτων προληπτικής αστυνόμευσης.

---

[38] Βλ. Andrew Ferguson, υποσημείωση 23

[39] Braga Antony, Webster Daniel, Michael White, and Hildy Saizow (2014), *Smart Approaches to Reducing Gun Violence*, διαθέσιμο σε pdf στο https://centerforimprovinginvestigations.org/wp-content/uploads/2018/08/SPI-Gun-Violence-Spotlight-FINAL-2014.pdf

[40] «very small number of neighborhoods in Chicago are responsible for most of the city's violence trends. The "city's" crime problem is in fact geographically and socially concentrated in a few highly impoverished and socially isolated neighborhoods. Data also revealed that most victims (and offenders) of gun violence in Chicago tend to be young African American men who live in neighborhoods on the West or South sides of the city.» Tracey Meares et al. (2009), Attention Felons: Evaluating Project Safe Neighborhoods in Chicago, Columbia Law School, διαθέσιμο σε pdf στο https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2393&context=faculty_scholarship

2.3.1 Παραδείγματα εφαρμογών

Οι ΗΠΑ, δικαιολογώντας για ακόμη μία φορά τον χαρακτηρισμό «μητέρα» της προληπτικής αστυνόμευσης, ήταν η χώρα που πρωτοστάτησε στη δημιουργία ανθρωποκεντρικών συστημάτων. Αρχικά το 2012, το αστυνομικό τμήμα του Σικάγο, προκειμένου να βρει μια λύση για την καταπολέμηση της ένοπλης βίας, δημιούργησε την SSL (Strategic Subjects List)[41], μία λίστα που περιλάμβανε με σειρά κατάταξης ατόμων που ήταν πιο επιρρεπή στο να αποτελέσουν θύτες ή θύματα περιστατικών ένοπλης βίας. Η λίστα χρησιμοποιούσε έναν αλγόριθμο που εξέταζε 11 μεταβλητές των υποκειμένων σχετικές με το ποινικό μητρώο τους. Για παράδειγμα αξιολογούσε το ιστορικό εγκληματικότητας, το αν ανήκουν σε κάποια συμμορία, το αν έχουν συλληφθεί ποτέ και αν η εγκληματική τους δραστηριότητα βρισκόταν σε έξαρση[42]. Η αξιολόγηση αυτή δημιουργούσε ένα σκορ επικινδυνότητας που καθόριζε την κατάταξη των υποκειμένων στη λίστα SSL. Βέβαια το πρόγραμμα τελικά κρίθηκε αναξιόπιστο με συνέπεια τον Ιανουάριο του 2020 να σταματήσει η χρήση του[43].

Την ίδια χρονική περίοδο άρχισαν να αναπτύσσονται εφαρμογές που εστίαζαν στην ανάλυση των κοινωνικών δικτύων των ανθρώπων. Η θεωρία των κοινωνικών δικτύων (Social Network Analysis, SNA) βασίζεται στην αντίληψη ότι οι ανθρώπινες σχέσεις μπορούν να παρέχουν πληροφορίες ή και να προβλέψουν μία ατομική συμπεριφορά[44]. Αυτό μπορεί να βοηθήσει τις αρμόδιες αρχές στο να αναλύσουν πως τα κοινωνικά δίκτυα επηρεάζουν τις εγκληματικές δραστηριότητες καθώς και να εντοπίσουν την ύπαρξη συμμοριών και εγκληματικών οργανώσεων μέσω της ανάλυσης κοινωνικών δικτύων. Αυτή η επεξεργασία μπορεί να συμβάλλει στην αποσυμφόρηση της εγκληματικότητας. Με βάση τη θεωρία αυτή αναπτύχθηκε από την ιδιωτική εταιρεία Palantir, μία εφαρμογή η οποία μέσω της SNA προσπαθούσε να εντοπίσει πολίτες που, λόγω των κοινωνικών τους επαφών, ήταν πιο πιθανό να εμπλακούν σε αξιόποινες πράξεις, είτε ως δράστες είτε ως θύματα. Αντίστοιχα στο Κάνσας δημιουργήθηκε το σύστημα SPI (Smart Policing Initiative)[45], το οποίο

---

[41] Βλ. Andrew Ferguson, υποσημείωση 25

[42] Βλ. Kate Robertson κ.α. υποσημείωση 35

[43] Sam Charles (2020), *CPD decommissions 'Strategic Subject List'*, διαθέσιμο στο https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson

[44] Andrew Papachristos and Michael Sierra-Arevalo (2018), *Policing the Connected World*, διαθέσιμο σε pdf στο https://cops.usdoj.gov/RIC/Publications/cops-w0859-pub.pdf

[45] Βλ. Braga Anthony κ.α. υποσημείωση 36

λειτουργούσε ακριβώς όπως το SSL στο Σικάγο, εφαρμόζοντας όμως την τεχνική της ανάλυσης κοινωνικών επαφών. Αξιολογώντας λοιπόν δεδομένα παραβατικότητας και δεδομένα συμμοριών, το πρόγραμμα προσπαθούσε να εντοπίσει κοινωνικά δίκτυα που θεωρούνταν κοινωνικές αποκλίσεις, καθώς και να βρει μία σύνδεση μεταξύ των αποκλίσεων αυτών. Έπειτα, ακριβώς όπως το SSL, αξιολογώντας τα ανωτέρω δεδομένα εντόπιζε τους πολίτες που είχαν ποινικό μητρώο και εντάσσονταν σε αυτά τα αποκλίνοντα δίκτυα και υπολόγιζε πόσο πιθανό ήταν να εμπλακούν σε ένοπλες επιθέσεις στο μέλλον.

Τέλος, άλλη μία εφαρμογή που χρήζει αναφοράς είναι η εφαρμογή LASER (Los Angeles Strategic Extraction and Restoration)[46]. Όπως και οι προαναφερθείσες εφαρμογές, έτσι και το LASER έχει ως στόχο τον εντοπισμό μελλοντικών παραβατών του νόμου. Αυτό που αλλάζει όμως είναι η μεθοδολογία. Αναλύοντας δεδομένα που προέρχονται από προγενέστερα εγκλήματα, η εφαρμογή δημιουργεί λίστες χρόνιων παραβατών (Chronic Offender Bulletins). Στις λίστες αυτές συγκαταλέγονται συγκεκριμένοι πολίτες, που είναι ιδιαίτερα πιθανό να επαναλάβουν βίαιες επιθέσεις ή μέλη συμμοριών με εγκληματική δράση σε μία συγκεκριμένη περιοχή. Αφού δημιουργηθούν οι λίστες, διανέμονται στα αστυνομικά τμήματα με σκοπό την παρακολούθηση και έρευνα των υπόπτων. Να σημειωθεί ότι, για λόγους που θα αναφερθούν και στη συνέχεια, το πρόγραμμα LASER δεν χρησιμοποιείται πλέον λόγω πολλών ασυνεπειών στη διαδικασία επιλογής των πολιτών και καταχώρισής τους στο σύστημα[47].

2.3.2 Εφαρμογές παρακολούθησης των μέσων κοινωνικής δικτύωσης (social media surveillance)

Στο πλαίσιο συλλογής δεδομένων σχετικά με την κοινωνική ζωή των πολιτών, άρχισαν να αναπτύσσονται εφαρμογές παρακολούθησης των μέσων κοινωνικής δικτύωσης. Τα τελευταία χρόνια, παρατηρείται παγκοσμίως ότι τα social media αποτελούν αναπόσπαστο κομμάτι της ανθρώπινης καθημερινότητας, σε σημείο όπου μελετώντας τις ενέργειες ενός ψηφιακού προφίλ, γίνεται αντιληπτή η κοινωνική ζωή του πραγματικού χρήστη του προφίλ καθώς και οι κοινωνικές επαφές του. Έτσι, οι εφαρμογές παρακολούθησης των social media περιέχουν έναν αλγόριθμο που συλλέγει προσωπικές πληροφορίες, αντλώντας στοιχεία

[46] Βλ. Ishmael Mugari υποσημείωση 15

[47] Tim Lau (2020), *Predictive Policing Explained*, διαθέσιμο στο https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

από τις διαδικτυακές δραστηριότητες και προσπαθεί να εντοπίσει μοτίβα συμπεριφοράς και κοινά σημεία επικοινωνίας μεταξύ των χρηστών.

Από τις πιο γνωστές εφαρμογές παρακολούθησης μέσων κοινωνικής δικτύωσης είναι η Media Sonar. Το λογισμικό αυτής της εφαρμογής επιτηρούσε τις αναρτήσεις δημοφιλών πλατφορμών, όπως το Twitter, το Facebook και το Instagram, εντόπιζε λέξεις-κλειδιά που σχετίζονταν με κάποια μορφής διαμαρτυρία, όπως για παράδειγμα το hashtag #BLACKLIVESMATTER[48], και ενημέρωνε τις αρχές ότι οι συγκεκριμένες αναρτήσεις αποτελούσαν απειλή για τη δημόσια ασφάλεια. Η εφαρμογή το 2016 απαγορεύθηκε από το Twitter και το Instagram, λόγω των κατάφορων παραβάσεων θεμελιωδών ανθρωπίνων δικαιωμάτων, τα οποία διασφαλίζονταν από τις πολιτικές απορρήτου των ανωτέρω εταιρειών[49].

Άλλη μία εφαρμογή ανάλυσης social media είναι η εφαρμογή Sysomos. Το πρόγραμμα αυτό δημιουργήθηκε τον Απρίλιο του 2018 από την εταιρεία Meltwater[50]. Ο τρόπος λειτουργίας του συστήματος είναι άγνωστος μέχρι στιγμής πάντως έχει ήδη αρχίσει να χρησιμοποιείται από τις αστυνομικές αρχές του Καναδά, των ΗΠΑ και του Ηνωμένου Βασιλείου[51].

2.3.3 Εφαρμογές αναγνώρισης προσώπου

Φυσικά, εφόσον το θέμα της συγκεκριμένης ενότητας είναι τα ανθρωποκεντρικά συστήματα προληπτικής αστυνόμευσης, δεν γίνεται να παραλειφθεί η βιομετρική μέθοδος της αναγνώρισης προσώπου. Σύμφωνα με το άρθρο 4 (14) του GDPR, βιομετρικά δεδομένα είναι τα δεδομένα που προέρχονται από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή

---

[48] Matt Cagle (2015), *This Surveillance Software is Probably Spying on #BlackLivesMatter*, διαθέσιμο στο https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter

[49] Amanda Margison (2017), Twitter and Instagram ban London, Ont., company for helping police track protesters, CBC, διαθέσιμο στο https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093

[50] Mike Butcher (2018), Media monitor Meltwater acquires social analytics player Sysomos, διαθέσιμο στο https://techcrunch.com/2018/04/24/media-monitor-meltwater-acquires-social-analytics-player-sysomos/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABgTMOxr-9vqeDB-Z6VyvYIn2tH63Qaonw5XP8wTQOORtzALT2qK4QZhDxmsWDLfXh77Cew1gn5DYeKCt1k2a_N_o4mfZsQQNtIClKTjKtumpG3t_JDL2l0Dt-qMkx8EFkhdEDHxKEvlw5DeBiR_hZgq_xfHdRtnnElcXGtqnI7g

[51] Rachel Cohn (2016), *Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide*, Brennar Center for Justice, διαθέσιμο στο https://www.brennancenter.org/our-work/analysis-opinion/mapping-reveals-rising-use-social-media-monitoring-tools-cities

επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου. Συνεπώς για να χαρακτηριστούν τα δεδομένα ως βιομετρικά θα πρέπει να έχει προηγηθεί ειδική επεξεργασία δεδομένων της ανθρώπινης φυσιολογίας με μηχανικά μέσα, η οποία έχει ως απόλυτο στόχο την ταυτοποίηση του υποκειμένου.

Στον χώρο της προληπτικής αστυνόμευσης, και πιο συγκεκριμένα στον τομέα των εφαρμογών αναγνώρισης προσώπου οι ανωτέρω προϋποθέσεις πληρούνται, γι' αυτό και οι συγκεκριμένες τεχνολογίες χαρακτηρίζονται ως βιομετρικές. Πιο συγκεκριμένα, το λογισμικό αναγνώρισης προσώπου αποτελεί μία τεχνολογία ταυτοποίησης, η οποία, με τη χρήση αλγορίθμων, ξεχωρίζει συγκεκριμένες διακριτικές λεπτομέρειες σχετικά με το πρόσωπο ενός ανθρώπου από μία φωτογραφία ή ένα βίντεο. Τέτοιες λεπτομέρειες, όπως για παράδειγμα η απόσταση μεταξύ των ματιών ή το μέγεθος της μύτης, μετατρέπονται σε δεδομένα τα οποία συγκρίνονται με δεδομένα άλλων προσώπων, που είχαν συλλεγεί και αποθηκευτεί προηγουμένως, σε μία βάση δεδομένων αναγνώρισης προσώπων[52]. Η αναγνώριση προσώπου έχει δύο τρόπους λειτουργίας. Ο πρώτος τρόπος περιλαμβάνει τη σύγκριση ενός προσώπου με μία συγκεκριμένη φωτογραφία ενός ανθρώπου σε μία βάση δεδομένων, με στόχο να επαληθευτεί ότι η ταυτότητα του ανθρώπου είναι αυτή που επικαλείται ο ίδιος (one-to-one). Ο δεύτερος τρόπος περιλαμβάνει τη σύγκριση ενός προσώπου με όλες τις φωτογραφίες της βάσης δεδομένων, ώστε να ταυτοποιηθεί ο ίδιος[53].

Αυτή η νέα ψηφιακή δυνατότητα ήταν μεν πολύ αποτελεσματική, καθώς συνεισφέρει τα μέγιστα στον γρήγορο εντοπισμό των εγκληματιών, παράλληλα όμως επιφέρει πολλαπλές παραβιάσεις ανθρωπίνων δικαιωμάτων, όπως θα αναλυθεί και εκτενώς στη συνέχεια. Μία από τις πιο σημαντικές, αλλά και πιο επικίνδυνη, εφαρμογή αναγνώρισης προσώπου είναι η εφαρμογή Clearview AI. Η εταιρεία αυτή ανέπτυξε ένα λογισμικό, το οποίο έχει τη δυνατότητα να συλλέγει φωτογραφίες πολιτών από τα μέσα κοινωνικής δικτύωσης (Facebook, Twitter, πλατφόρμες όπως YouTube, Venmo (ανήκει στην Paypal), αλλά και δημοσίως προσβάσιμων φωτογραφιών[54], στην συνέχεια τις επεξεργάζεται, προκειμένου να

---

[52] Jennifer Lynch (2018), *Face Off: Law Enforcement Use of Face Recognition Technology*, διαθέσιμο στο https://www.eff.org/wp/law-enforcement-use-face-recognition

[53] Future of Privacy Forum (2018), *Understanding Facial Detection, Characterization and Recognition Technologies*, διαθέσιμο σε pdf στο https://fpf.org/wp content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf

[54] CBS News (2020), *CEO speaks out about Clearview AI AI's controversial facial recognition technology*, διαθέσιμο σε μορφή βίντεο στο https://www.cbsnews.com/video/ceo-speaks-out-about-Clearview AI-ais-controversial-facial-recognition-technology/#x

εξαγάγει το βιομετρικό τους υπόδειγμα[55] και τις αποθηκεύει σε βάση δεδομένων. Αυτή η εφαρμογή διατίθεται προς πώληση σε κάθε ενδιαφερόμενο με την οποία μπορεί κανείς, εισάγοντας τη φωτογραφία ενός αγνώστου προσώπου, να αναζητήσει την ταυτοποίησή του από αυτή την βάση βιομετρικών δεδομένων της εταιρείας. Η απόκτηση και συλλογή του υλικού αυτού επιτυγχάνεται μέσω ενός εκτεταμένου «data scraping»[56] ήτοι «συγκομιδή ή απόξεση ή απόσπαση δεδομένων» η οποία γίνεται χειροκίνητα και συνηθέστερα λόγω του εξαιρετικά μεγάλου όγκου δεδομένων αυτοματοποιημένα με τη χρήση ειδικού λογισμικού, το οποίο στοχεύει στην απόσπαση δεδομένων που βρίσκονται στο διαδίκτυο και, πρακτικά, αποτελεί μια μορφή αντιγραφής δεδομένών, τα οποία συγκεντρώνονται για μεταγενέστερη ανάλυση και χρήση.

Για μεγάλο χρονικό διάστημα η ίδια η ύπαρξη της Clearview AI ήταν παντελώς άγνωστη. Ενώ η εταιρεία ιδρύθηκε το 2017, η πρώτη δημόσια αναφορά σε αυτήν πραγματοποιήθηκε τον Ιανουάριο του 2020 με άρθρο στις New York Times, που εξηγούσε τον τρόπο λειτουργίας του προγράμματος[57]. Τον επόμενο μήνα, διέρρευσαν έγγραφα από την εταιρεία που σχετίζονταν με το πελατολόγιό της. Σύμφωνα με τα στοιχεία αυτά η Clearview AI παρείχε τις υπηρεσίες τις σε πάνω από 600 αστυνομικές αρχές, σε όλον τον κόσμο, κυρίως σε αρχές των Ηνωμένων Πολιτειών[58] αλλά και σε ιδιώτες, όπως η Walmart και το NBA. Επιπλέον η εφαρμογή αποτελεί τη μεγαλύτερη βάση βιομετρικών δεδομένων παγκοσμίως, μιας και απαριθμεί σχεδόν 3 δισεκατομμύρια φωτογραφίες και η ακρίβεια ταυτοποίησης ξεπερνά το 99%, αποτελώντας ένα εξαιρετικά αποτελεσματικό εφόδιο για την αστυνομία, στον αγώνα της εξακρίβωσης εγκλημάτων.

Η διαρροή προκάλεσε θύελλα αντιδράσεων. Οι τεχνολογικοί κολοσσοί των μέσων κοινωνικής δικτύωσης, όπως το Twitter, η Google, το YouTube και το LinkedIn, καταδίκασαν την λειτουργία της Clearview AI και απαίτησαν να απέχει από κάθε παράνομη συμπεριφορά

[55] (μοναδικά χαρακτηριστικά της γεωμετρίας του προσώπου)
[56] Αδαμαντία Βολικού (2020), Η εποχή της "συγκομιδής" των προσωπικών δεδομένων, Homo Digitalis, διαθέσιμο στο https://www.homodigitalis.gr/posts/5046
[57] The New York Times (2020), *The Secretive Company That Might End Privacy as We Know It*, διαθέσιμο στο https://www.nytimes.com/2020/01/18/technology/Clearview AI-privacy-facial-recognition.html
[58] Ryan Mac, Caroline Haskins, Logan McDonald (2020), *Clearview AI's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA, Buzzfeed News*, διαθέσιμο στο https://www.buzzfeednews.com/article/ryanmac/Clearview AI-ai-fbi-ice-global-law-enforcement#4ldqpgc

και να άρει τυχόν προηγηθείσες ενέργειές της, ζητώντας να σταματήσει τη συλλογή δεδομένων και να διαγράψει όσα δεδομένα έχει ήδη συλλέξει από τις πλατφόρμες αυτές[59].

Η Ευρωπαϊκή Ένωση δεν έμεινε αμέτοχη. Τον Ιούνιο του 2020 το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB)[60], εξετάζοντας το ενδεχόμενο της χρήσης του λογισμικού Clearview AI, κατέληξε στο συμπέρασμα ότι οι αρχές μπορούν κάτω από συγκεκριμένες συνθήκες να χρησιμοποιούν τεχνικές αναγνώρισης προσώπου σε βάσεις δεδομένων που έχουν εγκατασταθεί σύμφωνα με το Κοινοτικό Δίκαιο ή το Δίκαιο της χώρας-μέλους[61], το Clearview AI όμως, δεν είναι συμβατό με το Ευρωπαϊκό Δίκαιο και τη δεδομένη στιγμή δεν μπορεί να χρησιμοποιηθεί από τις αρμόδιες αρχές. Παράλληλα η Γαλλική Αρχή Προστασίας Δεδομένων (CNIL), με το που διαπίστωσε παραβίαση έδωσε εντολή για διαγραφή των προσωπικών δεδομένων των κατοίκων της Γαλλίας[62] όπως και ο Επίτροπος προστασίας προσωπικών δεδομένων του Αμβούργου αντιστοίχως[63]. Ιδιαίτερα σημαντική είναι και η απόφαση που εξέδωσε η αρμόδια δικαστική αρχή στην Ιταλία τον Φεβρουάριο του 2022, η οποία επέβαλλε πρόστιμο 20 εκατομμυρίων ευρώ στην Clearview AI, απαγορεύοντας περαιτέρω την συλλογή και επεξεργασία βιομετρικών δεδομένων των Ιταλών πολιτών και διατάζοντας τη διαγραφή των σχετικών δεδομένων αναγνώρισης προσώπου[64]. Στην Ελλάδα έπειτα από ερώτηση που υποβλήθηκε από την ΜΚΟ Homo Digitalis ο Υπουργός Προστασίας του Πολίτη αρνήθηκε τη χρήση της εφαρμογής από την Ελληνική Αστυνομία[65].

---

[59] CNN Business (2020), *Is this facial recognition app going too far? We tested it*, διαθέσιμο σε βίντεο στο YouTube στο https://www.youtube.com/watch?v=pGJNXG2vmZw&ab_channel=CNNBusiness

[60] Περισσότερες πληροφορίες για το EDPB στο https://edpb.europa.eu/edpb_en

[61] Andrea Jelinek (2020), EDPB response to MEPs concerning the facial recognition app developed by Clearview AI, διαθέσιμο σε pdf στο https://edpb.europa.eu/sites/default/files/files/file1/edpb_lettertomepintveldonreviewpnrdirective.pdf

[62] Lawspot.gr (2021), *CLEARVIEW AI: Εντολή της CNIL για διαγραφή των προσωπικών δεδομένων των κατοίκων της Γαλλίας*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/Clearview AI-ai-entoli-tis-cnil-gia-diagrafi-ton-prosopikon-dedomenon-ton-katoikon-tis?fbclid=IwAR2d8kMgxof2tWqVH4u401lrN3P9KvmV0HrNJWWMx-u3Hz72ObTwBZ-yJ2A

[63] Δημήτρης Βέρρας (2021), *Clearview AI: Εντολή για διαγραφή βιομετρικών δεδομένων πολίτη από τον Επίτροπο Προστασίας Προσωπικών Δεδομένων Αμβούργου*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/Clearview AI-ai-entoli-gia-diagrafi-viometrikon-dedomenon-politi-apo-ton-epitropo-prostasias

[64] European Data Protection Board (2022), *Facial recognition: Italian SA fines Clearview AI EUR 20 million*, διαθέσιμο στο https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

[65] Κωνσταντίνος Ζουμπουλάκης και Κωνσταντίνος Κακαβούλης (2020), *Facial recognition και αντεγκληματική πολιτική: Μια βεβιασμένη συνύπαρξη*, διαθέσιμο στο https://www.homodigitalis.gr/posts/7258

Πέρα από την περίπτωση της Clearview AI, πολλές είναι οι περιπτώσεις όπου η τεχνολογία αναγνώρισης προσώπου δημιούργησε ανησυχίες στους πολίτες και τους θεσμούς. Το 2016 στις ΗΠΑ δημοσιεύτηκε μία αναφορά που γνωστοποιούσε ότι πολλά αστυνομικά τμήματα έκαναν ζωντανά (live) αναγνώριση προσώπων των πολιτών, από ζωντανό υλικό καμερών παρακολούθησης που ήταν εγκατεστημένες στους δρόμους[66]. Όπως ήταν λογικό αυτή η πρακτική φόβισε τους πολίτες, καθώς διεγείρονταν ζητήματα παραβίασης ανθρωπίνων δικαιωμάτων, όπως η ιδιωτικότητα και η ελευθερία του λόγου, καθώς και ζητήματα προκατάληψης. Αυτή η επικινδυνότητα ώθησε τους πολίτες και τους δημοκρατικούς θεσμούς, να απαιτήσουν να ρυθμιστεί νομοθετικά η τεχνολογία της αναγνώρισης προσώπου ζητώντας περισσότερη διαφάνεια. Μάλιστα πολλές πόλεις των Ηνωμένων Πολιτειών, όπως η Βοστώνη[67] και το Σαν Φρανσίσκο[68], απαγόρευσαν τη λειτουργία αυτής της τεχνολογίας στην επικράτειά τους. Το αποκορύφωμα της όλης αντίδρασης σημειώθηκε τον Ιούνιο του 2020. Τότε ήταν που η Επιτροπή Τεχνολογικής Πολιτικής των ΗΠΑ (US Technology Policy Committee, USTPC), του Συλλόγου Μηχανημάτων Υπολογισμού (Association for Computing Machinery, ACM), αιτήθηκε την άμεση διακοπή της ιδιωτικής και κυβερνητικής χρήσης της τεχνολογίας αναγνώρισης προσώπου, σε όλες τις περιπτώσεις που είναι γνωστό, ή αρκετά πιθανό, να θίγονται ανθρώπινα δικαιώματα[69]. Ταυτόχρονα ζητούσε την υιοθέτηση ενός καταλλήλου νομικού πλαισίου, το οποίο θα μπορούσε να ρυθμίσει την τεχνολογία με τέτοιο τρόπο, ώστε να μην παραβιάζονται τα δικαιώματα κανενός. Το αίτημα βασίστηκε σε αξιολογήσεις της τεχνολογίας αναγνώρισης προσώπου που έγιναν στο παρελθόν, και αποδείκνυαν ότι παρήγαγε αποτελέσματα που επιδείκνυαν προκατάληψη βασισμένη σε εθνικά, φυλετικά, γενετικά και άλλα ανθρώπινα χαρακτηριστικά, φέρνοντας πολλές φορές σε δυσμενή θέση τις μειονότητες του πληθυσμού των ΗΠΑ.

---

[66] Clare Garvie, Alvaro Bedoya, Jonathan Frankle (2016), *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, διαθέσιμο στο https://www.perpetuallineup.org/

[67] Jonathan Wilson (2020), *Boston City Council votes to ban facial-recognition tech*, διαθέσιμο στο https://eandt.theiet.org/content/articles/2020/06/boston-city-council-votes-to-ban-facial-recognition-tech/

[68] Kate Conger, Richard Fausset and Serge F. Kovaleski (2019), *San Francisco Bans Facial Recognition Technology*, New York Times, διαθέσιμο στο https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[69] ACM (2020), *ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies Cites Potential for Injury from Bias to Society's Most Vulnerable Populations*, διαθέσιμο στο https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies

2.3.4 Εφαρμογές προληπτικής αστυνόμευσης στην ποινική δικαιοσύνη

Αξίζει να γίνει ξεχωριστή αναφορά στα ανθρωποκεντρικά συστήματα εκτίμησης κινδύνου που χρησιμοποιούνται στον τομέα της Ποινικής Δικαιοσύνης. Σε αντίθεση με τα γεωγραφικά συστήματα, υπάρχουν αλγοριθμικά συστήματα που εντοπίζουν πολίτες και χρησιμοποιούνται κατά την προδικασία, κατά την ακροαματική διαδικασία και κατά τη διαδικασία επιβολής της ποινής από τον δικαστή[70]. Μία από τις πιο γνωστές εφαρμογές αυτού του είδους είναι η εφαρμογή COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) που χρησιμοποιείται από τα δικαστήρια των Ηνωμένων Πολιτειών. Κεντρική αποστολή του COMPAS είναι να αξιολογήσει πόσο πιθανό είναι ο κατηγορούμενος να διαπράξει ξανά έγκλημα[71]. Έχει καθαρά συμβουλευτικό ρόλο, καθώς βοηθά τον δικαστή να αποφασίσει αν είναι απαραίτητο ο κατηγορούμενος να εκτίσει την ποινή του στη φυλακή ή αν το ρίσκο δεν είναι πολύ μεγάλο να την εκτίσει εκτός φυλακής με επιτήρηση. Για την αξιολόγηση του κινδύνου ο αλγόριθμος του COMPAS περιέχει 43 ξεχωριστές κλίμακες που απαρτίζονται από 135 ερωτήσεις[72] οι οποίες απαντώνται από τον κατηγορούμενο ή από τα δεδομένα που έχει ήδη η αστυνομία. Οι ερωτήσεις εστιάζουν σε πολλές διαφορετικές πτυχές του κατηγορουμένου όπως η οικογενειακή του κατάσταση, το ποινικό μητρώο του και το εκπαιδευτικό και επαγγελματικό του υπόβαθρο.

Αντίστοιχα με την περίπτωση των ΗΠΑ, τα βρετανικά δικαστήρια και αστυνομικά τμήματα χρησιμοποιούν το σύστημα αξιολόγησης HART (Harm Assessment Risk Tool)[73]. Το σύστημα αυτό προβλέπει τον κίνδυνο υποτροπής των κρατουμένων. Βασίζεται σε έναν αλγόριθμο με 34 μεταβλητές εκ των οποίων οι 29 βασίζονται στο ιστορικό του δράστη και το ποινικό του μητρώο, ενώ οι υπόλοιπες 5 σχετίζονται με την ηλικία, το φύλο, τον ταχυδρομικό του κώδικα και το αν υπάρχουν προγενέστερες αναφορές από συστήματα προληπτικής αστυνόμευσης στο όνομά του[74]. Το πρόγραμμα HART εφαρμόζοντας τεχνικές machine learning υπολογίζει την πιθανότητα ενός ατόμου να διαπράξει σοβαρό έγκλημα, μη σοβαρό έγκλημα ή κανένα

---

[70] Βλ. Kate Robertson κ.α. υποσημείωση 35

[71] Βλ. Kate Robertson κ.α. υποσημείωση 35

[72] Jessica Gabel Cino (2018), *DEPLOYING THE SECRET POLICE: THE USE OF ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM*, Georgia State University Law Review, διαθέσιμο σε pdf στο https://www.courts.wa.gov/subsite/mjc/docs/2019/Deploying%20the%20Secret%20Police.pdf

[73] Matt Burgess (2018), *UK police are using AI to inform custodial decisions – but it could be discriminating against the poor*, διαθέσιμο στο https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit

[74] Marion Oswald (2018), *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, διαθέσιμο στο https://www.tandfonline.com/doi/full/10.1080/13600834.2018.1458455

έγκλημα κατά τα επόμενα 2 χρόνια. Με βάση αυτή την ανάλυση τα άτομα κατηγοριοποιούνται σε ομάδες υψηλού, μετρίου και χαμηλού κινδύνου αντίστοιχα. Η αξιολόγηση αυτή βοηθά τους κρατούμενους μετρίου και χαμηλού ρίσκου, καθώς τους δίνεται η δυνατότητα να συμμετέχουν σε προγράμματα απεξάρτησης εκτός φυλακής, εκτίοντας κατ' αυτόν τον τρόπο την ποινή τους.

2.4 Παραδείγματα άλλων προεγκληματικών εφαρμογών

Σε αυτό το σημείο είναι απαραίτητο να διευκρινιστούν ορισμένα ζητήματα. Οι εφαρμογές που αναλύθηκαν στις προηγούμενες ενότητες αναφέρθηκαν διότι είναι οι πιο δημοφιλείς στους αντίστοιχους τομείς και πολλές από αυτές μάλιστα εισήγαγαν ενδιαφέρουσες καινοτομίες στο χώρο της προληπτικής αστυνόμευσης. Αυτό βέβαια δεν σημαίνει ότι δεν υπάρχουν άλλες εφαρμογές προεγκληματικής δράσης. Ούτε σημαίνει ότι όλες οι μετέπειτα εφαρμογές βασίστηκαν στις προαναφερθείσες και λειτουργούν πανομοιότυπα. Αντιθέτως υπάρχουν αμέτρητες εφαρμογές που χρησιμοποιούνται αυτή τη στιγμή σε πάρα πολλές χώρες οι οποίες μάλιστα παρουσιάζουν μία ενδιαφέρουσα ποικιλομορφία. Ακόμα και εντός της ίδια χώρας δεν είναι ασυνήθιστο οι εφαρμογές προληπτικής αστυνόμευσης να διαφέρουν από πόλη σε πόλη[75]. Αυτό ακριβώς είναι και το αντικείμενο της συγκεκριμένης ενότητας.

Ενδεικτικά ένα δημοφιλές αλγοριθμικό σύστημα που βασίζεται στο risk terrain modeling αλλά λειτουργεί με έναν άκρως ιδιαίτερο τρόπο, είναι το λογισμικό ShotSpotter[76]. Όπως προκύπτει από το όνομα, το λογισμικό αυτό χρησιμοποιείται για τον εντοπισμό των πυροβολισμών ακόμα και αν η ανταλλαγή πυροβολισμών δεν έχει καταγγελθεί στην αστυνομία. Αυτό είναι εφικτό καθώς το πρόγραμμα συλλέγει δεδομένα από το οπτικό υλικό καμερών και από ειδικούς ανιχνευτές ήχου που είναι εγκατεστημένα σε διάφορα σημεία της πόλης και καταφέρνουν να ξεχωρίσουν τον πυροβολισμό από λοιπούς θορύβους της αστικής ζωής. Οι συσκευές αυτές είναι συνδεδεμένες με ένα κεντρικό σύστημα ελέγχου, το οποίο, αφού συλλέξει τα δεδομένα, εντοπίζει την ακριβή τοποθεσία του πυροβολισμού,

[75] Ενδεικτικά να αναφέρουμε το δικαστήριο στη Marcy County που έχει στην αποκλειστική του χρήση 3 εφαρμογές εκτίμησης κινδύνου, μία για προδικαστικές αποφάσεις, μία για ενδοοικογενειακή βία και άλλη μία για την επιτήρηση του κατηγορουμένου, πηγή βλ. Sarah Brayne and Angele Christin (2020), *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts*, Social Problems 2020

[76] Αναλυτικές πληροφορίες για την λειτουργία του λογισμικού είναι διαθέσιμες στο σχετικό site https://www.shotspotter.com/

συσχετίζοντας την ένταση του ήχου, την αντανάκλασή του στα κτίρια και το χρόνο ανίχνευσης θορύβου από τους αισθητήρες. Το ShotSpotter τη δεδομένη χρονική στιγμή χρησιμοποιείται σε παραπάνω από 100 πόλεις των ΗΠΑ με χαρακτηριστική επιτυχία.

Μιλώντας για γεωγραφικά συστήματα αξίζει να σημειωθεί ότι στη Γερμανία, παράλληλα με το Precobs, χρησιμοποιείται και το σύστημα GLADIS[77]. Πρόκειται για ένα πρόγραμμα, που αναλύοντας συγκεκριμένα εγκλήματα και δίνοντας έμφαση στο χρόνο τέλεσής τους, δημιουργεί χάρτες εγκληματικότητας και επισημαίνει τις περιοχές που χρήζουν περαιτέρω αστυνομικής επιτήρησης από τις συνηθισμένες περιπολίες. Αντίστοιχα στην Ολλανδία χρησιμοποιείται το σύστημα CAS (Crime Anticipation System)[78]. Πρόκειται για ακόμη ένα σύστημα γεωγραφικής αστυνόμευσης το οποίο έχει την ιδιαιτερότητα πως συνδυάζει δεδομένα εγκληματικών πράξεων με δημογραφικά και κοινωνικοοικονομικά δεδομένα. Αυτή η μίξη είναι που εντοπίζει εστίες μελλοντικών εγκλημάτων (hotspots) και ώρες αιχμής (hot times).

Ιδιαίτερα μεγάλη ποικιλομορφία παρατηρείται και στις εφαρμογές αναγνώρισης προσώπων. Η Γαλλία έχει δημιουργήσει ολόκληρες βάσεις δεδομένων αποκλειστικά για την αναγνώριση των πολιτών. Οι εγχώριες αστυνομικές αρχές χρησιμοποιούν συνδυαστικά τη βάση δεδομένων TAJ, το σύστημα Parafe για τον έλεγχο των συνόρων και τη βάση δεδομένων ALICEM για την αναγνώριση προσώπων[79]. Παράλληλα στην Κίνα, με πρόφαση την ασφάλεια του κράτους, έχουν τεθεί σε εφαρμογή πολλαπλά συστήματα παρακολούθησης πολιτών που βασίζονται στην αναγνώριση προσώπου. Η χρήση αυτών των συστημάτων είναι τόσο ολοκληρωτική και οι παραβιάσεις των ανθρωπίνων δικαιωμάτων τόσο έντονες, που κρίθηκε ορθότερο να αναλυθούν λεπτομερώς σε επόμενο κεφάλαιο.

Από τον κόσμο της προληπτικής αστυνόμευσης δεν απουσιάζει η Ελλάδα. Τον Μάρτιο του 2019 η ελληνική κυβέρνηση ανέθεσε το έργο έξυπνης αστυνόμευσης στην ιδιωτική εταιρεία Intracom με συνολικό προϋπολογισμό κοντά στα 4 εκατομμύρια ευρώ. Το έργο περιλαμβάνει τη χορήγηση έξυπνων φορητών συσκευών, σαν smartphones, στις αστυνομικές αρχές οι οποίες θα τα χρησιμοποιούν για ταυτοποίηση των πολιτών κατά τη διάρκεια των

[77] Βλ. Λ. Κανέλλος, υποσημείωση 4
[78] Cutting Crime Impact (CCI) (2020) *Fact Sheet: Predictive Policing*, διαθέσιμο σε pdf στο https://www.praeventionstag.de/html/download.cms?id=1026&datei=Factsheet_Predictive-Policing_English-1026.pdf
[79] Βλ. Λ. Κανέλλος, υποσημείωση 4

περιπολιών τους[80]. Η αναγνώριση των πολιτών θα γίνεται με λήψη φωτογραφίας ή δακτυλικών αποτυπωμάτων από τις συσκευές αυτές. Ο στόχος του προγράμματος είναι ο προσδιορισμός και η επαλήθευση της ταυτότητας των πολιτών κατά τον επιτόπιο έλεγχο, χωρίς να χρειάζεται να πάνε στο κοντινότερο αστυνομικό τμήμα για εξακρίβωση στοιχείων. Για να είναι πετυχημένη η ταυτοποίηση οι συσκευές είναι συνδεδεμένες με πολλαπλές βάσεις δεδομένων, τόσο εντός της χώρας όσο και με διεθνείς βάσεις δεδομένων όπως η Κεντρική Βάση Δεδομένων EURODAC, η Europol, αλλά και με υπερεθνικές βάσεις όπως η Interpol και το FBI. Ο αρχικός σχεδιασμός προβλέπει τη χορήγηση 1.000 φορητών έξυπνων συσκευών, με μακροπρόθεσμο στόχο ο τελικός αριθμός να ξεπεράσει τις 10.000[81].

2.5 Αξιολόγηση εφαρμογών προβλεπτικής αστυνόμευσης (και κίνδυνοι)

Αφού αναλύθηκε το σκεπτικό γύρω από τη δημιουργία εφαρμογών αλγοριθμικής αστυνόμευσης, καθώς και ο τρόπος λειτουργίας τους, ήρθε η ώρα να απαντηθεί η πιο κρίσιμη ερώτηση. Είναι αποτελεσματικές οι εφαρμογές αυτές; Η αλήθεια είναι πως η απάντηση μόνο απλή και εύκολη δεν είναι. Έχουν πραγματοποιηθεί πολλαπλές έρευνες πάνω σε αυτό το ερώτημα, με διαφορετικό όμως αποτέλεσμα. Υπάρχουν μελέτες που αποδεικνύουν ότι οι προβλέψεις των αλγοριθμικών συστημάτων είναι κατά βάση σωστές και το έγκλημα στην περιοχή που εφαρμόζονται αυτές έχει περιοριστεί. Ενδεικτικά, στο ίδιο το Site της PredPol καταγράφεται ότι το 2013 τα εγκλήματα μειώθηκαν κατά 20% στο Λος Άντζελες και κατά 19% στην Ατλάντα[82]. Επίσης, όπως αναφέρθηκε προηγουμένως, σύμφωνα με μελέτη που έγινε στη Ζυρίχη οι διαρρήξεις μειώθηκαν κατά 30% από τη στιγμή που η τοπική αστυνομική αρχή ξεκίνησε να χρησιμοποιεί το Precobs. Αντίστοιχες έρευνες με αισιόδοξο χαρακτήρα υπάρχουν και για άλλα συστήματα, γεωγραφικά και ανθρωποκεντρικά.

Από την άλλη πλευρά, μόνο μικρός δεν είναι ο αριθμός των ερευνών που υποδεικνύουν ότι αυτά τα συστήματα δεν επέφεραν καμία βελτίωση στην ποιότητα της αστυνόμευσης και την

---

[80] Κορίνα Πετρίδη (2021), Από αυτό το καλοκαίρι 1.000 φορητές συσκευές της ΕΛΑΣ θα σκανάρουν τα πρόσωπα των πολιτών σε περιπολίες, reporters united, διαθέσιμο στο https://www.reportersunited.gr/3643/apo-ayto-to-kalokairi-1-000-forites-syskeyes-tis-elas-tha-skanaroyn-ta-prosopa-ton-politon-se-kathimerines-peripolies/

[81] The Press Project (2021), «Προληπτική αστυνόμευση» με συσκευές αναγνώρισης προσώπου από την αστυνομία, διαθέσιμο στο https://thepressproject.gr/proliptiki-astynomefsi-me-syskeves-anagnorisis-prosopou-apo-tin-astynomia/

[82] Αναλυτικά οι επιδόσεις της PredPol είναι διαθέσιμες στο https://www.predpol.com/results/

αντιμετώπιση της εγκληματικότητας. Για παράδειγμα μία έρευνα που πραγματοποιήθηκε το 2018 στην πολιτεία του Κεντάκι από την καθηγήτρια νομικής Megan Stevenson[83], πάνω στα συστήματα προληπτικής αστυνόμευσης που χρησιμοποιεί η πολιτεία, απέδειξε ότι δεν είναι πολλά τα οφέλη των εφαρμογών αυτών ούτε μειώνουν σημαντικά την εγκληματικότητα. Οι σημαντικότερες όμως έρευνες είναι αυτές που έγιναν στην πολιτεία της Φλόριντα. Συγκεκριμένα στην περιοχή Πάσκο στην Φλόριντα το τοπικό αστυνομικό τμήμα ανέπτυξε μία δική του εφαρμογή πρόληψης εγκλημάτων[84]. Ύστερα από έρευνα παρατηρήθηκε ότι όχι μόνο δεν μειώθηκε ο αριθμός των εγκλημάτων στην περιοχή, αντιθέτως 21 οικογένειες ενοχλήθηκαν αδίκως από τις τοπικές αρχές, ενώ δεν υπήρχαν ενδείξεις παράνομων δραστηριοτήτων. Η σημαντικότερη ωστόσο μελέτη είναι αυτή που πραγματοποιήθηκε από τον μη κυβερνητικό οργανισμό ProPublica. Ο οργανισμός αυτός μελέτησε εξονυχιστικά τη λειτουργία του προγράμματος COMPAS[85] στο δικαστικό σύστημα της Φλόριντα. Κατά τη μελέτη του προγράμματος παρατηρήθηκε ότι η εκτίμηση κινδύνου των κατηγορουμένων ήταν ακραία άστοχη. Συγκεκριμένα μόλις το 20% των ανθρώπων που κρίθηκαν επικίνδυνοι να διαπράξουν σοβαρό έγκλημα υποτροπίασαν. Ακόμα και όταν διευρύνθηκε το πεδίο και συμπεριλήφθηκαν όλες οι αξιόποινες πράξεις που είναι πιθανό να διαπράξει κάποιος, ακόμα και τα λιγότερο σοβαρά αδικήματα (όπως οδήγηση με δίπλωμα που έχει λήξει), ο αλγόριθμος ήταν και πάλι άστοχος.

Το γεγονός ότι το αποτέλεσμα στις έρευνες δεν είναι το ίδιο, δημιουργεί μεγάλη σύγχυση. Αυτή η σύγχυση δεν μας βοηθά να καταλάβουμε αν η προληπτική αστυνόμευση είναι χρήσιμη στην παρεμπόδιση του εγκλήματος και έτσι καθίσταται αδύνατη η εδραίωση της στο Δικαιικό σύστημα. Μάλιστα πλήθος ερευνών που αποδεικνύουν την μείωση της εγκληματικότητας με τη βοήθεια των αλγοριθμικών συστημάτων διενεργούνται από τις

---

[83] Megan Stevenson (2018), *Assessing Risk Assessment in Action*, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=474090073005021098083067113102023086022027028059062003011090125000073006030003028000041101048107026028021105094003080117107026028085086079040085096087003102101081006026092079104102124019074066099094121069122125069019089011122092065099111029117120007114&EXT=pdf&INDEX=TRUE

[84] Kathleen Mcgrory and Neil Bedi (2020), *Targeted*, Tampa Bay Times, διαθέσιμο στο https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/

[85] Για ολόκληρη την έρευνα βλ. Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks*, ProPublica (2016), διαθέσιμο στο https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

ιδιωτικές εταιρείες που τα δημιούργησαν σε συνεργασία με ακαδημαϊκούς[86], γεννώντας κατ' αυτόν τον τρόπο έντονη δυσπιστία απέναντι στα συστήματα αυτά. Γιατί όμως συμβαίνει αυτό; Γιατί δεν είναι λειτουργική η αλγοριθμική αστυνόμευση; Η αλήθεια είναι ότι υπάρχουν πολλοί παράγοντες που λειτουργούν σαν τροχοπέδη. Αρχικά είναι πολύ πιο δύσκολο απ' όσο φαίνεται να συσχετιστεί η μείωση της εγκληματικότητας με τις προεγκληματικές εφαρμογές[87]. Το έγκλημα δεν είναι μια απλή ενέργεια, αλλά μια πολυδιάστατη πράξη που εξαρτάται από πολλαπλούς παράγοντες. Για παράδειγμα όσο σημαντικό μπορεί να είναι το μέρος για να διαπραχθεί το έγκλημα, άλλο τόσο σημαντικά είναι και άλλα στοιχεία, όπως το πόσο καλά περιπολείται μια περιοχή ή το κοινωνικό υπόβαθρο του δράστη. Συνεπώς, είναι φυσικό επόμενο και η αντιμετώπιση του εγκλήματος να βασίζεται σε πολλούς παράγοντες, γεγονός που καθιστά δυσχερή τον συσχετισμό ανάμεσα στη μείωση της εγκληματικότητας και στα υπολογιστικά συστήματα. Για να γίνει πιο κατανοητό θα χρησιμοποιηθεί ένα υποθετικό παράδειγμα του Precobs[88]. Η εφαρμογή εντοπίζει μία περιοχή κινδύνου και δίνεται η εντολή να αυξηθούν οι περιπολίες στην περιοχή αυτή. Εκεί υπάρχει ένας επίδοξος διαρρήκτης έτοιμος να παραβιάσει ένα σπίτι. Τον ακούει όμως ένας περαστικός και τηλεφωνεί στην αστυνομία. Τα κεντρικά της αστυνομίας ενημερώνουν τους αστυνομικούς που βρίσκονται σε περιπολία, και λόγω του Precobs είναι ήδη στην γειτονιά, και συλλαμβάνουν τον δράστη. Ακόμα και αν δεν υπήρχαν περιπολίες οι αστυνομικοί θα πήγαιναν στην περιοχή επειδή δέχτηκαν την κλήση. Άρα η επιτυχία οφείλεται στο Precobs ή όχι; Αυτό ακριβώς είναι και το πρόβλημα, το οποίο με τη σειρά του δυσκολεύει το έργο των αντίστοιχων ερευνών.

Επίσης, αντικείμενο δριμύτατης κριτικής αποτέλεσε το γεγονός ότι οι προβλεπτικές εφαρμογές είναι ικανές να προβλέψουν περιορισμένο αριθμό εγκλημάτων. Για παράδειγμα τα γεωγραφικά συστήματα είναι ικανά να προβλέψουν αποκλειστικά εγκλήματα περιουσιακής φύσεως, όπως αναφέρθηκε και προηγουμένως. Δεν έχει ανακαλυφθεί ακόμα κάποιο πρόγραμμα ικανό να προβλέπει όλα τα πιθανά εγκλήματα. Γι' αυτόν ακριβώς το λόγο οι επικριτές της προληπτικής αστυνόμευσης πιστεύουν ότι δεν πρέπει όλο το αστυνομικό και δικαστικό σύστημα να βασιστεί πάνω σε αυτές. Η αλήθεια είναι πως, επειδή

---

[86] Jeremiah Scanlan (2019), *Auditing Predictive Policing*, Brigham Young University Prelaw Review, διαθέσιμο σε pdf στο https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1302&context=byuplr

[87] Gerstner Dominik (2018), *Predictive Policing in the context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Wurttemberg*, European Journal for Security Research, διαθέσιμο σε pdf στο https://link.springer.com/article/10.1007/s41125-018-0033-0

[88] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

ο συγκεκριμένος χώρος είναι ακόμα υπό ανάπτυξη, ίσως να ήταν ορθότερο αυτές οι εφαρμογές να χρησιμεύουν σαν επιβοηθητικό εργαλείο και μόνο. Ακόμη, για να αντιμετωπιστεί η όλη σύγχυση και να γίνουν αποδεκτές αυτές οι εφαρμογές, θα πρέπει να διορθωθούν όλα τα προβλήματα που θίγουν οι ανωτέρω έρευνες. Επειδή τα προβλήματα αυτά εγκυμονούν σοβαρούς κινδύνους δέον είναι να αναλυθούν σε δικό τους κεφάλαιο.

2.5.1 Ο κίνδυνος των μη ποιοτικών δεδομένων.

Όπως έχει γίνει ήδη αντιληπτό, τα δεδομένα αποτελούν την «καρδιά» της προληπτικής αστυνόμευσης. Ο μοναδικός τρόπος για να αποκτήσει υπόσταση το όλο εγχείρημα είναι η επεξεργασία των δεδομένων που συλλέγονται, έτσι ώστε να βρεθούν μοτίβα συμπεριφοράς που θα καθιστούν με τη σειρά τους ευκολότερη την πρόβλεψη μελλοντικών εγκλημάτων. Αυτό λοιπόν που έχει ριζική σημασία είναι η λήψη και η επεξεργασία των κατάλληλων δεδομένων που οδηγούν σε ένα ακριβές συμπέρασμα. Δυστυχώς αυτό δεν είναι τόσο εύκολο όσο φαίνεται. Η απόκτηση των κατάλληλων δεδομένων έρχεται αντιμέτωπη με πολλές δυσκολίες, οι οποίες πολλές φορές οδηγούν στη συλλογή δεδομένων με ελλείψεις ή με κοινωνικές προκαταλήψεις, τα οποία ονομάζονται «κακά δεδομένα»[89].

Μπορεί η τελική πρόβλεψη των εγκλημάτων να πραγματοποιείται από υπολογιστικά συστήματα, ωστόσο τα δεδομένα που εισάγονται στο σύστημα προς επεξεργασία είναι προϊόντα ανθρώπινης δουλειάς. Πρόκειται για τα δεδομένα που συλλέγουν οι αστυνομικοί στον τόπο του εγκλήματος και επειδή σε κάθε ανθρώπινη δουλειά υπάρχει ο παράγοντας του λάθους έτσι και εδώ είναι πολύ πιθανό τα δεδομένα που συλλέγονται να είναι εσφαλμένα. Όταν διερευνάται μία σκηνή εγκλήματος, υπάρχουν, όπως είναι απόλυτα φυσιολογικό, πολλαπλές αβεβαιότητες και αρκετά άγνωστα στοιχεία σχετικά με την αξιόποινη πράξη[90]. Αυτή η αβεβαιότητα, κατά τη στιγμή της διερεύνησης, συνοδεύει και την παραγωγή των δεδομένων, τα οποία με τη σειρά τους μεταβιβάζονται στα συστήματα πρόληψης. Μάλιστα τέτοια λάθη μπορούν να συμβούν σε οποιοδήποτε στάδιο της αστυνομικής έρευνας. Παραδείγματος χάρη μπορεί να γίνει κάποιο λάθος στην αρχική συλλογή των στοιχείων, όταν ο αστυνομικός σημειώνει λανθασμένη οδό ή και στην μετέπειτα επεξεργασία όταν για παράδειγμα καταλάθος για την αποφυγή αντιγράφων διαγραφούν δεδομένα εγκλημάτων. Η αλήθεια είναι ότι τα τελευταία χρόνια

[89] Βλ. Andrew Ferguson, υποσημείωση 25
[90] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

πραγματοποιούνται ποιοτικοί έλεγχοι από την ίδια την αστυνομία σε όλα τα στάδια συλλογής και επεξεργασίας δεδομένων. Ωστόσο η αξιοπιστία των δεδομένων είναι ένα ζήτημα που πρέπει πάντοτε να θίγεται.

Ο σημαντικότερος κίνδυνος της χρήσης εφαρμογών προληπτικής αστυνόμευσης είναι η χρήση προκατειλημμένων δεδομένων. Αρχικά για να μπορέσει ένα έγκλημα να αξιοποιηθεί ως εγκληματολογικό δεδομένο θα πρέπει να ανιχνευθεί από την ίδια την αστυνομία ή να αναφερθεί σε αυτήν[91]. Τα εγκλήματα τα οποία δεν εντοπίζονται, και τα οποία είναι πολλά, δεν μπορούν να αποτελέσουν αντικείμενο μελέτης προληπτικής αστυνόμευσης καθιστώντας έτσι την αλγοριθμική αστυνόμευση περιορισμένη. Τα εγκλήματα ιδιοκτησίας, όπως η διάρρηξη και η κλοπή, αναφέρονται συχνά από τα θύματα στις αρχές επειδή σχετίζονται με ζητήματα ιδιωτικής ασφάλισης συνεπώς οι σχετικές εφαρμογές (Precobs κλπ.) είναι αρκετά αποδοτικές. Άλλες κατηγορίες εγκλημάτων όμως, όπως η εμπορία ναρκωτικών ανιχνεύονται και εντοπίζονται πολύ πιο δύσκολα. Ως συνέπεια τα δεδομένα που προκύπτουν από αυτά τα εγκλήματα μόνο αντιπροσωπευτικά δεν είναι και όποια εκτίμηση προκύπτει είναι άστοχη καθώς κατονομάζονται περιοχές σαν hotspots απλά και μόνο διότι υπάρχουν δεδομένα για αυτές.

Το ίδιο πρόβλημα μπορεί να προκληθεί από ορισμένες πρακτικές που εφαρμόζει η ίδια η αστυνομία. Η αλήθεια είναι ότι δεν επιτηρούνται όλες οι περιοχές με τον ίδιο τρόπο, ούτε οι περιπολίες διανέμονται ισόποσα σε όλη την πόλη. Αντιθέτως υπάρχουν περιοχές που έχουν αυστηρότερη αστυνομική επίβλεψη, όπως οι γειτονιές που μένουν μετανάστες και εθνικές μειονότητες, φτωχικές γειτονιές και περιοχές που έχουν καταφύγιο άστεγοι ή συχνάζουν χρήστες ναρκωτικών[92]. Ως αποτέλεσμα τα εγκλήματα που τελούνται σε αυτά τα μέρη είναι πιο πιθανό να εντοπιστούν από τις αρχές και να αποτελέσουν εγκληματολογικά δεδομένα. Έτσι οι εγκληματολογικές αναλύσεις που γίνονται πάνω σε αυτά τα δεδομένα τείνουν να δείχνουν ότι τα ποσοστά εγκληματικότητας σε αυτά τα μέρη είναι πολύ υψηλά δικαιολογώντας κατ' αυτόν τον τρόπο την ήδη αυστηρή επιτήρηση[93]. Ουσιαστικά μία εξ αρχής προκατειλημμένη πρακτική είναι υπεύθυνη για τη δημιουργία ενός προκατειλημμένου αποτελέσματος. Πρόκειται για λανθασμένο συλλογισμό καθώς το

[91] Biderman A D and Reiss A J (1967), *On Exploring the "Dark Figure'' of Crime*, The Annals of the American Academy of Political and Social Science

[92] Chavis K (2019), *The Pitfalls of Police Technology: A Minority Report*, The Cambridge Handbook of Policing in the United States

[93] Βλ. Andrew Ferguson, υποσημείωση 25

έγκλημα δεν σχετίζεται με συγκεκριμένους ανθρώπους και κοινωνικές τάξεις. Αντιθέτως υπάρχει σε όλα τα μέρη και σε όλα τα κοινωνικά σύνολα που σημαίνει ότι ο αστυνομικός έλεγχος θα πρέπει να γίνεται παντού χωρίς διακρίσεις αν θέλουμε να έχουμε ακριβή δεδομένα. Ειδάλλως όπως πολύ σωστά το έθεσε η καθηγήτρια νομικής Shima Baradaran αν οι περισσότερες έρευνες γίνονται σε μαύρους πολίτες το σύνολο των συλληφθέντων που προκύπτει δεν αντιπροσωπεύει όλους τους παραβάτες, αλλά μάλλον δυσανάλογα αντιπροσωπεύει τους μαύρους πολίτες[94].

Ο εντοπισμός περισσότερων εγκλημάτων στις περιοχές αυτές λόγω των προκατειλημμένων πρακτικών που αναφέρθηκαν έχει ως αποτέλεσμα να «επαληθεύεται» η αρχική προκατάληψη, καθώς ανιχνεύονται εγκλήματα τα οποία ήταν πολύ πιθανό να γίνουν βάσει των δεδομένων που είχαν οι αρχές[95]. Έτσι τα προεγκληματικά συστήματα μετατρέπονται από μηχανισμούς πρόβλεψης σε αυτοεκπληρούμενες προφητείες καθώς δεν κάνουν τίποτε άλλο πέρα από το να δημιουργούν τον ίδιο κίνδυνο εγκληματικότητας που σκοπεύουν να προβλέψουν. Αυτό που πρέπει να γίνει αντιληπτό είναι ότι, όπως το τόνισε και ο δικηγόρος Hanni Fakhoury, ο αλγόριθμος δεν πρόκειται να δείξει κάτι διαφορετικό από αυτό για το οποίο προγραμματίστηκε. Αν τα δεδομένα που εισάγονται σε αυτόν δείχνουν ότι τα περισσότερα εγκλήματα τα τελούν μαύροι πολίτες, τότε οι προβλέψεις του προγράμματος θα στρέφονται κατά των μαύρων πολιτών. Συνεπώς αν τα δεδομένα του αλγορίθμου είναι προκατειλημμένα, εξίσου προκατειλημμένα θα είναι και τα αποτελέσματα της επεξεργασίας[96].

Ο κίνδυνος των προκατειλημμένων δεδομένων δεν αποτελεί έναν θεωρητικό προβληματισμό αντιθέτως είναι η ωμή πραγματικότητα. Υπάρχουν πολλές έρευνες που

---

[94] "As law enforcement dedicates more of its resources to patrolling and investigating blacks in urban areas, the resulting arrest population is not a proportional representation of all offenders, but rather disproportionately represents black citizens." Shima Baradaran (2013), *Race, Prediction, and Discretion*, διαθέσιμο σε pdf στο https://www.gwlr.org/wp-content/uploads/2018/04/81-Geo.-Wash.-L.-Rev.-157.pdf

[95] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

[96] «It ends up being a self-fulfilling prophecy. . . . The algorithm is telling you exactly what you programmed it to tell you. "Young black kids in the south side of Chicago are more likely to commit crimes," and the algorithm lets the police launder this belief. It's not racism, they can say. They are making the decision based on what the algorithm is, even though the algorithm is going to spit back what you put into it. And if the data is biased to begin with and based on human judgment, then the results the algorithm is going to spit out will reflect those biases.» Απόσπασμα από Bryan Llenas (2014), *Brave New World Of 'Predictive Policing' Raises Specter Of High-Tech Racial Profiling*, Fox News, διαθέσιμο στο https://www.foxnews.com/world/brave-new-world-of-predictive-policing-raises-specter-of-high-tech-racial-profiling

αποδεικνύουν ότι οι εφαρμογές προληπτικής αστυνόμευσης λειτουργούν με διακρίσεις. Η σημαντικότερη από αυτές είναι η έρευνα της ProPublica[97] το 2016 που αναφέρθηκε και προηγουμένως. Αυτός ο μη κυβερνητικός οργανισμός διαπίστωσε ότι η εφαρμογή COMPAS δρα με προκατάληψη απέναντι στους μαύρους κατηγορουμένους. Ο αλγόριθμος είχε την τάση να χαρακτηρίζει εσφαλμένα ως μελλοντικούς εγκληματίες τους μαύρους, κάνοντας αυτό το λάθος με τη διπλάσια συχνότητα απ' ότι με τους λευκούς. Πιο συγκεκριμένα το 44,9% των αφροαμερικανών κατηγορουμένων χαρακτηρίστηκαν εγκληματίες υψηλού κινδύνου ενώ δεν υποτροπίασαν, με το αντίστοιχο ποσοστό των λευκών κατηγορουμένων να είναι 23,5%. Αντίθετα το 47,7% των λευκών κρίθηκαν ως χαμηλού κινδύνου εγκληματίες αλλά παρ' όλα αυτά τέλεσαν έγκλημα στο μέλλον, ενώ το αντίστοιχο ποσοστό στους αφροαμερικανούς ήταν 28%. Το φοβερό της υπόθεσης είναι ότι αυτή η ανισότητα δεν δικαιολογείται από το ιστορικό των κατηγορουμένων. Η ProPublica προχώρησε σε εκ νέου αξιολόγηση απομονώνοντας την επίδραση της φυλής από το ποινικό μητρώο καθώς και από την ηλικία και το φύλο του κατηγορουμένου[98]. Πάλι όμως ήταν κατά 77% πιθανότερο οι αφροαμερικανοί κατηγορούμενοι να χαρακτηριστούν ως υψηλού κινδύνου εγκληματίες. Ακόμη μία σημαντική έρευνα που πραγματοποιήθηκε πάλι από ΜΚΟ είναι η έρευνα[99] στην πόλη Oakland στην Καλιφόρνια που πραγματοποιήθηκε από την Human Rights Data Analysis Group. Η οργάνωση αυτή βρήκε πως ο αλγόριθμος που χρησιμοποιούσε η τοπική αστυνομία για να εντοπίσει εγκλήματα σχετικά με ναρκωτικά στόχευε περιοχές που κατοικούσαν Λατίνοι και Αφροαμερικανοί, παρόλο που υπήρχαν αποδεικτικά στοιχεία που υποδείκνυαν ότι η χρήση ναρκωτικών ήταν ομοιόμορφα διασκορπισμένη σε όλη την πόλη Oakland. Απ' ότι φαίνεται λοιπόν το επιχείρημα ότι είναι προτιμότερο να χρησιμοποιούμε μηχανές στις δουλειές μας διότι είναι αντικειμενικές και δεν κάνουν λάθη είναι απόλυτα άστοχο.

2.5.2 Ο κίνδυνος της προκατειλημμένης αστυνόμευσης

Η προκατάληψη δεν σταματάει στη σφαίρα των ψηφιακών δεδομένων. Η χρήση των προληπτικών συστημάτων ενδέχεται να επηρεάσει άμεσα τους ίδιους τους αστυνομικούς

---

[97] Βλ. Julia Angwin, Jeff Larson κλπ. Υποσημείωση 85

[98] Για το πως έγινε η ανάλυση του αλγορίθμου του COMPAS βλ. Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin (2016), *How We Analyzed the COMPAS Recidivism Algorithm*, ProPublica, διαθέσιμο στο https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

[99] Aaron Shapiro (2017), *Reform predictive policing*, διαθέσιμο στο https://www.nature.com/articles/541458a

και να τους ωθήσει σε διακριτικές συμπεριφορές. Όπως το υπογράμμισαν οι Simon Egbert και Matthias Leese στην έρευνα που έκαναν στις περιοχές της Γερμανίας και της Ελβετίας αξιολογώντας το πρόγραμμα Precobs[100], το ρίσκο που μπορεί να χαρακτηρίσει μία περιοχή ως περιοχή κινδύνου ή hotspot ενδέχεται να μεταφερθεί και στους ίδιους τους κατοίκους της περιοχής. Πρόκειται για μία υπόθεση σύμφωνα με την οποία όλοι οι άνθρωποι που ζουν σε κακόφημες συνοικίες αντιμετωπίζονται από την αστυνομία σαν να έχουν την «ηθική ευθύνη» της ίδιας της περιοχής. Ουσιαστικά δημιουργείται μία γενικευμένη υποψία[101] απέναντι στους κατοίκους και αφαιρείται η ατομική συμπεριφορά που καθιστά ύποπτο ένα συγκεκριμένο άτομο. Αρκεί να είσαι κάτοικος μίας περιοχής κινδύνου για να θεωρηθείς ύποπτος.

Αυτός ο χωρικός διαχωρισμός που πραγματοποιείται από τα προγράμματα γεωγραφικής αστυνόμευσης δημιουργεί και διάκριση στις ίδιες αστυνομικές συμπεριφορές. Αλλιώς λειτουργεί μια περιπολία σε μία θεωρητικά ασφαλή περιοχή και αλλιώς σε μία περιοχή κινδύνου. Στα hotspot η αστυνομία πραγματοποιεί περισσότερες και πιο άμεσες ενέργειες, που πολλές φορές χαρακτηρίζονται και ως υπέρβαση εξουσίας. Οι σωματικοί έλεγχοι και οι ταυτοποιήσεις περαστικών γίνονται συχνότερα απ' ότι σε άλλα μέρη, χωρίς να συνοδεύονται από κάποια αιτιολογημένη υποψία, μεταφέροντας κατ' αυτόν τον τρόπο την επικινδυνότητα της περιοχής στους ίδιους τους κατοίκους της. Η αντίληψη ότι αρκεί να είναι κάποιος κάτοικος μίας κακόφημης περιοχής για να θεωρηθεί επικίνδυνος για μελλοντικό έγκλημα μπορεί να ενθαρρύνει τους αστυνομικούς να εντοπίζουν ύποπτες συμπεριφορές ενώ στην πραγματικότητα δεν υπάρχουν[102].

Όπως αποδείχτηκε από την προηγούμενη ενότητα, τα ίδια τα δεδομένα φέρουν τον κίνδυνο να είναι προκατειλημμένα και να λειτουργούν διακριτικά έναντι ορισμένων μειονοτήτων. Το πρόβλημα αυτό ενυπάρχει και σε επόμενο επίπεδο καθώς η αστυνομία με τις πρακτικές της μπορεί να διαιωνίζει αυτά τα στερεότυπα. Αφού λοιπόν τους δοθεί ο διαμορφωμένος

---

[100] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

[101] Andrew Guthrie Ferguson (2017), *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York: New York University Press

[102] Elizabeth Joh (2014), *POLICING BY NUMBERS: BIG DATA AND THE FOURTH AMENDMENT*, Washington Law Review, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=084013121017005086024085098122023109118032061048043044009117116089082113106095070092005049039026020056054098121095081124102064108057014069082025064085001073095056085047013088090015025001095098077124075093095089097110015002080079021007112071065069&EXT=pdf&INDEX=TRUE

χάρτης που χαρακτηρίζει ως επικίνδυνες περιοχές που ζουν διάφορες μειονότητες, μιας και τα δεδομένα δεν είναι τα καταλληλότερα, οι αστυνομικές αρχές αυξάνουν τις περιπόλους σε αυτά τα μέρη οι οποίες είναι και πολύ πιο σκληρές. Έτσι από την μία οι μειονότητες καταλήγουν να είναι δέκτες εξονυχιστικών ελέγχων από την αστυνομία, και από την άλλη ισχυροποιείται το στερεότυπο ότι αυτές οι μειονότητες είναι απολύτως υπεύθυνες για τα περισσότερα εγκλήματα στην πόλη. Το στερεότυπο αυτό, όπως αναφέρθηκε και προηγουμένως, είναι πέρα για πέρα ανακριβές. Δεν υπάρχουν κατηγορίες ανθρώπων που παρανομούν περισσότερο από άλλες, υπάρχουν εγκλήματα που εντοπίζονται πιο δύσκολα. Είναι απαραίτητο να διευκρινιστεί ότι η αλγοριθμική εκτίμηση κινδύνου δεν πρέπει να συνοδεύεται από νομικές εξαιρέσεις και ακραίες πρακτικές. Όπως το λέει και το ίδιο το όνομα, είναι πρόβλεψη ρίσκου, όχι εντοπισμός υπαρκτού κινδύνου που καθιστά αναγκαία την επέμβαση των διωκτικών αρχών.

2.5.3 Ο κίνδυνος της διαφάνειας

Η έννοια της διαφάνειας υποδηλώνει τη δυνατότητα ενός οποιουδήποτε ανθρώπου να εξετάσει πλήρως τη λειτουργία ενός συστήματος. Στην περίπτωση της προληπτικής αστυνόμευσης η διαφάνεια έγκειται στη δυνατότητα του πολίτη να μάθει το λόγο που το πρόγραμμα τον χαρακτήρισε υψηλού κινδύνου ύποπτο για κάποιο μελλοντικό έγκλημα, καθώς και στη δυνατότητα της ίδιας της αστυνομίας να αιτιολογήσει πως λειτουργεί το σύστημα. Λόγω του ότι οι προεγκληματικές εφαρμογές σχετίζονται άμεσα με θεμελιώδη ανθρώπινα δικαιώματα, όπως το τεκμήριο αθωότητας και το δικαίωμα σε δίκαιη δίκη, η διαφάνεια των συστημάτων πρέπει να αποτελεί προτεραιότητα[103].

Η σκληρή πραγματικότητα είναι ότι η αλγοριθμική αστυνόμευση δεν παρέχει διαφάνεια και αυτό οφείλεται σε πολλούς λόγους. Αρχικά η ίδια η φύση των αλγορίθμων είναι αρκετά περίπλοκη. Πρόκειται για πολλαπλές σύνθετες μαθηματικές πράξεις που πραγματοποιούνται εξ ολοκλήρου από υπολογιστικά συστήματα, τα οποία με τη μέθοδο του machine-learning λαμβάνουν ορισμένες αποφάσεις. Αυτός ο πολύπλοκος σχεδιασμός καθιστά σχεδόν αδύνατο να γίνει κατανοητός ο όλος μηχανισμός από τους ανθρώπους. Η επεξεργασία και αξιολόγηση των δεδομένων πραγματοποιείται με τόσο σύνθετο τρόπο που

[103] Erik Bakke (2018), *Predictive Policing: The Argument for police Transparency*, NYU Annual. Survey of American Law, διαθέσιμο σε pdf στο https://annualsurveyofamericanlaw.org/wp-content/uploads/2019/08/74-1-Predictive-Policing-The-Argument-for-Public-Transparency.pdf

πολλές φορές είναι δύσκολο ακόμα και για τους ίδιους τους τεχνικούς αναλυτές να γίνει αντιληπτό[104]. Πρόκειται για το πρόβλημα του μαύρου κουτιού (black-box)[105] σύμφωνα με το οποίο είναι ορατές στο κοινό μόνο οι εισροές και οι εκροές (inputs and outputs) ενός συστήματος και όχι οι εσωτερικές του διαδικασίες και ο πηγαίος κώδικας (source code). Το πρόβλημα του μαύρου κουτιού δεν αφορά μόνο τους πολίτες αλλά και όλους τους κοινωνικούς φορείς, ιδίως την αστυνομία. Οι αστυνομικοί λαμβάνουν τα αποτελέσματα των προληπτικών συστημάτων, όμως λόγω της πολυπλοκότητάς τους δεν γνωρίζουν πως προέκυψαν και τι μαθηματικές πράξεις προηγήθηκαν. Μπορούν δηλαδή να δουν αν το σύστημα δουλεύει (εξετάζοντας τα αποτελέσματα), αλλά δεν μπορούν να δουν τον μηχανισμό πίσω από αυτό[106].

Σημαντικός παράγοντας που εντείνει το φαινόμενο του μαύρου κουτιού, είναι οι ιδιωτικές εταιρείες που κατασκευάζουν τα συγκεκριμένα λογισμικά. Οι εταιρείες κολοσσοί πίσω από την προληπτική αστυνόμευση αρνούνται να παρέχουν πληροφορίες σχετικά με τη λειτουργία του λογισμικού τους όπως ο αλγόριθμος, οι μεταβλητές και οι βάσεις δεδομένων που αξιοποιούνται, καθώς και τα επίπεδα αξιοπιστίας και αποτελεσματικότητας του συστήματος[107]. Η εγκατάσταση των προληπτικών συστημάτων από τις αρχές μπορεί να αποφέρει κέρδος πολλών εκατομμυρίων στους κατασκευαστές. Λόγω αυτού του οικονομικού ενδιαφέροντος οι ιδιωτικές εταιρείες δεν επιθυμούν να δημοσιεύσουν τη λειτουργία του λογισμικού τους για να μην αποτελέσει αντικείμενο αντιγραφής ο πηγαίος κώδικάς τους από ανταγωνιστές. Ως αποτέλεσμα οι πωλητές τεχνολογιών αστυνόμευσης ασκούν παρασκηνιακά πιέσεις στους αστυνομικούς φορείς να αγοράσουν το πρόγραμμά τους[108], χωρίς να έχει προηγηθεί επαρκής έλεγχος του λογισμικού, προστατεύοντάς το παράλληλα επικαλούμενοι εμπορικές συμφωνίες και μυστικά αλλά και νόμους διανοητικής ιδιοκτησίας[109].

---

[104] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

[105] Tom Simonite (2017), *AI Experts Want to End 'Black Box' Algorithms in Government*, διαθέσιμο στο https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/

[106] Βλ. Andrew Ferguson, υποσημείωση 25

[107] Βλ. Kate Robertson, Cynthia Koo and Yolanda Song υποσημείωση 35

[108] Jeff Gray (2016), Could a controversial gun-surveillance system help tackle Toronto crime?, The Globe and Mail, διαθέσιμο στο https://www.theglobeandmail.com/news/toronto/technology-offers-police-more-than-a-shot-in-the-dark/article30773005/

[109] Andrew D. Selbst (2017), *Disparate Impact in Big Data Policing*, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=535088111116102116000012094117081122000020077035034062072086122067098087127117106098056017035063031005018100101072115081092082121026023010011084 1

Για να γίνουν περισσότερο κατανοητές οι τακτικές των εταιρειών θα ακολουθήσει μία σύντομη αναφορά σε μία δικαστική υπόθεση. Πρόκειται για την υπόθεση State v. Loomis[110]. Στην υπόθεση αυτή, ο Eric Loomis κατηγορήθηκε για την οδήγηση ενός αυτοκινήτου, το οποίο ενεπλάκη σε ένοπλη επίθεση. Ο κατηγορούμενος, ενώπιον του Δικαστηρίου του Γουισκόνσιν, παραδέχτηκε ότι ήταν ο οδηγός του οχήματος, χωρίς όμως να έχει συμμετοχή στους πυροβολισμούς. Κατά την προδικαστική έρευνα, χρησιμοποιήθηκε η εφαρμογή COMPAS για την αξιολόγηση του κατηγορουμένου. Το COMPAS έκρινε πως ο Loomis είναι υπότροπος «υψηλού κινδύνου» («high-risk recidivist») και ότι αποτελεί σοβαρό κίνδυνο για την κοινωνία[111]. Λαμβάνοντας υπόψιν την ανωτέρω εκτίμηση κινδύνου, καθώς και τις κατηγορίες που επιβλήθηκαν, το Δικαστήριο επέβαλε στον κατηγορούμενο την ανώτατη δυνατή ποινή, βάσει των κατηγοριών. Η υπεράσπιση αιτήθηκε να διεξαχθεί εκ νέου η δίκη καθώς παραβιάστηκε το δικαίωμα του κατηγορουμένου σε δίκαιη δίκη, σύμφωνα με το οποίο η ποινή που επιβάλλεται πρέπει να βασίζεται σε ακριβείς πληροφορίες, κάτι που δεν συνέβη σε αυτή την περίπτωση μια και η πολιτεία του Γουισκόνσιν (State), δεν παρείχε πληροφορίες στον κατηγορούμενο για το πως ακριβώς χρησιμοποιήθηκε το COMPAS στην υπόθεσή του, ούτε τον ενημέρωσε για τον τρόπο που αποφασίστηκε η εκτίμηση κινδύνου (risk score) και για το ποιοι παράγοντες λήφθηκαν υπόψιν[112]. Αυτό συνέβη επειδή η κατασκευάστρια εταιρεία Northpointe επικαλέστηκε το ιδιοκτησιακό της καθεστώς και ότι η λειτουργία του προγράμματος είναι εμπορικό μυστικό. Απ' ότι φαίνεται η επίκληση αυτή ήταν αρκετή, αφού το δικαστήριο του Γουισκόνσιν έκρινε ότι δεν παραβιάστηκε το δικαίωμα του κατηγορουμένου σε δίκαιη δίκη λόγω της έλλειψης πληροφόρησης. Συγκεκριμένα παραδέχτηκε ότι η εκτίμηση κινδύνου δεν επεξηγεί από μόνη της τον τρόπο επεξεργασίας δεδομένων από το COMPAS, αλλά η αξιολόγηση του κατηγορουμένου βασίστηκε σε ελεύθερα διαθέσιμες πληροφορίες, όπως το ποινικό του μητρώο και το γενικότερο του ιστορικό. Επομένως εφόσον ο κατηγορούμενος μπορούσε να αποκρούσει αυτές τις πληροφορίες, δεν παραβιάστηκε το δικαίωμα σε δίκαιη δίκη. Μάλιστα ήταν από τότε γνωστό

271261020300301240230170480090901141050920640310260960750960051230180690070680761240940641001200220090970870&EXT=pdf&INDEX=TRUE

[110] Ολόκληρο το κείμενο της απόφασης είναι διαθέσιμο στο https://www.courts.ca.gov/documents/BTB24-2L-3.pdf

[111] Han-Wei Liu, Ching-Fu Lin, Yu-Jie Chen (2018), *Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/332457303_Beyond_State_v_Loomis_Artificial_Intelligence_Government_Algorithmization_and_Accountability

[112] State v. Loomis παράγραφος 51 της απόφασης.

ότι οι προβλέψεις του COMPAS είχαν χαμηλό ποσοστό επιτυχίας καθώς και ότι οι εκτιμήσεις κινδύνου λειτουργούσαν εις βάρος των μειονοτήτων[113] αλλά αυτό δεν έπαιξε κάποιο ρόλο στην έκβαση της υπόθεσης. Φαίνεται λοιπόν ότι η έννοια της διαφάνειας απουσιάζει από τα πρώιμα κιόλας στάδια λειτουργίας των μηχανισμών πρόληψης.

Η απουσία διαφάνειας έχει άμεσο αντίκτυπο στη σχέση της αστυνομίας με τους πολίτες. Αυτό είναι απόλυτα λογικό καθώς σταδιακά καθιερώνεται ένα καθεστώς μαζικής παρακολούθησης, στο οποίο οι πολίτες συλλαμβάνονται ενώ δεν έχουν τελέσει ακόμη κάποιο έγκλημα, χωρίς παράλληλα να υπάρχουν επαρκείς εξηγήσεις για το πως λειτουργεί το σύστημα[114]. Η αδιαφάνεια κάνει τους πολίτες να αντιμετωπίζουν με φόβο και εχθρική διάθεση τις αρχές οι οποίες τους επιτηρούν συνεχώς σαν να βρισκόμαστε στον κόσμο του Όργουελ. Ταυτόχρονα η άδικη στόχευση μειονοτήτων και συγκεκριμένων περιοχών είναι υπεύθυνη για την έλλειψη εμπιστοσύνης που παρατηρείται τα τελευταία χρόνια, τόσο απέναντι στον θεσμό της αστυνομίας όσο και απέναντι στην πολιτεία γενικότερα.

2.5.4 Η δυσχέρεια απόδοσης ευθυνών.

Άμεσο αποτέλεσμα της αδιαφάνειας είναι η αδυναμία προσδιορισμού της ευθύνης. Η έννοια της ευθύνης αποτελεί θεμελιώδη αρχή του δημοκρατικού πολιτεύματος. Προϋποθέτει ότι οι δημόσιες αρχές που ασκούν την εξουσία στο όνομα της πολιτείας έχουν την ηθική υποχρέωση να λογοδοτήσουν στο κοινό για τις πράξεις τους, τις πιθανές αποτυχίες τους και τα σφάλματά τους[115]. Πρακτικά σημαίνει ότι οι αρχές θα πρέπει να είναι σε θέση να εξηγήσουν τον τρόπο που πάρθηκαν οι αποφάσεις τους και το πως και γιατί προέβησαν στις αντίστοιχες ενέργειες. Για να συμβεί αυτό δίνεται στους θεσμούς το βήμα για να παρουσιάσουν τη δική τους εκδοχή για «το τι συνέβη». Εξετάζοντας τους ανωτέρω ισχυρισμούς οι πολίτες μπορούν να εντοπίσουν υπεύθυνες ή ανεύθυνες συμπεριφορές αλλά και ενδείξεις διαφθοράς[116]. Η αστυνομία σαν θεσμός της κοινωνίας έχει και αυτή την υποχρέωση, να λογοδοτεί στην κοινωνία για τις πράξεις της.

---

[113] Βλ. την έρευνα της Pro Publica, Julia Angwin, Jeff Larson κλπ. Υποσημείωση 85
[114] Βλ. Ishmael Mugari, υποσημείωση 15
[115] Tal Z. Zarsky (2013), *Transparent Predictions*, διαθέσιμο σε pdf στο https://www.illinoislawreview.org/wp-content/ilr-content/articles/2013/4/Zarsky.pdf
[116] Βλ. Simon Egbert και Matthias Leese υποσημείωση 26

Τι συμβαίνει όμως όταν οι αποφάσεις λαμβάνονται από τα αλγοριθμικά συστήματα και υλοποιούνται στη συνέχεια από την αστυνομία; Φέρουν οι αστυνομικές αρχές ευθύνη ή είναι απλώς το όργανο; Αυτό είναι το πρόβλημα που δημιουργήθηκε με την έλευση των συστημάτων προληπτικής αστυνόμευσης. Επειδή πλέον οι αστυνομικές αποφάσεις λαμβάνονται έπειτα από πολύπλοκες μαθηματικές πράξεις είναι δύσκολο, έως και ανέφικτο, οι αστυνομικοί να λογοδοτήσουν για τις πράξεις τους, διότι ούτε οι ίδιοι ξέρουν πώς πάρθηκε η απόφαση. Το πρόβλημα του μαύρου κουτιού είναι υπαρκτό και για τους ίδιους τους αστυνομικούς, καθώς δεν μπορούν ούτε οι ίδιοι να κατανοήσουν τη λειτουργία του λογισμικού. Εφόσον λοιπόν δεν μπορούν οι αστυνομικές αρχές να αναλύσουν πώς κατέληξε το σύστημα σε ένα συμπέρασμα, τότε δεν είναι σε θέση να λογοδοτήσουν για τις επιλογές τους. Συνεπώς η έλλειψη διαφάνειας προκαλεί ένα «πάγωμα» (chilling effect) ευθύνης της αστυνομίας για τις πράξεις της.

Συνοψίζοντας, τα συστήματα προληπτικής αστυνόμευσης με τον τρόπο που λειτουργούν είναι ικανά να υπονομεύσουν το δημοκρατικό πολίτευμα. Μέχρι στιγμής τα περισσότερα αλγοριθμικά συστήματα είναι από το σχεδιασμό τους αδιαφανή και λειτουργούν σαν τροχοπέδη για την απόδοση ευθυνών στους αρμόδιους φορείς. Παρόλο που υπάρχουν πολλές τεχνικές δυσχέρειες, η προληπτική αστυνόμευση οφείλει να φέρει σαν υποχρέωση τον σεβασμό των αρχών της διαφάνειας και της ευθύνης. Πρόκειται για μία μεγάλη πρόκληση, η οποία τη δεδομένη στιγμή είναι δύσκολο να επιτευχθεί, αλλά όχι και ανέφικτο.

3. ΥΓΕΙΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΣΤΥΝΟΜΕΥΣΗΣ

Στο κεφάλαιο αυτό θα αναλυθούν οι εφαρμογές που αναπτύχθηκαν για την ανίχνευση και την αντιμετώπιση του Covid-19. Θεωρήθηκε σώφρον να αποτελέσουν ξεχωριστό κεφάλαιο, λόγω της ιδιαίτερης φύσης του ζητήματος, μιας και σήμερα, 2 χρόνια μετά την κήρυξη της πανδημίας του νέου κορωνοϊού SARS-CoV-2, ο Covid-19 εξακολουθεί να κατέχει πρωταγωνιστικό ρόλο στην καθημερινότητά μας. Δεν έχει βρεθεί ακόμα μία αποτελεσματική θεραπεία, ενώ παράλληλα τα κρούσματα και οι θάνατοι σε όλο τον κόσμο κυμαίνονται σε υψηλά επίπεδα. Εκ πρώτης όψεως, φαίνεται αρκετά δύσκολο να βρεθεί κάποιος κοινός άξονας ανάμεσα στις εφαρμογές ανίχνευσης του κορωνοϊού με τις εφαρμογές προληπτικής αστυνόμευσης, που αναλύθηκαν στο προηγούμενο κεφάλαιο, η πραγματικότητα όμως είναι τελείως διαφορετική. Πληθώρα υγειονομικών εφαρμογών κατασκευάστηκε ύστερα από συνεργασία των κρατικών κυβερνήσεων με τις αστυνομικές

αρχές, εγκαθιδρύοντας πολλές φορές ένα σύστημα κοινωνικής επιτήρησης εντός της χώρας[117]. Ενώ λοιπόν το προστατευόμενο έννομο αγαθό είναι διαφορετικό, σε σχέση με τις προεγκληματικές εφαρμογές, στο τέλος απλώς καταλήγουμε να συζητάμε για μία διαφορετική μορφή αστυνόμευσης. Για τον λόγο αυτό οι εφαρμογές ανίχνευσης και ιχνηλάτησης του Covid-19 χαρακτηρίζονται και ως υγειονομικά συστήματα αστυνόμευσης.

Η ημέρα της 11ης Μαρτίου 2020 θεωρείται αλησμόνητη καθώς τότε, ο Παγκόσμιος Οργανισμός Υγείας κατέληξε ότι υπάρχει «Έκτακτη Ανάγκη Δημόσιας Υγείας Διεθνούς Ενδιαφέροντος», κήρυξε πανδημία και ένα συντριπτικό ποσοστό του δυτικού κόσμου οδηγήθηκε σε καραντίνα[118]. Το μέτρο της καραντίνας σε παγκόσμια (ουσιαστικά) κλίμακα θεωρήθηκε απαραίτητο, καθώς η ιατρική επιστήμη δεν γνώριζε πολλές πληροφορίες για τον κορωνοϊό, που θα ήταν ικανές να τον αντιμετωπίσουν, και ταυτόχρονα τα κρούσματα ήταν πολύ υψηλά για να μπορέσουν να ανταποκριθούν τα δημόσια νοσοκομεία της κάθε χώρας σε αυτές τις ιδιαίτερες συνθήκες. Εφόσον τη δεδομένη χρονική στιγμή η ιατρική πρόληψη και αντιμετώπιση του κορωνοϊού δεν επαρκούσε για να εξαλειφθεί η πανδημία, οι κυβερνήσεις αναγκάστηκαν να στραφούν σε άλλες λύσεις. Τότε είναι που ξεκίνησαν να ανακύπτουν στην επιφάνεια εφαρμογές αυτοματοποιημένης λήψης απόφασης που προήγαγαν πρακτικές μαζικής παρακολούθησης των πολιτών[119].

Το πρώτο βήμα για την υποδοχή του συστηματικού κοινωνικού ελέγχου πραγματοποιήθηκε από την Κίνα, χώρα όπου ξεκίνησε η πανδημία. Ήδη από τον Φεβρουάριο του 2020 είχε αρχίσει να εφαρμόζεται λογισμικό αναγνώρισης προσώπου, έτσι ώστε να εντοπίζονται οι πολίτες που δεν φορούσαν μάσκα κατά του κορωνοϊού[120]. Την ίδια χρονική περίοδο στη Μόσχα εγκαταστάθηκε ολόκληρο σύστημα καμερών παρακολούθησης για να διαβεβαιώνεται ότι όσοι είναι θετικοί στον ιό, ή ήρθαν σε επαφή με κρούσμα, βρίσκονται

---

[117] Από τις πιο χαρακτηριστικές περιπτώσεις είναι οι χώρες της Ασίας, όπως η Κίνα και το Ισραήλ, βλ. Λ. Κανέλλος, υποσημείωση 4

[118] CBC, (2020), *Coronavirus: WHO calls COVID-19 outbreak a pandemic as Italy orders most stores to close*, διαθέσιμο στο https://www.cbc.ca/news/world/coronavirus-who-says-covid-19-outbreak-is-apandemic-1.5493411

[119] European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2020), *Artificial Intelligence and Law Enforcement, Impact on Fundamental Rights*, European Parliament, διαθέσιμο σε pdf στο https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

[120] Rishabh Jain (2020), *Baidu's Face Detection AI Will Help China Identify People Without Masks*, International Business Times, διαθέσιμο στο https://www.ibtimes.com/baidus-face-detection-ai-will-help-china-identify-people-without-masks-2923502

στην καραντίνα και δεν κυκλοφορούν παράνομα στους δρόμους[121]. Παράλληλα, έχοντας διαφορετική οπτική, η εταιρεία Athena Security κυκλοφόρησε στις Ηνωμένες Πολιτείες ένα πρόγραμμα τεχνητής νοημοσύνης το οποίο μπορούσε να ανιχνεύσει τον πυρετό στους ανθρώπους που εξέταζε, χωρίς όμως να προβαίνει σε αναγνώριση προσώπου[122].

Ωστόσο, οι εφαρμογές που χρειάζονται πολύ μεγαλύτερη προσοχή είναι οι εφαρμογές που πραγματοποιούν αυτοματοποιημένες αποφάσεις (automated decision-making)[123]. Η χαρακτηριστικότερη περίπτωση είναι το πρόγραμμα Pattern[124] που εμφανίστηκε τον Απρίλιο του 2020 στις ΗΠΑ. Το πρόγραμμα περιείχε έναν αλγόριθμο, ο οποίος, εξετάζοντας τα προσωπικά στοιχεία των ασθενών, αποφάσιζε αυτοματοποιημένα ποιοι ασθενείς δικαιούνται «θεραπεία προτεραιότητας» (priority treatment). Πολλές ήταν οι αρνητικές κριτικές έναντι του προγράμματος αυτού. Αρχικά επικρίθηκε εντόνως, το γεγονός ότι λαμβάνονται αυτοματοποιημένες αποφάσεις για ένα τόσο ευαίσθητο ζήτημα, όπως η υγεία. Επίσης, ύστερα από πολλαπλές αξιολογήσεις κρίθηκε ότι το σύστημα διαιώνιζε τις ρατσιστικές και φυλετικές διακρίσεις καθώς σπάνια έθετε σε σειρά προτεραιότητας τους άστεγους, τους άπορους αλλά και τους Αφροαμερικανούς.

Από τον χορό του κοινωνικού ελέγχου δεν θα μπορούσε να λείψει η Κίνα. Η εγχώρια κυβέρνηση σε συνεργασία με την πλατφόρμα ηλεκτρονικού εμπορίου Alibaba[125], δημιούργησε το σύστημα υγείας Alipay[126], το οποίο μάλιστα εγκαταστάθηκε υποχρεωτικά

---

[121] Nicola Habersetzer (2020), *Moscow Silently Expands Surveillance of Citizens*, Human Rights Watch, διαθέσιμο στο https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens

[122] Joseph Cox (2020), *Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US*, διαθέσιμο στο https://www.vice.com/en/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras

[123] Όπως προκύπτει από τις αιτιολογικές σκέψεις 71, 72, 73, 75, 89, 90, 91 καθώς και από το άρθρο 22 του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), αυτοματοποιημένη λήψη απόφασης είναι η διαδικασία, κατά την οποία λαμβάνονται αποφάσεις που αφορούν ανθρώπινα υποκείμενα αποκλειστικά από υπολογιστικά συστήματα χωρίς ανθρώπινη παρέμβαση. Πολλές φορές απαραίτητη προϋπόθεση για τη λήψη αυτοματοποιημένης απόφασης είναι η κατάρτιση προφίλ των υποκειμένων. Κατάρτιση προφίλ είναι η αξιολόγηση προσωπικών πτυχών των ανθρώπων (όπως η ηλικία, το φύλο, η οικονομική κατάσταση κλπ.), ή η κατηγοριοποίηση των ανθρώπων βάσει αυτών των χαρακτηριστικών.

[124] The Leadership Conference on Civil and Human Rights (2020), *The use of the PATTERN risk assessment in prioritizing release in response to the COVID-19 pandemic*, διαθέσιμο σε pdf στο https://www.upturn.org/static/files/Final_Letter_on_PATTERN_in_Response_to_AG_Barr_Memo_on_4_26-4_3_2020.pdf

[125] Η Alibaba είναι από τις πιο δημοφιλείς πλατφόρμες ηλεκτρονικού εμπορίου (e-shop) παγκοσμίως, η οποία απαριθμεί περίπου 1 δις πελατών, περισσότερες πληροφορίες στο https://www.alibaba.com/

[126] Βλ. Λ. Κανέλλος, υποσημείωση 4

στα κινητά τηλέφωνα των πολιτών που χρησιμοποιούν αυτή την εφαρμογή ηλεκτρονικού εμπορίου. Η εφαρμογή περιλάμβανε ένα ερωτηματολόγιο, το οποίο συμπληρωνόταν μέσω διασταυρώσεων με ιατρικά και κρατικά αρχεία. Το ερωτηματολόγιο αφού συμπληρωθεί παράγει έναν κωδικό, που είναι αναγνώσιμος απ' όλες τις αρχές και καθορίζει ανάλογα με το αποτέλεσμα αν κάποιος μπορεί να κυκλοφορήσει ελεύθερα στην πόλη ή όχι, διότι ήρθε σε επαφή με κρούσμα ή διότι κατά πάσα πιθανότητα μολύνθηκε ο ίδιος. Οι επικρίσεις δεν έλειψαν ούτε σε αυτή την περίπτωση. Σύμφωνα με τον Διεθνή Τύπο αυτά τα συστήματα αποτελούν πρότυπα για νέες μορφές αυτοματοποιημένου κοινωνικού ελέγχου, οι οποίες μάλιστα είναι πιθανό να συνεχίσουν να υπάρχουν ακόμα και αν αντιμετωπιστεί πλήρως το θέμα του κορωνοϊού.

Βλέπουμε λοιπόν ότι οι πρώτες προσπάθειες για δημιουργία υγειονομικών συστημάτων αστυνόμευσης δεν ήταν απλώς αποτυχημένες αλλά και επικίνδυνες για την κοινωνία, καθώς παραβίαζαν σωρεία ατομικών δικαιωμάτων. Έγινε άμεσα φανερό ότι έπρεπε να βρεθεί μία διαφορετική λύση. Οι εφαρμογές υγείας οφείλουν να υπερασπίζονται τα θεμελιώδη δικαιώματα, που διασφαλίζονται από τους εγχώριους νόμους και τις Διεθνείς συνθήκες, και όχι να τα καταπατούν. Επομένως, για αρχή θα πρέπει οι εφαρμογές να επεξεργάζονται όσο το δυνατόν λιγότερα προσωπικά δεδομένα γίνεται, σεβόμενες τις αρχές που έθεσε ο GDPR[127] στην Ευρωπαϊκή Ένωση. Τότε είναι που «έπεσε στο τραπέζι» να αναπτυχθούν εφαρμογές που επεξεργάζονται μόνο τα δεδομένα θέσης.

3.1 Εφαρμογές που χρησιμοποιούν δεδομένα θέσης.

Ευθύς αμέσως άρχισαν να αναπτύσσονται εφαρμογές που επεξεργάζονται δεδομένα θέσης. Η ιδέα ήταν πολύ απλή. Οι πάροχοι υπηρεσιών τηλεπικοινωνιών θα διέθεταν τα δεδομένα θέσης των συνδρομητών τους στις αρχές, οι οποίες θα εξέταζαν πού βρισκόντουσαν οι άνθρωποι που διαγνώσθηκαν θετικοί στον ιό όταν κόλλησαν και τι διαδρομές έκαναν αφότου κόλλησαν. Ο απώτερος σκοπός ήταν φυσικά να καταστεί εφικτή η πρόβλεψη της εξάπλωσης του ιού στο μέλλον[128], μέσω της ιχνηλάτησης των επαφών. Βέβαια, για να μην υποπέσουν στο ίδιο λάθος, οι εφαρμογές αυτές θα έπρεπε να σέβονται τα θεμελιώδη

[127] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679, διαθέσιμος σε pdf στο https://eurlex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

[128] Βλ European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, υποσημείωση 93

ανθρώπινα δικαιώματα και τους σχετικούς Κανονισμούς και Συνθήκες που τα διασφαλίζουν. Στην Ευρωπαϊκή Ένωση θεσμικό ρόλο κατέχει ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) καθώς και η οδηγία e-Privacy[129], η οποία ρυθμίζει αποκλειστικά την προστασία των δεδομένων θέσης. Σεβόμενες τις αρχές που υπερασπίζονται τα ανωτέρω νομοθετήματα, πολλά κράτη-μέλη (όπως η Γαλλία και η Γερμανία) άρχισαν να συνεργάζονται με τους εγχώριους παρόχους, με τους τελευταίους να προσκομίζουν στις αρχές ανωνυμοποιημένα ή ψευδωνυμοποιημένα δεδομένα θέσης, ώστε να αποφεύγεται η ταυτοποίηση των υποκειμένων[130].

Η αλήθεια είναι ότι αυτό το εγχείρημα αποδείχτηκε τρομερά δύσκολο. Εξ αρχής η ολλανδική αρχή προστασίας δεδομένων ήταν πολύ επικριτική απέναντι σε αυτήν την προσπάθεια. Μάλιστα τον Απρίλιο του 2020, η αρχή δημοσίευσε ένα κείμενο στο οποίο μεταξύ άλλων ισχυριζόταν ότι η γενικότερα ανωνυμοποίηση των δεδομένων είναι πολύ δύσκολή αποστολή, ενώ ειδικότερα η ανωνυμοποίηση των δεδομένων θέσης είναι κάτι το ακατόρθωτο[131]. Ο φόβος της αρχής έγκειται στο γεγονός ότι είναι πάρα πολύ εύκολο, απλώς με την εξέταση των δεδομένων θέσης να ταυτοποιηθεί ένας πολίτης. Αυτό συμβαίνει γιατί υπάρχουν τοποθεσίες που τις επισκέπτεται κάθε μέρα, όπως το σπίτι του και ο χώρος εργασίας του. Επομένως, αντιστρόφως ανάλογα, είναι πολύ δύσκολο να «ανωνυμοποιηθούν» οι καθημερινές συνήθειες και υποχρεώσεις του καθενός.

Δυστυχώς, η ανωτέρω ανησυχία επιβεβαιώθηκε με σκληρό τρόπο καθώς πολλές χώρες όχι απλά δεν μπόρεσαν να ανωνυμοποιήσουν τα επίμαχα δεδομένα, αλλά δεν το προσπάθησαν καν. Αποκορύφωμα αυτής της ανομίας ήταν η Ουγγαρία, όπου τον Μάιο του 2020 η κυβέρνηση εξέδωσε διάταγμα έκτακτης ανάγκης, με το οποίο ανέστειλε την ισχύ του Κανονισμού GDPR με το επιχείρημα ότι έπρεπε να ληφθούν επείγοντα μέτρα για την καταπολέμηση του κορωνοϊού.

Βέβαια και στις υπόλοιπες Ηπείρους που ισχύουν οι Διεθνείς Συνθήκες για την προστασία της ιδιωτικότητας οι παραβάσεις μόνο λίγες δεν ήταν. Οι χώρες της Ανατολής, με

---

[129] ΟΔΗΓΙΑ 2002/58/ΕΚ, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EL

[130] Costica Dumbrava (2020), Tracking mobile devices to fight coronavirus, διαθέσιμο στο https://epthinktank.eu/2020/04/21/tracking-mobile-devices-to-fight-coronavirus/

[131] Autoriteit Persoonsgegevens (2020), *On the anonymity of aggregated telco location data*, διαθέσιμο σε pdf στο https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimity_and_aggregated_telco_location_data.pdf

πρωταγωνίστρια για ακόμη μία φορά την Κίνα, ανάγκασαν τους πολίτες τους να εγκαταστήσουν εφαρμογές, οι οποίες επεξεργάζονταν δεδομένα θέσης χωρίς καμία προσπάθεια ανωνυμοποίησης, και μπορούσαν να δουν που βρίσκονταν κάθε πολίτης όταν κόλλησε Covid (περίπτωση Νοτίου Κορέας[132]), καθώς και αν τηρούν την καραντίνα που τους επιβλήθηκε (περίπτωση Ταϊβάν[133]). Μάλιστα η Κίνα προχώρησε ένα βήμα πιο μπροστά, καθώς για την ιχνηλάτηση του κορωνοϊού, εγκατέστησε εκατομμύρια κάμερες σε όλη τη χώρα με δυνατότητα αναγνώρισης προσώπου, γνωστό και ως πρόγραμμα «face control». Πέρα από τις κάμερες, το πρόγραμμα έχει εγκατασταθεί και στα κινητά των πολιτών οι οποίοι έχουν υποχρέωση να ενημερώνουν το σύστημα ανά τακτά χρονικά διαστήματα αναφέροντας τη θερμοκρασία του σώματός τους και την ιατρική τους κατάσταση[134]. Κατ' αυτόν τον τρόπο οι κρατικές αρχές δεν εντοπίζουν άμεσα μόνο τους φορείς του ιού αλλά μέσω των καμερών που έχουν εγκατασταθεί μπορούν να ελέγξουν και τις κινήσεις τους και τα άτομα με τα οποία ήρθαν σε επαφή. Πρόκειται για την πιο αυστηρή και ολοκληρωτική μορφή ιχνηλάτησης επαφών μέχρι στιγμής.

3.2 Η λύση στο πρόβλημα

Οι ανωτέρω περιπτώσεις είχαν καθοριστικό ρόλο, γιατί υπέδειξαν στους ενωσιακούς και κρατικούς φορείς καθώς και στους ερευνητές ποιες ενέργειες πρέπει να αποφύγουν και γενικά ποιους παράγοντες να λάβουν υπόψη κατά τον σχεδιασμό των εφαρμογών ιχνηλάτησης. Αποδείχθηκε ότι η προσπάθεια ανωνυμοποίησης των δεδομένων θέσης ήταν σχεδόν ανέφικτη, ενώ παράλληλα η συνεχής πρόσβαση των κρατικών αρχών σε αυτά, όπως συνέβαινε στην Ασία, ήταν κατακριτέα. Η πρώτη σημαντική προσπάθεια επίλυσης του προβλήματος παρατηρείται τον Απρίλιο του 2020. Τότε οι δύο τεχνολογικοί κολοσσοί του 21ου αιώνα, Apple και Google, αποφάσισαν να φτιάξουν μαζί μία εφαρμογή ιχνηλάτησης επαφών, η οποία θα ήταν συμβατή τόσο με λογισμικό iOS (Apple), όσο και με λογισμικό Android[135] (Google). Προτάθηκε μία αποκεντρωμένη επεξεργασία δεδομένων προσωπικού

---

132 Isobel Asher Hamilton, (2020), *Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance*, διαθέσιμο στο https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3

133 BBC News, (2020), *Coronavirus: Under surveillance and confined at home in Taiwan*, διαθέσιμο στο https://www.bbc.com/news/technology-52017993

134 Yuval Noah Harari, (2020), *Yuval Noah Harari: the world after coronavirus | Free to read*, διαθέσιμο στο https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

135 The Guardian, (2020), *Apple and Google team up in bid to use smartphones to track coronavirus*

χαρακτήρα. Δηλαδή τα smartphones των χρηστών της εφαρμογής θα αντάλλαζαν μεταξύ τους δεδομένα με τη μέθοδο BLE (Bluetooth Low Energy)[136]. Εν συνεχεία τα δεδομένα δεν θα συλλέγονταν από ένα κεντρικό σύστημα, αντίθετα η επεξεργασία τους θα γινόταν από τα ίδια τα κινητά. Έτσι δεν θα συγκεντρώνονταν σε κανένα κεντρικό σύστημα όλα τα δεδομένα των χρηστών, ενισχύοντας έτσι τη διαφάνεια και την αξιοπιστία. Βέβαια επειδή ακόμα και σε αυτή την περίπτωση συνεχίζει να γίνεται επεξεργασία προσωπικών δεδομένων, φυσικό επακόλουθο είναι να εξακολουθούν να υπάρχουν ακόμα προβλήματα σχετικά με την επεξεργασία[137]. Την οριστική λύση στο πρόβλημα των εφαρμογών την έδωσε λίγο καιρό αργότερα μία νεοσύστατη ομάδα με την ονομασία DP-3T[138].

Η DP-3T παρατηρώντας συνεχώς τις εξελίξεις στον τομέα ανάπτυξης των εφαρμογών ιχνηλάτησης αντιλήφθηκε ότι εφόσον οι εφαρμογές θα επεξεργάζονται προσωπικά δεδομένα πάντοτε θα υπάρχουν προβλήματα. Η ιδανική λύση θα ήταν είτε να δημιουργηθεί ένα πρόγραμμα που θα τηρεί στο έπακρο την αρχή της ελαχιστοποίησης των προσωπικών δεδομένων[139] και θα επεξεργάζεται όσο το δυνατόν λιγότερα δεδομένα, είτε να κατασκευαστεί ένα σύστημα ιχνηλάτησης που δεν θα βασίζεται στην επεξεργασία δεδομένων. Με βάση αυτές τις σκέψεις καθώς και φανερά επηρεασμένη από την πρόταση της Apple και της Google για αποκεντρωμένο σύστημα η DP-3T υιοθέτησε μία απλή και ταυτόχρονα αποτελεσματική ιδέα.

Σύμφωνα με τη νεοσυσταθείσα ομάδα, σημασία δεν έχει σε ποιο μέρος κόλλησε κάποιος Covid-19, ούτε σε ποια τοποθεσία ήρθε κάποιος σε επαφή με κάποιο κρούσμα[140]. Επομένως τα δεδομένα θέσης και κίνησης δεν χρησιμεύουν, οπότε δεν χρειάζεται να αποθηκεύονται και να επεξεργάζονται. Αυτό που έχει πραγματικά σημασία είναι, αν δύο άνθρωποι ήρθαν τόσο κοντά μεταξύ τους και για πόση ώρα, ώστε να μεταδόθηκε ο ιός από τον έναν στον

---

spread, διαθέσιμο στο https://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-appprivacy

[136] Λεπτομερής ανάλυση της λειτουργίας BLE στο https://blog.google/documents/66/Overview_of_COVID-19_Contact_Tracing_Using_BLE_1.pdf/

[137] Dan Goodin, (2020), *Apple and Google detail bold and ambitious plan to track COVID-19 at scale*, διαθέσιμο στο https://arstechnica.com/information-technology/2020/04/apple-and-google-detail-bold-andambitious-plan-to-track-covid-19-at-scale/

[138] Πληροφορίες σχετικά με την DP-3T στο https://github.com/DP-3T/documents

[139] Βλ. άρθρο 5 ΓΚΠΔ

[140] Homo Digitalis, (2020), *COVID-19 & ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΗΝ ΕΛΛΑΔΑ*, διαθέσιμο σε pdf στο https://www.homodigitalis.gr/wpcontent/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf

άλλον. Έχοντας αυτό σαν πυρήνα της σκέψης τους, σε συνδυασμό με το μοντέλο αποκεντρωμένης διοίκησης που προτάθηκε από την Apple και Google, η DP-3T παρουσίασε μία εφαρμογή η οποία λειτουργεί ως εξής:

Αρχικά οι πολίτες, με τη θέλησή τους και μόνο (δεν υπάρχει εξαναγκασμός), εγκαθιστούν την εφαρμογή στο κινητό τους. Η εφαρμογή κατά τη λειτουργία της δημιουργεί συνεχώς κωδικούς αναγνώρισης, που ονομάζονται και ψευδώνυμα, οι οποίοι αλλάζουν συνεχώς σε τακτά χρονικά διαστήματα. Τα ψευδώνυμα αυτά είναι τυχαίες αλληλουχίες γραμμάτων και αριθμών που σε καμία των περιπτώσεων δεν είναι ικανές να ταυτοποιήσουν κάποιο φυσικό πρόσωπο. Οπότε πρόκειται για ανώνυμα δεδομένα. Όταν ένας χρήστης της εφαρμογής βρεθεί σε κοντινή απόσταση με άλλον χρήστη της ίδιας εφαρμογής, τότε τα κινητά τους ανταλλάζουν τους κωδικούς αναγνώρισης και τους αποθηκεύουν στη μνήμη τους σε κρυπτογραφημένη μορφή. Κατ' αυτόν τον τρόπο οι εφαρμογές θυμούνται τα ψευδώνυμα με τα οποία ήρθαν σε επαφή. Μέχρι αυτό το σημείο όλες οι ενέργειες και επεξεργασίες πραγματοποιούνται από τα κινητά. Δεν εμπλέκεται πουθενά κάποιο κεντρικό σύστημα ελέγχου.

Πώς μπορούν όμως οι συσκευές και ανταλλάζουν κωδικούς αναγνώρισης; Εδώ είναι που εμπλέκεται η τεχνολογία Bluetooth Low Energy[141], που προτάθηκε για πρώτη φορά από την Apple και τη Google, όπως αναφέρθηκε προηγουμένως. Πρόκειται για μία τεχνολογία που υποστηρίζεται τόσο από λογισμικό Android, όσο και από λογισμικό iOS. Το πρόγραμμα αυτό επιτρέπει στο κινητό να στέλνει τους κωδικούς και τα ψευδώνυμα που παράγει σε όλα τα κινητά γύρω του, αρκεί να είναι σε κοντινή εμβέλεια. Ταυτόχρονα με τη χρήση της ίδιας τεχνολογίας το κινητό λαμβάνει όλους τους κωδικούς από τα κοντινά κινητά τηλέφωνα. Για να γίνει αυτή η ανταλλαγή ψευδωνύμων πέρα από την τεχνολογία BLE απαιτείται να είναι εγκατεστημένη η ίδια εφαρμογή στα κινητά. Συνεπώς βασικό ρόλο παίζει η απόσταση των κινητών καθώς μόνο από κοντά μπορούν να ανταλλάξουν κωδικούς αναγνώρισης. Επίσης άλλη μία παράμετρος που πρέπει να τονιστεί είναι και ο χρόνος. Τα κινητά δεν απαιτείται μόνο να είναι σε κοντινή απόσταση, αλλά πρέπει να είναι και σε κοντινή απόσταση για ένα

[141] Γιώργος Τσίρτσης - Σπύρος Τάσσης, (2020), *Κορωνοϊός: Ιχνηλάτηση επαφών (Contact Tracing) και Ειδοποίηση Έκθεσης (Exposure Notification)*, διαθέσιμο στο https://www.lawspot.gr/nomikablogs/spiros_tassis/koronoios-ihnilatisi-epafon-contact-tracing-kai-eidopoiisi-ekthesis

χρονικό διάστημα τουλάχιστον 2 λεπτών και άνω. Αυτό συμβαίνει γιατί οι μελέτες έχουν δείξει ότι τόσο χρόνο θέλει περίπου ο Covid-19 για να μεταδοθεί.

Εάν τώρα ένας από τους χρήστες της εφαρμογής διαγνωστεί θετικός στον ιό, τότε ενημερώνει την εφαρμογή του και με τη σύμφωνη γνώμη του στέλνεται σε έναν κεντρικό server η λίστα με τα ψευδώνυμα που έχει παράγει η συσκευή του φορέα του ιού στο παρελθόν[142]. Εδώ για πρώτη φορά οι πληροφορίες του χρήστη ξεφεύγουν από το κινητό του και μεταφέρονται σε ένα cloud, ένα σύστημα ελέγχου. Στο cloud όμως πηγαίνουν τα ψευδώνυμα του ιδίου του χρήστη, όχι αυτά που απέκτησε με Bluetooth από άλλες συσκευές. Συνεπώς το cloud δεν μπορεί να ταυτοποιήσει τα άτομα με τα οποία ήρθε σε επαφή ο ασθενής παρά μόνο να δει τα ανωνυμοποιημένα ψευδώνυμά του. Το μόνο λοιπόν που κάνει ο κεντρικός διαχειριστής είναι να προωθήσει αυτή τη λίστα με τους κωδικούς σε όλες τις υπόλοιπες συσκευές που έχουν εγκατεστημένη την εφαρμογή.
Αφού τα κινητά των άλλων χρηστών λάβουν την κοινωποιημένη λίστα, αρχίζει η επεξεργασία της από τα ίδια τα κινητά. Ουσιαστικά τα κινητά μόλις λάβουν το αρχείο εξετάζουν τα ψευδώνυμα που έλαβαν και τα συγκρίνουν με τα ψευδώνυμα που έχουν αποθηκεύσει τα ίδια. Αν ένα ψευδώνυμο που βρίσκεται αποθηκευμένο στη μνήμη του κινητού, υπάρχει παράλληλα στο αρχείο που στάλθηκε από το cloud, τότε η εφαρμογή ειδοποιεί τον χρήστη ότι βρέθηκε σε επαφή με κρούσμα. Δεν πρόκειται όμως για μία στείρα ειδοποίηση, αντιθέτως η εφαρμογή τού δίνει συμβουλές για τα επόμενα βήματα που πρέπει να ακολουθήσει, όπως για παράδειγμα να επισκεφτεί κάποιον γιατρό ή να υποβληθεί σε μοριακό τεστ για Covid-19. Στο σημείο αυτό πρέπει να διευκρινιστεί κάτι σημαντικό. Ο χρήστης ειδοποιείται ότι ήρθε σε επαφή με κρούσμα χωρίς κανένα πρόσθετο στοιχείο. Δεν ειδοποιείται ούτε για το ποιο άτομο είναι το κρούσμα αυτό, ούτε για το μέρος που έγινε η επαφή, ούτε για το πότε έγινε. Αυτό συμβαίνει επειδή στον κεντρικό διαχειριστή στέλνονται μόνο τα ψευδώνυμα του φορέα του ιού και τίποτε παραπάνω. Έτσι, ενημερώνονται οι χρήστες των εφαρμογών χωρίς παράλληλα να παραβιάζονται τα δεδομένα τους και η ιδιωτική τους ζωή.

Η λύση αυτή εντυπωσίασε την Ευρωπαϊκή Ένωση, καθώς είδε για πρώτη φορά να λειτουργεί μία υγειονομική εφαρμογή που σέβεται απόλυτα τις αρχές που θέτουν οι Κανονισμοί της. Εντός του 2020 οι θεσμοί της Ένωσης είχαν εκδώσει κατευθυντήριες γραμμές και συστάσεις

[142] Ιωάννης Κροντήρης, (2020), *Κινητά τηλέφωνα στη μάχη κατά του κορωνοϊού: Συμβιβασμοί στην προστασία προσωπικών δεδομένων;*, διαθέσιμο στο https://www.homodigitalis.gr/posts/5391

που ξεκαθάριζαν ότι για να λειτουργήσει μία εφαρμογή ιχνηλάτησης οφείλει να σέβεται απόλυτα τους Κανονισμούς περί προστασίας προσωπικών δεδομένων[143]. Το σύστημα της DP-3T σέβεται απόλυτα το ενωσιακό δίκαιο τηρώντας την αρχή της ελαχιστοποίησης των δεδομένων και της περιορισμένης αποθήκευσης. Επομένως είναι απόλυτα λογικό η Ένωση να αγκαλιάσει αυτό το πρόγραμμα, όπως φαίνεται ξεκάθαρα από το κείμενο της Ευρωπαϊκής Επιτροπής που δημοσιεύθηκε τον Οκτώβριο του 2020[144]. Δεν είναι καθόλου τυχαίο το γεγονός ότι, από την δημιουργία της εφαρμογής και έπειτα, όλες οι συστάσεις της Επιτροπής προωθούν την ανάπτυξη εφαρμογών με παρόμοιο λογισμικό από τα κράτη-μέλη.

3.3 Αξιολόγηση της λύσης

Βλέποντας όλα αυτά τα διθυραμβικά σχόλια, θα μπορούσε κάποιος να πιστέψει ότι με την έλευση της κατάλληλης υγειονομικής εφαρμογής θα προβλέπεται αποτελεσματικά η διάδοση του ιού, οπότε θα πάρουμε τα ανάλογα προληπτικά μέτρα και το πρόβλημα λύθηκε; Είναι όμως τόσο απλό; Η απάντηση σε όλα μας τα προβλήματα είναι μία εφαρμογή που λειτουργεί με Bluetooth; Όπως και σε όλα τα σχετικά ζητήματα με την προληπτική αστυνόμευση, έτσι και εδώ η απάντηση είναι πιο σύνθετη.

Αρχικά, εφόσον πρόκειται για εφαρμογή που εγκαθίσταται σε smartphone, χρειάζεται να έχεις smartphone και να έχεις κατεβασμένη την εφαρμογή. Όσο περίεργο και να ακουστεί είναι μεγάλο το ποσοστό των ανθρώπων που δεν έχουν smartphone. Έρευνα έδειξε[145], ότι σε πολλές χώρες ανά τον κόσμο, περίπου το 50% του πληθυσμού δεν χρησιμοποιεί smartphone. Δηλαδή σε ζητήματα ιχνηλάτησης αυτό το ποσοστό θα είναι αόρατο, διότι δεν είναι σε θέση να εγκαταστήσει την εφαρμογή και να περαστεί στο σύστημα. Το ανησυχητικό είναι ότι οι περισσότεροι που δεν χρησιμοποιούν smartphone είναι ηλικιωμένοι άνθρωποι, που

---

[143] Βλ. ενδεικτικά τις κατευθυντήριες γραμμές που εξέδωσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EPDB) στις 19 Μαρτίου 2020, European Data Protection Board, (2020) *Statement on the processing of personal data in the context of the COVID-19 outbreak*, διαθέσιμο σε pdf στο https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[144] Πρόκειται για ένα κείμενο σε μορφή ερωτοαπαντήσεων που δείχνουν τη λειτουργία της εφαρμογής, τη χρησιμότητα της καθώς και απαραίτητες λεπτομέρειες που αναδεικνύουν την αξιοπιστία της. Το κείμενο της Επιτροπής είναι διαθέσιμο σε pdf στο file:///C:/Users/user/Downloads/_____nbsp___nbsp_____.pdf

[145] Pew Research Center, (2019), *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, διαθέσιμο στο https://www.pewresearch.org/global/2019/02/05/smartphone-ownershipis-growing-rapidly-around-the-world-but-not-always-equally/

αποτελούν ευπαθείς ομάδες, ως γνωστόν. Ακόμη όμως και σε χώρες που το μεγαλύτερο μέρος του πληθυσμού χρησιμοποιεί έξυπνα κινητά, οι εφαρμογές ιχνηλάτησης δεν είναι αποδοτικές, επειδή είναι εγκατεστημένες από μικρό ποσοστό πολιτών. Ενδεικτικά αναφέρονται οι περιπτώσεις της Ταϊβάν και της Νοτίου Κορέας, όπου οι εγχώριες εφαρμογές ιχνηλάτησης δεν πέτυχαν, διότι ήταν εγκατεστημένες μόλις από το 10% του πληθυσμού[146]. Γίνεται λοιπόν αντιληπτό ότι, για να είναι αποδοτικά αυτά τα συστήματα, θα πρέπει να είναι εγκατεστημένα από μία αντιπροσωπευτική μερίδα του πληθυσμού.

Όμως, το μεγάλο μειονέκτημα που υπονομεύει τις εφαρμογές αυτές είναι άλλο. Όπως αναλύθηκε ανωτέρω, οι εφαρμογές μπορούν να εντοπίσουν τη «διαδρομή» του κορωνοϊού, αν δύο χρήστες της ήρθαν σε κοντινή επαφή και ο ένας κόλλησε τον άλλον. Ο ιός όμως δεν μεταδίδεται μόνο έτσι. Ο ιός μπορεί να μεταδοθεί και έμμεσα, μέσω μολυσμένων επιφανειών. Στην περίπτωση που κάποιος φορέας του ιού ακουμπήσει μία επιφάνεια και φύγει και μετά από λίγο έρθει κάποιος άλλος και ακουμπήσει την ίδια επιφάνεια, είναι πιθανό να κολλήσει μεν αλλά δεν μπορεί να το εντοπίσει η εφαρμογή δε. Αυτό συμβαίνει επειδή η εφαρμογή λειτουργεί μέσω Bluetooth, όπου οι χρήστες σε κοντινή απόσταση ανταλλάσσουν κωδικούς αναγνώρισης. Εδώ όμως δεν συμβαίνει κάτι τέτοιο, αφού δεν πρόκειται για άμεση επαφή αλλά για έμμεση επαφή με μολυσμένη επιφάνεια. Το πρόβλημα αυτό το έθιξε η ελληνική ΜΚΟ Homo Digitalis στην έκθεση της σχετικά με τις εφαρμογές ιχνηλάτησης[147]. Το συμπέρασμα το οποίο προκύπτει είναι, ότι οι εφαρμογές αυτές δεν μπορούν να αποτελέσουν πρόσφορο και αποτελεσματικό μέτρο από μόνες τους για την αντιμετώπιση της πανδημίας. Λόγω αυτής της ανεπάρκειας είναι ορθότερο να λειτουργούν συμπληρωματικά με τις υπόλοιπες παραδοσιακές μεθόδους ανίχνευσης και καταπολέμησης του ιού.

4. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΚΑΙ ΝΟΜΙΚΟΙ ΚΙΝΔΥΝΟΙ

Στο σημείο αυτό θα εξεταστεί το νομοθετικό πλαίσιο στο οποίο υπάγονται οι προβλεπτικές εφαρμογές, καθώς και οι νομικοί κίνδυνοι που απορρέουν από το υπάρχον πλαίσιο. Κρίθηκε πρέπον να αναλυθούν σε πρώτο βαθμό οι σχετικές εφαρμογές, γιατί μόνο ύστερα από την

---

[146] Isobel Asher Hamilton, (2020), *Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance*, διαθέσιμο στο https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3

[147] Βλ. Homo Digitalis υποσημείωση 114

κατανόηση της λειτουργίας τους, είναι εύκολο να προσδιοριστεί ο νομικός χώρος στον οποίο εντάσσονται. Εξετάζοντας τα προγράμματα προληπτικής αλλά και υγειονομικής αστυνόμευσης, δύο είναι οι βασικές έννοιες που ξεχωρίζουν. Η πρώτη είναι τα προσωπικά δεδομένα των πολιτών, τα οποία αποτελούν αντικείμενο επεξεργασίας από τα αλγοριθμικά συστήματα, και στην ουσία είναι η πηγή της ζωής τους. Η δεύτερη έννοια είναι η τεχνητή νοημοσύνη, η οποία έχει τη δυνατότητα να επεξεργάζεται τα προσωπικά δεδομένα. Συνεπώς πρέπει να προσδιοριστεί το νομικό πλαίσιο για τα προσωπικά δεδομένα καθώς και για την τεχνητή νοημοσύνη.

4.1 Νομικό πλαίσιο για τα προσωπικά δεδομένα

Φυσικά, όταν η συζήτηση οδηγείται στα προσωπικά δεδομένα το πρώτο νομοθέτημα που έρχεται στο μυαλό όλων είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ευρύτερα γνωστός και ως GDPR[148]. Ο Κανονισμός εκδόθηκε το 2016, με την έλευση της νέας ψηφιακής εποχής, σε μία προσπάθεια της Ένωσης να εκσυγχρονίσει τη νομοθεσία της, έτσι ώστε να ανταποκριθεί καλύτερα στις ανάγκες της εποχής. Ο GDPR αντικατέστησε την Οδηγία 95/46[149] για την προστασία των δεδομένων, προστατεύοντας και ακολουθώντας πιστά τις βασικές αρχές και τα δικαιώματα του υποκειμένου των δεδομένων που ορίζονταν στην Οδηγία. Μάλιστα ενίσχυσε τη θέση του υποκειμένου των δεδομένων αυξάνοντας τα δικαιώματά του (Κεφάλαιο ΙΙΙ του Κανονισμού). Πλέον το υποκείμενο έχει δικαίωμα επεξεργασίας (άρθρο 16), δικαίωμα στη λήθη (άρθρο 17), δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18), δικαίωμα στη φορητότητα (άρθρο 20) και το κυριότερο όλων, υποχρέωση γνωστοποίησης σε περίπτωση παραβίασης των δεδομένων (άρθρο 33). Παράλληλα αυξήθηκαν οι υποχρεώσεις του υπεύθυνου επεξεργασίας, με κυριότερη την υποχρέωση προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, γνωστό και ως data protection by design and by default που ορίζεται στο άρθρο 25 του Κανονισμού.

Ο GDPR από εδαφικής άποψης έχει πολύ ευρύ πεδίο εφαρμογής. Όπως διατυπώνεται και στο άρθρο 3, ο Κανονισμός έχει ισχύ σε επιχειρήσεις εγκατεστημένες στην ΕΕ, καθώς επίσης και σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία μη εγκατεστημένους στην

[148] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679, διαθέσιμος σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR

[149] ΟΔΗΓΙΑ 95/46/ΕΚ, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL

ΕΕ, οι οποίοι παρέχουν αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους. Ουσιαστικά εφόσον το υποκείμενο των δεδομένων είναι πολίτης της Ένωσης, ο Κανονισμός έχει εφαρμογή, ανεξάρτητα από τον τόπο στον οποίο γίνεται η επεξεργασία ή από τον τόπο εγκατάστασης του υπεύθυνου. Πρόκειται για ένα ιδιαίτερα σημαντικό άρθρο, καθώς οι περισσότεροι τεχνολογικοί κολοσσοί που κερδοσκοπούν αναλύοντας προσωπικά δεδομένα είναι εγκατεστημένοι σε άλλες Ηπείρους. Συνεπώς ο GDPR προβλέπει ένα ενιαίο σύνολο κανόνων περί προστασίας προσωπικών δεδομένων με ισχύ σε όλη την Ευρώπη, θεσπίζοντας ένα περιβάλλον ασφάλειας δικαίου. Για τον λόγο αυτόν ο Κανονισμός χαρακτηρίζεται ως Γενικός.

Παρ' όλα αυτά υπάρχουν ορισμένα πεδία της καθημερινότητας όπου ο GDPR δεν έχει εφαρμογή και αυτό ορίζεται στο άρθρο 2. Σύμφωνα με τη δεύτερη παράγραφο του άρθρου ο Κανονισμός δεν έχει ισχύ σε 4 περιπτώσεις: Πρώτον, σε δραστηριότητες που δεν εμπίπτουν στο πεδίο εφαρμογής του Δικαίου της Ένωσης, δεύτερον, σε διαδικασίες όπως οι συνοριακοί έλεγχοι και οι μεταναστευτικές πολιτικές, τρίτον, σε φυσικά πρόσωπα που επεξεργάζονται δεδομένα στο πλαίσιο αποκλειστικά ιδιωτικής χρήσης, και τέταρτον, στην περίπτωση που γίνεται επεξεργασία δεδομένων από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια. Η τέταρτη περίπτωση είναι και αυτή που ανοίγει το δρόμο για την Οδηγία 2016/680[150] , καθώς εφαρμόζεται ακριβώς σε αυτόν τον τομέα και πουθενά αλλού. Γι' αυτόν ακριβώς το λόγο η Οδηγία αυτή ονομάζεται και Οδηγία επιβολής του νόμου (Law Enforcement Directive, LED).

4.1.1 Η Οδηγία 2016/680

Η Οδηγία 2016/680, εκδόθηκε την ίδια χρονιά με τον Κανονισμό και ανέλαβε την αποστολή να ορίσει ένα ενιαίο σύστημα προστασίας των προσωπικών δεδομένων στο πλαίσιο της επιβολής του νόμου, καλούμενη να έρθει αντιμέτωπη με όλες τις ιδιαιτερότητες της κρατικής ασφάλειας. Κύρια αποστολή της Οδηγίας είναι να επιτύχει ισορροπία μεταξύ των δικαιωμάτων των φυσικών προσώπων και των θεμιτών σκοπών της σχετιζόμενης με την

[150] ΟΔΗΓΙΑ (ΕΕ) 2016/680, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EN

ασφάλεια επεξεργασίας[151]. Σε δεύτερο βαθμό, διευκολύνεται η μεταφορά δεδομένων προσωπικού χαρακτήρα, ανάμεσα σε αρμόδιες αρχές εντός της Ένωσης (άρθρο 1 παρ. 2 Οδηγίας). Ουσιαστικά, είναι ένα κείμενο που λειτουργεί συμπληρωματικά με τον GDPR, παρέχοντας παράλληλα μια εξειδίκευση σε ένα πεδίο που δεν μπορεί να εφαρμοστεί ο τελευταίος. Επομένως οι βασικές αρχές που θα πρέπει να διέπουν την επεξεργασία, τα δικαιώματα των υποκειμένων και οι υποχρεώσεις των υπευθύνων επεξεργασίας είναι σχεδόν οι ίδιες και στα δύο κείμενα. Όμως, τα δύο κείμενα, παρά τις πολλές ομοιότητες, διαφέρουν κατά πολύ ως προς το πεδίο δράσης. Ο GDPR προβλέπει γενικούς κανόνες για την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν και για τη διασφάλιση της ελεύθερης κυκλοφορίας των εν λόγω δεδομένων στην ΕΕ (άρθρο 2 παρ. 1 GDPR). Αντιθέτως, η LED θεσπίζει γενικούς κανόνες για την προστασία των δεδομένων αποκλειστικά στους τομείς της δικαστικής συνεργασίας σε ποινικές υποθέσεις και της αστυνομικής συνεργασίας (άρθρο 1 παρ. 1 Οδηγία 2016/680). Για να γίνει πιο σαφής αυτός ο διαχωρισμός, εφόσον μια αρμόδια αρχή επεξεργάζεται προσωπικά δεδομένα για πρόβλεψη ή διερεύνηση ποινικών αδικημάτων εφαρμόζεται η LED, αντιθέτως, όταν οι αρμόδιες αστυνομικές αρχές επεξεργάζονται προσωπικά δεδομένα για άλλους σκοπούς (π.χ. αρχειοθέτηση), τότε εφαρμόζεται ο Γενικός Κανονισμός GDPR (άρθρο 9 Οδηγίας).

Μιας και ένας από τους δύο στόχους της Οδηγίας είναι η διασφάλιση της προστασίας δεδομένων προσωπικού χαρακτήρα, επαναλαμβάνονται σε μεγάλο βαθμό οι βασικές αρχές προστασίας δεδομένων[152], τα δικαιώματα των υποκειμένων των δεδομένων καθώς και οι υποχρεώσεις των υπεύθυνων επεξεργασίας. Για παράδειγμα οι διατάξεις σχετικά με την ασφάλεια των δεδομένων, την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού και τις γνωστοποιήσεις παραβίασης δεδομένων έχουν παρόμοια διατύπωση και στα δύο κείμενα. Όμως στην προσπάθεια της να βρει την ισορροπία ανάμεσα στην προστασία των δεδομένων και την αποτελεσματική επιβολή του Νόμου, η Οδηγία προβαίνει σε ορισμένες διαφοροποιήσεις.

---

[151] Οργανισμός Θεμελιωδών Δικαιωμάτων της ΕΕ και Συμβούλιο της Ευρώπης (2018), *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*, διαθέσιμο σε pdf στο https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[152] Βλ. άρθρο 5 του Κανονισμού και άρθρο της 4 Οδηγίας

Αρχικά, ως προς τις βασικές αρχές προστασίας των δεδομένων[153], υπάρχουν ουσιώδεις αλλαγές στη διατύπωση, που επηρεάζουν σημαντικά τα δικαιώματα των υποκειμένων. Η πρώτη βασική διαφορά είναι ότι στην Οδηγία δεν καταγράφεται ρητά η αρχή της διαφάνειας[154]. Στον χώρο του Ποινικού Δικαίου η ύπαρξη διαφάνειας πολλές φορές δεν είναι εφικτή, καθώς μπορεί να υπονομεύσει εγκληματολογικές έρευνες που βρίσκονται σε εξέλιξη. Με αυτό τον ελιγμό προσπαθεί να βρει μία μέση λύση η Οδηγία δημιουργώντας όμως πολλές απορίες στο κατά πόσο η απουσία της διαφάνειας για την διευκόλυνση του έργου των αρχών ευνοεί τους πολίτες ή όχι. Αντίστοιχα οι αρχές του περιορισμού του σκοπού[155] και της ελαχιστοποίησης των δεδομένων[156] έχουν μία πολύ πιο «ευρεία έννοια», στην Οδηγία, σε σχέση με τη διατύπωση τους στον Κανονισμό. Η αλήθεια είναι, ότι οι συγκεκριμένες διατυπώσεις επιτυγχάνουν την ισορροπία που επιδιώκει να βρει η Οδηγία ανάμεσα στην προστασία των δεδομένων και στην άσκηση της αστυνομικής εξουσίας[157]. Δεν γίνεται όμως να παραλειφθεί, η πιθανή κατάχρηση εξουσίας που μπορεί να προκύψει από αυτή τη «χαλαρή διατύπωση». Καταρχάς σύμφωνα με τα άρθρα 4 παράγραφος 1 περίπτωση β, σε συνδυασμό με τις παραγράφους 2 και 3 του ιδίου άρθρου της Οδηγίας, καθίσταται αρκετά εύκολο να δικαιολογηθεί η επεξεργασία δεδομένων για διαφορετικό σκοπό από τις αρμόδιες αρχές. Αυτό συμβαίνει γιατί η Οδηγία δεν απαιτεί έλεγχο συμβατότητας του σκοπού, κάτι που ισχύει στον Κανονισμό[158]. Αντίθετα το μόνο που απαιτεί η Οδηγία είναι να είναι εξουσιοδοτημένος για το σκοπό αυτό, είτε από το Ενωσιακό είτε από το εγχώριο Δίκαιο, ο υπεύθυνος επεξεργασίας, καθώς και να είναι απαραίτητη και ανάλογη με το σκοπό η επεξεργασία. Επιπλέον, ιδιαίτερα απλοϊκή φαίνεται η διατύπωση της αρχής

---

[153] Οι βασικές αρχές που προβλέπονται και στα δύο κείμενα είναι οι εξής: α) αρχή της νομιμότητας και της αντικειμενικότητας, β) αρχή του περιορισμού του σκοπού, γ) αρχή της ελαχιστοποίησης των δεδομένων, δ) αρχή της ακρίβειας, ε) αρχή του περιορισμού του χώρου αποθήκευσης, στ) αρχή της εμπιστευτικότητας και ακεραιότητας, ζ) αρχή της λογοδοσίας.

[154] Βλ. άρθρο 4 (1) (α) της Οδηγίας σε σχέση με άρθρο 5 (1) (α) του Κανονισμού

[155] Βλ. άρθρο 4 (1) (β) της Οδηγίας

[156] Βλ. άρθρο 4 (1) (γ) της Οδηγίας

[157] Paul De Hert & Juraj Sajfert (2021), *THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS: FRAMING BIG DATA POLICING THROUGH THE PURPOSE LIMITATION AND DATA MINIMISATION PRINCIPLES OF THE DIRECTIVE (EU) 2016/680*, BRUSSELS PRIVACY HUB, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=195074122123114102126066074012007025053087027082034055099022095106113069068102090110053035120006007034111112086009100031001007126082004073093125029122096025007025031013007074071071121002072027025089121086102068031018085102091109091080077116117106092&EXT=pdf&INDEX=TRUE

[158] Βλ. άρθρο 6 (4) του Κανονισμού

ελαχιστοποίησης των δεδομένων. Σύμφωνα με τον Κανονισμό[159] τα δεδομένα που συλλέγονται πρέπει να περιορίζονται στο αναγκαίο για τους σκοπούς της επεξεργασίας, διατύπωση αρκετά αυστηρή καθώς δεσμεύει τους υπεύθυνους να ελέγχουν συνεχώς τα δεδομένα που συλλέγουν και να διαγράφουν τα περιττά δεδομένα. Αντιθέτως στην Οδηγία, τα δεδομένα που συλλέγονται δεν πρέπει να είναι υπερβολικά σε σχέση με το σκοπό της επεξεργασίας. Πρόκειται για μία διατύπωση αρκετά πιο ήπια, που δίνει μεγαλύτερο εύρος δράσης στις αρμόδιες αρχές. Οι αρχές μπορούν ελεύθερα και με λιγότερη ακρίβεια να συλλέγουν και να επεξεργάζονται δεδομένα. Το μόνο που χρειάζεται, είναι να φροντίσουν να μην επεξεργάζονται υπερβολικά σύνολα δεδομένων. Αυτή η καινοτομία, από τη μία διευκολύνει και προωθεί τις πρακτικές ILP, εμποδίζοντας παράλληλα την συλλογή τεραστίου όγκου δεδομένων που μπορεί να οδηγήσει στη μαζική παρακολούθηση, από την άλλη όμως, αυτή η «χαλαρή» διατύπωση, δεν αποτελεί εγγύηση ότι οι αρμόδιες αρχές θα τηρήσουν αυτή την αρχή και θα απέχουν από την συγκεκριμένη υπερβολή.

Λόγω του ιδιαίτερου πεδίου εφαρμογής της Οδηγίας ορισμένα δικαιώματα του υποκειμένου, που περιλαμβάνονται στον Κανονισμό, ελλείπουν από την Οδηγία ή υπόκεινται σε αυστηρούς περιορισμούς, με κυριότερο το δικαίωμα στην φορητότητα[160] που απουσιάζει πλήρως από την τελευταία. Είναι αρκετά πάντως τα δικαιώματα που ενυπάρχουν και στα δύο κείμενα, όπως το δικαίωμα στην πληροφόρηση[161], το δικαίωμα στην πρόσβαση[162], το δικαίωμα διόρθωσης[163], το δικαίωμα διαγραφής[164] και το δικαίωμα περιορισμού της επεξεργασίας[165]. Η ομοιότητα είναι ακόμα πιο έντονη στις υποχρεώσεις του υπεύθυνου επεξεργασίας[166]. Ουσιαστικά στις διατάξεις της Οδηγίας επαναλαμβάνονται οι υποχρεώσεις του υπεύθυνου επεξεργασίας που είχαν διατυπωθεί για πρώτη φορά στον Κανονισμό. Λόγω της ιδιαιτερότητας του πεδίου εφαρμογής της Οδηγίας, προστέθηκαν δύο νέες υποχρεώσεις που εντοπίζονται στα άρθρα 6 και 7. Σύμφωνα με το άρθρο 6, όταν είναι εφικτό πρέπει να γίνεται, από τον υπεύθυνο επεξεργασίας, σαφής διάκριση μεταξύ προσωπικών δεδομένων διαφορετικών κατηγοριών υποκειμένων, όπως για παράδειγμα υπόπτων για αξιόποινες

[159] Βλ. άρθρο 5 (1) (γ) του Κανονισμού
[160] Βλ. άρθρο 20 του Κανονισμού
[161] Βλ. άρθρα 12-14 της Οδηγίας και άρθρα 12-14 του Κανονισμού
[162] Βλ. άρθρα 14-15 της Οδηγίας και άρθρο 15 του Κανονισμού
[163] Βλ. άρθρο 16 της Οδηγίας και άρθρο 16 του Κανονισμού
[164] Βλ. άρθρο 16 της Οδηγίας και άρθρο 17 του Κανονισμού
[165] Βλ. άρθρο 16 της Οδηγίας και άρθρο 18 του Κανονισμού
[166] Βλ. άρθρα 20-34 της Οδηγίας και άρθρα 25-39 του Κανονισμού

πράξεις και θυμάτων εγκληματικών ενεργειών. Επίσης σύμφωνα με το άρθρο 7, τα δεδομένα που προέρχονται από επιβεβαιωμένα γεγονότα, πρέπει να διακρίνονται από τα δεδομένα που βασίζονται σε προσωπικές εκτιμήσεις.

Τέλος, μία πολύ σημαντική διαφορά που χρήζει αναφοράς, είναι οι διαφορετικές προϋποθέσεις που απαιτούνται για τη νομιμότητα της επεξεργασίας των δεδομένων[167]. Το άρθρο 6 του Κανονισμού, ορίζει έξι περιπτώσεις που νομιμοποιούν την επεξεργασία, με την πρώτη να είναι η συναίνεση του υποκειμένου και οι υπόλοιπες πέντε αφορούν καταστάσεις όπου η επεξεργασία δεδομένων είναι αναγκαία, όπως η ανάγκη εκτέλεσης μίας σύμβασης, η ανάγκη συμμόρφωσης με μία έννομη υποχρέωση, ή η ανάγκη για την προστασία των ζωτικών συμφερόντων των υποκειμένων. Αντιθέτως, το άρθρο 8 της Οδηγίας, ορίζει μονάχα μία νομική βάση για την επεξεργασία δεδομένων, που είναι η αναγκαιότητα για την εκτέλεση καθήκοντος που ασκείται από αρμόδια αρχή, στο πλαίσιο της επιβολής του νόμου. Με άλλα λόγια, στην Οδηγία η συναίνεση του υποκειμένου όχι απλά δεν απαιτείται αλλά δεν αποτελεί καν νομική βάση για την νομιμότητα της επεξεργασίας. Αυτό έχει μία λογική, αν σκεφτεί κανείς ότι οι ύποπτοι για κάποιο έγκλημα είναι πιθανό να μην συναινούν για την επεξεργασία των δεδομένων τους, ενώ οι αστυνομικές αρχές χρειάζονται αυτά τα δεδομένα για να κάνουν τη δουλειά τους. Βέβαια το ίδιο καθεστώς ισχύει και με τα θύματα και τους μάρτυρες, που ενδεχομένως να μην θέλουν να δώσουν την συγκατάθεση τους διότι φοβούνται ή δεν νιώθουν ασφαλείς.

4.1.2 Λοιπά νομοθετήματα και Πρωτογενές Δίκαιο

Το γεγονός ότι ο GDPR και η LED είναι τα σημαντικότερα νομοθετήματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, δεν σημαίνει ότι είναι και τα μοναδικά. Αντιθέτως, η προσπάθεια της Ευρωπαϊκής Ένωσης στη διασφάλιση της καλύτερης δυνατής προστασίας των προσωπικών δεδομένων αποδεικνύεται από τις πολλαπλές Οδηγίες και προτάσεις Κανονισμών που έχουν δημοσιευθεί τα τελευταία χρόνια. Ιδιαίτερη αναφορά χρήζει η Οδηγία e-Privacy[168], που ρυθμίζει την προστασία της ιδιωτικής ζωής στον τομέα των

[167] Leiser, M.R. and Custers, B.H.M. (2019), *The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680*, European Data Protection Law Review. Vol. 5, nr. 3, p. 367-378, διαθέσιμο σε pdf στο https://scholarlypublications.universiteitleiden.nl/access/item%3A2980780/view

[168] ΟΔΗΓΙΑ 2002/58/ΕΚ, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EN

ηλεκτρονικών επικοινωνιών, καθώς και στον Κανονισμό 2018/1725[169] γνωστό και ως EU-DPR, που ρυθμίζει την προστασία των προσωπικών δεδομένων από τα θεσμικά όργανα και τους λοιπούς οργανισμούς της Ένωσης. Πάντως εκτός πεδίου εφαρμογής του Κανονισμού είναι η Europol[170] και η Ευρωπαϊκή Εισαγγελία (EPPO)[171].

Σε αυτό το σημείο είναι απαραίτητο να διευκρινιστεί κάτι. Όλα τα προαναφερθέντα νομοθετικά κείμενα δεν λειτουργούν ανεξάρτητα από τις αρχές και τις αξίες της Ένωσης. Αντιθέτως, αποτελούν δευτερογενές Δίκαιο, το οποίο σέβεται πλήρως τα δικαιώματα που διασφαλίζονται από το Πρωτογενές Δίκαιο. Για το δικαίωμα στην προστασία των προσωπικών δεδομένων καθώς και για την προστασία της ιδιωτικότητας, που είναι στενά συνδεδεμένο με την προστασία των δεδομένων προσωπικού χαρακτήρα, μίλησαν πρώτα η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)[172] με το άρθρο 8, και ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης με τα άρθρα 7 και 8[173]. Μάλιστα το άρθρο 8 του Χάρτη αναφέρεται αποκλειστικά στο δικαίωμα προστασίας των προσωπικών δεδομένων. Όλα αυτά τα κείμενα εξακολουθούν να ισχύουν. Οι Κανονισμοί και οι Οδηγίες που δημοσιεύονται είναι απόλυτα εξαρτημένοι από αυτά και προσπαθούν να ενισχύσουν την προστασία των δικαιωμάτων που προβλέπονται από το Πρωτογενές Δίκαιο.

4.2 Νομικοί κίνδυνοι σχετικά με τα προσωπικά δεδομένα

Το γεγονός ότι υπάρχουν πολλαπλά νομοθετήματα για την προστασία δεδομένων προσωπικού χαρακτήρα, εκφράζει την προσπάθεια της Ευρωπαϊκής Ένωσης για την εγκαθίδρυση ενός εναρμονισμένου νομικού πλαισίου, στο οποίο θα περιέχονται όλες οι διαδικασίες επεξεργασίας δεδομένων, ιδίως οι επεξεργασίες που διέπονται από τις αρχές επιβολής του νόμου[174]. Η πραγματικότητα όμως διαφέρει αισθητά. Τη δεδομένη χρονική

[169] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2018/1725, διαθέσιμος σε pdf στο https://edps.europa.eu/sites/edp/files/publication/regulation_eu_2018_1725_el.pdf
[170] Πληροφορίες για την Europol στο https://www.europol.europa.eu/
[171] Πληροφορίες για την EPPO στο https://www.eppo.europa.eu/en
[172] Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, διαθέσιμη σε pdf στο https://www.echr.coe.int/documents/convention_ell.pdf
[173] ΧΑΡΤΗΣ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ, διαθέσιμος σε pdf στο https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EL:PDF
[174] European Parliament (2014), *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in*

στιγμή του Ευρωπαϊκό Δίκαιο δεν παρέχει προστασία απέναντι σε όλων των ειδών τις επεξεργασίες. Μελετώντας το πεδίο εφαρμογής του κάθε σχετικού Κανονισμού, γίνεται ευθύς αμέσως αντιληπτό ότι υπάρχουν φορείς που εξαιρούνται, όπως για παράδειγμα η Europol από τον Κανονισμό EU-DPR, αλλά και διάφορες αρχές επιβολής του νόμου δεν εμπίπτουν στην LED. Για τον λόγο αυτό, η Ευρωπαϊκή Επιτροπή, τον Ιούνιο του 2020, ανακοίνωσε το σχέδιό της για επέκταση του πεδίου εφαρμογής της LED[175]. Επίσης, η ύπαρξη πολλών νομοθετημάτων με το ίδιο αντικείμενο (τα προσωπικά δεδομένα), αλλά με διαφορετικό πεδίο εφαρμογής, έχει ως αποτέλεσμα, αντί να δημιουργηθεί ένα εναρμονισμένο νομικό πλαίσιο, να δημιουργηθεί ένας πολυεπίπεδος χώρος προστασίας, όπου υπάρχουν διαφορετικές υποχρεώσεις και απαιτήσεις των υπευθύνων επεξεργασίας, οι οποίες επηρεάζουν, και πολλές φορές υποβαθμίζουν, την προστασία ενός θεμελιώδους ανθρώπινου δικαιώματος[176].

Επιπρόσθετα, ο πλουραλισμός νομοθετικών κειμένων δημιουργεί σύγχυση, καθώς δεν είναι πάντα ευκόλως διακριτό το πότε θα εφαρμοσθεί ένας συγκεκριμένος Κανονισμός. Ας πάρουμε για παράδειγμα την περίπτωση του GDPR και της LED. Σύμφωνα με το άρθρο 2 παράγραφος 2 περίπτωση δ του Κανονισμού, σε συνδυασμό με το άρθρο 1 της Οδηγίας, όταν οι αρμόδιες αρχές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την ανίχνευση και διερεύνηση ποινικών αδικημάτων, στο πλαίσιο επιβολής του νόμου, δεν εφαρμόζεται ο GDPR αλλά η LED. Οι επεξεργασίες προσωπικών δεδομένων όμως, δεν είναι τόσο ξεκάθαρες όσο φαίνεται από τη διατύπωση των κειμένων. Αντιθέτως, είναι πολύπλοκες διαδικασίες, όπου κάθε βήμα αυτής της διαδικασίας πραγματοποιείται με διαφορετικό τρόπο και με διαφορετικό σκοπό[177]. Επίσης, δεν αποκλείεται η ίδια διαδικασία να έχει διττό σκοπό. Δηλαδή ενδέχεται η ίδια επεξεργασία να πραγματοποιείται από αρμόδια αρχή τόσο για διερεύνηση εγκλημάτων, όπου θα εφαρμόζεται η LED, όσο και για άλλους σκοπούς άσχετους με την αρμοδιότητά της (π.χ. στατιστική έρευνα), όπου θα εφαρμόζεται ο GDPR. Αυτή η σύγχυση,

---

Justice and Home Affairs, διαθέσιμο σε pdf στο https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.pdf?redirect

[175] COM (2020), *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*, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

[176] Belfiore R. (2013), *The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters*, Springer, 2013, pp. 355-370

[177] Βλ European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, υποσημείωση 93

ελέω πολυπλοκότητας, επιφέρει δύο αρνητικές επιπτώσεις. Αρχικά, σε πολλές διαδικασίες επεξεργασίας δεδομένων από αρμόδιες αρχές εφαρμόζεται ο GDPR, ο οποίος έχει λιγότερο αυστηρές υποχρεώσεις από τη LED, όπως θα αναλυθεί στη συνέχεια και δεύτερον, αυτά τα διαφορετικά νομικά καθεστώτα, εξαιτίας των πολλαπλών πιθανών χρήσεων των δεδομένων, είναι απολύτως υπεύθυνα για το μείζον πρόβλημα της έλλειψης διαφάνειας[178].

4.2.1 Ο κίνδυνος της αυτοματοποιημένης λήψης απόφασης

Όπως αναλύθηκε σε προηγούμενο κεφάλαιο[179], αυτοματοποιημένη λήψη απόφασης είναι η διαδικασία, σύμφωνα με την οποία, ένα υπολογιστικό σύστημα λαμβάνει μία απόφαση για ένα υποκείμενο «μόνο του», δηλαδή χωρίς ανθρώπινη παρέμβαση. Μία μορφή αυτοματοποιημένης λήψης απόφασης είναι η κατάρτιση προφίλ (profiling)[180], η οποία τόσο στην LED (άρθρο 3 περίπτωση 4) όσο και στον GDPR (άρθρο 4 περίπτωση 4) έχει ακριβώς τον ίδιο ορισμό. Σύμφωνα λοιπόν με τα ανωτέρω κείμενα, κατάρτιση προφίλ είναι «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.». Εξετάζοντας τον ανωτέρω ορισμό, γίνεται άμεσα αντιληπτό ότι τα περισσότερα συστήματα προληπτικής αστυνόμευσης όχι μόνο λαμβάνουν αυτοματοποιημένες αποφάσεις, αλλά χρησιμοποιούν και τη μέθοδο του profiling, όπως για παράδειγμα το COMPAS, που εξετάζει πόσο επικίνδυνοι είναι οι εγκληματίες να διαπράξουν έγκλημα στο μέλλον, λαμβάνοντας υπόψιν πολλούς παράγοντες από την προσωπική τους ζωή. Για τον λόγο αυτό είναι απαραίτητη περαιτέρω ανάλυση.

Σύμφωνα με το άρθρο 11 της LED, η λήψη αυτοματοποιημένων αποφάσεων απαγορεύεται πλην ελαχίστων εξαιρέσεων, που ορίζονται στις επόμενες παραγράφους. Αυτή η

---

[178] Fondazione Giacomo Brodolini (FGB) (2019),*Fundamental rights review of EU data collection instruments and programmes: Final report*, διαθέσιμο σε pdf στο https://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf

[179] Βλ. υποσημείωση 97

[180] ARTICLE 29 DATA PROTECTION WORKING PARTY (2017), *Opinion 2/2017 on data processing at work*, διαθέσιμο σε pdf στο https://ec.europa.eu/newsroom/article29/items/610169

απαγόρευση εντοπίζεται και στο άρθρο 22 του GDPR, διατυπωμένη με παρόμοιο τρόπο. Παρ' όλα αυτά υπάρχουν ορισμένες σημαντικότατες διαφορές. Αρχικά στο άρθρο 11 της LED απαγορεύεται η λήψη απόφασης που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, ενώ στο άρθρο 22 του GDPR το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας. Δηλαδή η ίδια έννοια, στην πρώτη περίπτωση διατυπώνεται πιο σκληρά και προστατευτικά σαν απαγόρευση, ενώ στη δεύτερη περίπτωση πιο ήπια, ως δικαίωμα του υποκειμένου να μην υποστεί επεξεργασία. Η διατύπωση του άρθρου 22 του GDPR ως δικαίωμα, είναι ιδιαίτερα προβληματική και επίφοβη, καθώς μπορεί να οδηγήσει σε αυθαιρεσίες. Υπάρχει ο φόβος ότι αυτό το δικαίωμα μπορεί να λειτουργήσει αντίστροφα εις βάρος των υποκειμένων, δίνοντας το ελεύθερο στους υπεύθυνους επεξεργασίας να λαμβάνουν αυτοματοποιημένες αποφάσεις και να προσαρμόζουν τη συμπεριφορά τους μόνο σε περίπτωση που τα υποκείμενα επικαλεστούν τα δικαιώματά τους[181]. Αντιθέτως, αν ήταν διατυπωμένο σαν απαγόρευση, τότε θα ήταν και πιο εύκολο για τα υποκείμενα να προστατευτούν.

4.2.2 Ο κίνδυνος του άρθρου 23 του GDPR

Πέρα από το άρθρο 22 του Κανονισμού, ιδιαίτερα προβληματικό έχει αποδειχθεί και το επόμενο άρθρο του. Σύμφωνα λοιπόν με το άρθρο 23 του Κανονισμού, τα δικαιώματα του υποκειμένου που προβλέπονται στα άρθρα 12 έως 22 και στο άρθρο 34, καθώς και στο άρθρο 5 μπορούν να περιοριστούν από ενωσιακούς ή εθνικούς νόμους, όταν είναι αναγκαίο και αναλογικό μέτρο για τη διασφάλιση υπέρτερων αξιών, όπως η δημόσια ασφάλεια, η εθνική άμυνα, η διερεύνηση και ανίχνευση εγκλημάτων και άλλοι περιοριστικά αναφερόμενοι λόγοι δημοσίου συμφέροντος. Η διάταξη αυτή δικαίως έχει χαρακτηριστεί ακραία αντιφατική, καθώς επιτρέπει παρεκκλίσεις από βασικές έννοιες του GDPR, όπως τα δικαιώματα του υποκειμένου[182]. Ενώ γίνονται εντατικές προσπάθειες εντός Ένωσης για να διασφαλιστούν τα δικαιώματα των πολιτών, εμφανίζεται αυτό το άρθρο και τα ανατρέπει όλα. Πρόκειται για ένα νομικό «παραθυράκι» που βοηθά τις αρμόδιες αρχές και τους

[181] Margot E. Kaminski (2018), *The Right to Explanation, Explained*, University of Colorado Law School, διαθέσιμο σε pdf στο https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2335&context=articles

[182] Julian Wagner and Alexander Benecke (2016), *National Legislation within the Framework of the GDPR*, διαθέσιμο σε pdf στο http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/national-legislation-and-gdpr.pdf

υπεύθυνους επεξεργασίας να επεξεργάζονται ελεύθερα τα προσωπικά δεδομένα των Ευρωπαίων χωρίς να έχουν ιδιαίτερες δεσμεύσεις. Μάλιστα, το γεγονός ότι μπορεί να περιοριστεί και το δικαίωμα του άρθρου 22, θα έπρεπε να μας προβληματίζει, γιατί έτσι μπορεί να διαμορφωθεί μία ολόκληρη νέα πραγματικότητα βασισμένη στο profiling, καταρρίπτοντας κάθε έννοια ιδιωτικότητας και ανθρώπινης αξιοπρέπειας. Η αλήθεια είναι ότι μέχρι στιγμής δεν έχει αξιοποιηθεί το άρθρο ούτε από την Ένωση, ούτε από κάποια χώρα-μέλος. Ο κίνδυνος όμως παραμονεύει, οπότε πρέπει να είμαστε σε εγρήγορση. Στο σημείο αυτό, είναι απαραίτητο να αναφερθεί ότι και η δράση της LED μπορεί να περιοριστεί. Σύμφωνα με την αιτιολογική σκέψη 44 της Οδηγίας, τα δικαιώματα των υποκειμένων μπορούν να περιοριστούν για να αποφευχθεί η όποια παρεμπόδιση της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, αλλά και για να διασφαλιστεί η προστασία της δημόσιας ασφάλειας ή της εθνικής ασφάλειας ή η προστασία των δικαιωμάτων και των ελευθεριών τρίτων.

4.2.3 Ο κίνδυνος της επέκτασης της προβλεπόμενης χρήσης της AI (function creep)

Όπως προαναφέρθηκε ανωτέρω[183], στην Οδηγία 2016/680, η αρχή περιορισμού του σκοπού είναι διατυπωμένη με τέτοιο τρόπο, που διευκολύνει την καταστρατήγησή της από τις αρχές επιβολής του νόμου. Ουσιαστικά μελετώντας το άρθρο 4 παράγραφος 2 της Οδηγίας, η επεξεργασία δεδομένων για διαφορετικό σκοπό από τον πρωταρχικό επιτρέπεται εφόσον ο υπεύθυνος επεξεργασίας είναι εξουσιοδοτημένος να επεξεργάζεται τα εν λόγω δεδομένα για τον σκοπό αυτό σύμφωνα με το δίκαιο της Ένωσης ή το δίκαιο ενός κράτους μέλους και εφόσον η επεξεργασία είναι απαραίτητη και ανάλογη στον νέο αυτό σκοπό. Πρακτικά αυτό σημαίνει, ότι μία εφαρμογή προληπτικής αστυνόμευσης που έχει συγκεκριμένο έργο (για παράδειγμα να εντοπίσει περιοχές υψηλού κινδύνου εγκληματικότητας), μπορεί ελεύθερα να αρχίσει να επεξεργάζεται δεδομένα από διαφορετικές πηγές, εφόσον διευκολύνεται έτσι η αποστολή της. Αυτή η αυξημένη συλλογή νέων δεδομένων είναι ικανή να διαφοροποιήσει τον αρχικό σκοπό του συστήματος. Συνεχίζοντας το παράδειγμα, η εφαρμογή αυτή με τις νέες δυνατότητες μπορεί πέρα από το να εντοπίζει hotspots να παρακολουθεί και να συλλέγει στοιχεία των πολιτών που χαρακτηρίστηκαν ύποπτοι στο σύστημα. Αυτό είναι νόμιμο, καθώς πρόκειται για σκοπό που εμπίπτει στην προσπάθεια επιβολής του νόμου και η ίδια αστυνομική αρχή είναι εξουσιοδοτημένη και για αυτόν. Επιπλέον η περαιτέρω

[183] Βλ. ενότητα 4.1.1

επεξεργασία είναι απαραίτητη, καθώς έτσι λειτουργεί αποδοτικότερα η προληπτική αστυνόμευση. Αυτή η χρήση της τεχνητής νοημοσύνης για σκοπό διαφορετικό από αυτόν για τον οποίο κατασκευάστηκε σε πρώτο βαθμό αποτελεί το πρόβλημα του function creep[184].

Δύο είναι οι παράγοντες που συμβάλλουν στη γέννηση του function creep. Πρώτος παράγοντας είναι η ραγδαία τεχνολογική ανάπτυξη η οποία δημιούργησε τον κόσμο των big data και είναι αυτή που δίνει τη δυνατότητα στα προεγκληματικά συστήματα να αναλύουν και να αποθηκεύουν όλο και περισσότερα δεδομένα κατά τη διερεύνηση των εγκληματικών πράξεων. Δεύτερον, η ευνοϊκή διατύπωση της αρχής του περιορισμού του σκοπού, δίνει το ελεύθερο στις αρμόδιες αρχές, όχι απλώς να συνεχίσουν το έργο τους απρόσκοπτα, αλλά και να το εξελίξουν, καθώς η τεχνολογική πρόοδος και η συνεχώς αυξανόμενη διαθεσιμότητα των δεδομένων τις διευκολύνουν να λαμβάνουν υπόψιν περισσότερες μεταβλητές, με αποτέλεσμα να αυξάνονται τα μακροπρόθεσμα συμπεράσματα σχετικά με τις ανθρώπινες δραστηριότητες[185]. Συνεπώς αυτή η απουσία ενός νομοθετικού κειμένου που ορίζει με αυστηρό τρόπο την αρχή του περιορισμού του σκοπού, δίνει το έναυσμα στην ακραία διόγκωση των σκοπών των προληπτικών εφαρμογών που πραγματοποιείται με την ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων, γεγονός που μπορεί να οδηγήσει μέχρι και σε πρακτικές μαζικής παρακολούθησης.

4.3 Νομικό πλαίσιο για την τεχνητή νοημοσύνη και AI ACT

Αναπόσπαστο κομμάτι αυτής της νέας ψηφιακής πραγματικότητας αποτελεί φυσικά και η τεχνητή νοημοσύνη. Από το 2018 και έπειτα, η απορρόφηση της τεχνητής νοημοσύνης και των απείρων δυνατοτήτων της αποτέλεσε βασικό στόχο της Ένωσης, όπως εκδηλώθηκε με την ευρωπαϊκή στρατηγική για την τεχνητή νοημοσύνη, η οποία ξεκίνησε τον Απρίλιο του 2018[186]. Για να γίνει όμως εφικτή αυτή η αφομοίωση, θα έπρεπε να εξασφαλισθεί το κατάλληλο ηθικό και νομικό πλαίσιο, το οποίο θα είναι σύμφωνο με τις αρχές και αξίες του

---

[184] Ivo Emanuilov, Stefano Fantin, Thomas Marquenie, Plixavra Vogiatzolgou, (2020), *Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence*, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020, UNICRI Special Collection on AI, διαθέσιμο σε pdf στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3679850

[185] Wojciech Filipkowski (2019), *Predictive policing using the latest technological advancements*, διαθέσιμο στο https://www.researchgate.net/publication/337155284_Predictive_policing_using_the_latest_technological_advancements

[186] European Commission (2018), *A European approach to artificial intelligence*, διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

ενωσιακού Δικαίου[187]. Έτσι, τα τελευταία χρόνια παρατηρήθηκαν πολλαπλές συντονισμένες προσπάθειες των κρατών-μελών για να εντάξουν την τεχνητή νοημοσύνη στη νομική πραγματικότητα. Αποκορύφωμα αυτής της προσπάθειας ήταν η δημοσίευση της Λευκής Βίβλου για την τεχνητή νοημοσύνη το 2020[188]. Πρόκειται για ένα κείμενο ηπίου Δικαίου (soft law), το οποίο αναλύει τα πλεονεκτήματα και τους κινδύνους της τεχνητής νοημοσύνης, καθώς και τις δυνατότητές της, και τις ευκαιρίες της Ευρωπαϊκής Ένωσης στην παγκόσμια αγορά. Το κείμενο υπογραμμίζει την ανάγκη προστασίας της ανθρώπινης αξιοπρέπειας και ιδιωτικότητας και ανοίγει το δρόμο για νέες, πιο «σκληρές» απαιτήσεις απέναντι στους δημιουργούς της AI, έτσι ώστε να σέβονται τα ανθρώπινα δικαιώματα. Για τον λόγο αυτό, ορισμένους τομείς, στους οποίους εφαρμόζεται η τεχνητή νοημοσύνη, τους χαρακτηρίζει ως «υψηλού κινδύνου», όπως ο χώρος της υγείας αλλά και η ταυτοποίηση μέσο αναγνώρισης προσώπου.

Τη Λευκή Βίβλο την συμπληρώνει μία πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων Κανόνων για την τεχνητή νοημοσύνη, γνωστό και ως AI ACT[189]. Η πρόταση, αποτελεί πρωτοβουλία της Ευρωπαϊκής Επιτροπής και περιλαμβάνει την αιτιολογική της έκθεση και εννέα παραρτήματα, ως συνέχεια του κειμένου της Λευκής Βίβλου. Με το κείμενο αυτό, η Επιτροπή δηλώνει ότι η τεχνητή νοημοσύνη μπορεί να ρυθμιστεί νομοθετικά, ασχέτως αν βρισκόμαστε στα πρώιμα στάδια της νέας ψηφιακής εποχής και πολλές έννοιες είναι άγνωστες. Το πεδίο δράσης του Κανονισμού μοιάζει αρκετά με αυτό του GDPR καθώς αφορά όλους τους παρόχους που διαθέτουν συστήματα AI και τα χρησιμοποιούν ή τα πωλούν εντός Ευρωπαϊκής Ένωσης, καθώς και όλους τους πολίτες της Ένωσης που χρησιμοποιούν AI[190]. Ο Κανονισμός δεν

---

[187] Έλσα Παπαδοπούλου (2020), *Τεχνητή Νοημοσύνη και σχετικές ψηφιακές τεχνολογίες – οι πρωτοβουλίες της Ευρωπαϊκής Επιτροπής και του Ευρωπαϊκού Συμβουλίου Καινοτομίας*, Lawyer the Business Magazine, διαθέσιμο στο https://lawyermagazine.gr/texniti-nohmsunh-sxetikes-psifiakies-texnologies-protoboulies-eurwpaikis-epitropis/

[188] ΛΕΥΚΗ ΒΙΒΛΟΣ Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf

[189] Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ΓΙΑ ΤΗ ΘΕΣΠΙΣΗ ΕΝΑΡΜΟΝΙΣΜΕΝΩΝ ΚΑΝΟΝΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ (ΠΡΑΞΗ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ) ΚΑΙ ΤΗΝ ΤΡΟΠΟΠΟΙΗΣΗ ΟΡΙΣΜΕΝΩΝ ΜΟΜΟΘΕΤΙΚΩΝ ΠΡΑΞΕΩΝ ΤΗΣ ΕΝΩΣΗΣ, η αιτιολογική έκθεση είναι διαθέσιμη σε pdf στο https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF, και τα παραρτήματα είναι διαθέσιμα σε pdf στο https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_2&format=PDF

[190] Βλ. αιτιολογική σκέψη 1 της πρότασης του Κανονισμού

εφαρμόζεται στα συστήματα που χρησιμοποιούνται καθαρά για στρατιωτικούς σκοπούς και στους μηχανισμούς AI που χρησιμοποιούνται από κρατικές αρχές τρίτων χωρών και από διεθνείς οργανισμούς, στο πλαίσιο διεθνών συμφωνιών για την επιβολή του Νόμου.

Έχοντας σαν υπόδειγμα την Λευκή Βίβλο, έτσι και η πρόταση Κανονισμού, στην προσπάθειά της να σεβαστεί τις ευρωπαϊκές αξίες και τα ανθρώπινα δικαιώματα, ταξινόμησε τα προγράμματα τεχνητής νοημοσύνης σε τέσσερα επίπεδα κινδύνου, όπου ανάλογα με το πόσο επικίνδυνο είναι ένα πρόγραμμα θα διαμορφώνονται και οι υποχρεώσεις του παρόχου. Σύμφωνα με αυτή την κατηγοριοποίηση, η πρώτη κατηγορία περιλαμβάνει τα προγράμματα μη αποδεκτού κινδύνου, τα οποία, με ορισμένες εξαιρέσεις, απαγορεύονται πλήρως χωρίς περαιτέρω προϋποθέσεις[191], η δεύτερη κατηγορία περιλαμβάνει τα προγράμματα υψηλού κινδύνου, τα οποία υπόκεινται σε αυστηρότατες υποχρεώσεις, με κυριότερη την υποχρέωση αξιολόγησης και εκτίμησης του κινδύνου από ανεξάρτητη αρχή[192], η τρίτη κατηγορία περιλαμβάνει τα προγράμματα περιορισμένου κινδύνου, τα οποία έχουν λιγότερες υποχρεώσεις[193], και η τελευταία κατηγορία περιλαμβάνει τα προγράμματα ελαχίστου κινδύνου που δεν εμπίπτουν σε νέες υποχρεώσεις[194].

4.3.1 Σημαντικοί ορισμοί του άρθρου 3 της AI ACT

Η πρόταση Κανονισμού ασχολείται σε μεγάλο βαθμό με τις βιομετρικές τεχνολογίες ταυτοποίησης, τις οποίες, ανάλογα με το πεδίο εφαρμογής τους, τις διακρίνει είτε σε προγράμματα μη αποδεκτού κινδύνου, με αποτέλεσμα να απαγορεύεται πλήρως η χρήση τους πλην ελαχίστων εξαιρέσεων, είτε σε προγράμματα υψηλού κινδύνου, τα οποία υπόκεινται σε αυστηρούς περιορισμούς. Για να γίνει κατανοητή αυτή η κατηγοριοποίηση, είναι απαραίτητο να διατυπωθούν οι ορισμοί μερικών βασικών εννοιών που ενυπάρχουν στο άρθρο 3 της πρότασης.

---

[191] Βλ. Κεφάλαιο ΙΙ πρότασης Κανονισμού, όπου περιγράφονται και οι εξαιρέσεις από την πλήρη απαγόρευση

[192] Βλ. Κεφάλαιο ΙΙΙ πρότασης Κανονισμού

[193] Βλ. Κεφάλαιο ΙV πρότασης Κανονισμού

[194] Βλ. Κεφάλαιο ΙΧ πρότασης Κανονισμού

Αρχικά τα βιομετρικά δεδομένα είναι ορθή επανάληψη του σχετικού ορισμού του GDPR[195]. Ως σύστημα τεχνητής νοημοσύνης[196] ορίζεται «το λογισμικό που αναπτύσσεται με μία ή περισσότερες από τις τεχνικές και προσεγγίσεις που παρατίθενται στο παράρτημα Ι της πρότασης και μπορεί, για ένα δεδομένο σύνολο στόχων που έχουν καθοριστεί από τον άνθρωπο, να παράγει στοιχεία εξόδου όπως περιεχόμενο, προβλέψεις, συστάσεις ή αποφάσεις που επηρεάζουν τα περιβάλλοντα με τα οποία αλληλοεπιδρά». Το σύστημα αναγνώρισης συναισθημάτων[197] έχει τη δυνατότητα να προσδιορίσει ή να διαπιστώσει συναισθήματα ή προθέσεις φυσικών προσώπων βάσει των βιομετρικών δεδομένων τους. Το σύστημα βιομετρικής κατηγοριοποίησης[198], κατατάσσει τα φυσικά πρόσωπα σε κατηγορίες βασισμένο σε κριτήρια φυσιολογίας, όπως το φύλο, η ηλικία, το χρώμα των μαλλιών ή και η εθνοτική καταγωγή. Ως σύστημα εξ αποστάσεως βιομετρικής ταυτοποίησης[199] ορίζεται το σύστημα ΤΝ για την εξ αποστάσεως ταυτοποίηση φυσικών προσώπων μέσω της αντιπαραβολής των βιομετρικών δεδομένων του προσώπου με τα βιομετρικά δεδομένα που περιέχονται σε βάση δεδομένων αναφοράς και χωρίς ο χρήστης του συστήματος ΤΝ να γνωρίζει εκ των προτέρων αν το πρόσωπο θα είναι παρόν και μπορεί να ταυτοποιηθεί. Η τελευταία μορφής ταυτοποίηση μπορεί να πραγματοποιηθεί είτε σε ‘‘σε πραγματικό χρόνο”[200], δηλαδή χωρίς μεγάλη καθυστέρηση, σχεδόν άμεσα, είτε σε ‘‘σε ύστερο χρόνο”[201]. Ως δημόσια προσβάσιμος χώρος[202], ορίζεται κάθε φυσικός χώρος προσβάσιμος στο κοινό, ανεξάρτητα από το εάν τυχόν ισχύουν ορισμένοι όροι πρόσβασης. Τέλος, ακολουθώντας πιστά το πνεύμα των προηγούμενων νομοθετικών κειμένων ο ορισμός της αρμόδιας αρχής στην πρόταση είναι ρητή επανάληψη του ορισμού της Οδηγία 2016/680[203]. Αφού λοιπόν ορίστηκαν οι απαραίτητες έννοιες, τώρα μπορούν να εξεταστούν οι βασικές ρυθμίσεις της πρότασης Κανονισμού.

---

[195] Βλ. άρθρο 3 (33) της πρότασης Κανονισμού σε σχέση με άρθρο 4 (14) GDPR, επίσης βλ. ενότητα 2.3.3

[196] Βλ. άρθρο 3 (1) της πρότασης Κανονισμού

[197] Βλ. άρθρο 3 (34) της πρότασης Κανονισμού

[198] Βλ. άρθρο 3 (35) της πρότασης Κανονισμού

[199] Βλ. άρθρο 3 (36) της πρότασης Κανονισμού

[200] Βλ. άρθρο 3 (37) της πρότασης Κανονισμού

[201] Βλ. άρθρο 3 (38) της πρότασης Κανονισμού

[202] Βλ. άρθρο 3 (39) της πρότασης Κανονισμού

[203] Βλ. άρθρο 3 (40) της πρότασης Κανονισμού σε σχέση με άρθρο 3 (7) της Οδηγίας

4.3.2 Η βιομετρική ταυτοποίηση ως απαγορευμένη πρακτική

Σύμφωνα με το άρθρο 5 παράγραφος 1 περίπτωση δ της πρότασης του Κανονισμού απαγορεύεται η χρήση συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης «σε πραγματικό χρόνο», σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου. Όπως προσδιορίζεται στην αιτιολογική σκέψη 18 της πρότασης η χρήση αυτών των συστημάτων θεωρείται ιδιαιτέρως παρεμβατική στα δικαιώματα και τις ελευθερίες των πολιτών, καθώς δημιουργεί την εντύπωση ότι καθιερώνεται ένα καθεστώς συνεχούς και μαζικής παρακολούθησης. Παρ' όλα αυτά η απαγόρευση δεν είναι απόλυτη, αντιθέτως υπάρχουν εξαιρέσεις. Η απαγόρευση λοιπόν αίρεται, όταν η χρήση αυτής της πρακτικής είναι απολύτως αναγκαία για έναν από τους ακόλουθους στόχους:

i) τη στοχευμένη αναζήτηση συγκεκριμένων δυνητικών θυμάτων εγκληματικών πράξεων, συμπεριλαμβανομένων των αγνοούμενων παιδιών

ii) την πρόληψη συγκεκριμένης, ουσιώδους και επικείμενης απειλής κατά της ζωής ή της σωματικής ακεραιότητας φυσικών προσώπων ή απειλές τρομοκρατικής επίθεσης

iii) τον εντοπισμό, την ταυτοποίηση ή τη δίωξη δράστη ή υπόπτου για ποινικό αδίκημα που αναφέρεται στο άρθρο 2 παράγραφος 2 της απόφασης-πλαισίου 2002/584/ΔΕΥ του Συμβουλίου[204] και το οποίο τιμωρείται στο οικείο κράτος μέλος με στερητική της ελευθερίας ποινή ή στερητικό της ελευθερίας μέτρο ασφάλειας ανώτατης διάρκειας τουλάχιστον τριών ετών, όπως ορίζεται στο δίκαιο του εν λόγω κράτους μέλους.

Όπως αναφέρεται στην επόμενη παράγραφο του ιδίου άρθρου, για τους ανωτέρω στόχους πρέπει να ληφθεί υπόψη:
α) τη φύση της κατάστασης που οδηγεί στην πιθανή χρήση, ειδικότερα τη σοβαρότητα, την πιθανότητα και το μέγεθος της βλάβης που θα προκληθεί αν δεν χρησιμοποιηθεί το σύστημα

β) τις συνέπειες της χρήσης του συστήματος για τα δικαιώματα και τις ελευθερίες όλων των ενδιαφερομένων προσώπων, ειδικότερα τη σοβαρότητα, την πιθανότητα και την έκταση των εν λόγω συνεπειών.

---

[204] Απόφαση-πλαίσιο 2003/584/ΔΕΥ για το ευρωπαϊκό ένταλμά σύλληψης, L190/2002, https://eur- 176 lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32002F0584, η οποία μεταφέρθηκε στην εθνική έννομη τάξη με τον Ν. 3251/2004 (ΦΕΚ Α127). Στο άρθρο 10 του Ν. 3251/2004 αναφέρονται τα αδικήματα, για τα οποία επιτρέπεται η έκδοση του ευρωπαϊκού εντάλματος σύλληψης.

Η αλήθεια είναι πως η πρόταση δεν επεξηγεί αναλυτικά τον τρόπο ή τη μέθοδο αξιολόγησης των ανωτέρω παραγόντων. Ίσως ο νομοθέτης να το διατυπώνει με τέτοιο τρόπο, αναζητώντας την ισορροπία ανάμεσα στους κινδύνους που ενδέχεται να επέλθουν από την πιθανή μη-χρήση των συστημάτων και ανάμεσα στους κινδύνους σχετικά με τα ανθρώπινα δικαιώματα που ενδεχομένως να προκύψουν με τη χρήση των βιομετρικών συστημάτων[205]. Σε κάθε περίπτωση, τα συστήματα βιομετρικής ταυτοποίησης πρέπει να συμμορφώνονται με τις αναγκαίες και αναλογικές διασφαλίσεις και προϋποθέσεις που σχετίζονται με την χρήση, ιδιαίτερα όσον αφορά τους χρονικούς και γεωγραφικούς περιορισμούς, καθώς και τους περιορισμούς όσον αφορά τα πρόσωπα.

Σύμφωνα με την παράγραφο 3 του ιδίου άρθρου η εξ αποστάσεως βιομετρική ταυτοποίηση σε πραγματικό χρόνο μπορεί να πραγματοποιηθεί μόνο για σκοπούς επιβολής του νόμου και μόνο υπό ρητή και ειδική άδεια δικαστικής αρχή ή ανεξάρτητης διοικητικής αρχής, η οποία πρέπει να έχει ληφθεί πριν από τη χρήση του συστήματος ΤΝ. Παρά την ύπαρξη αυτής της γενικής απαίτησης, εισάγεται μία σημαντική εξαίρεση, σύμφωνα με την οποία, σε επείγουσες περιπτώσεις η χρήση του συστήματος μπορεί να αρχίσει και πριν χορηγηθεί άδεια, όταν η λήψη της τελευταίας καθίσταται πρακτικά και αντικειμενικά αδύνατη. Στην περίπτωση αυτή η άδεια μπορεί να ζητηθεί μόνο κατά τη διάρκεια της χρήσης ή αμέσως μετά τη χρήση. Αυτό που δεν ξεκαθαρίζεται όμως, είναι το τι συμβαίνει σε περίπτωση που η χρήση έχει ήδη πραγματοποιηθεί και η δικαστική αρχή αρνήθηκε τελικά να χορηγήσει τη δικαστική άδεια.

Τέλος, σύμφωνα με την τέταρτη, και τελευταία, παράγραφο του άρθρου τα κράτη-μέλη είναι αρμόδια με δικά τους νομοθετήματα να προσδιορίσουν τις ακριβείς συνθήκες κάτω από τις οποίες μπορεί να επιτραπεί η χρήση τεχνολογιών εξ αποστάσεως βιομετρικής ταυτοποίησης σε πραγματικό χρόνο. Η αρμοδιότητα αυτή ανατίθεται στα κράτη-μέλη διότι οι αναγκαίες και κατάλληλες διασφαλίσεις και συνθήκες που περιγράφονται στη δεύτερη παράγραφο δεν είναι ξεκάθαρες και έχουν γενικό χαρακτήρα. Όπως πολύ σωστά έθεσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, καθώς και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων[206], μία ακραία ενέργεια, όπως η βιομετρική ταυτοποίηση εξ αποστάσεως σε

[205] EPRS European Parliamentary Research Service (2021), *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence*, διαθέσιμο σε pdf στο https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf

[206] ΕΣΠΔ-ΕΕΠΔ (2021), *Κοινή γνωμοδότηση 5/2021*, διαθέσιμη σε pdf στο https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_el.pdf

πραγματικό χρόνο, απαιτεί πολύ συγκεκριμένες προβλέψιμες και κατάλληλες διασφαλίσεις που αφορούν μία αυστηρά προσδιορισμένη γεωγραφική περιοχή και λαμβάνουν υπόψη τις επιπτώσεις αυτής της πρακτικής στα δικαιώματα και τις ελευθερίες των ανθρώπων. Αντιθέτως η πρόταση του Κανονισμού αρκείται απλώς στο να θέσει πολύ γενικά γεωγραφικά και χωρικά όρια, τα οποία θα γίνουν πιο συγκεκριμένα από εγχώριους νόμους. Η διατύπωση είναι αρκετά προβληματική, καθώς έχει ήδη αποδειχθεί, το πόσο εύκολο είναι να καταπατηθούν οι ατομικές ελευθερίες, όταν ο προσδιορισμός των διασφαλίσεων ανατίθεται στα κράτη. Ενδεικτικά, δεν είναι λίγες οι χώρες, που εκμεταλλεύτηκαν την ελευθερία που τους δίνει το άρθρο 23 του GDPR, με αποτέλεσμα να περιορίσουν σε ακραίο βαθμό τα δικαιώματα των υποκειμένων των δεδομένων[207].

4.3.3 Η βιομετρική ταυτοποίηση ως σύστημα υψηλού κινδύνου

Στο άρθρο 6 της πρότασης Κανονισμού καθώς και στο παράρτημα ΙΙΙ εντοπίζονται τα συστήματα βιομετρικής ταυτοποίησης τα οποία χαρακτηρίζονται ως συστήματα υψηλού κινδύνου και απαιτούν την τήρηση ειδικής διαδικασίας προκειμένου να διατεθούν στην αγορά της Ένωσης και να χρησιμοποιηθούν. Σύμφωνα με την πρώτη επικεφαλίδα του παραρτήματος τα συστήματα βιομετρικής ταυτοποίησης και κατηγοριοποίησης φυσικών προσώπων θεωρούνται υψηλού κινδύνου. Βέβαια συνεχίζοντας την ανάγνωση του παραρτήματος, παρατηρούμε ότι συστήματα υψηλού κινδύνου θεωρούνται τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης φυσικών προσώπων «σε πραγματικό χρόνο» και «σε ύστερο χρόνο» και δεν γίνεται πουθενά λόγος για βιομετρική κατηγοριοποίηση, η οποία όμως αναφέρεται στον τίτλο. Οι υπόλοιπες κατηγορίες βιομετρικών συστημάτων που χαρακτηρίζονται ως υψηλού κινδύνου είναι, η διαχείριση και η λειτουργία υποδομών ζωτικής σημασίας[208], η εκπαίδευση και η επαγγελματική κατάρτιση[209], η απασχόληση, η διαχείριση εργαζομένων και η πρόσβαση στην αυτοαπασχόληση[210], η πρόσβαση και η απόλαυση βασικών ιδιωτικών υπηρεσιών και δημόσιων υπηρεσιών και παροχών[211], η

---

[207] COMMISSION STAFF WORKING DOCUMENT (2020), 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, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/1_en_swd_part1_v6.pdf

[208] Βλ. επικεφαλίδα (2) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού

[209] Βλ. επικεφαλίδα (3) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού

[210] Βλ. επικεφαλίδα (4) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού

[211] Βλ. επικεφαλίδα (5) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού

επιβολή του νόμου[212], η διαχείριση της μετανάστευσης, του ασύλου και των συνοριακών ελέγχων[213] και η Απονομή δικαιοσύνης και οι δημοκρατικές διαδικασίες[214].

Σύμφωνα με το άρθρο 7 η Ευρωπαϊκή Επιτροπή, έχει τη δυνατότητα να ενημερώνει τον κατάλογο του παραρτήματος προσθέτοντας νέα συστήματα τεχνητής νοημοσύνης, εφόσον αυτά πρόκειται να χρησιμοποιηθούν σε μία από τις ήδη υπάρχουσες κατηγορίες του παραρτήματος, και εάν ενέχουν κίνδυνο βλάβης για την υγεία και την ασφάλεια ή κίνδυνο δυσμενών επιπτώσεων στα θεμελιώδη δικαιώματα, δηλαδή όσον αφορά τη σοβαρότητα και την πιθανότητα εμφάνισης κινδύνου ισοδύναμου ή μεγαλύτερου από τον κίνδυνο βλάβης ή δυσμενών επιπτώσεων που ενέχουν τα συστήματα ΤΝ υψηλού κινδύνου που αναφέρονται ήδη στο παράρτημα. Στην πράξη αυτό σημαίνει ότι στο μέλλον μπορούν να προστεθούν στη λίστα νέα συστήματα ΑΙ μόνο εφόσον έχουν ισοδύναμες ή μεγαλύτερες αρνητικές επιπτώσεις στα θεμελιώδη δικαιώματα σε σχέση με τα συστήματα που ήδη υπάρχουν στο παράρτημα. Γεννάται λοιπόν η απορία, πώς ακριβώς μπορεί να εκτιμηθεί αυτός ο αντίκτυπος;

Την απάντηση τη δίνει η δεύτερη παράγραφος του άρθρου 7 που ορίζει μία σειρά κριτηρίων που πρέπει να λάβει υπόψιν της η Επιτροπή κατά την εκτίμηση του αντικτύπου. Ορισμένα από τα πιο σημαντικά κριτήρια είναι ο βαθμός στον οποίον ένα σύστημα ΑΙ έχει ήδη χρησιμοποιηθεί ή ενδέχεται να χρησιμοποιηθεί[215], και ο βαθμός στον οποίο η χρήση ενός συστήματος ΤΝ έχει ήδη προκαλέσει βλάβη στην υγεία και την ασφάλεια ή δυσμενείς επιπτώσεις στα θεμελιώδη δικαιώματα ή έχει εγείρει σοβαρές ανησυχίες σε σχέση με την επέλευση της βλάβης ή των δυσμενών επιπτώσεων, όπως καταδεικνύεται από εκθέσεις ή τεκμηριωμένους ισχυρισμούς που υποβάλλονται στις εθνικές αρμόδιες αρχές[216].

Η αλήθεια είναι πως η διατύπωση του συγκεκριμένου άρθρου δεν είναι πολύ σαφής σχετικά με το τι πρέπει να εκτιμηθεί στην πράξη από την Επιτροπή. Δεν γίνεται αντιληπτό αν τυχόν κάποιο κριτήριο έχει σπουδαιότερη σημασία από κάποιο άλλο. Επίσης είναι τόσο γενική η διατύπωση που δυσχεραίνει το έργο της Επιτροπής. Για παράδειγμα το κριτήριο (γ) αναφέρεται σε εκθέσεις και ισχυρισμούς αρμόδιων και εθνικών αρχών. Δεν γίνεται καμία προσπάθεια να προσδιοριστούν αυτές οι αρχές ή να οριστεί το χρονικό σημείο που πρέπει

[212] Βλ. επικεφαλίδα (6) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού
[213] Βλ. επικεφαλίδα (7) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού
[214] Βλ. επικεφαλίδα (8) Παράρτημα ΙΙΙ της πρότασης του Κανονισμού
[215] Βλ. άρθρο 7 (2) (β) της πρότασης Κανονισμού
[216] Βλ. άρθρο 7 (2) (γ) της πρότασης Κανονισμού

να υποβληθούν οι σχετικές εκθέσεις. Στην πραγματικότητα το μόνο που καταφέρνει η συγκεκριμένη διάταξη είναι να κάνει πιο δύσκολο τον μελλοντικό έλεγχο των συστημάτων AI.

4.3.4 Ρυθμιστικό πλαίσιο

Στο δεύτερο κεφάλαιο της πρότασης του Κανονισμού, εντοπίζονται οι απαιτήσεις που οφείλουν να πληρούν τα συστήματα υψηλού κινδύνου. Συνοπτικά προβλέπεται η λειτουργία ενός συστήματος κινδύνου[217] με αρμοδιότητες, τον προσδιορισμό και ανάλυση των γνωστών και προβλέψιμων κινδύνων, την εκτίμηση και αξιολόγηση των ενδεχόμενων κινδύνων υπό συνθήκες ευλόγως προβλέψιμής κακής χρήσης, την αξιολόγηση άλλων πιθανών κινδύνων και τη θέσπιση κατάλληλων μέτρων διαχείρισης κινδύνου. Επιπρόσθετα προβλέπονται αυστηροί κανόνες και περιορισμοί σχετικά με τα δεδομένα και τη διακυβέρνησή τους[218], η δημιουργία ενός τεχνικού φάκελου[219], που καταρτίζεται πριν από την διάθεση του συστήματος στην αγορά, με διαρκή επικαιροποίηση και που αποδεικνύει ότι το σύστημα συμμορφώνεται με τις απαιτήσεις του Κανονισμού, και αντιστοίχως η τήρηση αρχείου[220] αυτόματης καταγραφής συμβάντων. Ακόμη προβλέπονται κανόνες σχετικά με την τήρηση της διαφάνειας και την πληροφόρηση των χρηστών[221], την ανθρώπινη εποπτεία[222] καθώς και μέτρα που ρυθμίζουν την ακρίβεια των συστημάτων και την κυβερνοασφάλεια[223]. Οι τελευταίοι κανόνες υποχρεώνουν τον σχεδιασμό και την ανάπτυξη των συστημάτων με τέτοιο τρόπο ώστε να μπορούν να εποπτεύονται αποτελεσματικά από φυσικά πρόσωπα και να επιτυγχάνουν κατάλληλο επίπεδο ακρίβειας, στιβαρότητας και κυβερνοασφάλειας.

Οι πάροχοι εφαρμόζουν σύστημα διαχείρισης ποιότητας, που τεκμηριώνεται με συστηματικό και τακτικό τρόπο υπό τη μορφή γραπτών πολιτικών, διαδικασιών και οδηγιών, ενώ οι χρήστες χρησιμοποιούν τις πληροφορίες, που παρέχονται βάσει του άρθρου 13, για να συμμορφωθούν με την υποχρέωσή τους να διενεργούν εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει του άρθρου 35 ΓΚΠΔ ή του 27 Οδ2016/680. Πριν την

[217] Βλ. άρθρο 9 της πρότασης του Κανονισμού
[218] Βλ. άρθρο 10 της πρότασης του Κανονισμού
[219] Βλ. άρθρο 11 της πρότασης του Κανονισμού
[220] Βλ. άρθρο 12 της πρότασης του Κανονισμού
[221] Βλ. άρθρο 13 της πρότασης του Κανονισμού
[222] Βλ. άρθρο 14 της πρότασης του Κανονισμού
[223] Βλ. άρθρο 15 της πρότασης του Κανονισμού

διάθεση του συστήματος ΤΝ ο πάροχος οφείλει να έχει δημιουργήσει τον τεχνικό φάκελο του άρθρου 11, τον φάκελο του συστήματος διαχείρισης ποιότητας του άρθρου 17, φάκελο με αλλαγές που έχουν εγκριθεί, να καταθέσει την δήλωση συμμόρφωσης με τις απαιτήσεις του ενωσιακού δικαίου για συμμόρφωση με την σήμανση CE και να καταχωρίσει το σύστημα στην σχετική βάση δεδομένων της ΕΕ.

5. ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΑΙ ΣΤΑ ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ

Δυστυχώς, οι κίνδυνοι της τεχνητής νοημοσύνης στο πλαίσιο της προληπτικής αστυνόμευσης δεν σταματούν εκεί. Αντιθέτως, η αλγοριθμική αστυνόμευση είναι ένα εργαλείο που, εφόσον χρησιμοποιηθεί αυθαίρετα από τις αρχές, είναι ικανή να θίξει τον πυρήνα θεμελιωδών ανθρωπίνων δικαιωμάτων. Μάλιστα στην προκειμένη περίπτωση που το κεντρικό θέμα είναι η χρήση της τεχνητής νοημοσύνης στο πλαίσιο επιβολής του νόμου και στην ποινική δικαιοσύνη, ο κίνδυνος αποκτά αυτομάτως μεγαλύτερη σημασία. Σε προηγούμενα κεφάλαια[224], αναλύοντας τη λειτουργία των συστημάτων προληπτικής αστυνόμευσης, ήδη παρουσιάστηκε μία σειρά περιπτώσεων όπου οι σχετικές εφαρμογές «θίγουν» τα ανθρώπινα δικαιώματα. Στο κεφάλαιο αυτό θα αναλυθούν περαιτέρω τα ερωτήματα που τίθενται συχνότερα. Να σημειωθεί ότι ο κίνδυνος των διακρίσεων και των προκαταλήψεων, που προφανώς και θίγουν το δικαίωμα της ισότητας, αναλύθηκε εκτενώς σε προηγούμενη ενότητα[225], οπότε δεν θα γίνει αναφορά σε αυτό στο κατωτέρω κεφάλαιο.

Πολλοί θεσμοί της Ένωσης προσπάθησαν τα τελευταία χρόνια να επισημάνουν τις αρνητικές επιπτώσεις της τεχνητής νοημοσύνης στα ανθρώπινα δικαιώματα. Η Λευκή Βίβλος θέτει την γενική διαπίστωση ότι η ΑΙ «μπορεί να βλάψει», εξηγώντας στη συνέχεια ότι αυτή η βλάβη δεν είναι υλική, αλλά συνεπάγεται σε βλάβη δικαιωμάτων όπως η απώλεια της ιδιωτικότητας, της ελευθερίας της έκφρασης αλλά και της ανθρώπινης αξιοπρέπειας. Μάλιστα η Λευκή Βίβλος καταλήγει στο συμπέρασμα ότι οι βασικότεροι κίνδυνοι της τεχνητής νοημοσύνης αφορούν τα ανθρώπινα δικαιώματα, τα οποία πρέπει να διασφαλιστούν.

[224] Βλ. ενδεικτικά ενότητα 3.4
[225] Βλ. ενδεικτικά ενότητα 3.4.2

Άλλος ένας θεσμός που έθιξε τον συγκεκριμένο κίνδυνο ήταν η Επιτροπή Εμπειρογνωμόνων στα Ανθρώπινα Δικαιώματα και την Αυτοματοποιημένη Επεξεργασία Δεδομένων πάνω σε διαφορετικές μορφές AI (Human Rights Dimensions of Automated Data Processing and Different forms of AI) στο Συμβούλιο της Ευρώπης το 2019[226]. Η Επιτροπή πραγματοποίησε μία μελέτη σχετικά με τις επιπτώσεις της αυτοματοποιημένης λήψης απόφασης και ιδίως του profiling. Η μελέτη κατέληξε στο συμπέρασμα ότι αυτές οι τεχνικές είναι άμεσες απειλές ανθρωπίνων δικαιωμάτων, όπως το δικαίωμα σε δίκαιη δίκη, το δικαίωμα της ελευθερίας του λόγου, το δικαίωμα προστασίας απέναντι σε διακρίσεις και φυσικά το δικαίωμα της ιδιωτικότητας.

Μελετώντας την έρευνα, το Συμβούλιο της Ευρώπης εξέδωσε μία σύσταση[227] μέσω της οποίας ισχυριζόταν ότι η προσκόλληση στην τεχνητή νοημοσύνη δημιουργεί καθημερινές προκλήσεις στα ανθρώπινα δικαιώματα, που απαρίθμησε και η Επιτροπή προηγουμένως. Αφού αναφέρθηκαν τα θεμελιώδη δικαιώματα που ευρίσκονται σε κίνδυνο, ας δούμε κάθε δικαίωμα χωριστά.

5.1 Το δικαίωμα της ιδιωτικότητας

Φυσικά, το πρώτο δικαίωμα που θα αναλυθεί, δεν θα μπορούσε να είναι άλλο από το δικαίωμα προστασίας της ιδιωτικής ζωής. Πρόκειται για ένα δικαίωμα που είναι άμεσα συνδεδεμένο με την προστασία των προσωπικών δεδομένων. Μάλιστα, πολλοί θεωρούν τα προσωπικά δεδομένα ως ένα παρακλάδι της ιδιωτικότητας, μιας και τα δεδομένα προσωπικού χαρακτήρα μπορούν να δείξουν πολλά στοιχεία από την προσωπική ζωή ενός υποκειμένου. Η άποψη αυτή στηρίζεται στο επιχείρημα ότι η ΕΣΔΑ, σε αντίθεση με τον Χάρτη, δεν έχει ένα αυτοτελές άρθρο σχετικά με την προστασία των προσωπικών δεδομένων, αντιθέτως, τα συμπεριλαμβάνει στο άρθρο 8, ως μία πτυχή του δικαιώματος του σεβασμού στην ιδιωτική ζωή.

Είναι αρκετά εύκολο να αντιληφθεί κανείς τους λόγους που η προληπτική αστυνόμευση θέτει σε κίνδυνο την ιδιωτική ζωή. Αρχικά, για να λειτουργήσουν τα αλγοριθμικά

---

[226] Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT) (2019), *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*, διαθέσιμο σε pdf στο https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab

[227] Βλ. υποσημείωση 97

συστήματα πρόληψης, χρειάζονται συνεχώς δεδομένα, τα οποία με τη σειρά τους είναι σε θέση να δείξουν ποια είναι η ζωή του κάθε ανθρώπου. Επομένως, το πρόβλημα είναι διττό, διότι αρχικά είναι απαραίτητο να ζούμε σε ένα καθεστώς συνεχούς παρακολούθησης όπου διάφορες βιομετρικές μέθοδοι, όπως κάμερες CCTV, λαμβάνουν συνεχώς δεδομένα προς επεξεργασία[228], τα οποία δεδομένα είναι προσωπικού χαρακτήρα βοηθώντας τις αρμόδιες αρχές να δημιουργήσουν ψηφιακά προφίλ για όλους τους πολίτες. Δηλαδή εγκαθίσταται ένα σύστημα ολοκληρωτικής παρακολούθησης, το οποίο έχει σαν αποτέλεσμα οι κυβερνήσεις να συλλέγουν πολλά και διαφορετικά είδη προσωπικών δεδομένων των πολιτών τους, επεμβαίνοντας ουσιαστικά στην ιδιωτική τους ζωή[229].

Το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ)[230], κλήθηκε αμέτρητες φορές να εξετάσει ζητήματα παρακολούθησης που παραβιάζουν το άρθρο 8 της ΕΣΔΑ. Εξετάζοντας τη νομολογία που προέκυψε, παρατηρείται ότι το ΕΔΔΑ θίγει συνεχώς δύο ζητήματα. Το πρώτο είναι ότι τα συστήματα προβλεπτικής αστυνόμευσης λειτουργούν απρόσκοπτα εις βάρος όλων των πολιτών. Δηλαδή για να εντοπίσουν τα συστήματα τους υπόπτους για κάποιο μελλοντικό έγκλημα, χρειάζεται να παρακολουθήσουν όλους τους πολίτες σε πρώτο βαθμό και αξιολογώντας τα στοιχεία τους, να φτιάξουν στη συνέχεια μία λίστα με τους πιο επικίνδυνους μελλοντικούς εγκληματίες. Όπως έθιξε πολύ σωστά το Δικαστήριο στην υπόθεση Liberty and Others v. the United Kingdom[231], αντί να υπάρχει σεβασμός στην αρχή της αναλογικότητας και να εξηγείται αναλυτικά στον κόσμο η διαδικασία επιλογής του πληθυσμού, η αξιολόγηση τους και τα σχετικά συμπεράσματα, αντιθέτως εγκαθιδρύεται μία διαδικασία που παρακολουθεί τους πολίτες μαζικά χωρίς καμία δικαιολογία, γεγονός που παραβιάζει κατάφορα το άρθρο 8 της ΕΣΔΑ. Το δεύτερο ζήτημα είναι η απουσία ενημέρωσης των πολιτών ότι έχουν ληφθεί τα δεδομένα τους και υπόκεινται σε επεξεργασία. Πράγματι, ελάχιστες εφαρμογές παρέχουν ουσιαστική ενημέρωση στον κόσμο ότι έχουν λάβει τα δεδομένα τους και τα αξιολογούν. Η απουσία γνωστοποίησης καθιστά αδύνατο το δικαίωμα εναντίωσης απέναντι στην επεξεργασία,

---

[228] Alice Norga (2021), *4 Benefits And 4 Drawbacks Of Predictive Policing*, διαθέσιμο στο https://www.liberties.eu/en/stories/predictive-policing/43679

[229] Data Ethics Commission of the German Federal Government (2019), Opinion of the Data Ethics Commission, διαθέσιμο σε pdf στο https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

[230] Περισσότερες πληροφορίες για το ΕΔΔΑ στο https://www.echr.coe.int/Pages/home.aspx?p=home

[231] Υπόθεση Liberty and Others v. the United Kingdom (2008), η περίληψη διαθέσιμη σε pdf στο https://brill.com/journals/hudi/article-p1061

καθώς και τη δυνατότητα προσφυγής στα αρμόδια δικαστήρια. Εφόσον ο πολίτης δεν ξέρει ότι βρίσκεται υπό παρακολούθηση, δεν μπορεί να αντιταχθεί σε αυτή την κατάσταση. Πρόκειται για ένα ιδιαίτερα σοβαρό πρόβλημα, το οποίο παρατηρήθηκε τόσο στην Ευρωπαϊκή Ένωση[232] όσο και στις ΗΠΑ[233].

Το ΕΔΔΑ δεν είναι το μοναδικό δικαστήριο που ασχολήθηκε με τα δικαιώματα που προσβάλλει η προληπτική αστυνόμευση. Ενεργό ρόλο σε αυτόν τον αγώνα κατέχει και το Ανώτατο Δικαστήριο της Χάγης (CJEU)[234]. Το Δικαστήριο κλήθηκε να εξετάσει τη νομιμότητα της λειτουργίας ενός προγράμματος εκτίμησης κινδύνου με την ονομασία (SyRi). Με την απόφαση που δημοσιεύθηκε στις 5 Φεβρουαρίου 2020[235], το Δικαστήριο έκρινε ότι η εφαρμογή είναι επικίνδυνη για τα ανθρώπινα δικαιώματα, καθώς διακρίνεται από έλλειψη διαφάνειας και επεξήγησης της λειτουργίας της. Η ρύθμιση που νομιμοποιούσε το πρόγραμμα δεν παρείχε επαρκείς εξηγήσεις σχετικά με το πως λειτουργούσε η αξιολόγηση του συστήματος, με αποτέλεσμα να μην μπορεί να δικαιολογηθεί πώς κάποιος πολίτης χαρακτηριζόταν ως υψηλού κινδύνου εγκληματίας. Αυτές οι ασάφειες καθιστούσαν αδύνατη την προστασία των υποκειμένων των δεδομένων απέναντι στα αποτελέσματα του συστήματος. Παρατηρείται λοιπόν, ότι και τα δύο δικαστήρια θίγουν τα ίδια ζητήματα.

5.2 Το δικαίωμα της ελευθερίας της έκφρασης και η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι

Ιδιαίτερα στενή είναι η σχέση του δικαιώματος στην ιδιωτικότητα με την ελευθερία της έκφρασης, το οποίο διασφαλίζεται στο άρθρο 11 του ΧΘΔΕΕ. Για τον λόγο αυτό, πολλές παραβιάσεις της ιδιωτικότητας είναι ταυτοχρόνως παραβίαση του δικαιώματος της ελευθερίας της έκφρασης. Χαρακτηριστικότερη περίπτωση αποτελούν οι εφαρμογές παρακολούθησης των μέσων κοινωνικής δικτύωσης. Ουσιαστικά μέσω των εφαρμογών αυτών παρακολουθούνται τα σχόλια και οι αναρτήσεις ενός προφίλ, και αξιολογείται κατά πόσο ο χρήστης αποτελεί «απειλή» για την κοινωνία, ενημερώνοντας τις αρχές. Αυτή η

---

[232] Υπόθεση Weber and Saravia v. Germany (2006), διαθέσιμη στο https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76586%22]}

[233] Nicole Lindsey (2018), Predictive Policing Raises Important Privacy and Human Rights Concerns, CPO Magazine, διαθέσιμο στο https://www.cpomagazine.com/data-privacy/predictive-policing-raises-important-privacy-and-human-rights-concerns/

[234] Περισσότερες πληροφορίες για το Δικαστήριο στο https://curia.europa.eu/jcms/jcms/j_6/en/

[235] Υπόθεση υπ' αριθμόν C/09/550982, διαθέσιμη στο https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878

παρακολούθηση τρομοκρατεί τους πολίτες, οι οποίοι με τη σειρά τους γίνονται πιο προσεκτικοί στις δημόσιες αναρτήσεις τους, αφού όπως είναι λογικό δεν θέλουν να θεωρηθούν επικίνδυνοι και να μπουν στο στόχαστρο των αρχών. Δημιουργείται έτσι ένα καθεστώς αυτολογοκρισίας, όπου οι πολίτες «παγώνουν» τις απόψεις τους (chilling effect)[236], γίνονται πιο επιφυλακτικοί και εκφράζονται σύμφωνα με τα ιδανικά πρότυπα που προβάλλουν οι ίδιες αστυνομικές αρχές και κυβερνήσεις.

Αντίστοιχες παραβιάσεις παρατηρούνται και στο δικαίωμα του συνέρχεσθαι και συνεταιρίζεσθαι (άρθρο 12 ΧΘΔΕΕ). Πρόκειται για ένα δικαίωμα ορόσημο για τη δημοκρατική κοινωνία, καθώς δίνει το ελεύθερο στους πολίτες να συσπειρώνονται για να εκφράσουν φανερά την άποψή τους, να διορθώσουν ανισορροπίες εξουσίας και να προστατευτούν απέναντι σε πιο ισχυρές ολότητες[237]. Σημαντικός παράγοντας στην άσκηση του δικαιώματος είναι η ανωνυμία. Το γεγονός ότι κάποιος μπορεί να συμμετέχει σε μία πορεία διαμαρτυρίας, χωρίς να μπορεί να ταυτοποιηθεί, αποτελεί κίνητρο για την δημόσια τοποθέτηση των πολιτών και τον σεβασμό της ιδιωτικότητας τους[238]. Πλέον αυτή η ανωνυμία δεν είναι δεδομένη. Η αυξημένη χρήση της τεχνολογίας αναγνώρισης προσώπου, σε συνδυασμό με την συνεχή παρακολούθηση πολιτών μέσω καμερών κλειστού κυκλώματος, βοηθούν τις αρχές να αναγνωρίσουν εύκολα και γρήγορα τους υπόπτους, υποβαθμίζοντας την έννοια της ανωνυμίας, που διευκόλυνε την άσκηση του δικαιώματος. Αυτός ο φόβος της συνεχούς παρακολούθησης από τις κυβερνήσεις προκαλεί αντιστοίχως chilling effect στη συμμετοχή των πολιτών σε δημόσιες συναθροίσεις. Ήδη ορισμένες αστυνομικές αρχές έχουν ξεκινήσει να χρησιμοποιούν τεχνικές αναγνώρισης προσώπου για να ταυτοποιήσουν τους συμμετέχοντες σε πορείες διαμαρτυρίας. Πιο συγκεκριμένα, το 2018 η αστυνομική αρχή της Ουαλίας είχε κατηγορηθεί ότι χρησιμοποιούσε ένα σύστημα αναγνώρισης προσώπου σε μία αντιπολεμική διαμαρτυρία[239]. Βλέπουμε λοιπόν, ότι δεν

---

[236] Eva Schlehahn, Patrick Aichroth, Sebastian Mann, Rudolf Schreiner, Ifan Shepherd and B.L. William Wong (2015), *Benefits and Pitfalls of Predictive Policing*, διαθέσιμο σε pdf στο file:///C:/Users/user/Downloads/benefits_pitfalls_FINAL.pdf

[237] Human Rights Committee (2020), *General comment No. 37 Article 21: right of peaceful assembly*,διαθέσιμο στο https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

[238] Privacy International (2019), *Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR*, διαθέσιμο σε pdf στο https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf

[239] Ed Bridges (2018), *Why I'm Challenging Cardiff Police On Their Invasive Facial Recognition Technology*, HuffPost, διαθέσιμο στο https://www.huffingtonpost.co.uk/entry/facial-recognition_uk_5b227088e4b0bbb7a0e53760

πρόκειται απλώς για υποθετικά σενάρια, αντιθέτως η παραβίαση ανθρωπίνων δικαιωμάτων είναι η ωμή πραγματικότητα.

5.3 Το δικαίωμα σε δίκαιη δίκη

Το δικαίωμα σε δίκαιη δίκη εδραιώνεται στο άρθρο 6 της ΕΣΔΑ. Πρόκειται για ένα σύνθετο δικαίωμα, καθώς καθορίζει τις απαραίτητες προϋποθέσεις που πρέπει να πληρούνται, έτσι ώστε να δικαστεί ένας πολίτης δίκαια, νόμιμα και με λογική. Για το λόγο αυτό, το άρθρο τονίζει ότι είναι απαραίτητος ο σεβασμός πολλών επιμέρους δικαιωμάτων, όπως το τεκμήριο της αθωότητας, το δικαίωμα της ταχείας και πλήρους ενημέρωσης για την αιτία και τη φύση της κατηγορίας, το δικαίωμα της εκδίκασης από αμερόληπτη δικαστική αρχή, το δικαίωμα της δίκαιης ακρόασης και το δικαίωμα υπεράσπισης του κατηγορουμένου[240].

Η χρήση συστημάτων προληπτικής αστυνόμευσης στο πλαίσιο επιβολής του νόμου, αλλά και στην ποινική δικαιοσύνη, εγκυμονεί κινδύνους για την τήρηση των απαραίτητων προϋποθέσεων για τη διεξαγωγή δίκαιης δίκης. Αρχικά, πολλές εφαρμογές, όπως το COMPAS και το HART[241], λειτουργούν με τέτοιο τρόπο, που ουσιαστικά στέλνουν στον δικαστή μία αξιολόγηση του κατηγορουμένου σχετικά με το πόσο επικίνδυνος είναι στο να διαπράξει κάποιο έγκλημα στο μέλλον. Το σκεπτικό των εφαρμογών αυτών είναι να μη χρειάζεται να περάσουν από ένδικες διαδικασίες πολίτες που δεν είναι εγκληματίες υψηλού κινδύνου. Αλλά από την άλλη, το Δικαστήριο προκαταλαμβάνεται αρνητικά από την έκθεση αξιολόγησης του συστήματος, διότι ουσιαστικά γνωρίζει από πριν ότι ο κατηγορούμενος θεωρείται επικίνδυνος από το σύστημα. Δεν αίρεται κατ' αυτόν τον τρόπο το τεκμήριο αθωότητάς του; Το Δικαστήριο θα έπρεπε να αντιμετωπίζει τον κάθε κατηγορούμενο σαν αθώο μέχρι αποδείξεως του εναντίου. Τώρα όμως με τη χρήση της τεχνητής νοημοσύνης η κατάσταση σε ορισμένες χώρες έχει αλλάξει δραματικά[242]. Το πρόβλημα επιδεινώνεται, αν αναλογιστεί κανείς ότι πολλά από τα συστήματα που χρησιμοποιούνται στην ποινική

---

[240] Committee of Experts on Internet Intermediaries (MSI-NET) (2018), *Study on The Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms), and Possible Regulatory Implications*, Council of Europe, διαθέσιμο για λήψη σε μορφή pdf στο https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

[241] Βλ. Κεφάλαιο 3.2.4 Εφαρμογές προληπτικής αστυνόμευσης στην ποινική δικαιοσύνη

[242] Fair Trials (2020), *Webinar: Criminal justice by algorithm - Predictive policing*, το webinar είναι διαθέσιμο σε βίντεο στο https://www.fairtrials.org/articles/film-video/webinar-criminal-justice-by-algorithm-predictive-policing/

δικαιοσύνη έχουν αποδειχθεί πως είναι αναξιόπιστα και ότι προβαίνουν σε διακρίσεις, μιας και χρησιμοποιούν προκατειλημμένα δεδομένα[243].

Η έλλειψη διαφάνειας, που παρατηρήθηκε σε πολλές περιπτώσεις προεγκληματικών εφαρμογών[244], έχει δημιουργήσει αμφιβολίες σχετικά με το δικαίωμα υπεράσπισης του κατηγορουμένου. Για να μπορέσει να εφαρμοσθεί πλήρως το δικαίωμα υπεράσπισης, είναι απαραίτητο ο κατηγορούμενος να έχει όλες τι απαραίτητες πληροφορίες, που να αιτιολογούν την στοχοποίησή του από το σύστημα προληπτικής αστυνόμευσης και την αποδιδόμενη κατηγορία που καλείται να αποκρούσει[245]. Πολλές φορές όμως, η πληροφόρηση, που κανονικά θα έπρεπε να είναι δεδομένη, απουσιάζει. Όπως αναλύθηκε στο κεφάλαιο της διαφάνειας, είναι πολύ δύσκολο να γίνει αντιληπτό από τους ανθρώπους ο ακριβής τρόπος λειτουργίας των αλγορίθμων. Πρόκειται για πολύπλοκες πράξεις που συνυπολογίζουν δεδομένα από διαφορετικές πηγές, χωρίς να γίνεται ευκόλως αντιληπτό ποια δεδομένα έχουν μεγαλύτερη αξία. Συνεπώς καταλήγουν σε ένα αποτέλεσμα, για το οποίο δεν μπορούμε να καταλάβουμε την συλλογιστική του πορεία. Κρίνεται ένας κατηγορούμενος ως εγκληματίας υψηλής επικινδυνότητας και ο δικαστής δεν μπορεί να καταλάβει απόλυτα πώς προέκυψε αυτό το αποτέλεσμα, παρ' όλα αυτά το λαμβάνει υπόψιν του και το δικάζει κανονικά. Παράλληλα, ο κατηγορούμενος δεν μπορεί να αποκρούσει αυτό το αποτέλεσμα, καθώς δεν γνωρίζει τη λειτουργία του συστήματος, επομένως δεν μπορεί να επιχειρηματολογήσει εις βάρος του. Συνεπώς καταλήγουμε στο παράδοξο να έχουμε ένα αλγοριθμικό σύστημα αμφιβόλου ποιότητας, αφού δεν γνωρίζουμε πώς λειτουργεί άρα δεν μπορούμε να το αξιολογήσουμε, το οποίο όμως με την ανάλυση που κάνει, παίζει καθοριστικό ρόλο στην έκβαση της δίκης[246]. Αλήθεια, πώς μπορεί ο κατηγορούμενος να αμυνθεί αποτελεσματικά απέναντι στο άγνωστο;

Είναι προφανές ότι για την αποτελεσματική χρήση των συστημάτων της προληπτικής αστυνόμευσης επιβάλλεται να πραγματοποιούνται ποιοτικοί έλεγχοι σε όλα τα στάδια της συλλογής και επεξεργασίας των δεδομένων. Κάτι τέτοιο όμως είναι σχεδόν αδύνατον να

---

[243] Βλ. την έρευνα που έγινε για το σύστημα COMPAS, Julia Angwin, Jeff Larson κλπ. Υποσημείωση 82

[244] Βλ. Κεφάλαιο 3.4.3 Ο κίνδυνος της διαφάνειας

[245] Βλ. Kate Robertson κ.α. υποσημείωση 35

[246] Fair Trials (2021), AUTOMATING *INJUSTICE: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe*, διαθέσιμο σε pdf στο https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf

ρυθμιστεί νομοθετικά[247], διότι, όπως προαναφέρθηκε σε προηγούμενο Κεφάλαιο, οι ιδιωτικές εταιρείες που κατασκευάζουν τα συστήματα δεν επιθυμούν να γνωστοποιήσουν τη λειτουργία τους. Η συγκεκριμένη απόκρυψη επιτυγχάνεται με την επίκληση σε ιδιωτικές εμπορικές συμφωνίες και σε νόμους και Κανονισμούς διανοητικής ιδιοκτησίας. Έτσι δημιουργείται το φαινόμενο του μαύρου κουτιού (black box problem), το οποίο με τη σειρά του εμποδίζει την πληροφόρηση του κατηγορουμένου για τη λειτουργία του αλγορίθμου, θίγοντας βαθύτατα το δικαίωμα της δίκαιης δίκης. Είναι αναγκαίο λοιπόν, να βρεθούν ορισμένες εφικτές λύσεις έτσι ώστε τα αλγοριθμικά συστήματα προληπτικής αστυνόμευσης να επιτελούν αποτελεσματικά το έργο τους, διευκολύνοντας την αποστολή των αστυνομικών και δικαστικών αρχών, δείχνοντας παράλληλα τον απαραίτητο σεβασμό στα ανθρώπινα δικαιώματα.

6. ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ

Σύμφωνα με την ανάλυση που προηγήθηκε στις προηγούμενες ενότητες έγινε αντιληπτό ότι οι εφαρμογές προληπτικής αστυνόμευσης είναι ικανές (και πολλές φορές το κάνουν) να παραβιάσουν πληθώρα ανθρωπίνων δικαιωμάτων. Παράλληλα, αυτός ο νέος θεσμός αποτελεί ένα χρήσιμο εργαλείο, για τις αστυνομικές αρχές στην σύγχρονη εποχή, καθώς μέσω της επεξεργασίας των κατάλληλων δεδομένων, μπορεί όντως να γίνει μία σωστή εκτίμηση κινδύνου και πράγματι να προληφθεί μία εγκληματική ενέργεια, που ενδέχεται να διαταράξει την δημόσια ασφάλεια. Πρόκειται δηλαδή, για μία νέα τάξη πραγμάτων, η οποία είναι ικανή να βοηθήσει την κοινωνική ευημερία και εξέλιξη, εφόσον φυσικά ρυθμιστεί καταλλήλως. Συνεπώς, η ιδέα της ολικής απαγόρευσης της χρήσης των προεγκληματικών εφαρμογών είναι απολύτως άστοχη. Μάλιστα, δεν είναι τυχαίο, που ενώ υπάρχουν πάρα πολλές μελέτες με αντικείμενο τα μειονεκτήματα και τους κινδύνους της προληπτικής αστυνόμευσης, παρόλα αυτά καμία από αυτές τις μελέτες δεν προτείνει την οριστική διακοπή αυτής της σύγχρονης πρωτοβουλίας[248]. Αντιθέτως, υποδεικνύουν τους τομείς, που επιβάλλεται να βελτιστοποιηθούν έτσι ώστε να σέβονται τα ανθρώπινα δικαιώματα, λειτουργώντας ταυτόχρονα αποτελεσματικά στη διαλεύκανση εγκλημάτων. Πρέπει λοιπόν, να εξεταστούν ποιοι είναι οι τομείς που χρειάζεται να βελτιωθούν.

[247] Βλ. Kate Robertson κ.α. υποσημείωση 35
[248] Βλ. Ishmael Mugari, υποσημείωση 15

Κατά τη μελέτη των κινδύνων της αλγοριθμικής αστυνόμευσης, παρατηρήθηκε ότι όλα τα στάδια της προληπτικής αστυνόμευσης μπορούν να αποβούν άκρως επικίνδυνα για τα θεμελιώδη δικαιώματα που διασφαλίζονται στην ΕΣΔΑ και στον ΧΘΔΕΕ. Είτε πρόκειται για το στάδιο συλλογής των απαραίτητων δεδομένων, είτε για την επεξεργασία τους, είτε για τα αποτελέσματα του αλγορίθμου, ο πυρήνας των ανθρωπίνων δικαιωμάτων θίγεται, και πολλές φορές θίγεται ανεπανόρθωτα. Η κατάσταση επιδεινώνεται, αν αναλογιστεί κανείς ότι απ' όλα τα στάδια της διαδικασίας απουσιάζει φανερά η έννοια της διαφάνειας, η οποία από μόνη της δημιουργεί πληθώρα νέων ζητημάτων. Το σωστό λοιπόν είναι, να πραγματοποιηθούν πρακτικές διορθωτικές κινήσεις που αφορούν τόσο τη συνολική μορφή του θεσμού της προεγκληματικής αστυνόμευσης, όσο και τα επιμέρους στάδια λειτουργίας της.

6.1 Βελτιστοποίηση της ποιότητας των δεδομένων

Απαραίτητη προϋπόθεση για την εύρυθμη και αποτελεσματική λειτουργία ενός αλγοριθμικού συστήματος είναι η συλλογή και η επεξεργασία των κατάλληλων δεδομένων, έργο που, όπως αναλύθηκε σε προηγούμενο κεφάλαιο[249], αποδείχθηκε αρκετά δύσκολο. Πράγματι, η συλλογή και η επεξεργασία δεδομένων κακής ποιότητας αποτελεί πηγή πολλών προβλημάτων, όπως τα εσφαλμένα και ανακριβή αποτελέσματα των προεγκληματικών συστημάτων, αλλά και πιο σοβαρών ζητημάτων όπως οι ρατσιστικές προβλέψεις, που δημιουργούν με τη σειρά τους τη λεγόμενη «προκατειλημμένη αστυνόμευση». Δημιουργείται λοιπόν το ερώτημα, τι αλλαγές χρειάζεται να πραγματοποιηθούν για να βελτιωθεί η κατάσταση;

6.1.1 Αναγνώριση του λάθους

Το πρώτο βήμα που χρειάζεται να γίνει, σε αυτό το στάδιο βελτίωσης της λειτουργίας της προληπτικής αστυνόμευσης, είναι να αναγνωριστεί από τις αστυνομικές αρχές ότι οι εφαρμογές τους ενδέχεται να σφάλλουν. Γενικά τα συστήματα τεχνητής νοημοσύνης προωθούνται τόσο πολύ στις μέρες μας, διότι επικρατεί η άποψη ότι οι αλγόριθμοι είναι αντικειμενικοί και δεν επηρεάζονται από προκαταλήψεις, σε αντίθεση με τους ανθρώπους που δεν είναι αμερόληπτοι. Το σκεπτικό αυτό, όπως αποδείχθηκε προηγουμένως, είναι

[249] Βλ. κεφάλαιο 2.5.1 και επόμενα.

αβάσιμο καθώς τα δεδομένα που επεξεργάζονται οι αλγόριθμοι πολλές φορές μπορεί να αποδειχθούν εσφαλμένα, ελλιπή ή και προκατειλημμένα[250]. Συνεπώς οι προβλεπτικές τεχνολογίες, μπορούν να κάνουν και λάθη, και αυτά τα λάθη πρέπει να αναγνωρίζονται πρώτα από τις ίδιες τις αστυνομικές αρχές που χρησιμοποιούν αυτά τα συστήματα. Η ύπαρξη λαθών και ανακριβειών δεν υποβαθμίζει την προληπτική αστυνόμευση σαν θεσμό, αντιθέτως υποδεικνύει τα σημεία στα οποία έγινε το λάθος και προετοιμάζει το έδαφος για να ελεγχθεί, σε πρώτο βαθμό, για ποιο λόγο συνέβη το λάθος καθώς και για να διορθωθεί το λάθος σε επόμενο στάδιο[251]. Επίσης η αναγνώριση των λαθών συμβάλει στην κατάρριψη της άποψης ότι τα συστήματα τεχνητής νοημοσύνης είναι αλάνθαστα και πιο αποτελεσματικά από τα συστήματα που ελέγχονται από τους ανθρώπους. Μετριάζει την αδιαμφισβήτητη αποδοχή των αλγορίθμων και καθιστά σαφές ότι αυτά τα συστήματα από μόνα τους δεν είναι η λύση σε όλα τα προβλήματα. Επομένως η απόλυτη εξάρτηση από τις προβλέψεις των αλγορίθμων, όπως συνέβη στην υπόθεση State v Loomis ενδέχεται να δημιουργήσει περισσότερες αδικίες απ' όσες μπορεί να επιλύσει.

6.1.2 Διόρθωση του λάθους

Αφού πραγματοποιηθεί το πρώτο βήμα, που είναι η αναγνώριση του σφάλματος, το αμέσως επόμενο, και πολύ πιο δύσκολο, βήμα είναι η διόρθωσή του. Αλήθεια τι ενέργειες χρειάζεται να βελτιωθούν οι μηχανισμοί προληπτικής αστυνόμευσης; Η απάντηση σε αυτή την ερώτηση ευρίσκεται στον τρόπο λειτουργίας των προγραμμάτων. Τα αλγοριθμικά συστήματα για να παράγουν αποτελέσματα χρειάζεται να επεξεργαστούν δεδομένα. Συνεπώς, σε πρώτο στάδιο, κρίνεται απαραίτητο τα δεδομένα προς επεξεργασία να είναι όσο το δυνατόν πιο ποιοτικά γίνεται. Όσο υψηλότερη είναι η ποιότητα των δεδομένων τόσο πιο αποτελεσματικές μπορούν να γίνουν και οι προβλέψεις. Επομένως μία ρεαλιστική λύση είναι η εγκαθίδρυση εσωτερικών μηχανισμών ελέγχου, με κύριο μέλημα τους τον έλεγχο των εισροών[252]. Πρόκειται για μία αρκετά απλή λύση, καθώς επόπτες και αναλυτές, εντός των αστυνομικών αρχών, θα έχουν την υποχρέωση να ελέγχουν λεπτομερώς τις ημερήσιες εγκληματολογικές αναφορές των αστυνομικών, καθώς και να πραγματοποιούν ελέγχους

---

[250] Βλ. Julia Angwin, Jeff Larson κλπ. Υποσημείωση 85

[251] Βλ. Andrew Ferguson, υποσημείωση 25

[252] David N. Kelley, Sharon L. McCarthy, (2013), *The report of the Crime Reporting Review Committee to Commissioner Raymond w. Kelly concerning COMPSTAT auditing*, διαθέσιμο σε pdf στο https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/crime_reporting_review_committee_final_report_2013.pdf

μεγάλης κλίμακας του συστήματος αναφοράς (reporting system). Μέσω των ελέγχων αυτών, θα εντοπίζονται στις βάσεις δεδομένων διπλότυπες ή λανθασμένες εγγραφές οι οποίες θα διαγράφονται.

Για να βελτιωθεί η διαδικασία ελέγχου κρίνεται αναγκαίο, από τον γράφοντα, να προηγηθεί κατάλληλη εκπαίδευση των αστυνομικών που αναλαμβάνουν τις έρευνες των εγκληματικών πράξεων[253]. Εφόσον το κεντρικό θέμα είναι οι εφαρμογές πρόληψης, είναι απαραίτητο να καταστεί σαφές πόσο απαραίτητες είναι για το έργο των συγκεκριμένων λογισμικών οι έννοιες της λεπτομέρειας και της ακρίβειας κατά τη συλλογή δεδομένων στη σκηνή του εγκλήματος. Τα εσφαλμένα δεδομένα, όπως για παράδειγμα μία λάθος διεύθυνση υπονομεύουν την ακρίβεια και την ακεραιότητα του συστήματος. Συνεπώς, οι αστυνομικές αρχές οφείλουν να εκπαιδεύσουν καταλλήλως τους αστυνομικούς ώστε να κατανοήσουν τη δέουσα σημασία της έρευνας και να γίνουν πιο προσεκτικοί και σχολαστικοί οι ίδιοι.

6.2 Ποιοτικός έλεγχος των αλγορίθμων και ενίσχυση της διαφάνειας

Ωστόσο η διαδικασία ελέγχου δεν πρέπει να σταματήσει στα εγκληματολογικά δεδομένα. Πολλές φορές, είναι πιθανό, ο ίδιος ο αλγόριθμος που συλλέγει και επεξεργάζεται τα δεδομένα να λειτουργεί αναποτελεσματικά καθώς και να παράγει προκατειλημμένα αποτελέσματα. Τα προβλήματα διογκώνονται, αν αναλογιστεί κανείς ότι ούτε οι αρμόδιες αρχές αλλά ούτε και οι πολίτες, τα υποκείμενα της επεξεργασίας, δεν γνωρίζουν απόλυτα πως λειτουργούν οι αλγόριθμοι. Πρόκειται, όπως προαναφέρθηκε[254], για το πρόβλημα του μαύρου κουτιού (black box problem), σύμφωνα με το οποίο, οι ιδιωτικές εταιρείες, που δημιουργούν το λογισμικό, δεν δημοσιεύουν τον τρόπο λειτουργίας του για να μην αποτελέσει αντικείμενο αντιγραφής ο πηγαίος κώδικας του. Ως αποτέλεσμα, ενδέχεται να παραβιάζονται ανθρώπινα δικαιώματα ή να παράγονται ρατσιστικά αποτελέσματα και να μην είναι γνωστό στον υπόλοιπο κόσμο ο λόγος που συμβαίνει αυτό. Πρόκειται για μία κατάσταση που επιβάλλεται να αλλάξει άμεσα.

Συνεπώς, πέρα από τον έλεγχο των δεδομένων που συλλέγονται και επεξεργάζονται από τις αρχές, πρέπει ο έλεγχος να συνεχιστεί και σε επόμενο στάδιο αυτή τη φορά πάνω στον

---

[253] Darwin Bond-Graham (2014), *Forget the NSA, the LAPD spies on millions of innocent folks*, διαθέσιμο στο https://www.laweekly.com/forget-the-nsa-the-lapd-spies-on-millions-of-innocent-folks/

[254] Βλ. κεφάλαιο 2.5.3 Ο κίνδυνος της διαφάνειας

ίδιο τον αλγόριθμο. Ο έλεγχος θα πρέπει να εστιάζει στα αποτελέσματα των προβλέψεων των συστημάτων προληπτικής αστυνόμευσης, καθώς έτσι θα γίνεται πιο εύκολα αντιληπτό πόσο αποτελεσματικά είναι τα συστήματα ως προς την εκπλήρωση των στόχων τους, αν οι προβλέψεις αντικατοπτρίζουν φυλετικές-ρατσιστικές προκαταλήψεις, ή αν οι προβλέψεις τους καταλήγουν σε υπερβολική αστυνόμευση[255]. Είναι προτιμότερη η εξέταση του αποτελέσματος των αλγορίθμων, γιατί δεν χρειάζεται να αναλυθεί ο πηγαίος κώδικας του κάθε συστήματος, μία ανάλυση αρκετά δυσχερής που απαιτεί εξειδικευμένες γνώσεις από τους αναλυτές. Αντιθέτως με τον έλεγχο του αποτελέσματος των εφαρμογών γίνεται πιο κατανοητή, πιο «χειροπιαστή», η αξιολόγηση της ισχύος της προληπτικής αστυνόμευσης. Μπορούμε με αυτόν τον τρόπο να κατανοήσουμε με ευκολία τι ακριβώς κάνουν οι προεγκληματικές εφαρμογές, απέναντι σε ποιον στρέφονται και για ποιο σκοπό.

Για να καταστεί αποτελεσματικός και αντικειμενικός, ο έλεγχος των αλγορίθμων θα πρέπει να γίνεται από μία ανεξάρτητη αρχή, εξωτερική του σώματος της αστυνομίας. Οι αλγόριθμοι, με τις προβλέψεις τους, επηρεάζουν άμεσα τους πολίτες, είτε χαρακτηρίζοντας τους ως πιθανούς υπόπτους είτε ως υποψήφια θύματα. Συνεπώς επηρεάζουν άμεσα την κοινωνική ζωή, μιας και η καταπολέμηση της εγκληματικότητας είναι ένα μείζον κοινωνικό ζήτημα. Λόγω αυτής της υψηλά κοινωνικής σημασίας, δεν αρκεί ο έλεγχος να γίνεται εσωτερικά, εντός της αστυνομίας όπως γίνεται με τα δεδομένα. Αντιθέτως πρέπει να δημιουργηθούν ανεξάρτητες αρχές που να απαρτίζονται από εξειδικευμένους αναλυτές δεδομένων[256]. Η αρχή αυτή οφείλει να είναι εξωτερικό σώμα και ανεξάρτητο καθώς έτσι δεν θα μοιράζεται τα ίδια συμφέροντα με τις αστυνομικές αρχές. Κατ' αυτόν τον τρόπο θα είναι εφικτό να γίνει ένας δίκαιος και ακριβής έλεγχος του αλγορίθμου, έχοντας σαν γνώμονα την κοινωνική ευημερία και την προστασία των ανθρωπίνων δικαιωμάτων και όχι αποκλειστικά την αστυνομική αποτελεσματικότητα. Χρειάζεται λοιπόν μία «διττή» προσέγγιση που να περιλαμβάνει τόσο εσωτερικούς μηχανισμούς ελέγχου (δεδομένα), όσο και εξωτερικούς (αλγόριθμος)[257].

---

[255] Bonnie Sheehey (2020), *Ethics Beyond Transparency in advance: Resisting the Racial Injustice of Predictive Policing*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/343582715_Ethics_Beyond_Transparency_in_advance_Resisting_the_Racial_Injustice_of_Predictive_Policing

[256] Βλ. Andrew Ferguson, υποσημείωση 25

[257] Ben Shneiderman (2016), *The dangers of faulty, biased, or malicious algorithms requires independent oversight*, PNAS, διαθέσιμο στο https://www.pnas.org/doi/10.1073/pnas.1618211113

Αυτά τα προτεινόμενα βήματα μπορεί να φαίνονται ενθαρρυντικά ωστόσο δεν αρκούν. Για να επιτευχθεί ένας τόσο σημαντικός, αλλά και απαιτητικός, στόχος, όπως η διαφάνεια, χρειάζονται λύσεις που να αφορούν άμεσα όλη την κοινωνία. Η προληπτική αστυνόμευση έχει σαν κεντρική αποστολή την εξάλειψη της εγκληματικότητας, ένα μείζον κοινωνικό πρόβλημα. Για την επίτευξη του στόχου τα προληπτικά συστήματα συλλέγουν και επεξεργάζονται προσωπικά δεδομένα των πολιτών και μέσω αυτών τους χαρακτηρίζουν ως πιθανούς εγκληματίες ή πιθανά θύματα. Εφόσον λοιπόν, οι προβλέψεις αφορούν τους πολίτες, και μπορούν να καθορίσουν τη ζωή τους, είναι απαραίτητο τα υποκείμενα των δεδομένων να ξέρουν πως προέκυψε αυτή η πρόβλεψη, αν η πρόβλεψη είναι προϊόν προκατάληψης και κυρίως πόσο αποτελεσματική μπορεί να είναι. Κατ' αυτόν τον τρόπο, οι πολίτες θα μπορούν να αμυνθούν δικαστικά κατά των αξιολογήσεων που προκύπτουν από την προβλεπτική αστυνόμευση[258]. Παράλληλα όμως, εφόσον τους καταστεί γνωστή η λειτουργία και η αποτελεσματικότητα του αλγορίθμου, θα αρχίσει σταδιακά να χτίζεται ένα αίσθημα εμπιστοσύνης απέναντι στις αξιολογήσεις με μηχανικά μέσα.

Για την επίτευξη της διαφάνειας, είναι αναγκαίο τα αποτελέσματα των ελέγχων των ανεξάρτητων αρχών να δημοσιεύονται, ώστε να γνωρίζει ο κόσμος την αποδοτικότητα του συστήματος. Πέραν όμως από τις αξιολογήσεις, καλό είναι να δημοσιοποιούνται και τα αποτελέσματα των προβλέψεων των ίδιων των συστημάτων. Αυτά θα δημοσιοποιούνται μαζί με ορισμένες αντικειμενικές μετρήσεις, όπως για παράδειγμα τα ποσοστά εγκληματικότητας σε μία πόλη, ο συνολικός αριθμός των εγκλημάτων ή ο αριθμός των ανθρώπων που συνελήφθησαν από τους προβλεπτικούς μηχανισμούς[259]. Τα αποτελέσματα θα συγκρίνονται με τις ανωτέρω μετρήσεις και έτσι θα καθίσταται σαφής σε όλους η λειτουργικότητα του συστήματος.

6.3 Σεβασμός στα ανθρώπινα δικαιώματα και τροποποιήσεις των σχετικών κειμένων

Τέλος, μία απαραίτητη ενέργεια στην οποία οφείλουν να προβούν τόσο οι αρχές επιβολής του νόμου, όσο και οι ιδιώτες κατασκευαστές των λογισμικών για τις εφαρμογές προληπτικής αστυνόμευσης, είναι ο απόλυτος σεβασμός των ανθρωπίνων δικαιωμάτων[260].

---

[258] Διατηρώντας το δικαίωμα σε δίκαιη δίκη, βλ. υπόθεση State v Loomis.

[259] Βλ. Andrew Ferguson, υποσημείωση 25

[260] Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, John S. Hollywood (2013), *PREDICTIVE POLICING: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation,

Πρέπει να καταστεί σαφές, ότι οι εφαρμογές πρόληψης μπορεί να επιτελούν ιδιαίτερα σοβαρό έργο, όπως είναι η καταπολέμηση της εγκληματικότητας, παρ' όλα αυτά υπάρχουν ορισμένα όρια που πρέπει να τηρηθούν. Τα όρια αυτά είναι ο σεβασμός στο δικαίωμα της ιδιωτικότητας και της ανθρώπινης αξιοπρέπειας, δικαιώματα που διασφαλίζονται στην ΕΣΔΑ και τον ΧΘΔΕΕ[261]. Είναι ανεπίτρεπτο η προληπτική αστυνόμευση να λειτουργεί εις βάρος αυτών των δικαιωμάτων και να είναι υπεράνω του νόμου, παρά μόνο σε περιπτώσεις που ενδέχεται να πληγωθεί βαθύτατα η δημόσια ασφάλεια, όπου και εκεί πάλι απαιτείται αυστηρή εφαρμογή της αρχής της αναλογικότητας. Παράλληλα επειδή τα συστήματα προληπτικής αστυνόμευσης χρειάζονται προσωπικά δεδομένα για να αποδώσουν, είναι υπόχρεα να σέβονται τις βασικές αρχές της προστασίας των δεδομένων καθώς και τα δικαιώματα των υποκειμένων που ορίζονται στον ΓΚΠΔ καθώς και στην Οδηγία 2016/680.

Τις ανωτέρω σκέψεις, τις διατύπωσε το Ευρωπαϊκό Κοινοβούλιο με έκθεση του που δημοσιεύθηκε στις 6 Οκτωβρίου 2021[262]. Όπως διατυπώνεται στην έκθεση, οι εφαρμογές τεχνητής νοημοσύνης είναι υποχρεωμένες να σέβονται τις αρχές της ανθρώπινης αξιοπρέπειας, της μη διάκρισης, της ελευθερίας κινήσεων, το τεκμήριο αθωότητας και το δικαίωμα σε δίκαιη δίκη, συμπεριλαμβανομένου το δικαίωμα της σιωπής, την ελευθερία της έκφρασης και της πληροφόρησης, την ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι, την ίση μεταχείριση απέναντι στο νόμο και την αρχή της ισότητας των όπλων, δικαιώματα που προβλέπονται στην ΕΣΔΑ και τον ΧΘΔΕΕ. Πρέπει λοιπόν, να απαγορευθεί η χρήση εφαρμογών τεχνητής νοημοσύνης όταν είναι ασυμβίβαστη με τα ανωτέρω θεμελιώδη δικαιώματα. Επιπρόσθετα, μιας και οι εφαρμογές τεχνητής νοημοσύνης επεξεργάζονται προσωπικά δεδομένα, η επεξεργασία αυτή οφείλει να είναι συμβατή με το ισχύον νομικό πλαίσιο (Κανονισμός GDPR και Οδηγία 2016/680). Πιο αναλυτικά ο σκοπός της επεξεργασίας θα πρέπει να είναι συγκεκριμένος, σαφής και νόμιμος και η επεξεργασία με τη σειρά της θα πρέπει να είναι σύμφωνη με τον σκοπό και να μην τον υπερβαίνει. Επίσης μόνο τα απολύτως απαραίτητα δεδομένα θα πρέπει να αποτελούν αντικείμενο επεξεργασίας και να αποθηκεύονται μόνο για το αναγκαίο διάστημα της επεξεργασίας, όχι για παραπάνω (αρχή του περιορισμού της περιόδου αποθήκευσης). Για να τηρηθεί η τελευταία αρχή, θα πρέπει

διαθέσιμο σε pdf στο
https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

[261] Βλ. άρθρο 8 ΕΣΔΑ και άρθρο 1 και 7 ΧΘΔΕΕ.

[262] Ολόκληρη η έκθεση είναι διαθέσιμη σε pdf στο
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf, European Parliament (2021), *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*

επιπλέον να οριστούν αυστηρά χρονικά όρια. Τέλος, πέρα από τις βασικές αρχές προστασίας των δεδομένων, είναι βασικό να υπάρχει ανάλογος σεβασμός και στα δικαιώματα των υποκειμένων της επεξεργασίας, με βασικότερο δικαίωμα την ενημέρωση του υποκειμένου ότι τα προσωπικά δεδομένα του αποτελούν αντικείμενο επεξεργασίας[263]. Πέρα από την έμφαση που δόθηκε στον σεβασμό των ανθρωπίνων δικαιωμάτων, το Κοινοβούλιο, μέσω της έκθεσής του εξέφρασε τους προβληματισμούς του για τα προκατειλημμένα αποτελέσματα των αλγορίθμων, απαιτώντας οι αλγόριθμοι να είναι διαφανείς, ανιχνεύσιμοι και επαρκώς τεκμηριωμένοι[264]. Ακόμη, για τον σεβασμό της ιδιωτικής ζωής, το Κοινοβούλιο αιτήθηκε την απαγόρευση αυτοματοποιημένης αναγνώρισης ατόμων σε δημόσιους χώρους, απαιτώντας η παρακολούθηση να γίνεται μόνο όταν οι πολίτες είναι ύποπτοι για κάποια αξιόποινη πράξη.

Για να επιτευχθεί ο στόχος της αποτελεσματικής προστασίας των ανθρωπίνων δικαιωμάτων και του δικαιώματος στην ιδιωτικότητα, είναι αναγκαίο να υπάρξουν ορισμένες τροποποιήσεις και στα σχετικά κείμενα. Πιο συγκεκριμένα, είναι ανεπίτρεπτο στην Οδηγία 2016/680 να είναι διατυπωμένη με τέτοιο τρόπο η αρχή του περιορισμού του σκοπού. Η διατύπωση αυτή όχι απλώς δεν περιορίζει αυστηρά το σκοπό της επεξεργασίας, αντιθέτως ανοίγει το δρόμο για το πρόβλημα του function creep. Μία κίνηση που ενδεχομένως να βελτιώσει την κατάσταση, είναι η εφαρμογή της αρχής ήδη από τη διαδικασία σχεδιασμού των προληπτικών εφαρμογών (scope limitation by design)[265]. Πιο συγκεκριμένα, κατά τον σχεδιασμό των συστημάτων, θα ήταν πρέπον όλοι οι σχετικοί παράγοντες, από τους κατασκευαστές μέχρι και τις αστυνομικές αρχές που θα χρησιμοποιήσουν τα συστήματα, να συζητήσουν και να εκτιμήσουν τον επαρκή όγκο δεδομένων που θα χρειαστούν τα συστήματα AI για να εντοπίσουν τις τάσεις των εγκληματικών ενεργειών (crime trends), τα απαραίτητα μοτίβα επανάληψης καθώς και να προχωρήσουν σε εκτιμήσεις αντικτύπου. Αυτή η μορφή έρευνας από κοινού, συμβάλλει στο να γίνει περισσότερο κατανοητή η λειτουργία αυτών των συστημάτων, καθώς και οι κατηγορίες δεδομένων που είναι απαραίτητες για τον επιδιωκόμενο σκοπό κάθε συγκεκριμένου συστήματος τεχνητής νοημοσύνης. Αφού λοιπόν εντοπιστούν οι

[263] Άρθρα 12-14 ΓΚΠΔ και άρθρα 12,13 Οδηγία 2016/680.
[264] Lawspot (2021), *Τεχνητή νοημοσύνη και αστυνόμευση: Κατά της μαζικής παρακολούθησης το Ευρωπαϊκό Κοινοβούλιο*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-kai-astynomeysi-kata-tis-mazikis-parakoloythisis-eyropaiko-koinovoylio
[265] Βλ. Ivo Emanuilov και λοιποί υποσημείωση 188

συγκεκριμένες κατηγορίες δεδομένων, οι οποίες είναι χρήσιμες για την επίτευξη του συγκεκριμένου σκοπού, τότε είναι που θα πρέπει να εφαρμοστεί η αρχή περιορισμού του σκοπού, η οποία με τη σειρά της θα εμποδίζει τη συλλογή και την επεξεργασία διαφορετικής ομάδας δεδομένων. Κατ' αυτόν τον τρόπο η συγκεκριμένη αρχή μπορεί να εφαρμοστεί στην πράξη και να μην είναι απλώς μία αόριστη θεωρητική αρχή που δεν μπορεί να βρει πεδίο εφαρμογής.

Επίσης, για να μειωθούν, ή και να εξαλειφθούν πλήρως, οι επιβλαβείς επιπτώσεις της AI στα ανθρώπινα δικαιώματα, κρίνεται απαραίτητο να τροποποιηθούν ορισμένες διατάξεις της AI ACT. Ήδη έχει αναλυθεί η προβληματική του άρθρου 5 παράγραφος 4 της πρότασης του Κανονισμού, όπου ουσιαστικά ανατίθεται στα κράτη-μέλη ο προσδιορισμός των αναγκαίων διασφαλίσεων, που επιτρέπουν με τη σειρά τους τη χρήση τεχνολογιών εξ αποστάσεως βιομετρικής ταυτοποίησης σε «πραγματικό χρόνο»[266]. Όπως συνέβη και στην περίπτωση του άρθρου 23 του GDPR, έτσι και στην περίπτωση της τεχνητής νοημοσύνης, υπάρχει σημαντικός κίνδυνος να καταπατηθούν τα ανθρώπινα δικαιώματα κατά τη διαδικασία προσδιορισμού, από τα κράτη, των σχετικών διασφαλίσεων και περιορισμών που πρέπει να υπάρχουν για να είναι σύμφωνη με το νόμο η χρήση συστημάτων AI υψηλού κινδύνου. Η λύση στο πρόβλημα, η οποία έχει ήδη δοθεί από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων[267], είναι η δημιουργία του κατάλληλου νομοθετικού πλαισίου, που εξασφαλίζει τις απαραίτητες διασφαλίσεις, ήδη από τα κείμενα του Ευρωπαϊκού Δικαίου, χωρίς να χρειάζεται να γίνει ο απαραίτητος προσδιορισμός από τα κράτη-μέλη. Κατ' αυτόν τον τρόπο θα υπάρχει ένα κοινό νομοθετικό πλαίσιο για όλες τις χώρες της Ευρωπαϊκής Ένωσης, το οποίο θέτει τις απαραίτητες και στιβαρές βάσεις για την προστασία των ανθρωπίνων δικαιωμάτων εξ' αρχής. Συνεπώς αυτό που πρέπει να αλλάξει, είναι η προσθήκη των απαραίτητων διασφαλίσεων, στις περιπτώσεις που επιτρέπεται η βιομετρική ταυτοποίηση σε πραγματικό χρόνο, στο κείμενο της ίδιας της πρότασης του Κανονισμού.

Εξίσου προβληματική είναι και η διατύπωση του άρθρου 7 παράγραφος 2 που αφορά τη δυνατότητα προσθήκης νέων συστημάτων τεχνητής νοημοσύνης στην ήδη υπάρχουσα λίστα των συστημάτων που χαρακτηρίζονται ως «υψηλού κινδύνου»[268]. Τη δεδομένη χρονική

---

[266] Βλ. ενότητα 4.3.2

[267] European Data Protection Supervisor (EDPS) (2020), *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence –A European approach to excellence and trust*, διαθέσιμο σε pdf στο https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

[268] Βλ. ενότητα 4.3.3

στιγμή, η συγκεκριμένη διαδικασία μόνο ξεκάθαρη δεν είναι. Το άρθρο περιλαμβάνει μία λίστα γενικών και αορίστων κριτηρίων που πρέπει να ληφθούν υπόψη από την Επιτροπή, χωρίς να αναλύεται διεξοδικά πώς ακριβώς θα εκτιμηθούν αυτά τα κριτήρια, ο τρόπος διεξαγωγής της όλης διεργασίας, πώς μπορεί να ξεκινήσει αυτή η αξιολόγηση[269] ή ακόμη και ποια θα είναι η διάρκεια της. Όλες αυτές οι ασάφειες πρέπει να γίνουν πιο ξεκάθαρες, διότι είναι ορατός ο κίνδυνος να τεθούν σε εφαρμογή συστήματα AI που θίγουν τα ανθρώπινα δικαιώματα ενώ η Επιτροπή αδυνατεί να τα χαρακτηρίσει ως υψηλού κινδύνου. Για να διαλευκανθεί η κατάσταση, η προτεινόμενη λύση περιλαμβάνει η δημιουργία ενός ταχύτερου, διαφανούς και ευκόλως προσβάσιμου συστήματος αξιολόγησης των εφαρμογών. Στο έργο αυτό μπορούν να συνδράμουν ανεξάρτητες αρχές και οργανώσεις της κοινωνίας των πολιτών, που θα έχουν την αρμοδιότητα να κρούουν τον κώδωνα του κινδύνου, επιβλέποντας τις αρνητικές επιπτώσεις που μπορεί να επιφέρουν τα συστήματα τεχνητής νοημοσύνης στην κοινωνία και τους πολίτες. Η ορθή εφαρμογή λοιπόν του πρωτογενούς και δευτερογενούς Κοινοτικού Δικαίου μπορεί να παρέχει σημαντική βοήθεια στην προστασία των πολιτών και την ορθή εφαρμογή της προληπτικής αστυνόμευσης, συνεισφέροντας παράλληλα στην ενίσχυση της εμπιστοσύνης ανάμεσα στους πολίτες και την τεχνητή νοημοσύνη μαζί με τις προτεινόμενες λύσεις που αναφέρθηκαν προηγουμένως.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Αν είναι να προκύψει ένα συμπέρασμα από τη μελέτη που πραγματοποιήθηκε, είναι το γεγονός ότι η ραγδαία τεχνολογική ανάπτυξη των τελευταίων δεκαετιών προσέφερε στον άνθρωπο ένα αξιοθαύμαστο εργαλείο, την τεχνητή νοημοσύνη. Πρόκειται για μία τεχνολογία ικανή να συνεισφέρει σε όλους τους τομείς της καθημερινότητας, από τα πιο απλά πράγματα όπως είναι τα social media, μέχρι και τα πιο σύνθετα, όπως η ιατρική. Ήταν φυσικό επόμενο λοιπόν να αρχίσουν να αναπτύσσονται εφαρμογές τεχνητής νοημοσύνης στο πλαίσιο της επιβολής του νόμου. Ο στόχος ήταν να κατασκευαστούν τα κατάλληλα λογισμικά, τα οποία, με τη βοήθεια των big data, θα ήταν ικανά να βελτιώσουν το έργο των αστυνομικών αρχών. Πράγματι, η εξέλιξη έχει θετικό πρόσημο, καθώς η αστυνομία επιλύει ολοένα και περισσότερα εγκλήματα, και σε συντομότερο χρονικό διάστημα, ενώ ο αριθμός

[269] Για παράδειγμα αν χρειάζεται κάποια αίτηση να υποβληθεί

των ανεξιχνίαστων υποθέσεων έχει μειωθεί αισθητά. Μάλιστα η πρόοδος της τεχνητής νοημοσύνης είναι τόσο μεγάλη, που πλέον αναπτύσσονται συστήματα ικανά να εντοπίσουν μοτίβα συμπεριφοράς, είτε αναλύοντας δεδομένα προσωπικού χαρακτήρα, είτε σκηνές εγκλήματος. Τα μοτίβα αυτά δίνουν τη δυνατότητα στις αρχές να προβλέψουν μία εγκληματική συμπεριφορά και να τη σταματήσουν πριν καν εκδηλωθεί. Αυτή η καινοτομία είναι γνωστή και ως προληπτική αστυνόμευση η οποία προβλέπει είτε τα πρόσωπα που είναι πιθανό να εμπλακούν σε ένα έγκλημα, ή τον τόπο που είναι πιθανό να εκδηλωθεί μία εγκληματική ενέργεια.

Το γεγονός όμως ότι οι προβλέψεις προέρχονται από αλγοριθμικά συστήματα και όχι από ανθρώπινη δραστηριότητα δεν τα κάνει αυτομάτως και πιο αποτελεσματικά. Υπάρχουν πολλοί παράγοντες, όπως η κακή ποιότητα των δεδομένων, που καθιστούν τις προβλέψεις όχι απλώς άστοχες, αλλά και επικίνδυνες για την κοινωνική ισότητα, λειτουργώντας πολλές φορές προκατειλημμένα εις βάρος συγκεκριμένων κοινωνικών ομάδων. Παράλληλα αυτά τα συστήματα χρειάζονται δεδομένα προσωπικού χαρακτήρα για τις προβλέψεις τους. Όπως αναλύθηκε τα σχετικά νομοθετικά κείμενα του Δικαίου της Ένωσης έχουν πολύ σημαντικά κενά τα οποία δίνουν το ελεύθερο στα συστήματα τεχνητής νοημοσύνης να επεξεργάζονται προσωπικά δεδομένα σε επικίνδυνο βαθμό για τα ανθρώπινα δικαιώματα. Είναι ικανά να εγκαταστήσουν ένα σύστημα μαζικής παρακολούθησης των πολιτών καταστρατηγώντας θεμελιώδη δικαιώματα όπως το δικαίωμα της ιδιωτικότητας και του συνέρχεσθαι και του συνεταιρίζεσθαι.

Επομένως, λόγω των πολλών εσφαλμένων προβλέψεων, δεν πρέπει καταρχάς οι αστυνομικές αρχές να είναι απόλυτα εξαρτημένες από την προληπτική αστυνόμευση. Αντιθέτως η τελευταία πρέπει να είναι απλώς ένας επιπλέον τομέας, ένα επιπλέον βοήθημα στην καταπολέμηση της εγκληματικότητας. Επιπρόσθετα, για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα, αλλά και των ανθρωπίνων δικαιωμάτων γενικότερα, είναι επιτακτική ανάγκη να πραγματοποιηθούν ριζικές αλλαγές τόσο στην λειτουργία των συστημάτων, όσο και στα σχετικά νομοθετήματα. Οι αλλαγές αυτές έχουν ως στόχο την ποιοτική βελτίωση της λειτουργίας της προληπτικής αστυνόμευσης, τη διαφάνεια καθώς και την προστασία των ατομικών ελευθεριών και αξιών. Δεν πρέπει να ξεχνάμε, ότι το ύψιστο αγαθό είναι οι ανθρώπινες ελευθερίες, οι οποίες είναι υπεράνω κάθε τεχνολογικής και κάθε κοινωνικής αλλαγής. Με αυτή την ιεράρχηση, η τεχνητή νοημοσύνη στην ανίχνευση εγκλημάτων θα παραμείνει ένα χρήσιμο εργαλείο και

όχι ένα όπλο ικανό να πληγώσει τα θεμελιώδη ανθρώπινα δικαιώματα. Τέλος, στην άποψη ότι μπορούν να περιοριστούν η ατομικές ελευθερίες χάριν δημοσίας ασφάλειας, κρίνεται χρήσιμο να παρατεθεί ένα ρητό του Μπέντζαμιν Φράνκλιν, σύμφωνα με τον οποίο «Όσοι θυσιάζουν στοιχειώδεις ελευθερίες για λίγη ασφάλεια, δεν αξίζουν ούτε ελευθερία ούτε ασφάλεια».

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνόγλωσση

Βέρρας Δημήτρης (2021), *Clearview AI: Εντολή για διαγραφή βιομετρικών δεδομένων πολίτη από τον Επίτροπο Προστασίας Προσωπικών Δεδομένων Αμβούργου*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/ClearviewAI-ai-entoli-gia-diagrafi-viometrikon-dedomenon-politi-apo-ton-epitropo-prostasias

Βολικού Αδαμαντία (2020), *Η εποχή της "συγκομιδής" των προσωπικών δεδομένων*, Homo Digitalis, διαθέσιμο στο https://www.homodigitalis.gr/posts/5046

Γαλάζιου Λίντα (2016), *Τι είναι πράγματι τα Big Data;*, διαθέσιμο στο https://www.epixeiro.gr/article/2728

ΕΣΠΔ-ΕΕΠΔ (2021), *Κοινή γνωμοδότηση 5/2021*, διαθέσιμη σε pdf στο https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_el.pdf

Ζουμπουλάκης Κωνσταντίνος και Κωνσταντίνος Κακαβούλης (2020), *Facial recognition και αντεγκληματική πολιτική: Μια βεβιασμένη συνύπαρξη*, διαθέσιμο στο https://www.homodigitalis.gr/posts/7258

Λ. Κανέλλος (2021), *ΕΦΑΡΜΟΓΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ στο δίκαιο και στη δικαστική πρακτική*, εκδόσεις Νομική Βιβλιοθήκη

Κροντήρης Ιωάννης, (2020), *Κινητά τηλέφωνα στη μάχη κατά του κορωνοϊού: Συμβιβασμοί στην προστασία προσωπικών δεδομένων;*, διαθέσιμο στο https://www.homodigitalis.gr/posts/5391

Οργανισμός Θεμελιωδών Δικαιωμάτων της ΕΕ και Συμβούλιο της Ευρώπης (2018), *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών*

δεδομένων, διαθέσιμο σε pdf στο https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

Παπαδοπούλου Έλσα (2020), *Τεχνητή Νοημοσύνη και σχετικές ψηφιακές τεχνολογίες – οι πρωτοβουλίες της Ευρωπαϊκής Επιτροπής και του Ευρωπαϊκού Συμβουλίου Καινοτομίας*, Lawyer the Business Magazine, διαθέσιμο στο https://lawyermagazine.gr/texniti-nohmsunh-sxetikes-psifiakies-texnologies-protoboulies-eurwpaikis-epitropis/

Πετρίδη Κορίνα (2021), *Από αυτό το καλοκαίρι 1.000 φορητές συσκευές της ΕΛΑΣ θα σκανάρουν τα πρόσωπα των πολιτών σε περιπολίες*, reporters united, διαθέσιμο στο https://www.reportersunited.gr/3643/apo-ayto-to-kalokairi-1-000-forites-syskeyes-tis-elas-tha-skanaroyn-ta-prosopa-ton-politon-se-kathimerines-peripolies/

Ρεφανίδης Γ. (2005), *Τεχνητή Νοημοσύνη: Μια σύγχρονη προσέγγιση*, εκδόσεις Κλειδάριθμος.

Τσίρτσης Γιώργος - Τάσσης Σπύρος, (2020), *Κορωνοϊός: Ιχνηλάτηση επαφών (Contact Tracing) και Ειδοποίηση Έκθεσης (Exposure Notification)*, διαθέσιμο στο https://www.lawspot.gr/nomikablogs/spiros_tassis/koronoios-ihnilatisi-epafon-contact-tracing-kai-eidopoiisi-ekthesis

Lawspot.gr (2021), *Τεχνητή νοημοσύνη και αστυνόμευση: Κατά της μαζικής παρακολούθησης το Ευρωπαϊκό Κοινοβούλιο*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-kai-astynomeysi-kata-tis-mazikis-parakoloythisis-eyropaiko-koinovoylio

Lawspot.gr (2021), *CLEARVIEW AI: Εντολή της CNIL για διαγραφή των προσωπικών δεδομένων των κατοίκων της Γαλλίας*, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/ClearviewAI-ai-entoli-tis-cnil-gia-diagrafi-ton-prosopikon-dedomenon-ton-katoikon-tis?fbclid=IwAR2d8kMgxof2tWqVH4u401lrN3P9KvmV0HrNJWWMx-u3Hz72ObTwBZ-yJ2A

The Press Project (2021), *«Προληπτική αστυνόμευση» με συσκευές αναγνώρισης προσώπου από την αστυνομία*, διαθέσιμο στο https://thepressproject.gr/proliptiki-astynomefsi-me-syskeves-anagnorisis-prosopou-apo-tin-astynomia/

Ξενόγλωσση

ACM (2020), *ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies Cites Potential for Injury from Bias to Society's Most Vulnerable*

Populations, διαθέσιμο στο https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies

Angwin Julia, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks*, ProPublica (2016), διαθέσιμο στο https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

ARTICLE 29 DATA PROTECTION WORKING PARTY (2017), *Opinion 2/2017 on data processing at work*, διαθέσιμο σε pdf στο https://ec.europa.eu/newsroom/article29/items/610169

Autoriteit Persoonsgegevens (2020), *On the anonymity of aggregated telco location data*, διαθέσιμο σε pdf στο

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimity_and_aggregated_telco_location_data.pdf

Bachner Jennifer (2017), *Predictive Policing: Preventing Crime with Data and Analytics* διαθέσιμο σε pdf στο https://www.businessofgovernment.org/sites/default/files/Management%20Predictive%20Policing.pdf

Bakke Erik (2018), *Predictive Policing: The Argument for police Transparency*, NYU Annual. Survey of American Law, διαθέσιμο σε pdf στο https://annualsurveyofamericanlaw.org/wp-content/uploads/2019/08/74-1-Predictive-Policing-The-Argument-for-Public-Transparency.pdf

Baradaran Shima (2013), *Race, Prediction, and Discretion*, διαθέσιμο σε pdf στο https://www.gwlr.org/wp-content/uploads/2018/04/81-Geo.-Wash.-L.-Rev.-157.pdf

BBC News, (2020), *Coronavirus: Under surveillance and confined at home in Taiwan*, διαθέσιμο στο https://www.bbc.com/news/technology-52017993

Belfiore R. (2013), *The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters*, Springer, 2013, pp. 355-370

Biderman A D and Reiss A J (1967), *On Exploring the "Dark Figure'' of Crime*, The Annals of the American Academy of Political and Social Science

BJS (2021), *Law Enforcement*, διαθέσιμο στο https://bjs.ojp.gov/topics/law-enforcement

Bond-Graham Darwin (2014), *Forget the NSA, the LAPD spies on millions of innocent folks*, διαθέσιμο στο https://www.laweekly.com/forget-the-nsa-the-lapd-spies-on-millions-of-innocent-folks/

Braga Antony, Webster Daniel, Michael White, and Hildy Saizow (2014), *Smart Approaches to Reducing Gun Violence*, διαθέσιμο σε pdf στο https://centerforimprovinginvestigations.org/wp-content/uploads/2018/08/SPI-Gun-Violence-Spotlight-FINAL-2014.pdf

Brayne Sarah and Angele Christin (2020), *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal courts*, Oxford University Press

Bridges Ed (2018), *Why I'm Challenging Cardiff Police On Their Invasive Facial Recognition Technology*, HuffPost, διαθέσιμο στο https://www.huffingtonpost.co.uk/entry/facial-recognition_uk_5b227088e4b0bbb7a0e53760

Burgess Matt (2018), *UK police are using AI to inform custodial decisions – but it could be discriminating against the poor*, διαθέσιμο στο https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit

Butcher Mike (2018), *Media monitor Meltwater acquires social analytics player Sysomos*, διαθέσιμο στο https://techcrunch.com/2018/04/24/media-monitor-meltwater-acquires-social-analytics-player-sysomos/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABgTMOxr-9vqeDB-Z6VyvYIn2tH63Qaonw5XP8wTQOORtzALT2qK4QZhDxmsWDLfXh77Cew1gn5DYeKCt1k2a_N_o4mfZsQQNtIClKTjKtumpG3t_JDL2l0Dt-qMkx8EFkhdEDHxKEvlw5DeBiR_hZgq_xfHdRtnnElcXGtqnI7g

Cagle Matt (2015), *This Surveillance Software is Probably Spying on #BlackLivesMatter*, διαθέσιμο στο https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter

Caplan Joel, Leslie Kennedy, Jeremy Barnum and Eric Piza (2017), *Crime in Context: Utilising Risk. Terrain Modelling and Conjunctive Analysis of Case Configuations to Explore the Dynamics of Criminogenic Behaviour Settings*, Journal of Contemporary Criminal Justice

CBC, (2020), *Coronavirus: WHO calls COVID-19 outbreak a pandemic as Italy orders most stores to close*, διαθέσιμο στο https://www.cbc.ca/news/world/coronavirus-pandemic-1.5493411

CBS News (2020), *CEO speaks out about Clearview AI AI's controversial facial recognition technology*, διαθέσιμο σε μορφή βίντεο στο https://www.cbsnews.com/video/ceo-speaks-out-about-Clearview AI-ais-controversial-facial-recognition-technology/#x

Charles Sam (2020), *CPD decommissions 'Strategic Subject List'*, διαθέσιμο στο https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson

Chavis K (2019), *The Pitfalls of Police Technology: A Minority Report*, The Cambridge Handbook of Policing in the United States

CNN Business (2020), *Is this facial recognition app going too far? We tested it*, διαθέσιμο σε βίντεο στο YouTube στο https://www.youtube.com/watch?v=pGJNXG2vmZw&ab_channel=CNNBusiness

Cohn Rachel (2016), *Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide*, Brennar Center for Justice, διαθέσιμο στο https://www.brennancenter.org/our-work/analysis-opinion/mapping-reveals-rising-use-social-media-monitoring-tools-cities

COM (2020), *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*, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

COMMISSION STAFF WORKING DOCUMENT (2020), *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*, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/1_en_swd_part1_v6.pdf

Committee of Experts on Internet Intermediaries (MSI-NET) (2018), *Study on The Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms), and Possible Regulatory Implications*, Council of Europe, διαθέσιμο για λήψη σε μορφή pdf στο https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

Conger Kate, Richard Fausset and Serge F. Kovaleski (2019), *San Francisco Bans Facial Recognition Technology, New York Times*, διαθέσιμο στο https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Cox Joseph (2020), *Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US*, διαθέσιμο στο https://www.vice.com/en/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras

Cutting Crime Impact (CCI) (2020) *Fact Sheet: Predictive Policing*, διαθέσιμο σε pdf στο https://www.praeventionstag.de/html/download.cms?id=1026&datei=Factsheet_Predictive-Policing_English-1026.pdf

Data Ethics Commission of the German Federal Government (2019), *Opinion of the Data Ethics Commission*, διαθέσιμο σε pdf στο

https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

Degeling M and Berendt B (2018), *What is wrong with Robocops as consultants? A technology-centric critique of predictive policing*, AI and Society 33, 347-356

De Hert Paul & Juraj Sajfert (2021), *THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS: FRAMING BIG DATA POLICING THROUGH THE PURPOSE LIMITATION AND DATA MINIMISATION PRINCIPLES OF THE DIRECTIVE (EU) 2016/680*, BRUSSELS PRIVACY HUB, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=195074122123114102126066074012007025053087027082034055099022095106113069068102090110053035120006007034111112086009100031001007126082004073093125029122096025007025031013007074071071121002072027025089121086102068031018085102091109091080077116117106092&EXT=pdf&INDEX=TRUE

Dumbrava Costica (2020), *Tracking mobile devices to fight coronavirus*, διαθέσιμο στο https://epthinktank.eu/2020/04/21/tracking-mobile-devices-to-fight-coronavirus/

Egbert Simon and Matthias Leese (2020), *Criminal Futures: Predictive Policing and Everyday Police Work,* Routledge Studies in Policing and society

Emanuilov Ivo, Fantin Stefano, Marquenie Thomas, Vogiatzolgou Plixavra, (2020), *Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence*, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020, UNICRI Special Collection on AI, διαθέσιμο σε pdf στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3679850

EPRS European Parliamentary Research Service (2021), *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence*, διαθέσιμο σε pdf στο https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf

European Commission (2018), *A European approach to artificial intelligence*, διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Data Protection Board, (2020) *Statement on the processing of personal data in the context of the COVID-19 outbreak*, διαθέσιμο σε pdf στο https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

European Data Protection Board (2022), *Facial recognition: Italian SA fines Clearview AI EUR 20 million*, διαθέσιμο στο https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

European Data Protection Supervisor (EDPS) (2020), *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence –A European approach to excellence and trust*, διαθέσιμο σε pdf στο https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

European Parliament (2014), *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, διαθέσιμο σε pdf στο https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.pdf?redirect

European Parliament (2021), *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, διαθέσιμη σε pdf στο https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2020), *Artificial Intelligence and Law Enforcement, Impact on Fundamental Rights*, European Parliament, διαθέσιμο σε pdf στο

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT) (2019), *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*, διαθέσιμο σε pdf στο https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab

Fair Trials (2020), *Webinar: Criminal justice by algorithm - Predictive policing*, το webinar είναι διαθέσιμο σε βίντεο στο https://www.fairtrials.org/articles/film-video/webinar-criminal-justice-by-algorithm-predictive-policing/

Fair Trials (2021), *AUTOMATING INJUSTICE: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe*, διαθέσιμο σε pdf στο https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf

Ferguson Andrew (2017), *Policing Predictive Policing, Washington University Law Review*, διαθέσιμο σε pdf στο https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6306&context=law_lawreview

Ferguson Andrew (2020), *Predictive Policing Theory*, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=527000067124025069089116075074096108039003024042071075093075112088116121097095010067114102007027106035006118101122070002026084005082039040022094024066121104030086084045079095094027068065114126090080114084000092023070097004116118087010071028007111101&EXT=pdf&INDEX=TRUE

Filipkowski Wojciech (2019), *Predictive policing using the latest technological advancements*, διαθέσιμο στο

https://www.researchgate.net/publication/337155284_Predictive_policing_using_the_latest_technological_advancements

Fondazione Giacomo Brodolini (FGB) (2019), *Fundamental rights review of EU data collection instruments and programmes: Final report*, διαθέσιμο σε pdf στο https://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf

Future of Privacy Forum (2018), *Understanding Facial Detection, Characterization and Recognition Technologies*, διαθέσιμο σε pdf στο https://fpf.org/wp content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf

Gabel Cino Jessica (2018), *DEPLOYING THE SECRET POLICE: THE USE OF ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM*, Georgia State University Law Review, διαθέσιμο σε pdf στο https://www.courts.wa.gov/subsite/mjc/docs/2019/Deploying%20the%20Secret%20Police.pdf

Garvie Clare, Alvaro Bedoya, Jonathan Frankle (2016), *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, διαθέσιμο στο https://www.perpetuallineup.org/

Gerstner Dominik (2018), *Predictive Policing in the context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Wurttemberg*, European Journal for Security Research, διαθέσιμο σε pdf στο https://link.springer.com/article/10.1007/s41125-018-0033-0

Goodin Dan, (2020), *Apple and Google detail bold and ambitious plan to track COVID-19 at scale*,

διαθέσιμο στο https://arstechnica.com/information-technology/2020/04/apple-and-google-detail-bold-andambitious-plan-to-track-covid-19-at-scale/

Gray Jeff (2016), *Could a controversial gun-surveillance system help tackle Toronto crime?*, The Globe and Mail, διαθέσιμο στο https://www.theglobeandmail.com/news/toronto/technology-offers-police-more-than-a-shot-in-the-dark/article30773005/

Guthrie Ferguson Andrew (2017), *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York: New York University Press

Habersetzer Nicola (2020), *Moscow Silently Expands Surveillance of Citizens*, Human Rights Watch, διαθέσιμο στο https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens

Hamilton Isobel Asher, (2020), *Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance*, διαθέσιμο στο https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3

Han-Wei Liu, Ching-Fu Lin, Yu-Jie Chen (2018), *Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/332457303_Beyond_State_v_Loomis_Artificial_Intelligence_Government_Algorithmization_and_Accountability

Harari Yuval Noah, (2020), *Yuval Noah Harari: the world after coronavirus* | Free to read, διαθέσιμο στο https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Homo Digitalis, (2020), *COVID-19 & ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΗΝ ΕΛΛΑΔΑ*, διαθέσιμο σε pdf στο

https://www.homodigitalis.gr/wpcontent/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf

Human Rights Committee (2020), *General comment No. 37 Article 21: right of peaceful assembly*, διαθέσιμο στο https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

Jelinek Andrea (2020), *EDPB response to MEPs concerning the facial recognition app developed by Clearview AI*, διαθέσιμο σε pdf στο https://edpb.europa.eu/sites/default/files/files/file1/edpb_lettertomepintveldonreviewpnrdirective.pdf

Joh Elizabeth (2014), *POLICING BY NUMBERS: BIG DATA AND THE FOURTH*

AMENDMENT, Washington Law Review, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=084013121017005086024085098122023109118032061048043044009117116089082113106095070092005049039026020056054098121095081124102064108057014069082025064085001073095056085047013088090015025001095098077124075093095089097110015002080079021007112071065069&EXT=pdf&INDEX=TRUE

Kaminski Margot E. (2018), *The Right to Explanation, Explained, University of Colorado Law School*, διαθέσιμο σε pdf στο

https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2335&context=articles

Katzenbach Christian, Lena Ulbricht, (2019), *Algorithmic governance*, διαθέσιμο στο https://policyreview.info/concepts/algorithmic-governance

Kelley David N., McCarthy Sharon L., (2013), *The report of the Crime Reporting Review Committee to Commissioner Raymond w. Kelly concerning COMPSTAT auditing*, διαθέσιμο σε pdf στο https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/crime_reporting_review_committee_final_report_2013.pdf

Kosta Eleni (2020), *Algorithmic state surveillance: Challenging the notion of agency in human rights*, διαθέσιμο στο https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12331

Lau Tim (2020), *Predictive Policing Explained*, διαθέσιμο στο https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

Larson Jeff, Surya Mattu, Lauren Kirchner and Julia Angwin (2016), *How We Analyzed the COMPAS Recidivism Algorithm*, ProPublica, διαθέσιμο στο https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Leiser, M.R. and Custers, B.H.M. (2019), *The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680*, European Data Protection Law Review. Vol. 5, nr. 3, p. 367-378, διαθέσιμο σε pdf στο https://scholarlypublications.universiteitleiden.nl/access/item%3A2980780/view

Llenas Bryan (2014), *Brave New World Of 'Predictive Policing' Raises Specter Of High-Tech Racial Profiling*, Fox News, διαθέσιμο στο https://www.foxnews.com/world/brave-new-world-of-predictive-policing-raises-specter-of-high-tech-racial-profiling

Lynch Jennifer (2018), *Face Off: Law Enforcement Use of Face Recognition Technology*, διαθέσιμο στο https://www.eff.org/wp/law-enforcement-use-face-recognition

Lynskey Orla (2019), *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, διαθέσιμο σε pdf στο https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/criminal-justice-profiling-and-eu-data-protection-law-precarious-protection-from-predictive-policing/10FD4B64364191B619FBCB864CD40A7F

Mac Ryan, Caroline Haskins, Logan McDonald (2020), *Clearview AI's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News, διαθέσιμο στο https://www.buzzfeednews.com/article/ryanmac/Clearview AI-ai-fbi-ice-global-law-enforcement#4ldqpgc

Margison Amanda (2017), *Twitter and Instagram ban London, Ont., company for helping police track protesters*, CBC, διαθέσιμο στο https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093

Martens Pascal (2016), *PREDICTIVE POLICING TENSION BETWEEN ANALYTICS AND INTUITION A Literature Review in accordance with the requirements for the degree of Master of Science in Policing*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/346400071_PREDICTIVE_POLICING_TENSION_BETWEEN_ANALYTICS_AND_INTUITION_A_Literature_Review_in_accordance_with_the_requirements_for_the_degree_of_Master_of_Science_in_Policing

Mcgrory Kathleen and Neil Bedi (2020), *Targeted, Tampa Bay Times*, διαθέσιμο στο https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/

Meares Tracey et al. (2009), *Attention Felons: Evaluating Project Safe Neighborhoods in Chicago*, Columbia Law School, διαθέσιμο σε pdf στο https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2393&context=faculty_scholarship

Menlo Park (2021), *Facebook Reports First Quarter 2021 Results*, διαθέσιμο στο https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results/default.aspx

Miro-Llinares Fernando (2020), *Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/339638731_Predictive_policing_utopia_or_dystopia_On_attitudes_towards_the_use_of_big_data_algorithms_for_law_enforcement

Mugari Ishmael and Emeka Obioha (2021), *Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, διαθέσιμο στο https://www.mdpi.com/2076-0760/10/6/234/htm

New Law Journal, Volume 123, Part 1 - Page 358, 1974

Nilsson, N. (2010), *The Quest for Artificial Intelligence*, United Kingdom: Stanford University

Norga Alice (2021), *4 Benefits And 4 Drawbacks Of Predictive Policing*, διαθέσιμο στο https://www.liberties.eu/en/stories/predictive-policing/43679

Oswald Marion (2018), *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, διαθέσιμο στο https://www.tandfonline.com/doi/full/10.1080/13600834.2018.1458455

Papachristos Andrew and Michael Sierra-Arevalo (2018), *Policing the Connected World*, διαθέσιμο σε pdf στο https://cops.usdoj.gov/RIC/Publications/cops-w0859-pub.pdf

Pearsall Beth (2010) *Predictive Policing: The Future of Law Enforcement?*, διαθέσιμο στο https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement

Perry Walter L., Brian McInnis, Carter C. Price, Susan C. Smith, John S. Hollywood (2013), *PREDICTIVE POLICING: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, διαθέσιμο σε pdf στο

https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

Pew Research Center, (2019), *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, διαθέσιμο στο https://www.pewresearch.org/global/2019/02/05/smartphone-ownershipis-growing-rapidly-around-the-world-but-not-always-equally/

Privacy International (2019), *Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR*, διαθέσιμο σε pdf στο https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf

Rishabh Jain (2020), *Baidu's Face Detection AI Will Help China Identify People Without Masks, International Business Times*, διαθέσιμο στο https://www.ibtimes.com/baidus-face-detection-ai-will-help-china-identify-people-without-masks-2923502

Robertson Kate, Cynthia Koo and Yolanda Song (2020), *TO SURVEIL AND PREDICT a human rights analysis of algorithmic policing in Canada*, University of Toronto

SAS, *Data Mining What it is & why it matters*, διαθέσιμο στο https://www.sas.com/en_us/insights/analytics/data-mining.html#dmtechnical

Scanlan Jeremiah (2019), *Auditing Predictive Policing, Brigham Young University Prelaw Review*, διαθέσιμο σε pdf στο https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1302&context=byuplr

Schlehahn Eva, Aichroth Patrick, Mann Sebastian, Schreiner Rudolf, Shepherd Ifan and B.L. Wong William (2015), *Benefits and Pitfalls of Predictive Policing*, διαθέσιμο σε pdf στο file:///C:/Users/user/Downloads/benefits_pitfalls_FINAL.pdf

Selbst Andrew D. (2017), *Disparate Impact in Big Data Policing*, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=535088111116102116000012094117081122000020077035034062072086122067098087127117106098056017035063031005018100101072115081092082121026023010011084127126102030030124023017048009090114105092064031026096075096005123018069007068076124094064100120022009097087&EXT=pdf&INDEX=TRUE

Shapiro Aaron (2017), *Reform predictive policing*, διαθέσιμο στο https://www.nature.com/articles/541458a

Sheehey Bonnie (2020), *Ethics Beyond Transparency in advance: Resisting the Racial Injustice of Predictive Policing*, διαθέσιμο σε pdf στο https://www.researchgate.net/publication/343582715_Ethics_Beyond_Transparency_in_advance_Resisting_the_Racial_Injustice_of_Predictive_Policing

Shneiderman Ben (2016), *The dangers of faulty, biased, or malicious algorithms requires independent oversight*, PNAS, διαθέσιμο στο https://www.pnas.org/doi/10.1073/pnas.1618211113

Simonite Tom (2017), *AI Experts Want to End 'Black Box' Algorithms in Government*, διαθέσιμο στο https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/

Stevenson Megan (2018), *Assessing Risk Assessment in Action*, διαθέσιμο σε pdf στο https://deliverypdf.ssrn.com/delivery.php?ID=474090073005021098083067113102023086022027028059062003011090125000073006030003028000041101048107026028021105094003080117107026028085086079040085096087003102101081006026092079104102124019074066099094121069122125069019089011122092065099111029117120007114&EXT=pdf&INDEX=TRUE

The Guardian, (2020), *Apple and Google team up in bid to use smartphones to track coronavirus spread*, διαθέσιμο στο https://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-appprivacy

The New York Times (2020), *The Secretive Company That Might End Privacy as We Know It*, διαθέσιμο στο https://www.nytimes.com/2020/01/18/technology/Clearview_AI-privacy-facial-recognition.html

The Leadership Conference on Civil and Human Rights (2020), *The use of the PATTERN risk assessment in prioritizing release in response to the COVID-19 pandemic*, διαθέσιμο σε pdf στο https://www.upturn.org/static/files/Final_Letter_on_PATTERN_in_Response_to_AG_Barr_Memo_on_4_26-4_3_2020.pdf

Wagner Julian and Benecke Alexander (2016), *National Legislation within the Framework of the GDPR*, διαθέσιμο σε pdf στο http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/national-legislation-and-gdpr.pdf

Wilson Jonathan (2020), *Boston City Council votes to ban facial-recognition tech*, διαθέσιμο στο https://eandt.theiet.org/content/articles/2020/06/boston-city-council-votes-to-ban-facial-recognition-tech/

Zarsky Tal (2013), *Transparent Predictions*, διαθέσιμο σε pdf στο https://www.illinoislawreview.org/wp-content/ilr-content/articles/2013/4/Zarsky.pdf

Ιστοσελίδες

https://blog.google/documents/66/Overview_of_COVID-19_Contact_Tracing_Using_BLE_1.pdf/

https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

https://curia.europa.eu/jcms/jcms/j_6/en/

https://edpb.europa.eu/edpb_en

https://el.wikipedia.org/wiki/Instagram

https://github.com/DP-3T/documents

https://land-der-ideen.de/en/project/Precobs-software-for-predicting-crimes-355

https://www.alibaba.com/

https://www.echr.coe.int/Pages/home.aspx?p=home

https://www.eppo.europa.eu/en

https://www.europol.europa.eu/

https://www.predpol.com/how-predictive-policing-works/

https://www.predpol.com/results/

https://www.shotspotter.com/

https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/?fbclid=IwAR08yhtuhoWLQo26hgwnmi1ZB3S3Q5SlhKIZo5Y8o3nyRTs28Ka6h4DKpww

Νομοθετικά κείμενα

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, διαθέσιμη σε pdf στο https://www.echr.coe.int/documents/convention_ell.pdf

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679, διαθέσιμος σε pdf στο https://eurlex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2018/1725, διαθέσιμος σε pdf στο https://edps.europa.eu/sites/edp/files/publication/regulation_eu_2018_1725_el.pdf

ΛΕΥΚΗ ΒΙΒΛΟΣ Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, διαθέσιμο σε pdf στο https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf

ΟΔΗΓΙΑ 95/46/ΕΚ, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL

ΟΔΗΓΙΑ 2002/58/ΕΚ, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EL

ΟΔΗΓΙΑ (ΕΕ) 2016/680, διαθέσιμη σε pdf στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ΓΙΑ ΤΗ ΘΕΣΠΙΣΗ ΕΝΑΡΜΟΝΙΣΜΕΝΩΝ ΚΑΝΟΝΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΤΕΧΝΗΤΗ

ΝΟΗΜΟΣΥΝΗ (ΠΡΑΞΗ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ) ΚΑΙ ΤΗΝ ΤΡΟΠΟΠΟΙΗΣΗ ΟΡΙΣΜΕΝΩΝ ΜΟΜΟΘΕΤΙΚΩΝ ΠΡΑΞΕΩΝ ΤΗΣ ΕΝΩΣΗΣ, η αιτιολογική έκθεση είναι διαθέσιμη σε pdf στο https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF, και τα παραρτήματα είναι διαθέσιμα σε pdf στο https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_2&format=PDF

ΧΑΡΤΗΣ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ, διαθέσιμος σε pdf στο

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EL:PDF

Δικαστικές αποφάσεις

Υπόθεση υπ' αριθμόν ***C/09/550982***, διαθέσιμη στο https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878

Liberty and Others v. the United Kingdom (2008), η περίληψη διαθέσιμη σε pdf στο https://brill.com/journals/hudi/article-p1061

STATE v. LOOMIS, Supreme Court of Wisconsin, διαθέσιμο στο https://www.courts.ca.gov/documents/BTB24-2L-3.pdf

Weber and Saravia v. Germany (2006), διαθέσιμη στο https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76586%22]}