

# ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ



## ΤΜΗΜΑ ΔΙΕΘΝΩΝ & ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ  
«ΔΙΕΘΝΕΙΣ ΚΑΙ ΕΥΡΩΠΑΪΚΕΣ ΣΠΟΥΔΕΣ»

Διπλωματική Εργασία

**ΠΛΗΡΟΦΟΡΗΣΗ (INTELLIGENCE) ΚΑΙ ΕΠΙΒΟΛΗ ΝΟΜΟΥ ΚΑΙ  
ΤΑΞΗΣ**

Φοιτήτρια: Σουλιώτη Ευρυδίκη (ΜΘ18032)

Επιβλέπων Καθηγητής: Κωνσταντόπουλος Ιωάννης

Μέλη Τριμελούς Επιτροπής: Καθηγητής Πλατιάς  
Αθανάσιος και Επίκουρος Καθηγητής Λιαρόπουλος  
Ανδρέας

ΠΕΙΡΑΙΑΣ, Νοέμβριος 2021

## **ΕΥΧΑΡΙΣΤΙΕΣ**

Με την παρούσα διπλωματική εργασία ολοκληρώνονται οι σπουδές μου στο μεταπτυχιακό πρόγραμμα του Πανεπιστημίου Πειραιώς με θέμα τις Διεθνείς Σχέσεις και τις Ευρωπαϊκές Σπουδές.

Στους καθηγητές μου οφείλω να εκφράσω τις θερμές κι ειλικρινείς ευχαριστίες μου για τη συμβολή τους στην ολοκλήρωση των σπουδών μου και τη γνώση που μου μετέδωσαν η οποία θα με συνοδεύει στη ζωή μου.

Ιδιαίτερως επιθυμώ να ευχαριστήσω τους καθηγητές μου κ.κ. Πλατιά Αθανάσιο, Λιαρόπουλο Ανδρέα και Κωνσταντόπουλο Ιωάννη για την εμπιστοσύνη τους να μου αναθέσουν το συγκεκριμένο θέμα καθώς και για την επιστημονική και συμβουλευτική τους καθοδήγηση στην εκπόνηση της διατριβής μου.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους γονείς μου π.Κωνσταντίνο και Γεωργία Σουλιώτη, οι οποίοι αποτελούν πάντα ένα ανεκτίμητο στήριγμα για εμένα και στους οποίους οφείλω όλη τη διαδρομή των σπουδών μου μέχρι σήμερα.

ΣΟΥΛΙΩΤΗ Κ. Ευρυδίκη  
Πειραιάς, Νοέμβριος 2021

Στους Καθηγητές μου  
και τη μονάκριβή μου Ζωή

## Περιεχόμενα

### Πίνακας περιεχομένων

Περιεχόμενα.....	1
Εισαγωγή.....	2
Κεφάλαιο 1. Επιβολή του νόμου και πληροφόρηση.....	8
1.1. Επιβολή του νόμου .....	8
1.3.Επιβολή του νόμου και πληροφόρηση .....	28
1.4. Ιστορική αναδρομή.....	50
2.1. Ζητήματα διακρίσεων και δημοκρατίας .....	52
2.2. Τεχνητή νοημοσύνη και δημοκρατία .....	77
Κεφάλαιο 3. Μελέτες περίπτωσης.....	82
3.1. Αμερική.....	82
3.2. Βρετανία.....	87
3.3. Ευρώπη.....	91
Κεφάλαιο 4. Συμπεράσματα .....	97
Βιβλιογραφία.....	102

## Εισαγωγή

Η πληροφόρηση είναι ένα υποσύστημα γενικότερης κοινωνικής παρακολούθησης (Gill&Phythian, 2006). Από την μία πλευρά είναι κοινωνικά ενσωματωμένη: οι νοοτροπίες, οι τεχνολογίες και οι πρακτικές της επιτήρησης δεν είναι ουδέτερες, αλλά θεσπίζονται εντός συγκεκριμένων θεσμικών ρυθμίσεων. Επομένως, ενεργούν με τρόπο που ενισχύουν τις υπάρχουσες σχέσεις εξουσίας (Johnston&Shearing, 2003; Monahan, 2006). Δεν πρέπει όμως να αποκλειστεί η πιθανότητα να ενεργούν με τρόπο που μεταβάλλει τις σχέσεις εξουσίας έτσι ώστε να ενισχυθεί το γενικό δημόσιο συμφέρον. Επομένως, πρέπει να ληφθούν υπόψη οι συνέπειες των τρεχουσών πολιτικών πληροφόρησης αλλά και των νόμων και πρακτικών. Δεν έχουν αλλάξει όλα αυτά από την 11<sup>η</sup> Σεπτεμβρίου, αλλά σίγουρα το πλαίσιο έχει. Σίγουρα, η 11<sup>η</sup> Σεπτεμβρίου αντικατόπτριζε μια επίθεση απέναντι στις Ηνωμένες Πολιτείες. Ωστόσο, η κήρυξη πολέμου κατά της τρομοκρατίας που ακολούθησε είχε κάποιες σημαντικές συνέπειες, τόσο εκούσιες όσο και ακούσιες, αν και ορισμένες από τις τελευταίες ήταν προβλέψιμες. Σε αυτό το πλαίσιο η πληροφόρηση απέκτησε ιδιαίτερη σημασία. Αυτό οφείλεται στις γενικότερες θεωρίες της κοινωνίας των κινδύνων που ασχολούνται με το τι θα μπορούσε να συμβεί και τις υψηλότερες αβεβαιότητες ως προς το τι ακριβώς είναι ο κίνδυνος. Η σημασία και η ορατότητα των απειλών που πλήττουν την κοινωνία κινδύνου σημαίνει ότι όλες οι γνώσεις σχετικά με αυτές διαμεσολαβούνται και εξαρτώνται από την ερμηνεία τους (Adam&vanLoon, 2000).

Εννοιολογικά η πληροφόρηση, αντικατοπτρίζει την υπερβολική πίστη στον θετικισμό, δηλαδή, η μέτρηση των εμπειριών, κατά

προτίμηση ποσοτική, βρίσκεται στο επίκεντρο της δημιουργίας γνώσης και θεωρείται ότι περισσότερες πληροφορίες θα μειώσουν την αβεβαιότητα. Υπάρχουν όμως και άλλες διαστάσεις που θα πρέπει να λαμβάνονται υπόψη. Για παράδειγμα, η νομοθεσία μετά την 11<sup>η</sup> Σεπτεμβρίου τόσο στις ΗΠΑ όσο και στο Ηνωμένο Βασίλειο επεκτείνει τις εξουσίες των οργανισμών να συλλέγουν πληροφορίες και να το πράττουν για έναν αυξημένο αριθμό ενεργειών που θεωρείται ότι σχετίζονται με την τρομοκρατία. Μεμονωμένα, αυτά μπορεί να είναι λογικά βήματα ή ενέργειες των κυβερνήσεων που φοβούνται ότι θα κατηγορηθούν για αδράνεια, αλλά συλλογικά καθιστούν τη δουλειά των οργανισμών να εντοπίζουν τρομοκράτες δυσκολότερη αυξάνοντας το δίκτυ των υπόπτων και προσθέτοντας στην υπερφόρτωση της πληροφόρησης. Οι κυβερνήσεις πρέπει να διαβεβαιώνουν τους πληθυσμούς τους ότι η ασφάλεια είναι η βασική τους ανησυχία. Αυτό δεν είναι καινούργιο αλλά το έργο τους είναι απίστευτα πιο δύσκολο στο νέο κλίμα που έχει διαμορφωθεί και έχουν τεθεί σημαντικά ζητήματα που σχετίζονται με τα ανθρώπινα δικαιώματα.

Η σχέση μεταξύ της κοινότητας και της αστυνομίας μπορεί μερικές φορές να είναι αδύναμη. Λόγω διαφόρων εντάσεων και συγκρούσεων δεκαετίες τώρα, οι αστυνομικές υπηρεσίες αγωνίζονται να βελτιώσουν τις σχέσεις τους με τις κοινότητες. Η αστυνομία επιδιώκει να δημιουργήσει και να ενισχύσει προγράμματα για την οικοδόμηση σχέσεων, τη συμμετοχή των κατοίκων και την αύξηση της νομιμότητας της αστυνομίας, συχνά μέσω διαφόρων κοινοτικών προγραμμάτων αστυνόμευσης. Ωστόσο, η αστυνόμευση υπό την ηγεσία της πληροφόρησης είναι επίσης ικανή να προωθήσει και να επιτύχει αυτούς τους στόχους μέσω ανάλυσης των πλούσιων δεδομένων που προσφέρει και της χρήσης

πληροφοριών για τα εγκλήματα. Όταν τα δεδομένα χρησιμοποιούνται σε μία εστιασμένη προσέγγιση ως κινητήρια δύναμη στην αστυνόμευση υπό την καθοδήγηση της πληροφόρησης, μπορεί να αποτελέσει ένα καινοτόμο μέσο συνεργασίας μεταξύ της αστυνομίας και των πολιτών.

Η τεχνολογία έχει μεταμορφώσει την επιβολή του νόμου. Οι πλατφόρμες κοινωνικών μέσων και τα δεδομένα που συλλέγονται από ιδιωτικά συστήματα παρακολούθησης έχουν γίνει και εξακολουθούν να αποτελούν αναπόσπαστο μέρος των αστυνομικών πρακτικών έρευνας και της ανάλυσης εγκληματικών πληροφοριών. Όταν χρησιμοποιείται σε συνεργασία με την κοινότητα, υπάρχει η δυνατότητα μετατροπής των σχέσεων μεταξύ της αστυνομίας και της κοινότητας και η αλλαγή ενός απελευθερωμένου πολίτη σε έναν εξουσιοδοτημένο πολίτη με ευκαιρίες να αυξήσει την προσωπική του ασφάλεια.

Όπως και η κοινοτική αστυνόμευση, υπάρχουν αρκετές παραλλαγές ή ερμηνείες της αστυνόμευσης υπό την καθοδήγηση της πληροφόρησης. Παρόλο που δεν υπάρχει καθολικός ορισμός για την αστυνόμευση με γνώμονα τη πληροφόρηση, εντούτοις είναι αποδεκτό ότι δίνει έμφαση στην ανάλυση και τη πληροφόρηση ως καθοριστικό στοιχείο για ένα αντικειμενικό πλαίσιο λήψης αποφάσεων που δίνει προτεραιότητα στα σημαντικά σημεία του εγκλήματος, τα θύματα, τους παραβάτες και τις εγκληματικές ομάδες. Διευκολύνει την μείωση, την αναστάτωση και την πρόληψη της εγκληματικότητας και της πρόληψης μέσω στρατηγικής και τακτικής διαχείρισης, ανάπτυξης και επιβολής (Ratcliffe, 2016).

Ουσιαστικά, η αστυνόμευση με γνώμονα την πληροφόρηση είναι μια προσέγγιση βάσει δεδομένων που απαιτεί

την ολοκλήρωση και ανάλυση δεδομένων από μια ευρεία επιλογή πηγών. Αυτή η ανάλυση είναι ζωτικής σημασίας για τους υπεύθυνους λήψης αποφάσεων για τον καθορισμό προτεραιοτήτων, τη λήψη αποφάσεων σε εκτελεστικό επίπεδο και τη δημιουργία της καλύτερης τεχνολογίας για περαιτέρω ακριβή και εστιασμένη αστυνόμευση (Ratcliffe, 2016). Η ανάλυση είναι επίσης αναπόσπαστο μέρος της κατανομής των απαραίτητων πόρων, συμπεριλαμβανομένης της ανάπτυξης των αστυνομικών. Η αστυνόμευση υπό την ηγεσία της πληροφόρησης ως ένα μοναδικό μοντέλο αστυνόμευσης εστιάζει στον εντοπισμό και τη σύλληψη σοβαρών παραβατών (Ratcliffe, 2016). Η έρευνα έδειξε ότι η εφαρμογή αυτού του μοντέλου αστυνόμευσης είναι μια αποτελεσματική τεκμηριωμένη προσέγγιση για την μείωση του εγκλήματος, της διεξοδικής ανάλυσης των σημαντικών σημείων του εγκλήματος, των εγκληματικών ομάδων και των παραβατών (Ratcliffe, 2016).

Η αστυνόμευση με γνώμονα την πληροφόρηση ενσωματώνει στρατηγικά την ανάλυση πληροφοριών στη συνολική αποστολή του αστυνομικού τμήματος που απαιτεί τρία βασικά στοιχεία, τα οποία ο Ratcliffe(2016) χαρακτηρίζει ως το μοντέλο 3i. Πρώτον, οι αναλυτές πρέπει να ερμηνεύσουν το εγκληματικό περιβάλλον. Αυτό απαιτεί προληπτική προσπάθεια από τον αναλυτή να αναζητήσει πληροφορίες από αξιωματικούς και άλλες πηγές για να κατανοήσει τα εγκλήματα στην κοινότητα. Δεύτερον, ο αναλυτής πρέπει να είναι σε θέση να επηρεάσει τους υπεύθυνους λήψης αποφάσεων του τμήματος. Οι ηγέτες πρέπει να κατανοήσουν την αξία της ανάλυσης της εγκληματικότητας και της πληροφόρησης, καθώς και να είναι ανοιχτοί στις συστάσεις των αναλυτών. Τέλος, απαιτεί από τους κύριους υπεύθυνους λήψης αποφάσεων να είναι δεκτικοί και να



χρησιμοποιούν, πληροφορίες και αναλύσεις που έχουν αντίκτυπο στο εγκληματικό περιβάλλον και διευκολύνουν την μείωση του εγκλήματος.

Η αστυνόμευση με γνώμονα την πληροφόρηση καθώς και τα εργαλεία και οι πόροι της μπορούν να διαδραματίσουν σημαντικό ρόλο στην ενημέρωση του κοινού και τη δημιουργία ευκαιριών εμπιστοσύνης. Επομένως, είναι σημαντικό να ληφθεί υπόψη ότι η απουσία δεδομένων, στατιστικών και αναλύσεων που διατίθενται στην κοινότητά μπορεί να προκαλέσουν μεγάλες διαμάχες και λόγους δυσπιστίας στην αστυνομία.

Η τεχνητή νοημοσύνη παίζει όλο και μεγαλύτερο ρόλο σε όλους τους τομείς της κοινωνίας, συμπεριλαμβανομένης και της αστυνόμευσης. Πολλές αστυνομικές δυνάμεις χρησιμοποιούν ήδη την τεχνητή νοημοσύνη για να βοηθήσουν στην πρόβλεψη και τον εντοπισμό ύποπτων προσώπων και τόπων.

Στην αστυνόμευση, ο όρος τεχνητή νοημοσύνη μπορεί να είναι καλύτερα κατανοητός αν εξηγηθεί ότι αναφέρεται στην αυξανόμενη χρήση τεχνολογιών που εφαρμόζουν αλγόριθμους σε μεγάλα σύνολα δεδομένων είτε για να βοηθήσουν την ανθρώπινη αστυνομική εργασία είτε για να την αντικαταστήσουν (Joh, 2017). Με αυτόν τον τρόπο, η τεχνητή νοημοσύνη είναι ήδη ένας σημαντικός παράγοντας στο έργο της αστυνομίας που, αυξάνοντας την αποτελεσματικότητα και παρέχοντας πληροφορίες από μεγάλα δεδομένα, μπορεί να προσφέρει πραγματικά οφέλη καθώς αντιμετωπίζει το έγκλημα και επιβάλλει το νόμο.

Εάν μπορούν να υπάρχουν βελτιώσεις στην ιατρική, τη γεωργία και την επικοινωνία, θα μπορούσε επίσης να εκσυγχρονιστεί και η αστυνόμευση. Αλλά η αστυνόμευση είναι επίσης διαφορετική

από άλλους τομείς που έχουν υιοθετήσει την τεχνητή νοημοσύνη. Η αστυνομία μπορεί να συλλάβει, να συλλάβει, ακόμη και να χρησιμοποιήσει θανατηφόρα βία στις κατάλληλες συνθήκες. Και ο ιδιαίτερος ρόλος της αστυνομίας προκαλεί κατανοητούς φόβους στην περίπτωση της τεχνητής νοημοσύνης (Joh, 2017).

Αυτό είναι και το βασικό ερώτημα της παρούσας έρευνας που εξετάζει την συμβολή της πληροφόρησης στην επιβολή του νομού και της τάξης, λαμβάνοντας υπόψιν την επίπτωση των τεχνολογικών εξελίξεων στη δημοκρατία. Στην ουσία εστιάζει στο κατά πόσο είναι συμβατή η χρήση με τις δημοκρατικές ελευθερίες και τα ανθρώπινα δικαιώματα και κατά πόσο η αστυνομία μπορεί να τις τηρήσει με θεμιτό τρόπο.

Η μεθοδολογική προσέγγιση της παρούσας είναι η ποιοτική έρευνα και πιο συγκεκριμένα η μελέτη περίπτωσης (casestudy). Η μελέτη περίπτωσης είναι μια ερευνητική προσέγγιση που χρησιμοποιείται για να δημιουργήσει μια σε βάθος, πολύπλευρη κατανόηση ενός πολύπλοκου ζητήματος στο πραγματικό περιβάλλον του. Είναι ένας καθιερωμένος σχεδιασμός έρευνας που χρησιμοποιείται εκτενώς σε μια μεγάλη ποικιλία κλάδων, ιδιαίτερα στις κοινωνικές επιστήμες. Μια μελέτη περίπτωσης μπορεί να οριστεί με διάφορους τρόπους με κεντρικό δόγμα την ανάγκη διερεύνησης ενός γεγονότος ή φαινομένου σε βάθος και στο φυσικό του πλαίσιο.

## **Κεφάλαιο 1. Επιβολή του νόμου και πληροφόρηση**

### **1.1.Επιβολή του νόμου**

Η επιβολή του νόμου ειδικά στην περίπτωση του οργανωμένου εγκλήματος δεν είναι εύκολη. Πλέον έχει αναπτυχθεί σε τέτοιο βαθμό που οι παραδοσιακές μέθοδοι επιβολής του νόμου δεν μπορούν εύκολα να το αντιμετωπίσουν οδηγώντας πλέον στην ανάγκη ανάπτυξης νέων μεθόδων και πρακτικών. Προς αυτή την κατεύθυνση κινείται πλέον και η αστυνομική επιστήμη που εστιάζει τόσο στους οργανισμούς και τις υπηρεσίες επιβολής του νόμου όσο και στις διαδικασίες που χρησιμοποιούνται (Gottschalk, 2010).

Η έννοια της διαταραχής έχει χρησιμοποιηθεί για την ανάλυση και την κατανόηση της απόκρισης της επιβολής του νόμου στο οργανωμένο έγκλημα για κάποιο χρονικό διάστημα (Innes&Sheptycki, 2004; Kirby&Nailer, 2013; Kirby&Snow, 2016; Roberts&Everton, 2016). Ωστόσο, υπήρξαν λίγες προσπάθειες να οριστεί ο όρος διαταραχή. Οι Kirby&Penna (2010) ορίζουν τον όρο ως ευέλικτη, μεταβατική και δυναμική τακτική, η οποία μπορεί να χρησιμοποιηθεί γενικότερα για να κάνει το περιβάλλον εχθρικό για την ομάδα του οργανωμένου εγκλήματος. Αυτή η προσέγγιση επικεντρώνεται στη διαταραχή των δικτύων του δράστη, τους τρόπους ζωής και τις ρουτίνες.

Ο όρος της διαταραχής μπορεί να λειτουργήσει με διαφορετικούς τρόπους από διαφορετικούς ενδιαφερόμενους φορείς ή παράγοντες σε όλο τον τομέα της επιβολής του νόμου. Τρία είναι τα βασικά στοιχεία. Το πρώτο είναι ο ενεργός χαρακτήρας της εμπλοκής με το οργανωμένο έγκλημα από τα ενδιαφερόμενα μέρη, η οποία μπορεί να ποικίλλει σε μεγάλο βαθμό ανάλογα με τις περιστάσεις και τη φύση της εγκληματικής δραστηριότητας. Μια

πρόκληση για τη νέα νομοθεσία και την πρακτική επιβολής του νόμου είναι ο εκτοπισμός των τακτικών εγκλημάτων, όπου οι εγκληματίες τροποποιούν και εξελίσσουν την τακτική τους για να παρακάμψουν το μεταβαλλόμενο περιβάλλον τους (Roweetal., 2013). Όπως σημείωσαν οι Kirby&Snow (2016), η διαταραχή αφορά το παρόν, ενώ η επιβολή (όσον αφορά την αναζήτηση διώξεων) επικεντρώνεται στο παρελθόν και η πρόληψη σχετίζεται με το μέλλον. Το δεύτερο στοιχείο είναι οι προσπάθειες των διαχειριστών των περιβαλλόντων εντός των οποίων λειτουργούν οι οργανωμένες εγκληματικές ομάδες, με σκοπό να καταστήσουν δυσκολότερη την επιτυχία τους. Υπό αυτήν την έννοια, η διαταραχή συνδέεται στενά με την έννοια του τριγώνου του εγκλήματος (Felson&Clarke, 1998), η οποία εφαρμόζεται με διάφορους τρόπους σε οργανωμένες εγκληματικές ομάδες (Bright, 2015; Kleemansetal., 2012; vonLampe, 2011). Η θεωρία του τριγώνου του εγκλήματος υποστηρίζει ότι πρέπει να υπάρχουν τρία στοιχεία για να συμβεί ένα έγκλημα: ένας ευάλωτος στόχος (ένα άτομο ή αντικείμενο), ένας παρακινημένος παραβάτης και η απουσία ενός ικανού διαχειριστή. Αυτές οι προσεγγίσεις έχουν χρησιμοποιηθεί προηγουμένως για την ανάλυση των παρεμβάσεων κατά των οργανωμένων εγκληματικών ομάδων (Bright, 2015; Kleemansetal., 2012). Τέλος, αυτός ο ορισμός της διαταραχής αναγνωρίζει την εστίαση στη διακοπή των δικτύων, του τρόπου ζωής και της ρουτίνας των παραβατών. Αυτό περιγράφει ουσιαστικά την καθοδηγούμενη από τη πληροφόρηση προσέγγιση για τη στόχευση ατόμων και ομάδων και διατυπώνει την ποικιλία των κατευθύνσεων στις οποίες οι ενδιαφερόμενοι μπορούν να εστιάσουν τις δραστηριότητές τους.

Τα τελευταία χρόνια, η έννοια της διαταραχής στο πλαίσιο του οργανωμένου εγκλήματος έχει εμφανιστεί σε μεγάλο βαθμό μέσω

της προσέγγισης διαφορετικών χωρών για το σοβαρό και οργανωμένο έγκλημα όπως στην περίπτωση του Ηνωμένου Βασιλείου. Η στρατηγική για το σοβαρό και οργανωμένο έγκλημα στο Ηνωμένο Βασίλειο αναπτύχθηκε αρχικά το 2003 και δημοσιοποιήθηκε το 2006. Η πολιτική ευθυγραμμίζεται σημαντικά με την αντιτρομοκρατική στρατηγική του Ηνωμένου Βασιλείου, η οποία χωρίζεται σε τέσσερα ρεύματα: πρόληψη, επιδίωξη, προστασία και προετοιμασία. Ο πυλώνας «επιδίωξη» ασχολείται με την μείωση της απειλής της τρομοκρατίας διαταράσσοντας τους τρομοκράτες και τις επιχειρήσεις τους. Ενώ η διαταραχή των τρομοκρατικών δραστηριοτήτων θα μπορούσε να αποτρέψει την τρομοκρατία, είναι κάτι παραπάνω από την πρόληψη και, ενδιαφέρεται περισσότερο για το παρόν, ενώ η πρόληψη επικεντρώνεται στο μέλλον (Kirby&Snow, 2016). Η διαταραχή της τρομοκρατικής δραστηριότητας περιλαμβάνει την λήψη μέτρων για την αποτροπή τρομοκρατικών επιθέσεων και την προσαγωγή τρομοκρατών στη δικαιοσύνη μέσω δίωξης και άλλων μέσων, συμπεριλαμβανομένης της ενίσχυσης του νομικού πλαισίου κατά της τρομοκρατίας (π.χ. εισάγοντας νομοθεσία για την απέλαση εκείνων που κρίνονται ότι δεν ευνοούν το δημόσιο καλό).

Η διαταραχή είναι μια καλή περιγραφή για την πρόθεση πίσω από την έννοια της διακοπής, είτε πρόκειται για τρομοκρατία είτε για οργανωμένο έγκλημα. Αυτός ο όρος έχει χρησιμοποιηθεί περισσότερο στις ρυθμίσεις πολιτικής συγκριτικά με τη διακοπή. Αυτό ενδεχομένως να οφείλεται στο ότι είναι αντιπροσωπευτική μιας ρεαλιστικής θέσης ότι είναι δύσκολο το οργανωμένο έγκλημα να εξαλειφθεί εντελώς (Reuter&Tonry, 2020).

Ορισμένοι προτείνουν ότι είναι καλύτερα να γίνεται αντιληπτό το οργανωμένο έγκλημα ως εγκληματικές επιχειρήσεις που μιμούνται νόμιμα επιχειρησιακά μοντέλα (Chiuetal., 2011; Roweetal., 2013). Οι οργανωμένες εγκληματικές ομάδες δομούν τις δραστηριότητές τους για να καλύψουν τις απαιτήσεις των πελατών τους και επιδιώκουν να παρέχουν παράνομα αγαθά και υπηρεσίες. Όπως με τις νόμιμες επιχειρήσεις, τα εγκληματικά επιχειρησιακά μοντέλα χρειάζονται προμηθευτές αποθεμάτων (π.χ. προμηθευτές όπλων), τοποθεσίες αποθήκευσης προμηθειών και κατασκευής (π.χ. αποθήκες), μηχανήματα, μεταφορά για τα αγαθά τους, επικοινωνίες (π.χ. τηλέφωνα και τηλεφωνικά προγράμματα), πελάτες προς πώληση και τραπεζικούς λογαριασμούς για αποθήκευση παράνομων χρημάτων από πωλήσεις (και αργότερα δραστηριότητες για τη νομιμοποίηση αυτών των χρημάτων). Απασχολούν επίσης μια σειρά ατόμων που αναλαμβάνουν εγκληματικές επιχειρηματικές δραστηριότητες και εμπλέκουν μια σειρά επαγγελματιών, όπως λογιστές, χρηματοοικονομικούς συμβούλους και δικηγόρους. Η διαταραχή συνεπώς συνεπάγεται δραστηριότητες που διακόπτουν διαφορετικά στοιχεία μιας εγκληματικής επιχείρησης. Η ανάλυση ενός σεναρίου εγκλήματος, όπου τα εγκληματικά επιχειρηματικά μοντέλα κατανοούνται ως προς τις βήμα-βήμα ενέργειες και τις αποφάσεις που λαμβάνονται, μπορεί να βοηθήσει στην διαταραχή (Chiuetal., 2011; Roweetal., 2013). Με αυτόν τον τρόπο, οι υπηρεσίες επιβολής του νόμου και οι συνεργάτες τους μπορούν να κάνουν το έγκλημα πιο δύσκολο, αποτρέποντας τις προσπάθειες οργανωμένων εγκληματικών ομάδων να αναλάβουν τις δραστηριότητές τους και να τις μετατρέψουν σε νόμιμα κεφάλαια.

Οι δραστηριότητες που επιδιώκουν να διαταράξουν το οργανωμένο έγκλημα περιλαμβάνουν μια σειρά από επιβολές,

κανονιστικές, πολιτικές και νομοθετικές απαντήσεις. Η διαταραχή απαιτεί μια συντονισμένη προσέγγιση από διάφορους παράγοντες. Υπήρξε σημαντική εστίαση στη διαταραχή του οργανωμένου εγκλήματος στα στρατηγικά και επιχειρησιακά σχέδια των υπηρεσιών σε όλο τον τομέα της επιβολής του νόμου. Για παράδειγμα, στην Αυστραλία, η στρατηγική διαχείρισης της εγκληματικής πληροφόρησης συγκεντρώνει μια σειρά διαφορετικών ενδιαφερόμενων φορέων που έχουν διαφορετικά χαρακτηριστικά και μπορούν να συμβάλλουν στη διαταραχή του οργανωμένου εγκλήματος. Πολλοί από αυτούς τους ενδιαφερομένους εντάσσονται με αυτό τον τρόπο στο πεδίο της επιβολής του νόμου. Για παράδειγμα, ενώ η αστυνομία μπορεί να έχει πρωταρχική έμφαση στη διερεύνηση ομάδων οργανωμένου εγκλήματος και στις διάφορες δραστηριότητές τους, τα τελωνεία και οι συνοριακοί οργανισμοί μπορεί να επικεντρωθούν σε δραστηριότητες οργανωμένου εγκλήματος όπου η εισαγωγή αποτελεί βασικό στοιχείο, οι χρηματοοικονομικοί οργανισμοί ενδέχεται να επικεντρωθούν στο ρόλο της απάτης και της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και οι οργανισμοί εσόδων ενδέχεται να επικεντρωθούν σε ομάδες οργανωμένου εγκλήματος από την άποψη των φορολογικών αδικημάτων.

Οι προσεγγίσεις και οι τακτικές της διαταραχής μπορούν να ομαδοποιηθούν σε τρεις κύριες κατηγορίες: επιτήρηση και πληροφόρηση, ενεργή εμπλοκή και σύλληψη και κατάσχεση (Behlendorf&Jacome, 2015). Σε αυτές τις ευρείες κατηγορίες, διαφορετικοί ενδιαφερόμενοι μπορούν να εφαρμόσουν τις εκτελεστικές, κανονιστικές, πολιτικές και νομοθετικές τους εξουσίες με διάφορους τρόπους. Η στόχευση αναφέρεται στη χρήση πληροφοριών για τον εντοπισμό στόχων για παρεμβάσεις. Για

παράδειγμα, η επιβολή του νόμου μπορεί να επιλέξει τους υψηλότερους κινδύνους ή παράγοντες ή ομάδες, οι οποίοι εκτιμάται ότι προκαλούν τη μεγαλύτερη ζημιά. Για παράδειγμα, ο στόχος των ερευνών της Εθνικής Υπηρεσίας Εγκλήματος στο Ηνωμένο Βασίλειο είναι η σύλληψη και δίωξη τέτοιων παραβατών, αλλά, όπου αυτό δεν είναι δυνατόν, η διαταραχή των εγκληματικών επιχειρήσεων με άλλα μέσα.

Ο όρος επιτήρηση και πληροφόρηση χρησιμοποιείται σε αυτό το πλαίσιο για να συμπεριλάβει διάφορες δραστηριότητες που αναλαμβάνονται από τις υπηρεσίες επιβολής του νόμου σε μια προσπάθεια να προσδιορίσουν πού να κατευθύνουν την προσοχή τους και συμπεριλαμβάνει ένα ευρύ φάσμα παρεμβατικών μεθόδων που στοχεύουν σε συγκεκριμένες εγκληματικές ομάδες ή άτομα. Η παρακολούθηση, στον πυρήνα της, είναι μια μορφή συλλογής δεδομένων ή / και πληροφοριών που προορίζονται για συγκεκριμένο σκοπό (Lyon & Wood, 2012). Μπορεί να λάβει πολλές μορφές, συμπεριλαμβανομένης της μυστικής παρατήρησης, αλλά σε ένα πλαίσιο αστυνομικής πληροφόρησης περιλαμβάνεται η παθητική και ενεργή παρακολούθηση συσκευών, η παρακολούθηση της κίνησης ανθρώπων ή εμπορευμάτων, και η παρακολούθηση χρηματοοικονομικών συναλλαγών (Innes & Sheptycki, 2004). Σε ένα πλαίσιο με γνώμονα την πληροφόρηση, η χρησιμότητα των δραστηριοτήτων παρακολούθησης και συλλογής πληροφοριών είναι κάπως περιορισμένη χωρίς την εφαρμογή διαδικασιών πληροφοριών σε αυτές τις διαφορετικές πηγές. Δηλαδή, η πληροφόρηση περιλαμβάνει την εφαρμογή αναλυτικών εργαλείων και τεχνικών σε διαθέσιμα δεδομένα και πληροφορίες, έτσι ώστε να ενημερώνεται η λήψη αποφάσεων και η χρήση οργανωτικών πόρων προκειμένου να επηρεάσουν το εγκληματικό περιβάλλον με τον πιο αποτελεσματικό



και αποδοτικό τρόπο (Ratcliffe, 2016; Sheptycki, 2017). Η πληροφόρηση μπορεί να είναι μια προσπάθεια να διαταραχθούν οι ίδιες οι οργανωμένες εγκληματικές ομάδες, ή ένα μέσο για έναν μεγαλύτερο σκοπό, ο οποίος αντιμετωπίζεται σε σχέση με την ενεργό εμπλοκή και τη σύλληψη και κατάσχεση.

Η ενεργή δέσμευση περιγράφει εκείνες τις δραστηριότητες όπου οι υπηρεσίες επιβολής του νόμου ή άλλοι ενδιαφερόμενοι εμπλέκονται ενεργά σε ύποπτες οργανωμένες εγκληματικές ομάδες, άτομα και τα διάφορα στοιχεία των δραστηριοτήτων τους. Αυτό περιλαμβάνει διείσδυση ή εμπλοκή μέσω της χρήσης πληροφοριοδοτών και μυστικών πράξεων. Ορισμένες ενέργειες μπορεί να είναι ευκαιριακές, όπως οι πληροφοριοδότες που προωθούν εθελοντικά πληροφορίες σχετικά με τις δραστηριότητες μιας συγκεκριμένης ομάδας. Άλλες μορφές ενεργού δέσμευσης περιλαμβάνουν τη συνέντευξη υπόπτων ή τον εξαναγκασμό τους να παρέχουν πληροφορίες σε ανακριτές, όπως και με τις καταναγκαστικές εξουσίες που παρέχονται σε εγκληματικές υπηρεσίες πληροφοριών και τη διείσδυση σε εγκληματική ομάδα μέσω μυστικών πράξεων.

Η ενεργή δέσμευση μπορεί να λάβει διάφορες μορφές ανάλογα με τον εν λόγω φορέα επιβολής του νόμου. Για παράδειγμα, ενώ η ενεργή εμπλοκή για την αστυνομία μπορεί να περιλαμβάνει ανάκριση σε έναν ύποπτο, για μια υπηρεσία εισοδήματος μπορεί να περιλαμβάνει τη διενέργεια ελέγχων εταιρειών ή καταπιστευμάτων που μπορεί να έχουν χρησιμοποιηθεί για τη νομιμοποίηση εσόδων από εγκλήματα. Ένα από τα πιο γνωστά παραδείγματα διαταραχής του οργανωμένου εγκλήματος ήταν η φυλάκιση του διαβόητου αμερικανικού γκάνγκστερ AlCarone το

1931, όχι για παραδοσιακές μορφές εγκλήματος, αλλά για το αδίκημα της φοροδιαφυγής (Kirby&Snow, 2016).

Οι συλλήψεις και οι κατασχέσεις περιλαμβάνουν όχι μόνο την απομάκρυνση συγκεκριμένων ομάδων ή ατόμων από δίκτυα, αλλά και την απόπειρα διακοπής εγκληματικών δραστηριοτήτων με την κατάσχεση παράνομων προϊόντων. Τα οφέλη των συλλήψεων είναι απλά: η απομάκρυνση και η επιβολή κυρώσεων σε άτομα που εμπλέκονται σε οργανωμένες εγκληματικές δραστηριότητες αποτελεί αντικίνητρο και μπορεί να αποτρέψει άλλους από την ανάληψη παρόμοιας δραστηριότητας (Ayling&Broadhurst, 2014). Ένα βασικό στοιχείο της διαταραχής του οργανωμένου εγκλήματος είναι η άρση των ανταμοιβών (ή των κινήτρων) της συμμετοχής στο οργανωμένο έγκλημα. Πρέπει να σημειωθεί, ωστόσο, ότι οι συλλήψεις και οι κατασχέσεις δεν οδηγούν πάντα σε διαταραχές οργανωμένων εγκληματικών ομάδων. Για παράδειγμα, ο Bouchard (2007) διαπίστωσε ότι η αντικατάσταση των συλληφθέντων εμπόρων ναρκωτικών μπορεί να οδηγήσει σε ανεπιθύμητες συνέπειες επεκτείνοντας πραγματικά την ομάδα ατόμων που προσλαμβάνονται, υπονομεύοντας έτσι τυχόν διαταραχές.

Δύο βασικές στρατηγικές που προέκυψαν περιλαμβάνουν τον ανεξήγητο πλούτο και τα έσοδα από εγκλήματα. Η νομοθεσία περί πλούτου είναι μια σχετικά νέα προσθήκη στη νομοθεσία δήμευσης, αλλά γενικά δεν επιτρέπει τη δήμευση περιουσιακών στοιχείων. Οι νόμοι περί πλούτου είναι αστικού χαρακτήρα και χρησιμοποιούνται ως ερευνητικά εργαλεία. Αυτές οι παρεμβάσεις απαιτούν από ένα άτομο που ζει πέρα από τα προφανή μέσα του να δικαιολογήσει τη νομιμότητα του πλούτου του (Bartels, 2010). Αυτοί οι νόμοι θέτουν μια αντίστροφη ευθύνη στο άτομο να εξηγήσει πώς απέκτησε νόμιμα

τον πλούτο του. Πολλές χώρες έχουν επίσης θεσπίσει κάποια μορφή προϊόντος της εγκληματικής νομοθεσίας. Αυτοί οι νόμοι επιτρέπουν την κατάσχεση κεφαλαίων και περιουσιακών στοιχείων που πιστεύεται ότι προήλθαν από εγκληματικές δραστηριότητες. Για παράδειγμα, το Σχέδιο Δράσης ανάκτησης περιουσιακών στοιχείων του Ηνωμένου Βασιλείου το 2019 διατυπώνει με σαφήνεια τέσσερις βασικούς στόχους: να διαταράξει, να στερήσει, να δυσφημίσει και να αποτρέψει. Το Ηνωμένο Βασίλειο έχει επίσης ιδρύσει Ομάδες Επιβολής Κατασχέσεων Περιουσιακών Στοιχείων εντός των αστυνομικών δυνάμεων για την εφαρμογή των προϊόντων της εγκληματικής νομοθεσίας.

Οι υπηρεσίες επιβολής του νόμου και ασφάλειας μπορούν να αναλάβουν μια σειρά παρεμβάσεων εναντίον των οργανωμένων εγκληματικών ομάδων. Αυτές οι παρεμβάσεις περιλαμβάνουν φυσική και ηλεκτρονική παρακολούθηση, χρήση πληροφοριοδοτών και μυστικών επιχειρήσεων και προσπάθειες σύλληψης και δίωξης ατόμων. Τέτοιες παρεμβάσεις, ειδικά όταν απευθύνονται σε ομάδες (σε σύγκριση με παρεμβάσεις που απευθύνονται σε άτομα), περιλαμβάνουν άμεσες δαπάνες (π.χ. ώρες προσωπικού, διοικητικές δαπάνες, κόστος εξειδικευμένου εξοπλισμού) και έμμεσες δαπάνες όπως κόστος ευκαιρίας. Ο όρος «κόστος ευκαιρίας» αναφέρεται στο κόστος που προκύπτει όταν κάποιος επιλέγει να αναλάβει μια πορεία δράσης έναντι μίας άλλης. Για την επιβολή του νόμου, αυτό σχετίζεται με την ιεράρχηση των στόχων. Τόσο το άμεσο όσο και το έμμεσο κόστος είναι σχετικά υψηλό για τις υπηρεσίες επιβολής του νόμου, επειδή τέτοιες έρευνες τείνουν να είναι χρονοβόρες και δαπανηρές όσον αφορά τις ώρες προσωπικού, τις διοικητικές ώρες και τις συναφείς δαπάνες, όπως εξοπλισμός, τεχνολογία και νομικά έξοδα (Bright, 2015).

Επιπλέον, οι υπηρεσίες επιβολής του νόμου και ασφάλειας περιορίζονται σε πόρους. Δεν μπορούν να ερευνήσουν όλες τις ομάδες που βρίσκονται στο ραντάρ τους, και σπάνια θα μπορούσαν να διερευνήσουν όλα τα μέλη μιας ενιαίας οργανωμένης εγκληματικής ομάδας. Είναι ακόμη πιο σπάνιο ότι η επιβολή του νόμου θα μπορούσε να διευρύνει αυτήν την έρευνα σε ένα εκτεταμένο δίκτυο συνεργατών μιας εγκληματικής ομάδας. Για παράδειγμα, στις περισσότερες περιπτώσεις, η παρακολούθηση δεν μπορεί να απευθύνεται σε όλα τα μέλη μιας οργανωμένης εγκληματικής ομάδας, πράγμα που σημαίνει ότι πρέπει να ληφθούν αποφάσεις σχετικά με το ποιοι παράγοντες θα πρέπει να επιλεγούν ειδικά για έρευνα. Με άλλα λόγια, οι υπηρεσίες επιβολής του νόμου πρέπει να λαμβάνουν στρατηγικές αποφάσεις σχετικά με το ποιες ομάδες και παράγοντες σε μια συγκεκριμένη ομάδα θα στοχεύονται ανά πάσα στιγμή.

Έχουν γίνει πολύ λίγες προσπάθειες να περιγραφούν και να εξηγηθούν οι διάφοροι τρόποι με τους οποίους η διαταραχή μπορεί να εννοηθεί χρησιμοποιώντας μια προοπτική δικτύου. Ο Everton (2012) έκανε διάκριση μεταξύ δύο γενικών προσεγγίσεων για την αναστάτωση των σκοτεινών δικτύων: τις κινητικές και μη κινητικές παρεμβάσεις. Οι κινητικές παρεμβάσεις αναφέρονται σε επιθετικά μέτρα που έχουν σχεδιαστεί για την εξάλειψη ή τη σύλληψη μελών του δικτύου και των υποστηρικτών τους (Everton, 2012). Αυτά γίνονται συχνά κατανοητά από την άποψη των στρατηγικών στόχευσης και μπορούν να κατευθυνθούν κατά πάσα πιθανότητα σε άτομα, ομάδες ή οργανισμούς. Σε όρους δικτύου, περιλαμβάνουν την απομάκρυνση βασικών παραγόντων ή ομάδων παραγόντων. Οι μη κινητικές παρεμβάσεις περιλαμβάνουν τη χρήση λεπτών, μη καταναγκαστικών μέσων που έχουν σχεδιαστεί για να μειώσουν την

αποτελεσματικότητα ενός δικτύου και να βλάψουν τη βούληση κάποιου να πολεμήσει (Everton, 2012). Στα παραδείγματα περιλαμβάνονται παρεμβάσεις που κατευθύνονται στο ευρύτερο πλαίσιο στο οποίο λειτουργεί ένα δίκτυο (π.χ. το ρυθμιστικό περιβάλλον), λειτουργίες πληροφοριών που προορίζονται να δημιουργήσουν ψυχολογικά ή πληροφοριακά πλεονεκτήματα, προγράμματα αποκατάστασης και επανένταξης και παρακολούθηση, συμπεριλαμβανομένων παραγόντων παρακολούθησης και παρακολούθησης σε τέτοιες ομάδες.

Οι υπηρεσίες επιβολής του νόμου δεν έχουν στη διάθεσή τους όλες τις πληροφορίες σχετικά με τις οργανωμένες εγκληματικές ομάδες (Burcher&Whelan, 2018; 2019; Hashimi&Bouchard, 2017). Για παράδειγμα, τα όρια της ομάδας σπάνια είναι σαφή (Bouchard, 2020; Burcher&Whelan, 2015). Για να καλυφθούν τα κενά πληροφοριών και να διευκρινιστούν τα όρια του δικτύου, οι υπηρεσίες επιβολής του νόμου πρέπει να επικεντρωθούν στη συλλογή πληροφοριών. Οι μη κινητικές παρεμβάσεις συχνά περιλαμβάνουν μια σκόπιμη στρατηγική για τη συστηματική οικοδόμηση της εικόνας πληροφοριών έως ότου οι αρχές επιβολής του νόμου ή / και οι υπηρεσίες ασφαλείας έχουν μεγάλη αυτοπεποίθηση ότι έχουν σαφή κατανόηση ενός εν λόγω δικτύου. Σε ορισμένες περιπτώσεις, ειδικά σε τρομοκρατικά δίκτυα, είναι προτιμότερο οι υπηρεσίες ασφαλείας να στοχεύουν ένα δίκτυο στο σύνολό του - ή όσο το δυνατόν περισσότερους παράγοντες - ταυτόχρονα, καθώς υπάρχει υψηλός βαθμός αβεβαιότητας που σχετίζεται με την παρέμβαση. Για παράδειγμα, ακόμη και αν ορισμένοι φορείς της περιφέρειας ενός δικτύου δεν αφαιρεθούν, ενδέχεται να είναι υπό εντολή να πραγματοποιήσουν τις επιχειρήσεις τους αμέσως εάν χάσουν την επαφή με άλλα μέλη ενός

δικτύου (π.χ., για να πραγματοποιήσουν κάποια τρομοκρατική επίθεση κάποιου τύπου). Σε άλλα πλαίσια, είναι πιθανό να υπάρχει μια σειρά πιθανών παρεμβάσεων που μπορεί να επιλέξει η επιβολή του νόμου.

Η ανάλυση των κοινωνικών δικτύων μπορεί να είναι μια πολύ χρήσιμη μεθοδολογία για να καθοδηγήσει τη συλλογή τέτοιων πληροφοριών, να οργανώσει τις πληροφορίες για τους παράγοντες και τους δεσμούς μεταξύ τους, να αναλύσει αυτές τις πληροφορίες με τρόπους που εξετάζουν τους παράγοντες και τις σχέσεις μεταξύ τους και να καθοδηγήσει τη λήψη αποφάσεων για την επιλογή στόχου και άλλες πιθανές πορείες δράσης. Η ανάλυση των κοινωνικών δικτύων μπορεί να χρησιμοποιηθεί για τον προσδιορισμό των πιο πολύτιμων στόχων για παρεμβάσεις. Για παράδειγμα, μπορεί να εντοπίσει κόμβους δικτύου των οποίων η αφαίρεση έχει τη δυνατότητα να κατακερματιστεί ένα δίκτυο. Μπορεί επίσης να χρησιμοποιηθεί για να εκτιμηθεί ο αντίκτυπος τέτοιων παρεμβάσεων για να προσδιοριστεί εάν κατάφεραν να κατακερματιστούν ένα δίκτυο (π.χ., καταγράφοντας σχετικά μέτρα όπως συνδεσιμότητα δικτύου ή πυκνότητα δικτύου πριν και μετά από αυτήν την αφαίρεση). Οι υπηρεσίες επιβολής του νόμου θα μπορούσαν να χρησιμοποιήσουν μοντέλα υπολογιστών για να προβλέψουν τον αντίκτυπο συγκεκριμένων συλλήψεων ή άλλων τύπων παρεμβάσεων χρησιμοποιώντας μοντέλα δικτύου που προσομοιώνουν τον αντίκτυπο τέτοιων παρεμβάσεων στο δίκτυο. Διάφορες άλλες πιθανές παρεμβάσεις, συμπεριλαμβανομένου του εντοπισμού πιθανών τρόπων διείσδυσης μιας οργανωμένης εγκληματικής ομάδας για μυστικές επιχειρήσεις και εντοπισμός χρηματοοικονομικών ροών για την ενημέρωση των κατασχέσεων

παράνομα αποκτηθέντων περιουσιακών στοιχείων, θα μπορούσαν επίσης να ενημερωθούν από τις προοπτικές του δικτύου.

Η έρευνα που εστιάζει στη διακοπή οργανωμένων εγκληματικών ομάδων υπό το πρίσμα των δικτύων κυριαρχείται από μελέτες που εξετάζουν τη χρήση της ανάλυσης των κοινωνικών δικτύων για την επιλογή στόχων για σύλληψη ή απομάκρυνση και για τη μέτρηση του αντικτύπου της. Είναι σημαντικό να τονιστεί ότι η ανάλυση των κοινωνικών δικτύων δεν είναι από μόνη της λήψη αποφάσεων και ότι οι υπηρεσίες επιβολής του νόμου πρέπει να εξισορροπήσουν ορισμένα ζητήματα πριν αποφασίσουν για την καλύτερη παρέμβαση ή στρατηγική για τη στόχευση μιας οργανωμένης εγκληματικής ομάδας. Όπως σημείωσε ο Everton (2012), εκτός από οποιαδήποτε καθοδήγηση από την ανάλυση κοινωνικών δικτύων, συμπεριλαμβανομένου του προσδιορισμού πιθανών στόχων για παρέμβαση, είναι επίσης απαραίτητο να ληφθούν υπόψη το πλαίσιο, οι πιθανοί κίνδυνοι και το κόστος και τυχόν πιθανές ακούσιες συνέπειες μιας συγκεκριμένης παρέμβασης ή στρατηγικής.

Ορισμένες μελέτες έχουν εξετάσει την αποτελεσματικότητα των παρεμβάσεων επιβολής του νόμου που χρησιμοποιούν βαθμολογίες κεντρικότητας για να στοχεύσουν (δηλαδή, την σύλληψη) παραγόντων, αλλά δεν έχουν μοντελοποιήσει κανένα είδος προσαρμογής δικτύου. Οι Keeganetal. (2010) αξιολόγησαν την αποτελεσματικότητα της στόχευσης με βάση τις βαθμολογίες σε ένα δίκτυο διακίνησης ναρκωτικών. Διαπίστωσαν ότι, ενώ η αφαίρεση των παραγόντων τυχαία δεν κατακερμάτισε ένα δίκτυο, η στόχευση των παραγόντων διαδοχικά με βάση τις βαθμολογίες της κεντρικής βαθμολογίας έσπασε ένα δίκτυο. Οι Brightetal. (2010) συνέκριναν

την τυχαία στόχευση με τη στόχευση με βάση την κεντρικότητα σε δύο οργανωμένες εγκληματικές ομάδες και διαπίστωσαν ότι η στόχευση των παραγόντων με βαθμό κεντρικότητας οδήγησε σε πιο γρήγορο και πιο έντονο κατακερματισμό σε σύγκριση με την απομάκρυνση των παραγόντων τυχαία. Οι Cavallaroetal. (2020) προσομοίωσαν δύο τύπους παρεμβάσεων επιβολής του νόμου εναντίον δικτύων μαφίας: πρώτον, διαδοχική αφαίρεση κόμβων κατά την οποία ένας παράγοντας αφαιρείται κάθε φορά και δεύτερον, η κατάργηση του μπλοκ, η οποία προσομοίωσε τις αστυνομικές επιδρομές στις οποίες αφαιρούνταν πέντε παράγοντες ταυτόχρονα. Οι μελετητές διαπίστωσαν ότι η στόχευση της αφαίρεσης του παράγοντα χρησιμοποιώντας κεντρικότητα μεταξύ των δύο ήταν η πιο αποτελεσματική στην παραγωγή διαταραχών, αλλά δεν υπήρχε διαφορά μεταξύ της διαδοχικής αφαίρεσης κόμβων και της αφαίρεσης μπλοκ.

Άλλες μελέτες προσομοίωσαν τις συλλήψεις παραγόντων δικτύου που ενημερώθηκαν από ένα σύνθετο ζήτημα κοινωνικού κεφαλαίου (δηλ. Βαθμολογίες κεντρικότητας) και θέματα ανθρώπινου κεφαλαίου (δηλ. χαρακτηριστικά παραγόντων). Καμία από αυτές τις μελέτες δεν μοντελοποίησε την προσαρμογή του δικτύου στις παρεμβάσεις. Ο Carley (2006) δοκίμασε τη διαδοχική απομάκρυνση παραγόντων με υψηλές βαθμολογίες με την απομάκρυνση πιθανών ή αναδυόμενων ηγετών. Η απομάκρυνση των αναδυόμενων ηγετών ήταν η πιο αποτελεσματική όσον αφορά τη διακοπή του προσομοιωμένου δικτύου, γεγονός που υποδηλώνει ότι τα χαρακτηριστικά του παράγοντα μπορεί να είναι ένα σημαντικό ζήτημα κατά τον σχεδιασμό παρεμβάσεων που έχουν σχεδιαστεί για να διαταράξουν ένα δίκτυο. Οι Brightetal. (2014) εξέτασαν τις παρεμβάσεις επιβολής του νόμου που αφαίρεσαν / συνέλαβαν τους



παράγοντες με βάση την κεντρικότητα του βαθμού και τους ρόλους που διαδραμάτισαν οι παράγοντες (π.χ. κατασκευαστές μεθαμφεταμίνης, εργάτες). Οι παρεμβάσεις επιβολής του νόμου που στοχεύουν τους παράγοντες με βάση το βαθμό και τους συνδυασμούς βαθμού και ρόλων οδήγησαν στην πιο έντονη αναστάτωση και κατακερματισμό. Η αφαίρεση παραγόντων βάσει ρόλου ήταν λιγότερο αποτελεσματική και η τυχαία αφαίρεση ήταν η λιγότερο αποτελεσματική. Παρόλο που αυτές οι μελέτες, σε συνδυασμό, υποδηλώνουν ότι η στόχευση του κοινωνικού κεφαλαίου και του ανθρώπινου κεφαλαίου μπορεί να είναι αποτελεσματικοί τρόποι για να διαταραχθούν οι οργανωμένες εγκληματικές ομάδες, ενδέχεται να έχουν υπερεκτιμήσει τον αντίκτυπο των παρεμβάσεων επιβολής του νόμου.

Ορισμένες έρευνες έχουν ενσωματώσει τις προσαρμογές δικτύου σε προσομοιώσεις παρεμβάσεων επιβολής του νόμου χρησιμοποιώντας την ανάλυση κοινωνικών δικτύων για τον καθορισμό στόχων σύλληψης. Οι Tsvetovat&Carley (2003) προσομοίωσαν τις αλληλεπιδράσεις μεταξύ φορέων επιβολής του νόμου και τρομοκρατικών ομάδων. Στόχευσαν τους παράγοντες των οποίων η αφαίρεση οδήγησε σε αύξηση του αριθμού των στοιχείων σε ένα δίκτυο και προσομοιωμένη προσαρμογή δικτύου (δηλαδή, εάν θα μπορούσαν να σχηματιστούν νέοι σύνδεσμοι μεταξύ των υπαρχόντων μελών του δικτύου). Διαπίστωσαν ότι άλλοι παράγοντες μπόρεσαν να καλύψουν γρήγορα τους ρόλους που άφησαν κενούς οι παράγοντες που αφαιρέθηκαν διευκολύνοντας την προσαρμογή του δικτύου. Οι Duijn et al. (2014) αξιολόγησαν την αποτελεσματικότητα πέντε παρεμβάσεων: στόχευση τυχαίων παραγόντων, στόχευση παραγόντων υψηλού βαθμού, στόχευση παραγόντων υψηλού επιπέδου, στόχευση παραγόντων υψηλού βαθμού εντός της

αλυσίδας επίθεσης και στόχευση παραγόντων που έπαιξαν σημαντικό ρόλο στην αλυσίδα επίθεσης. Επίσης μοντελοποίησαν τρεις τύπους προσαρμογής δικτύου που περιλαμβάνουν αντικατάσταση παραγόντων με φορείς εκτός του εγκληματικού δικτύου. Σε όλες τις παρεμβάσεις, το δίκτυο έγινε πιο αποτελεσματικό και πιο πυκνό, υποδηλώνοντας ότι τέτοιες παρεμβάσεις μπορεί να έχουν αντιπαραγωγική επίδραση όταν συμβαίνει προσαρμογή του δικτύου. Η πιο αποτελεσματική στρατηγική ήταν η στόχευση παραγόντων βάσει των ρόλων που έπαιξαν σε ένα δίκτυο. Μόλις ένας παράγοντας που έπαιξε εξειδικευμένο ρόλο αφαιρέθηκε και δεν μπορούσε να αντικατασταθεί, το σενάριο εγκλήματος για την επιχείρηση διακόπηκε και ένα δίκτυο τερματίστηκε αποτελεσματικά.

Αντίθετα, οι Brightetal. (2017) εξέτασαν τον αντίκτυπο έξι παρεμβάσεων σε μια οργανωμένη εγκληματική ομάδα. Οι παρεμβάσεις είχαν σχεδιαστεί για να απομακρύνουν τους παράγοντες που είχαν υψηλό βαθμό ή κεντρικότητα μεταξύ των συμμετεχόντων. Η προσαρμογή του δικτύου μοντελοποιήθηκε επιτρέποντας την αντικατάσταση των αφαιρεθέντων παραγόντων από παράγοντες που βρίσκονται κοντά στον κοινωνικό χώρο με τον αφαιρεθέντα παράγοντα, και οι οποίοι θα μπορούσαν να παράσχουν τους απαραίτητους πόρους για να καλύψουν τις ανάγκες του σεναρίου εγκλήματος. Η στόχευση του κέντρου ήταν η πιο αποτελεσματική παρέμβαση, ακολουθούμενη από στόχευση φορέων που συμμετείχαν σε χρηματοοικονομικές ροές μέσω ενός δικτύου. Τέλος, οι Duxbury&Haynie (2019) χρησιμοποίησαν έναν καινοτόμο συνδυασμό μοντελοποίησης που βασίζεται σε παράγοντες και ανάλυση κοινωνικών δικτύων για να προσομοιώσουν την ανάκτηση δικτύου με την πάροδο του χρόνου ως απόκριση σε απόπειρες

διακοπής. Οι ερευνητές αξιολόγησαν τη στόχευση βαθμού, τη στόχευση μεταξύ των στόχων και τη βασική στόχευση παραγόντων του Borgatti (2003), η οποία στοχεύει τους παράγοντες με τα μικρότερα μήκη διαδρομής με όλους τους άλλους παράγοντες σε ένα δίκτυο (μια μέτρηση που μοιάζει με την προσέγγιση της κεντρικότητας). Κατά μέσο όρο, η στόχευση βαθμού και μεταξύ των σχέσεων ξεπέρασε τη στόχευση βασικών παραγόντων όσον αφορά τον άμεσο αντίκτυπο και έδειξε μακροχρόνια αποτελέσματα. Οι μελετητές διαπίστωσαν ότι τα αποτελέσματα ποικίλλουν ανάλογα με το εάν ένα δίκτυο οργανώθηκε για ασφάλεια ή αποτελεσματικότητα (Morsellietal., 2007).

Τα δίκτυα με προσανατολισμό την ασφάλεια ήταν πιο ανθεκτικά. Ωστόσο, τα προσανατολισμένα στην αποδοτικότητα δίκτυα ανέκαμψαν γρήγορα σε μεγαλύτερο μέγεθος και τον αριθμό των συνδεδεμένων στοιχείων, οπότε μπορεί να είναι σε θέση να ανακτήσουν τα προηγούμενα ποσοστά εγκληματικής δραστηριότητας πιο γρήγορα. Η έρευνα τείνει να συγκλίνει στο εύρημα ότι η μεγαλύτερη διαταραχή επηρεάζεται από την απομάκρυνση των παραγόντων που έχουν υψηλό κοινωνικό κεφάλαιο και ειδικά εκείνων που έχουν υψηλό βαθμό μεταξύ τους και βαθμού κεντρικότητας. Επιπλέον, ορισμένες μελέτες δείχνουν επίσης ότι τα δίκτυα μπορούν να διαταραχθούν με τη στόχευση παραγόντων που παρέχουν βασικά στοιχεία του ανθρώπινου κεφαλαίου που είναι κρίσιμα για το συγκεκριμένο σενάριο εγκλήματος που εφαρμόζεται από ένα δίκτυο.

## **1.2. Έννοια της πληροφόρησης**

Η πληροφόρηση αποτελεί μια δυναμική έννοια, της οποίας ο ορισμός και ο καθορισμός του αντικειμένου του πεδίου δεν

ακολουθούν νόρμες. Η πληροφόρηση σημαίνει πολλά πράγματα, ωστόσο θεμελιωδώς, βασική της αποστολή είναι η παροχή της γνώσης για τον κόσμο στον οποίο ζούμε. Ο όρος «Πληροφόρηση» χρησιμοποιείται ποικιλοτρόπως, γεγονός που δυσχεραίνει τη συναίνεση και την κατάληξη σε έναν κοινά αποδεκτό ορισμό της, τόσο μεταξύ της ακαδημαϊκής κοινότητας όσο ανάμεσα σε εκείνους που την ασκούν ως κρατική δραστηριότητα. Η κύρια δυσκολία φαίνεται ότι έγκειται στην ίδια τη λέξη η οποία σημαίνει ταυτόχρονα το τι πράττουν οι άνθρωποι του επαγγέλματος και σε ποιες ιδέες καταλήγουν μέσω των πράξεων αυτών. Με άλλα λόγια, « η πληροφόρηση είναι μια διαδικασία την ίδια στιγμή που αποτελεί και ένα τελικό προϊόν». (Kent 1946: 117). Κατά τους Gill και Phythian οι ορισμοί που έχουν δοθεί μέχρι σήμερα δημιουργούν τόσο ερωτήσεις, όσο και απαντήσεις.» (Gill & Phythian 2012: 17). Σύμφωνα με τον David Kahn: «Κανένας από τους ορισμούς που έχω δει, δεν λειτουργεί. Είναι όπως ο όρος 'ειδήσεις'.» (Kahn 2001: 79), ενώ ο Michael Warner σημειώνει: «δεν διαθέτουμε έναν αποδεκτό ορισμό της πληροφόρησης», και αυτό μας οδηγεί σε προβλήματα διότι ο όρος «ορίζεται εκ νέου από κάθε συγγραφέα [...] και οι [διαφορετικοί] αυτοί ορισμοί σπάνια αναφέρεται ο ένας στον άλλον ή βασίζονται σε ό,τι έχει γραφτεί προηγουμένως.» (Gill & Phythian 2012: 17).

Διαφορετικοί ορισμοί δίνουν έμφαση σε διαφορετικά στοιχεία της πληροφόρησης. Βασικά, ο Νόμος Εθνικής Ασφάλειας των ΗΠΑ (U.S. National Security Act) του 1947 ορίζει την πληροφόρηση ως

«... πληροφορία που σχετίζεται με τις ικανότητες, προθέσεις, ή δραστηριότητες ξένων κυβερνήσεων ή στοιχεία τους, ξένων οργανισμών, ή ξένων προσώπων.» (Gill & Phythian 2012: 17). Το 1996, ο ορισμός της Επιτροπής Brown-Aspen κινείται πανομοιότυπα, καθώς ορίζεται ως πληροφορία για «ξένα πράγματα – ανθρώπους, χώρους, πράγματα, και γεγονότα – που χρειάζεται η κυβέρνηση για την άσκηση των λειτουργιών της.» (Gill & Phythian 2012: 17).

Από την άλλη, ανεξάρτητοι συγγραφείς και ακαδημαϊκοί διαθέτουν μεγαλύτερη ελευθερία, ευελιξία, καθώς και φαντασία. Ο Sherman Kent ορίζει την πληροφόρηση ως τη «[...] γνώση την οποία πρέπει να διαθέτουν οι υψηλά ιστάμενοι πολιτικοί και στρατιωτικοί άνδρες, προκειμένου να διασφαλίσουν την εθνική ευημερία.» (Kent 1949). Οι Shulsky και Schmit

εννοούν την πληροφόρηση ως «[...] πληροφορίες σχετικές με τον σχεδιασμό και την εφαρμογή πολιτικής εκ μέρους μίας κυβέρνησης, προκειμένου να προάγει τα συμφέροντα εθνικής ασφάλειας της και να αντιμετωπίσει απειλές προερχόμενες από πραγματικούς ή δυνητικούς αντιπάλους.» (Shulsky & Schmitt 2002: 1). Για τον Edward Luttwak και τον Stuart Koehl ο όρος πληροφόρηση σημαίνει «τη συλλογή, σύνδεση, ανάλυση και διανομή των πληροφοριών σχετικά με τις ικανότητες και προθέσεις πραγματικών ή δυνητικών αντιπάλων.» (Luttwak & Koehl 1999: 307-8). Ο Mark Lowenthal, ο οποίος διαθέτει μία διπλή ιδιότητα, εκείνη του ακαδημαϊκού και εκείνη του insider της κοινότητας των αμερικανικών υπηρεσιών πληροφοριών, ξεχωρίζει την

πληροφόρηση από την πληροφορία (information), αν και εκ πρώτης όψεως φαίνεται ότι έχουν μικρή εννοιολογική διαφορά. Θεωρεί ότι ενώ η πληροφορία περιλαμβάνει οτιδήποτε μπορεί να καταστεί γνωστό, ανεξάρτητα με ποιο τρόπο ανακαλύφθηκε, η πληροφόρηση αποτελεί υποσύνολο της πληροφορίας και αναφέρεται στις «πληροφορίες εκείνες που καλύπτουν τις ανάγκες των διαμορφωτών των αποφάσεων και έχουν συλλεχθεί, επεξεργαστεί, και περιοριστεί για να καλύπτουν αυτές τις ανάγκες.» (Lowenthal 2003: 1-2). Το σύνολο της πληροφόρησης αποτελεί κομμάτι της πληροφορίας, αλλά δεν αποτελούν όλες οι πληροφορίες μέρος της πληροφόρησης (Lowenthal 2003: 1-2). Ο Michael Turner θεωρεί την πληροφόρηση ως τις «πληροφορίες που σχετίζονται με την πολιτική, συλλέγονται μέσω ανοικτών και μυστικών μέσων και υπόκεινται σε ανάλυση, με σκοπό την εκπαίδευση, διαφώτιση και βοήθεια [...] στους διαμορφωτές των αποφάσεων στη διαμόρφωση και εφαρμογή της εθνικής ασφάλειας και της εξωτερικής πολιτικής.» (Turner 2005: 4). Ο Loch Johnson ισχυρίζεται ότι η πληροφόρηση είναι «γνώση – και ιδεατά πρότερα γνώση – που αναζητούν τα κράτη προς απάντηση στις εξωτερικές απειλές και για να προστατεύσουν τα ζωτικά τους συμφέροντα, ειδικά την ευημερία του λαού τους.» (Johnson 1997: 365). Ο Michael Warner εξειδικεύει περισσότερο τον ορισμό, καθώς περιορίζει την πληροφόρηση μόνον στη « [...]μυστική, κρατική δραστηριότητα προκειμένου να κατανοηθούν ή να επηρεαστούν ξένες οντότητες.» (Warner 2002: 21). Ο ορισμός της Jennifer Sims δίνει έμφαση στην ανταγωνιστική διάσταση της πληροφόρησης: «η συλλογή, ανάλυση και διανομή των πληροφοριών στους διαμορφωτές των αποφάσεων που εμπλέκονται σε ένα

ανταγωνιστικό εγχείρημα» και «μία διαδικασία με την οποία οι ανταγωνιστές βελτιώνουν τη λήψη αποφάσεων σχετικά με τους αντιπάλους τους.» (Gill & Phythian 2012: 18). Τελικά, οι Gill και Phythian λαμβάνοντας υπόψη όλη την παραπάνω συζήτηση δίνουν το δικό τους ολοκληρωμένο ορισμό: «η πληροφόρηση είναι ένας ολιστικός ορισμός [και] αναφέρεται σε ένα εύρος δραστηριοτήτων – από το σχεδιασμό και τη συλλογή πληροφοριών στην ανάλυση και τη διανομή– που διεξάγονται μυστικά και στοχεύουν στη διατήρηση ή την αύξηση της σχετικής ασφάλειας παρέχοντας προειδοποίηση για απειλές ή δυνητικές απειλές με έναν τρόπο που επιτρέπει την έγκαιρη εφαρμογή μίας προληπτικής πολιτικής ή στρατηγικής, περιλαμβανομένων, όπου κρίνεται επιθυμητό, των μυστικών δραστηριοτήτων.» (Gill & Phythian 2012: 19).

### **1.3.Επιβολή του νόμου και πληροφόρηση**

Η αστυνόμευση με γνώμονα την πληροφόρηση (ILP) είναι μια σχετικά πρόσφατη φιλοσοφία αστυνόμευσης στις Ηνωμένες Πολιτείες, που εμφανίστηκε μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001. Αν και οι ρίζες της βρίσκονται στο Ηνωμένο Βασίλειο, η εμπειρία των ΗΠΑ οφείλεται σε μεγάλο βαθμό στην αποτυχία των υπηρεσιών επιβολής του νόμου να μοιράζονται πληροφορίες που οδήγησαν στις επιθέσεις της 11<sup>ης</sup> Σεπτεμβρίου και το αίτημα της αστυνομίας να είναι πιο αποτελεσματική με περιορισμένους πόρους (Ratcliffe, 2016).

Παρά το γεγονός ότι πολλά πρακτορεία αυτόαναφέρουν την υιοθέτηση της αστυνόμευσης με γνώμονα την πληροφόρηση και την αυξημένη επιστημονική έρευνα σχετικά με το μοντέλο, παραμένει ουσιαστική ασάφεια γύρω από το εννοιολογικό θεμέλιο και την κατάλληλη μέτρηση τηςILP. Οι περισσότεροι μελετητές συμφωνούν ότι ηILP είναι πράγματι μια μοναδική φιλοσοφία αστυνόμευσης. Ωστόσο, υπάρχει λιγότερη συναίνεση σχετικά με τη σχέση μεταξύ της ILP και του διαρκώς υπάρχοντος μοντέλου αστυνόμευσης με γνώμονα την κοινότητα (COP). Εν ολίγοις, η βιβλιογραφία αρθρώνει τη σχέση μεταξύ COP και ILP σε ένα συνεχές που κυμαίνεται από στενά συνδεδεμένα (Bullock, 2013; Carter&Carter, 2009; Clarke, 2006; McGarrelletal., 2007), με ελάχιστη ομοιότητα (Innesetal., 2009), και σαφώς διαφορετικά (Deukmedjian&deLint, 2007; Ratcliffe, 2016).

Από την ακαδημαϊκή προοπτική, υπάρχει μια απαίτηση για εννοιολογική καθοδήγηση για τη βελτίωση των μελετών της ILP. Αυτή η εκλεπτυσμένη εννοιολογική κατανόηση ελπίζει ότι θα δώσει εγκυρότητα σε μελλοντικές εξετάσεις τηςILP που μπορεί να μεταφραστούν σε πιο αποτελεσματικές παρεμβάσεις για την πρακτική. Όσον αφορά την πρακτική, μια βελτιωμένη κατανόηση της σχέσης μεταξύ ILP και COP θα βοηθήσει τους οργανισμούς να πλοηγηθούν στις διαδικασίες ανάπτυξης και εφαρμογής που σχετίζονται με τηνILP. Δεδομένου ότι πολλοί οργανισμοί συμμετέχουν επί του παρόντος σε κάποιο επίπεδο COP, ενδέχεται να υπάρχει μία οργανωτική τάση να αξιοποιούνται τα υπάρχοντα προγράμματα και πρακτικές για τη διευκόλυνση της υιοθέτησης τηςILP.



Ενώ η ILP σπάνια ορίζεται, ειδικά επειδή θεωρείται συμβατή με τις εξελίξεις στη σύγχρονη αστυνόμευση, οι Carter&Carter (2009) την αντιλαμβάνονται ως την συλλογή και ανάλυση πληροφοριών που σχετίζονται με το έγκλημα και τις συνθήκες που συμβάλλουν στο έγκλημα, με αποτέλεσμα ένα προϊόν ευφυούς πληροφοριών που προορίζεται να βοηθήσει την επιβολή του νόμου στην ανάπτυξη τακτικών απαντήσεων σε απειλές ή / και στρατηγικό σχεδιασμό που σχετίζεται με αναδυόμενες ή μεταβαλλόμενες απειλές.

Με βάση αυτές τις ευρύτερες αρχές 1) συλλογή πληροφοριών, 2) ανάλυση και 3) εφαρμογή για την ανάπτυξη στρατηγικών και τακτικών απαντήσεων σε απειλές εγκλήματος, η ILP καταδεικνύει υψηλό βαθμό πιστότητας εφαρμογής μεταξύ των υπηρεσιών. Η ILP έχει σημειώσει σημαντική επιτυχία τα τελευταία χρόνια και θεωρείται ως η ώθηση για τη δημιουργία περιφερειακών κέντρων στελεχωμένων από ομοσπονδιακές, πολιτειακές και τοπικές αρχές επιβολής του νόμου, προκειμένου να μοιραστούν πληροφορίες και δεδομένα μεταξύ των υπηρεσιών (Lewandowski et al., 2018). Στην ουσία, ο στόχος της ILP είναι να αξιοποιήσει τις πρώτες πληροφορίες που εισέρχονται μέσω ποσοτικών και ποιοτικών αναλύσεων για την προληπτική παρακολούθηση και πρόληψη της εγκληματικής δραστηριότητας, κυρίως στοχεύοντας σε συνηθισμένους (δηλαδή παραγωγικούς) παραβάτες και πιθανές απειλές για μια κοινότητα. Η ILP αξιοποιεί τις πληροφορίες που αποκτήθηκαν μέσω διαφόρων πηγών, συμπεριλαμβανομένης της παρακολούθησης, των πληροφοριοδοτών και άλλων υπηρεσιών, για να στοχεύσουν τους συνηθισμένους παραβάτες και να ενισχύσουν την αποτελεσματικότητα της μείωσης του εγκλήματος.

Οι σύγχρονοι ορισμοί της ILP αντικατοπτρίζουν επίσης μια ευρύτερη επιχειρησιακή έμφαση και, για ορισμένους μελετητές, την ένταξη βασικών συνιστωσών από άλλες αστυνομικές φιλοσοφίες. Για παράδειγμα, στο Ηνωμένο Βασίλειο η υιοθέτηση του Εθνικού Μοντέλου Πληροφοριών επέφερε μια αλλαγή στην ILP που ενσωμάτωσε μια προσέγγιση επίλυσης προβλημάτων (Haleetal., 2004; Oakensen et al., 2002) και επέκτεινε την εφαρμογή πέρα από τους συνηθισμένους παραβάτες σε μια ποικιλία θεμάτων στα οποία είναι υπεύθυνη η αστυνομία (Barton&Evans, 1999). Με αυτόν τον τρόπο, η ILP μπορεί να ευθυγραμμιστεί και με άλλες σημαντικές εννοιολογικές φιλοσοφίες αστυνόμευσης, όπως η αστυνόμηση με προβλήματα (POP) και η COP, αλλά επίσης να διατηρήσει μοναδικές αρχές που τη διακρίνουν ως ένα μοναδικό μοντέλο αστυνόμευσης.

Σε αντίθεση με την παραδοσιακή προοπτική επιβολής του νόμου που εστιάζει στη διατήρηση εντολών, η COP είναι μια αστυνομική φιλοσοφία που δίνει έμφαση στη συμμετοχή της κοινότητας στις προσπάθειες πρόληψης του εγκλήματος (Gilletal., 2014). Η COP έγινε γνωστή στη δεκαετία του 1990 ως μια νέα μέθοδος καταπολέμησης του εγκλήματος χρησιμοποιώντας τις συνεργατικές προσπάθειες της επιβολής του νόμου και των κοινοτήτων που υπηρετεί (Gilletal., 2014). Ο πρωταρχικός στόχος της COP είναι η μείωση του εγκλήματος και της αναταραχής με τον προληπτικό εντοπισμό και επίλυση προβλημάτων μέσω της χρήσης συνεργασιών αστυνομίας-κοινότητας και ισχυρών σχέσεων με την κοινότητα (Mastrofskietal., 1995). Καθώς οι κάτοικοι της περιοχής είναι η κύρια πηγή πληροφοριών σχετικά με τα προβλήματα της γειτονιάς, η COP στοχεύει στην ενίσχυση του ρόλου των πολιτών και της πληροφόρησης στην πρόληψη και επίλυση του εγκλήματος (Rosenbaum&Lurigio, 1994). Συνήθως, η COP υλοποιείται μέσω

κοινοτικών αστυνομικών μονάδων που εκπαιδεύονται σε σχέσεις με την κοινότητα και στη δημιουργία σχέσεων, τη χρήση περιπολιών και την ανάθεση αξιωματικών σε συγκεκριμένες γεωγραφικές περιοχές προκειμένου να ενθαρρύνει τους κατοίκους να γνωρίσουν την αστυνομία, να δημιουργηθεί εμπιστοσύνη στην κοινότητα και να χρησιμεύσει μέσω της ενεργούς συμμετοχής της στη δημόσια ασφάλεια (Gilletal., 2014; Rosenbaum&Lurigio, 1994; Weisburd&McElroy, 1988). Η έμφαση της COP στη δημιουργία σχέσεων αναφέρεται στην εξάρτησή της από τη νομιμότητα, την εμπιστοσύνη και τη συλλογή πληροφοριών για τον εντοπισμό, την πρόληψη και την επίλυση εγκλημάτων.

Η COP έχει επιτύχει ευρεία υποστήριξη σε αστυνομικές υπηρεσίες σε όλο τον κόσμο (Gilletal., 2014) και το 1994, το Κογκρέσο ίδρυσε το Γραφείο Κοινοτικών Υπηρεσιών Αστυνομίας (COPS) στο Υπουργείο Δικαιοσύνης των ΗΠΑ, το οποίο έχει δεχτεί επιχορηγήσεις άνω των 14 δισεκατομμυρίων δολαρίων για την προώθηση της υλοποίησης, της αξιολόγησης και της κατάρτισης της κοινοτικής αστυνομίας για την επιβολή του νόμου. Ενώ οι πρώτες αξιολογήσεις της αποτελεσματικότητας της COP δείχνουν μέτριες μειώσεις του φόβου του εγκλήματος και των ποσοστών εγκληματικότητας (Rosenbaum&Lurigio, 1994), η έρευνα διαπιστώνει με μεγαλύτερη συνέπεια ότι η COP έχει άλλα οφέλη, όπως η αύξηση της ικανοποίησης των πολιτών και η εμπιστοσύνη στην αστυνομία (Weisburd&Eck, 2004). Μια μετα-ανάλυση των Gilletal. (2014) ανέλυσε 37 μελέτες αξιολόγησης της COP και διαπίστωσε ότι δεν υπήρχε σημαντική επίδραση στη γενική μείωση του εγκλήματος, του αισθήματος ασφάλειας, των αντιλήψεων των πολιτών για την αστυνομική δικαιοσύνη ή την κοινοτική διαταραχή, αλλά υπήρξε

μείωση του βίαιου εγκλήματος και βελτίωση της ικανοποίησης των πολιτών από την αστυνομία.

Όπως και η COP, η ILP είναι μια προληπτική φιλοσοφία αστυνόμευσης που αποσκοπεί στον εντοπισμό και την πρόληψη προβλημάτων εγκληματικότητας, ιδανικά πριν εμφανιστούν ή γίνουν σοβαρά. Ωστόσο, τόσο η COP όσο και η ILP είναι απλώς πλαίσια για την εφαρμογή στρατηγικών και όχι μια στρατηγική από μόνη της (Gilletal., 2014). Με άλλα λόγια, ούτε η COP ούτε η ILP προορίζονται να είναι τακτικές που μπορούν να εφαρμοστούν για την επίλυση ενός συγκεκριμένου προβλήματος και στη συνέχεια να εγκαταλειφθούν μόλις επιτευχθεί ο στόχος. Επιπλέον, δεδομένου ότι τόσο η COP όσο και η ILP είναι ευρύτερα πλαίσια που μπορούν να εφαρμοστούν με πολλούς τρόπους σε διαφορετικούς οργανισμούς και ποικίλλουν με την πάροδο του χρόνου, ο καθορισμός ενός συγκεκριμένου ορισμού και η αξιολόγηση των ILP και COP αντιμετωπίζουν σημαντικές προκλήσεις (Carter& Phillips, 2015; Mastroskietal., 2007). Άλλες σημαντικές ομοιότητες είναι η εξάρτηση της COP και της ILP από τις κοινοτικές πληροφορίες για την ανάπτυξη ενεργητικών πληροφοριών σχετικά με πιθανά ή τρέχοντα προβλήματα εγκλήματος, η αμφίδρομη ροή πληροφοριών μεταξύ της αστυνομίας και του κοινού και η χρήση δεδομένων για την ενημέρωση της λήψης αποφάσεων βάσει τεκμηριωμένων στοιχείων (Carter&Phillips, 2015; McGarrell et al., 2007).

Υπάρχουν αρκετές αξιοσημείωτες διαφορές μεταξύ ILP και COP. Κατά κύριο λόγο, η έμφαση της COP στην ενδυνάμωση της κοινότητας και στην οικοδόμηση εμπιστοσύνης στην αστυνομία δεν αποτελεί επίκεντρο της ILP (Bullock, 2013). Αντίθετα, η ILP είναι μια φιλοσοφία όπου η πληροφόρηση και τα δεδομένα χρησιμοποιούνται

για τον αντικειμενικό εντοπισμό απειλών εγκλήματος και την αποτελεσματική αντιμετώπισή τους (Bullock, 2013). Ενώ πιο ορατά ζητήματα, όπως οι νέοι που περιπλανιούνται σε μια γωνιά του δρόμου, μπορεί να τραβήξουν την προσοχή των μελών της κοινότητας και να επικεντρωθούν περισσότερο στην COP, η ILP βασίζεται σε πληροφορίες και δεδομένα για να δώσει προτεραιότητα σε ζητήματα που η κοινότητα δεν γνωρίζει γενικά. Με άλλα λόγια, ενώ οι πληροφορίες από το κοινό αναζητούνται και εκτιμώνται τόσο στην COP όσο και στην ILP, η αντικειμενική ανάλυση που χρησιμοποιείται για τον προσδιορισμό των πιο σημαντικών εγκληματικών απειλών είναι η κορυφαία προτεραιότητα και ο μηχανισμός που χρησιμοποιείται για την προληπτική αστυνομία βάσει του μοντέλου ILP.

Η ILP έχει επίσης δώσει έμφαση στην εστίαση στους πιο σοβαρούς και παραγωγικούς παραβάτες, καθώς η έρευνα δείχνει ότι η προτεραιότητα αυτών των περιπτώσεων έναντι άλλων οδηγεί σε πιο αποτελεσματικές προσπάθειες μείωσης του εγκλήματος (Ratcliffe, 2016). Αντίθετα, η COP τείνει να επικεντρώνεται σε ζητήματα σε επίπεδο γειτονιάς, με βάση την ενημέρωση σχετικά με τις ανησυχίες της κοινότητας (Ratcliffe, 2016). Το μοντέλο της ILP ενθαρρύνει τις υπηρεσίες επιβολής του νόμου να εργάζονται πιο έξυπνα, όχι πιο σκληρά όταν αντιμετωπίζουν εγκληματικές απειλές στην κοινότητά τους. Αντί να περιμένει να γίνουν μεγαλύτερα μικρά προβλήματα ή να αντιμετωπίζει ζητήματα μόνο όταν η κοινότητα εκφράζει ανησυχία, η ILP στοχεύει στη χρήση δεδομένων για αποτελεσματικότερη μείωση, αναστάτωση και πρόληψη του εγκλήματος (Ratcliffe, 2016). Σύμφωνα με τους Wood & Shearing (2007), η ILP αποτελεί μία ευκαιρία για την αστυνομία να μπορεί να είναι πιο έξυπνη στην εφαρμογή της μοναδικής εξουσίας και

ικανοτήτων της. Εν ολίγοις, ο πρωταρχικός στόχος της COP είναι η αύξηση της δημόσιας συνεργασίας και των αντιλήψεων για την αστυνομική νομιμότητα για την προληπτική αντιμετώπιση του εγκλήματος και της αναταραχής, ενώ η ILP στοχεύει στη χρήση δεδομένων και πληροφοριών από την κοινότητα και άλλους οργανισμούς για την αποτελεσματικότερη και προληπτική ανάπτυξη των πόρων της αστυνομίας για αντιμετώπιση των πιο σοβαρών και παραγωγικών εγκληματικών απειλών (Bullock, 2013).

Η ILP επιδιώκει την μετάβαση από έναν τρόπο που κατευθύνεται από τη δίωξη της αστυνόμευσης σε μία μορφή πρόληψης του εγκλήματος (Innesetal., 2005; Innes&Sheptycki, 2004). Αυτό συνεπάγεται μια μετατόπιση από την απάντηση σε μεμονωμένα περιστατικά και απειλές σε έναν προσανατολισμό στο μέλλον με στρατηγικό χαρακτήρα (Ratcliffe, 2016). Η ILP επιδιώκει να το επιτύχει αυτό, τοποθετώντας αυτό που συχνά αναφέρεται ως πληροφόρηση για τα εγκλήματα στην πρώτη γραμμή των αποφάσεων σχετικά με την πρόληψη και τον έλεγχο του εγκλήματος (Guidette&Martinelli, 2009; Ratcliffe, 2016). Σύμφωνα με αυτό το μοντέλο, η εγκληματική πληροφόρηση θα πρέπει να καθοδηγεί τις επιχειρήσεις και όχι οι επιχειρήσεις να υπαγορεύουν την συγκέντρωση πληροφοριών (Ratcliffe, 2016).

Η ILP υιοθετήθηκε ευρέως σε ολόκληρο το Ηνωμένο Βασίλειο μετά την έγκριση του Εθνικού Μοντέλου Πληροφοριών (NIM) από την Ένωση Αστυνομικών Αρχηγών του Ηνωμένου Βασιλείου το 2000. Το NIM, εν συντομία, είναι ένα επιχειρησιακό μοντέλο που ακολουθεί μια καθοδηγούμενη από την πληροφόρηση προσέγγιση για την αστυνόμευση (Belur&Johnson, 2016). Το 2004, η κυβέρνηση του Ηνωμένου Βασιλείου νομοθέτησε ότι όλες οι αστυνομικές αρχές

στην Αγγλία και την Ουαλία έπρεπε να έχουν εφαρμόσει πλήρως το ΝΙΜμέχρι το επόμενο έτος. Από τότε, η ILP έχει υιοθετηθεί ευρέως σε πολλές χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας (Ratcliffe, 2016).

Η εγκληματική πληροφόρηση ή η διαδικασία πληροφόρησης, ευρύτερα, είναι συχνά αντιληπτή ως προς τα ιδανικά μοντέλα. Το πιο γνωστό από αυτά τα μοντέλα είναι ο κύκλος πληροφόρησης. Υπάρχουν πολλές εκδοχές του κύκλου πληροφόρησης. Ωστόσο, ακολουθούν γενικά τα ίδια έξι στάδια: σχεδιασμός, συλλογή, αξιολόγηση, ανάλυση, διάδοση και ανατροφοδότηση (Gill&Phythian, 2013). Η πιο συνηθισμένη κριτική του κύκλου πληροφόρησης είναι ότι η πρακτική του είναι πολύ πιο ρευστή από ό, τι απεικονίζεται στο μοντέλο. Μια άλλη κριτική είναι το πώς βλέπει την πληροφόρηση μεμονωμένα, χωρίς να λαμβάνει υπόψη το ευρύτερο περιβάλλον επιβολής του νόμου στο οποίο βρίσκεται, συμπεριλαμβανομένης της αποτυχίας να διασαφηνιστεί πώς συνδέεται η ανάλυση πληροφοριών με τη λήψη αποφάσεων. Αντίθετα, το μοντέλο 3-1 του Ratcliffe (2016) επιδιώκει να απεικονίσει με σαφήνεια τον ρόλο της πληροφόρησης στην αστυνόμευση. Το μοντέλο 3-1 δεν αποτελεί απαραίτητα μια αναπαράσταση του τρόπου λειτουργίας της πληροφόρησης στο πλαίσιο της επιβολής του νόμου, αλλά μια απεικόνιση του τρόπου λειτουργίας των οργανισμών επιβολής του νόμου εάν πρόκειται να είναι πραγματικά οι επικεφαλής των πληροφοριών. Το μοντέλο 3-1 αποτελείται από τρία στοιχεία (ανάλυση πληροφοριών εγκληματικότητας, υπεύθυνοι λήψης αποφάσεων και εγκληματικό περιβάλλον) και τρεις διαδικασίες που συνδέουν αυτά τα στοιχεία (ερμηνεία, επιρροή και αντίκτυπος), δημιουργώντας ένα τρίγωνο. Υπάρχουν δύο κύριες διαφορές μεταξύ του κύκλου πληροφόρησης και του μοντέλου 3-1. Η πρώτη είναι η

σημασία που δίνεται στους αναλυτές πληροφοριών για εγκλήματα που επηρεάζουν τους υπεύθυνους λήψης αποφάσεων. Η δεύτερη, με τη σειρά της, αφορά τους υπεύθυνους λήψης αποφάσεων προκειμένου να εφαρμόσουν πραγματικά διάφορες παρεμβάσεις που έχουν αντίκτυπο στο έγκλημα. Αυτό είναι ίσως το πιο αμφιλεγόμενο συστατικό αυτού του μοντέλου και είναι μια βασική διαφορά από άλλα μοντέλα που συχνά βλέπουν τη δημιουργία ενός προϊόντος πληροφόρησης και τη διάδοσή του ως το τέλος αυτής της διαδικασίας (Coyne&Bell, 2011; Ratcliffe, 2016).

Μετά την υιοθέτηση της ILP, τουλάχιστον κατ' αρχήν, από πολλές υπηρεσίες επιβολής του νόμου στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000, αρκετές μελέτες έχουν εξετάσει τη χρήση της ανάλυσης πληροφοριών κατά την αστυνόμευση (Cope, 2004; Darroch&Mazerolle, 2013; Ratcliffe, 2005; Sandersetal., 2015). Για παράδειγμα, ο Cope (2004) πραγματοποίησε συνολικά 38 συνεντεύξεις με αναλυτές πληροφοριών, ερευνητικούς υπαλλήλους, χειριστές πληροφοριοδοτών και διευθυντές πληροφοριών από τις αστυνομικές δυνάμεις στο Ηνωμένο Βασίλειο. Ενώ ήταν σαφές ότι η ανάλυση ως εργαλείο καθοδήγησης της αστυνομικής δραστηριότητας ήταν γενικά αποδεκτή, η κακή κατανόηση του τι είναι η ανάλυση πληροφοριών μεταξύ των αστυνομικών και η περιορισμένη κατανόηση της αστυνόμευσης μεταξύ των αναλυτών είχε αρνητικό αντίκτυπο στη χρησιμότητα των προϊόντων πληροφοριών. Ο Cope (2004) κατέληξε στο συμπέρασμα ότι υπάρχει ένα χάσμα μεταξύ της θεωρίας και της πρακτικής της αστυνόμευσης με γνώμονα την πληροφόρηση και του ρόλου της ανάλυσης. Σε μια παρόμοια μελέτη, ο Ratcliffe (2005) πήρε συνέντευξη από 50 υπεύθυνους λήψης αποφάσεων και προσωπικό πληροφοριών από την Αστυνομία της Νέας Ζηλανδίας,



διαπιστώνοντας ότι υπήρχε αντιληπτή έλλειψη κατανόησης της ILP στα ανώτερα επίπεδα του οργανισμού. Εκφράστηκαν επίσης ανησυχίες σχετικά με την καταλληλότητα της κατάρτισης που λαμβάνει το προσωπικό πληροφοριών και την ποιότητα και τη διαθεσιμότητα των δεδομένων, τα οποία μπορούν να επηρεάσουν σημαντικά την πρακτική της ILP.

Ορισμένες μελέτες έχουν επίσης επισημάνει τις πολυάριθμες προκλήσεις στην εφαρμογή της ILP (Darroch&Mazerolle, 2013; Fyfeetal., 2017; Sandersetal., 2015; Sheptycki, 2004). Ο Sheptycki (2004) εντόπισε 11 οργανωτικές παθολογίες που επηρέαζαν τα συστήματα πληροφοριών των υπηρεσιών επιβολής του νόμου, συμπεριλαμβανομένης της έλλειψης διαλειτουργικότητας, της μη αναφοράς και μη καταγραφής σχετικών πληροφοριών, της υπερφόρτωσης πληροφοριών και της επανάληψης. Σε μια πιο πρόσφατη μελέτη, οι Darroch&Mazerolle (2013) διεξήγαγαν μια έρευνα σε 286 αξιωματικούς και διεξήγαγαν 32 συνεντεύξεις με τα μέλη της Αστυνομίας της Νέας Ζηλανδίας για να προσδιορίσουν τους οργανωτικούς παράγοντες, συμπεριλαμβανομένων των αλλαγών στην πολιτική, τη διαδικασία, την εκπαίδευση και την ηγεσία, που επηρεάζουν την υιοθέτηση της ILP. Οι Darroch&Mazerolle(2013) πρότειναν ότι η ηγεσία είναι ιδιαίτερα κρίσιμη για την υιοθέτηση της ILP, σημειώνοντας ότι όπου η ηγεσία ήταν ανεπαρκής στη δομή της διοίκησης, η ILP αντιμετώπιζε προβλήματα.

Αυτό υποστηρίζεται και από μια λεπτομερή εξέταση της εφαρμογής του NIM στο Ηνωμένο Βασίλειο, όπου διαπιστώθηκε ότι η αντίθεση από τους ανώτερους διοικητές συνέβαλε σημαντικά στην συνολική αποτυχία του NIM και δεν μπορούσε να έχει ουσιαστικό αντίκτυπο στην επιχειρησιακή πρακτική (James, 2014). Στον Καναδά,

οι Sandersetal. (2015) πραγματοποίησαν 86 σε βάθος συνεντεύξεις και παρατηρήσεις συμμετεχόντων σε έξι διαφορετικές αστυνομικές υπηρεσίες, αναδεικνύοντας ότι αυτές οι υπηρεσίες είχαν υιοθετήσει ρητορικά την ILP αλλά την είχαν μεταφράσει ως μία μορφή λογοδοσία σε μια εποχή λιτότητας» Όπως οι Sandersetal. (2015) εξήγησαν, οι αναλυτές ένιωθαν την υποχρέωση να παρέχουν δεδομένα τόσο για να δικαιολογήσουν τους τρέχοντες ανθρώπινους όσο και τους χρηματοοικονομικούς πόρους, καθώς και να επεξηγήσουν την ανάγκη για πρόσθετες επενδύσεις. Με άλλα λόγια, δεν εφαρμόστηκε στην πραγματικότητα η ILP, αλλά μεταφράστηκε σε εργαλείο λογοδοσίας για να δικαιολογήσουν τις δαπάνες τους. Τέλος, προτάθηκε από τους Fyfeetal. (2017) ότι η εφαρμογή της ILP θα αμφισβητήσει την ιεραρχική δομή διοίκησης στις περισσότερες υπηρεσίες επιβολής του νόμου, λόγω της ώθησης η λήψη αποφάσεων να ενημερώνεται από τις πληροφορίες για το έγκλημα. Ως εκ τούτου, για τους Fyfeetal. (2017), η αλλαγή νοοτροπίας μεταξύ των αστυνομικών στελεχών είναι απαραίτητη για την επιτυχία της ILP.

Ενώ είναι σαφές ότι η ILP έχει υιοθετηθεί ευρέως στη θεωρία, το υπάρχον σώμα της βιβλιογραφίας δείχνει ότι η εφαρμογή της στην πράξη δεν είναι καθόλου απλή. Κάθε εμπειρική μελέτη υπογραμμίζει νέες προκλήσεις που φαινομενικά περιορίζουν το βαθμό στον οποίο οι αστυνομικές υπηρεσίες ακολουθούν στην πραγματικότητα τις αρχές της ILP. Είναι, επιπλέον, επίσης προφανές ότι η εμπειρική έρευνα για την ILP δεν συμβαδίζει με τις εξελίξεις στην πολιτική και την πρακτική. Για παράδειγμα, ο Carter (2016) παρατήρησε ότι η ILP έχει ακόμη λάβει σχετικά μικρό βαθμό επιστημονικής προσοχής σε σύγκριση με άλλα μοντέλα αστυνόμευσης, όπως η αστυνόμευση με γνώμονα την κοινότητα.

Επιπλέον, οι Lewandowski et al. (2018) πρότειναν ότι οι διαφοροποιήσεις εντός των υπηρεσιών επιβολής του νόμου (π.χ. πολιτισμικές διαφορές) είναι κρίσιμες για την κατανόηση της πληροφόρησης και απαιτούν περαιτέρω μελέτη σε μια ποικιλία πλαισίων. Χωρίς συνεχή εξέταση, ο κίνδυνος, σύμφωνα με τον Ratcliffe (2016), είναι ότι είναι εύκολο να ασκείται η αστυνόμευση υπό την καθοδήγηση των πληροφοριών και να χαθεί λόγω των αποτυχημένων προσπαθειών της επιβολής του νόμου να απομακρυνθεί από την παραδοσιακή εστίαση στην αντιδραστική, διερευνητική αστυνόμευση.

Η πρόσβαση σε ακριβή δεδομένα είναι ένα σιωπηρό πρώτο στάδιο της διαδικασίας ανάλυσης πληροφοριών (Chan & Bennett-Moses, 2017). Ωστόσο, σύμφωνα με την προηγούμενη έρευνα (Ratcliffe, 2005; Sheptycki, 2004), οι αναλυτές τους εντόπισαν ορισμένα ζητήματα με τα δεδομένα τους, συμπεριλαμβανομένης της ατελούς εκτέλεσης (π.χ. ελλιπή δεδομένα) και της ανακρίβειας (π.χ. πληροφορίες που εισήχθησαν λανθασμένα στις εσωτερικές τους βάσεις δεδομένων για εγκλήματα). Αρκετοί αναλυτές υποστήριξαν ότι θα δουλέψουν αναπόφευκτα με ελλιπή δεδομένα. Ένας από τους βασικούς αντίκτυπους των ελλιπών δεδομένων, είναι ότι υπάρχουν στιγμές που οι αναλυτές δεν διαθέτουν επαρκείς πληροφορίες για να βασίσουν τις αξιολογήσεις τους. Υπάρχουν περιπτώσεις όπου πραγματικά δεν έχουν πολλά για να στηρίξουν τις αξιολογήσεις. Χρησιμοποιώντας μόνο ένα σύστημα που θα δείξει μόνο άτομα που τους βλέπουν μαζί ταυτόχρονα ή να μιλούν, κάποιοι αστυνομικοί θα πιστέψουν ότι ήταν συνδεδεμένα με κάποιο τρόπο. Μερικές φορές οι πληροφορίες που έχουν οι αναλυτές να αξιολογήσουν δεν είναι εξαιρετικές. Απλά κοιτάζοντας τι έχουν, τις πληροφορίες που έχουν, δεν είναι πραγματικά ένας

ακριβής τρόπος για τη διεξαγωγή της ανάλυσης τους. Στηριζόμενοι στις δικές τους εσωτερικές βάσεις δεδομένων για εγκλήματα, είναι πιθανό να έχουν μια πολύ ελλιπή εικόνα του ατόμου, της ομάδας ή του τύπου εγκλήματος που ερευνούν και αυτό εισάγει πιθανές ανησυχίες σχετικά με την ακρίβεια των αξιολογήσεων των πληροφοριών. Ωστόσο, η απόκτηση πρόσβασης σε περαιτέρω πληροφορίες παρεμποδίζεται επίσης από την περιορισμένη ανταλλαγή πληροφοριών τόσο μεταξύ όσο και εντός των οργανισμών και υπηρεσιών. Η ανταλλαγή πληροφοριών ιδίως μεταξύ διαφορετικών κυβερνητικών φορέων πρέπει να αλλάξει. Υπάρχουν πολλοί νόμιμοι λόγοι για την απόκρυψη πληροφοριών ως ουσιαστικό μέσο προστασίας. Ωστόσο, έχει επίσης σημειωθεί ότι τέτοιες περιπτώσεις είναι αποτέλεσμα πολλών παραγόντων, όπως η υπερβολική εξάρτηση από περιορισμούς ασφαλείας, τα θέματα τεχνολογικής διαλειτουργικότητας και ο ανταγωνισμός / αντιπαλότητα μεταξύ διαφόρων υπηρεσιών (Carter&Carter, 2009; Sanders&Henderson, 2013). Ενώ η έρευνα έχει επίσης επισημάνει τη σημασία της ενδο-οργανωτικής ανταλλαγής πληροφοριών και γνώσεων, συμπεριλαμβανομένων μεταξύ διαφορετικών μονάδων, όπως των εξειδικευμένων ομάδων (Giacomantonio, 2014), τα εσωτερικά δίκτυα έχουν ερευνηθεί πολύ λιγότερο από τα δίκτυα αλληλεπιδράσεων (Whelan&Duront, 2017). Διαφαίνεται όμως ότι η ανταλλαγή πληροφοριών είναι εξίσου προβληματική εντός των εσωτερικών τους ορίων, όπως και μεταξύ των οργανισμών και των υπηρεσιών.

Είναι σαφές ότι η έλλειψη ανταλλαγής πληροφοριών, τόσο εσωτερικά όσο και εξωτερικά, έρχεται σε αντίθεση με τις αρχές της ILP, η οποία στον πυρήνα της θεωρείται ως εργαλείο ανταλλαγής πληροφοριών (Carter&Carter, 2009). Ακόμη και αν οι αστυνομικές

υπηρεσίες επιδιώκουν να είναι πραγματικά επικεφαλής των πληροφοριών, βασίζονται στην αμοιβαιότητα των εταίρων τους και στη συνεργασία μεταξύ των εσωτερικών μονάδων εργασίας. Μια αστυνομική υπηρεσία μπορεί από μόνη της να έχει υιοθετήσει τις αρχές της ILP, αλλά μπορεί να μην έχει πραγματική καθοδήγηση από τις πληροφορίες εάν οι άλλες υπηρεσίες δεν υιοθετούν παρόμοια προσέγγιση.

Ένα άλλο ζήτημα είναι η υπερφόρτωση δεδομένων ή πληροφοριών. Αν και υπάρχει συνήθως η επιθυμία να υπάρχει πρόσβαση σε περισσότερες πληροφορίες, αυτό μπορεί επίσης να δημιουργήσει μεγάλη απόσπαση της προσοχής. Η υπερφόρτωση δεδομένων έχει αναγνωριστεί εδώ και πολύ καιρό ως πρόβλημα στο πλαίσιο της επιβολής του νόμου (Haucketal., 2002; Sheptycki, 2004; Whelan, 2017). Το πρόβλημα της υπερφόρτωσης δεδομένων έχει επιδεινωθεί από την αύξηση του όγκου και της ακρίβειας των πληροφοριών που συλλέγει πλέον η αστυνομία (James, 2014; Sanders&Sheptycki, 2017), η οποία περιλαμβάνει e-mail, γραπτά μηνύματα, σκληρούς δίσκους υπολογιστών και ανταλλαγή άμεσων μηνυμάτων (Decary-Hetu&Dupont, 2012). Οι νέες πηγές πληροφοριών απεικονίζονται ίσως καλύτερα από την άνοδο των κοινωνικών μέσων (π.χ. Facebook), ενώ πολλές υπηρεσίες επιβολής του νόμου χρησιμοποιούν τα κοινωνικά μέσα ως πηγή πληροφοριών κατά τη διάρκεια ερευνών. Ένας από τους πρώτους ελέγχους που γίνεται πλέον είναι αυτός του Facebook αλλά υπάρχουν ανησυχίες σχετικά με την αξιοπιστία των κοινωνικών μέσων ως πηγή πληροφοριών.

Σύμφωνα με το μοντέλο 3-I του Ratcliffe (2016), υπάρχουν πολλοί πιθανοί πελάτες που πρέπει να λάβουν υπόψη οι αναλυτές

των πληροφοριών όταν προσπαθούν να επηρεάσουν τους υπεύθυνους λήψης αποφάσεων, συμπεριλαμβανομένων των αξιωματικών της πρώτης γραμμής, η αστυνομία, οι ρυθμιστικές υπηρεσίες, το ευρύ κοινό και τα δίκτυα ασφαλείας. Έχει προταθεί ότι οι θετικές εργασιακές σχέσεις - δηλαδή αυτές που χαρακτηρίζονται από χαρακτηριστικά όπως ο αμοιβαίος σεβασμός και η αμοιβαιότητα - οδηγούν σε βελτιωμένη ανταλλαγή πληροφοριών και αυξημένα επίπεδα εμπιστοσύνης (Schafer, 2010). Οι εργασιακές σχέσεις των αναλυτών με τους διευθυντές και τους αστυνομικούς είναι ζωτικής σημασίας για την επίτευξη των στόχων τους. Εντούτοις, η σχέση εργασίας τους με τους διευθυντές της πληροφόρησης δεν είναι πάντα ιδανική. Αυτή η ένταση οφείλεται εν μέρει στους ανώτερους διευθυντές που δεν κατανοούν πλήρως τι είναι η πληροφόρηση και πώς παράγεται, παρά το γεγονός ότι ως πολύτιμος πόρος ενημερώνει την λήψη αποφάσεών τους. Η έρευνα υποδηλώνει ότι οι ανώτεροι διευθυντές δεν ήταν προετοιμασμένοι για τη μετάβαση προς την ILP, όπου η πληροφόρηση θα πρέπει να οδηγήσει στη λήψη αποφάσεων (Phillips, 2012; Ratcliffe, 2016; Sanders et al., 2015). Για παράδειγμα, ο Ratcliffe (2016) προτείνει ότι απλά δεν έχουν προετοιμάσει τα επίπεδα διοίκησης της αστυνόμευσης για το νέο ρόλο που τους ζητείται να εκτελέσουν. Αυτό έχει αναγνωριστεί ως ζήτημα στην επιβολή του νόμου για κάποιο χρονικό διάστημα (Core, 2004; Ratcliffe, 2005) και παρά την πάροδο του χρόνου λίγα έχουν αλλάξει. Η λύση σε αυτό το ζήτημα είναι μεγαλύτερη εκπαίδευση και ευαισθητοποίηση σχετικά με την πληροφόρηση τόσο ως διαδικασία όσο και ως προϊόν.

Σημαντική είναι επίσης η σχέση των αναλυτών με τους αστυνομικούς. Αυτοί είναι συνήθως υπεύθυνοι των ερευνών. Με την έννοια της καθοδήγησης ή της κατεύθυνσης της πορείας της

έρευνας, ο υπεύθυνος της έρευνας είναι ο αστυνομικός. Συνεπώς η σχέση εργασίας τους με τους αστυνομικούς είναι κρίσιμη για την ανάληψη του ρόλου τους. Κατά τη διάρκεια ορισμένων ερευνών οι εργασιακές τους σχέσεις με τους αστυνομικούς θα είναι θετικές και, στη συνέχεια, θα οδηγήσουν σε περισσότερες πληροφορίες. Σε αυτήν την περίπτωση, οι αναλυτές θεωρούν τις σχέσεις τους με τους αστυνομικούς ως θετικές όταν συμπεριλαμβάνονται ουσιαστικά στη διερευνητική διαδικασία. Σε περιπτώσεις όπου οι αναλυτές αισθάνονται ότι έχουν θετική σχέση εργασίας με τους αστυνομικούς, φαίνεται ότι αισθάνονται επιβεβαιωμένοι στο ρόλο τους. OSheptycki (2017) αναφέρεται σε αυτό ως αστυνομικό διαχωρισμό εργασίας που αποτελεί την ροή πληροφοριών εντός του οργανισμού που οριοθετείται στην αρχέτυπη μορφή της πολυλειτουργικής αστυνομικής υπηρεσίας.

Υπάρχουν επίσης περιπτώσεις όπου η σχέση εργασίας με τους αστυνομικούς θα μπορούσε να χαρακτηριστεί ως αρνητική είτε ως προς την υποτίμηση τους ή την πλήρη εξαίρεσή τους. Υπάρχουν διαφορετικές απόψεις ως προς το τι συμβάλλει σε τέτοιες αρνητικές εργασιακές σχέσεις. Αυτό μπορεί να είναι κληρονομιά των παραδοσιακών πρακτικών αστυνόμευσης, όπου οι αναλυτές πληροφοριών δεν είχαν κανέναν ρόλο στη διαδικασία έρευνας. Άτομα που έχουν πιο παραδοσιακά αστυνομικά υπόβαθρα μπορεί να μην έχουν απαραίτητα τόσο στενή σχέση με την ομάδα πληροφοριών. Επίσης, μπορεί εν μέρει να είναι αποτέλεσμα μιας πρώην πρακτικής τοποθέτησης αξιωματικών που θα συνταξιοδοτηθούν σύντομα σε θέσεις πληροφοριών προκειμένου οι υπηρεσίες να απαλλαγούν από αυτούς. Είναι καλά τεκμηριωμένο ότι η ανάλυση πληροφοριών έχει περιθωριοποιηθεί ιστορικά από αξιωματικούς, αστυνομικούς και ανώτερα στελέχη (Core, 2004;

O'Shea&Nicholls, 2002; Sandersetal., 2015; Tayloretal., 2007), υποδηλώνοντας ότι η τοποθέτηση μη ενδιαφερόμενων αξιωματικών σε θέσεις πληροφοριών υπονομεύει την αξία της ανάλυσης πληροφοριών. Ωστόσο, ένας από τους βασικούς παράγοντες που συμβάλλουν στις κακές εργασιακές σχέσεις μεταξύ ορισμένων αναλυτών και αστυνομικών είναι ότι πολλοί δεν καταλαβαίνουν πλήρως τι είναι η πληροφόρηση και, συγκεκριμένα, τι μπορούν πραγματικά να κάνουν οι αναλυτές για αυτούς.

Φαίνεται να υπάρχει συναίνεση ότι τόσο οι αστυνομικοί όσο και οι διευθυντές δεν καταλαβαίνουν πλήρως τι είναι η πληροφόρηση και πώς παράγεται παρά το ότι μπορεί να θεωρούν ότι είναι ένας πολύτιμος πόρος από τους διευθυντές για να υποστηρίξουν τη λήψη αποφάσεών τους. Ορισμένοι αστυνομικοί όμως δεν θεωρούν την πληροφόρηση πολύτιμο πόρο καθότι δεν είναι πάντα προσανατολισμένη στη δίωξη και ενδέχεται να μην πληροί τα αποδεικτικά πρότυπα. Φαίνεται να υπάρχει ένα συνεπές εύρημα στο οποίο οι κύριοι πελάτες των αναφορών πληροφοριών δεν φαίνεται να εκτιμούν σωστά την πληροφόρηση (Cope, 2004; Phillips, 2012; Ratcliffe, 2005; Sandersetal., 2015). Ωστόσο, δεν υπάρχει αναφορά στην υπάρχουσα βιβλιογραφία, ότι αυτή η έλλειψη γνώσης της πληροφόρησης είναι το πιο σημαντικό θέμα. Ένα επίσης σημαντικό ζήτημα προκύπτει από τον εξαιρετικά διαφορετικό χαρακτήρα των αστυνομικών οργανισμών και υπηρεσιών. Ορισμένες υπηρεσίες επιβολής του νόμου οδηγούν περισσότερο στις πληροφορίες από άλλες. Αυτό υποδηλώνει ότι χρειάζεται πολύ μεγαλύτερη κατανόηση του τρόπου με τον οποίο οι υπηρεσίες επιβολής του νόμου είναι δομημένες και λειτουργούν εσωτερικά για να εκτιμήσουν πραγματικά τον τρόπο με τον οποίο ασκείται ηILP.



Η ILP υπήρχε στη θεωρία πριν από την εισαγωγή του NIM. Ωστόσο, η έρευνα συνέχισε να καταδεικνύει τις πολλές προκλήσεις που εμπλέκονται στην εφαρμογή της ILP στην πράξη, υποδηλώνοντας ότι εξακολουθεί να είναι πιο ρητορική από την πραγματικότητα στις αστυνομικές υπηρεσίες. Έχουν προταθεί πολλές εξηγήσεις σχετικά με την τρέχουσα κατάσταση της ILP, συμπεριλαμβανομένης της κακής κατανόησης του τι είναι η ανάλυση πληροφοριών μεταξύ των αστυνομικών (Core, 2004), διάφορες οργανωτικές παθολογίες (Sheptycki, 2004) και έλλειψη υποστήριξης της ηγεσίας (Darroch&Mazerolle , 2013; James, 2013). Η έρευνα αμφισβήτησε επίσης τον πιθανό αντίκτυπο της αστυνομικής κουλτούρας (Whelan, 2017) όσον αφορά την αντίσταση στην αλλαγή και, ως εκ τούτου, την απροθυμία απομάκρυνσης από αντιδραστικούς ή διαισθητικούς τρόπους αστυνόμευσης (Belur&Johnson, 2018).

Οι προκλήσεις που υπάρχουν έχουν αναγνωριστεί ευρέως στη βιβλιογραφία. Όπως σημειώνει Olnnes (2006), για παράδειγμα, η ανάλυση πληροφοριών είναι ένα πεδίο που αντιμετωπίζει αβεβαιότητα, πράγμα που σημαίνει ότι πολλές από τις ανησυχίες σχετικά με την ακρίβεια των δεδομένων δεν μπορούν να αντιμετωπιστούν πλήρως. Ωστόσο, φαίνεται ότι πολλά από τα ζητήματα που εγείρονται από τους αναλυτές σχετίζονται εν μέρει με τα πρότυπα και τις πρακτικές των δεδομένων εντός των αστυνομικών οργανώσεων, υποδηλώνοντας ότι τουλάχιστον ορισμένα από αυτά τα ζητήματα θα μπορούσαν να ξεπεραστούν με περισσότερη αυστηρότητα και έλεγχο όσον αφορά τον τρόπο λήψης και καταγραφής δεδομένων από την αστυνομία στα συστήματα πληροφοριών (Sheptycki, 2004). Όσον αφορά την κοινή χρήση δεδομένων, οι αναλυτές αναφέρονται τόσο στα συστήματα που διαθέτουν όσο και στην ικανότητά τους να ανταλλάσσουν

πληροφορίες - συμπεριλαμβανομένων των ζητημάτων διαλειτουργικότητας - και των κανόνων που περιορίζουν τον τρόπο ανταλλαγής πληροφοριών. Συγκεκριμένα, οι αναλυτές αναφέρονται στην αντιληπτή έλλειψη κοινής χρήσης μεταξύ ορισμένων οργανωτικών μονάδων (Giacomantonio, 2014), η οποία ενισχύει την ανάγκη να εκτιμηθεί καλύτερα το εσωτερικό τμήμα της αστυνομικής εργασίας (Sheptycki, 2017). Δηλαδή, ενώ πολλοί έχουν επισημάνει ζητήματα σχετικά με τη δια-οργανωτική ανταλλαγή πληροφοριών (Whelan&Dupont, 2017), δεν η ανταλλαγή πληροφοριών δεν γίνεται ελεύθερα μέσα στους οργανισμούς και στις υπηρεσίες (Tsai, 2002).

Μια άλλη ενδιαφέρουσα παρατήρηση είναι ότι, σύμφωνα με τους αναλυτές, η υπερφόρτωση των πληροφοριών γίνεται όλο και μεγαλύτερο πρόβλημα που συνάδει με την πρόοδο της τεχνολογίας, η οποία όμως δεν μπορεί να προσφέρει λύση σε αυτό το ζήτημα. Ένα θέμα που προκύπτει στην έρευνα για την άνοδο των λεγόμενων μεγάλων δεδομένων (Chan&BennettMoses, 2017; Cukier&Mayer-Schownberger, 2014; Sanders&Sheptycki, 2017), δείχνει ότι η τεράστια αύξηση του όγκου των δεδομένων ξεπερνά την ικανότητα των αναλυτών και των οργανισμών και των υπηρεσιών να επεξεργάζονται και να αναλύουν ουσιαστικά. Αυτό που είναι σαφές, ωστόσο, είναι ότι περαιτέρω προσπάθειες πρέπει να κατευθυνθούν προς τις οργανωτικές και τεχνολογικές βελτιώσεις στον ενδο- και δια-οργανωτικό συντονισμό των αστυνομικών πληροφοριών.

Η έρευνα σε βάσεις δεδομένων και συστήματα της αστυνομίας έχει εντοπίσει επανειλημμένα ζητήματα σχετικά με το σχεδιασμό και τη λειτουργικότητα τους (Sanders&Henderson, 2013). Αυτό οφείλεται σε μεγάλο βαθμό έλλειψη κατάρτισης των αναλυτών όσον αφορά τη χρήση των εργαλείων που διαθέτουν. Οι αναλυτές πραγματοποιούν

ένα αρχικό εκπαιδευτικό μάθημα όταν εντάσσονται για πρώτη φορά στην υπηρεσία (στην περίπτωση νέων μελών) ή όταν διορίζονται για πρώτη φορά ως αναλυτές (στην περίπτωση των υπαρχόντων μελών), αλλά στη συνέχεια έχουν περιορισμένες ευκαιρίες για συνεχή εκπαίδευση. Αυτή η έλλειψη συνεχιζόμενης εκπαίδευσης είναι ιδιαίτερα προβληματική καθώς τα εργαλεία αλλάζουν, συμπεριλαμβανομένων των ενημερώσεων σε υπάρχουσες εφαρμογές καθώς και την εισαγωγή εντελώς νέων συστημάτων. Η διαθεσιμότητα συνεχόμενης εκπαίδευσης για πολλά από αυτά τα εργαλεία χρειάζεται να βελτιωθεί. Η περισσότερη κατάρτιση θα παράγει καλύτερα αποτελέσματα από ότι αν υπάρχει περισσότερο προσωπικό, κάτι που υπογραμμίζει τη σημασία της εκπαίδευσης ως εμπόδιο στην ανάλυση πληροφοριών ως πρακτική. Όπως έχει καταλήξει παρόμοια πρόσφατη έρευνα (Belur& Johnson, 2018), η καλύτερη εκπαίδευση για τους αναλυτές και διευθυντές φαίνεται να είναι απαραίτητη για τους οργανισμούς προκειμένου να εφαρμόσουν πραγματικά την ILP.

Σημαντικό ρόλο επίσης στην αποτελεσματικότητα των αναλυτών διαδραματίζουν συγκεκριμένα χαρακτηριστικά συμπεριλαμβανομένης της ικανότητας παραγωγής μίας ανάλυσης, της συνολικής στάσης ενός αναλυτή (π.χ. τι μπορεί να κάνει) και μεμονωμένα χαρακτηριστικά (π.χ. εμπιστοσύνη). Όλα αυτά μπορούν να εμποδίσουν τη χρήση πληροφοριών στην επιβολή του νόμου (Evans&Kebbell, 2012).

Ο επηρεασμός των υπευθύνων λήψης αποφάσεων αποτελεί βασικό συστατικό της ILP. Η λήψη αποφάσεων αφορά τους διευθυντές πληροφοριών και τους ανώτερους υπαλλήλους της αστυνομίας και τους αστυνομικούς ή τους ανακριτές που εργάζονται

σε συγκεκριμένες περιπτώσεις. Αυτό που είναι σαφές και από τις δύο κατηγορίες είναι ότι υπάρχει μεγάλη ασυνέπεια στις υπηρεσίες επιβολής του νόμου όσον αφορά τη γνώση για την πληροφόρηση, συμπεριλαμβανομένου του πώς παράγεται και πώς μπορεί να ενημερώσει την λήψη αποφάσεων. Οι διευθυντές με μεγαλύτερη κατανόηση της πληροφόρησης έχουν πολύ περισσότερες πιθανότητες να εκτιμήσουν την αξία της και, ως εκ τούτου, να τη χρησιμοποιούν ως βάση για την λήψη αποφάσεων. Αντίθετα, οι υπεύθυνοι λήψης αποφάσεων με περιορισμένη κατανόηση της πληροφόρησης είναι πιο πιθανό, σκόπιμα ή ακούσια, να περιθωριοποιήσουν τους αναλυτές, συμπεριλαμβανομένης της κατανομής τους πολύ λιγότερο σημαντικών καθηκόντων. Αυτή η κατανόηση της πληροφόρησης εξαρτάται σε μεγάλο βαθμό από την εμπειρία του κάθε διευθυντή και αστυνομικού. Όσοι έχουν περάσει χρόνο σε πιο εξειδικευμένες μονάδες - συμπεριλαμβανομένων των ειδικών μονάδων πληροφοριών καθώς και μονάδων που ασχολούνται με το οργανωμένο έγκλημα και την αντιτρομοκρατία, για παράδειγμα - είναι πολύ πιο πιθανό να έχουν μεγαλύτερη κατανόηση της πληροφόρησης σε σύγκριση με εκείνους που έχουν περιοριστεί σε αστυνομικές επιχειρήσεις.

Επομένως, για να κατανοηθεί καλύτερα ο ρόλος της ILP, πρέπει να εκτιμηθεί καλύτερα ο τρόπος με τον οποίο ασκείται διαφορετικά εντός και μεταξύ των πολλών οργανωτικών μονάδων που περιλαμβάνουν οι αστυνομικές υπηρεσίες. Όπως επισημαίνει ο Sheptycki (2017), οι αντιλήψεις για το αστυνομικό επίπεδο και τα επίσημα και άτυπα όρια εντός των αστυνομικών υπηρεσιών διαμορφώνουν τη λειτουργία της πληροφόρησης με σημαντικούς τρόπους. Η συντριπτική πλειοψηφία της υπάρχουσας έρευνας για την ανάλυση του εγκλήματος ή την ILP έχει επικεντρωθεί σε

αστυνομικές υπηρεσίες στο σύνολό της. Αυτό οδηγεί στην απαίτηση μεγαλύτερης προσοχής στις ομοιότητες και τις διαφορές μεταξύ των αστυνομικών υπηρεσιών. Υπάρχει εξίσου μεγάλη ανάγκη να εξεταστούν οι αστυνομικές υπηρεσίες για να εκτιμηθούν οι ομοιότητες και οι διαφορές μεταξύ των οργανωτικών μονάδων και των τρόπων με τους οποίους διαμορφώνουν την πρακτική της ILP.

#### **1.4. Ιστορική αναδρομή**

Η ILP είναι ένα μοντέλο αστυνόμευσης που βασίζεται στην εκτίμηση και τη διαχείριση του κινδύνου. Οι αξιωματικοί των υπηρεσιών πληροφοριών χρησιμεύουν ως οδηγοί στις επιχειρήσεις, και δεν είναι οι επιχειρήσεις που καθοδηγούν τις πληροφορίες (DeLint, 2006).

Οι εκκλήσεις για αστυνόμευση με γνώμονα την πληροφόρηση προέρχονται από τη δεκαετία του 1990, τόσο στη Βρετανία όσο και στις Ηνωμένες Πολιτείες. Στις ΗΠΑ, το βιβλίο του Mark Riebling το 1994 «Ο μυστικός πόλεμος μεταξύ του FBI και της CIA» επισήμανε τη σύγκρουση μεταξύ της επιβολής του νόμου και των πληροφοριών και προέτρεψε τους αστυνομικούς να λειτουργήσουν περισσότερο σαν κατάσκοποι. Η ILP κατέκτησε σημαντική δυναμική παγκοσμίως μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου στις Ηνωμένες Πολιτείες. Πλέον υποστηρίζεται από τις κορυφαίες αστυνομικές υπηρεσίες στη Βόρεια Αμερική και το Ηνωμένο Βασίλειο (McGarrelletal., 2007).

Παρόλο που η ILP βασίζεται σε προηγούμενα παραδείγματα, όπως η αστυνόμευση της κοινότητας, η αστυνόμευση με προσανατολισμό στα προβλήματα και το μοντέλο συνεργασίας της

αστυνόμησης, προήλθε κυρίως από την απόρριψη της αντιδραστικής εστίασης στο έγκλημα της κοινοτικής αστυνόμησης, με εκκλήσεις η αστυνομία να αφιερώσει περισσότερο χρόνο χρησιμοποιώντας πληροφοριοδότες και επίβλεψη για την καταπολέμηση των παραβατών που υποτροπιάζαν (McGarrelletal., 2007). Στη συνέχεια, η ILP δέχτηκε μία επέκταση που επέτρεψε την ενσωμάτωση της αστυνόμησης της γειτονιάς (Haleetal., 2004; Maguire&John, 2006).

Πριν από την ILP, η στρατηγική ανταποκρίσεως ήταν η κύρια μέθοδος αστυνόμησης. Ωστόσο, καθώς το έγκλημα θεωρήθηκε ότι υπερέβαινε τους αστυνομικούς πόρους στο Ηνωμένο Βασίλειο, υπήρχε κενό ζήτησης και ανάγκη για μια νέα στρατηγική που θα χρησιμοποιούσε πιο αποτελεσματικά τους διαθέσιμους πόρους εκείνη τη στιγμή. Η πρώιμη ανάπτυξη της ILP έγινε στο Ηνωμένο Βασίλειο. Έγινε αντιληπτό ότι η αστυνομία ξόδευε πολύ χρόνο για να ανταποκριθεί σε συγκεκριμένα περιστατικά και δεν αντιμετώπιζε το πρόβλημα των επαναλαμβανόμενων παραβατών. Ως εκ τούτου, υποστηρίχθηκε η αυξημένη χρήση πληροφοριών, επιτήρησης και πληροφοριοδοτών για να στοχεύουν υποτροπιάζοντες παραβάτες, έτσι ώστε η αστυνομία να μπορεί να είναι πιο αποτελεσματική στην καταπολέμηση του εγκλήματος (Ratcliffe, 2016). Η ILP θεωρήθηκε ιδιαίτερα σημαντική με την άνοδο της τρομοκρατικής απειλής. Οι αλλαγές που υπήρξαν επηρέασαν την πληροφόρηση που συλλέγουν οι αστυνομικές υπηρεσίες (Ratcliffe, 2016; Ratcliffe&Taniguchi, 2008).

Καθώς η αστυνόμηση υπό την ηγεσία των πληροφοριών αποτελεί κίνηση προς την επιτήρηση, επικεντρώνεται στη συλλογή πληροφοριών και στην ανάλυση δεδομένων. Ωστόσο, ο τρόπος

συλλογής αυτών των δεδομένων αποτελεί ανησυχία για τους υπερασπιστές της ιδιωτικής ζωής. Το Ανώτατο Δικαστήριο των Ηνωμένων Πολιτειών δεν έχει λάβει συγκεκριμένες αποφάσεις σε σχέση με έρευνες που ασχολούνται ειδικά με την αστυνόμευση υπό την ηγεσία πληροφοριών. Το ζήτημα Που ανακύπτει είναι σε τι είδους προσδοκία απορρήτου ένα άτομο μπορεί να ελπίζει να έχει με την τεχνολογία. Η τεχνολογία έχει δώσει στους αστυνομικούς πρόσβαση σε πληροφορίες που δεν ήταν εφικτές στο παρελθόν. Τέλος, η αστυνόμευση υπό την ηγεσία των πληροφοριών έχει περιγραφεί ως μέρος μιας μεγαλύτερης τάσης θόλωσης της διάκρισης μεταξύ εθνικής ασφάλειας και εγχώριας αστυνόμευσης, διακινδυνεύοντας τους ίδιους κινδύνους που έχουν αμαυρώσει την αστυνόμευση στο παρελθόν, όπως πολιτική παρέμβαση, παραβίαση πολιτικών ελευθεριών και μεγαλύτερη πιθανότητα κατάχρησης της αστυνομικής εξουσίας με την αυξημένη μυστικότητα που συνεπάγεται η συλλογή πληροφοριών (Brodeur&Dupont, 2006; Pickering, 2004).

## **Κεφάλαιο 2. Τεχνητή νοημοσύνη**

### **2.1. Ζητήματα διακρίσεων και δημοκρατίας**

Είναι ένα αξιοσημείωτο γεγονός ότι οι ταχείες εξελίξεις στην τεχνητή νοημοσύνη και στις τεχνολογίες που βασίζονται σε δεδομένα τις τελευταίες δεκαετίες έχουν θέσει τη σύγχρονη κοινωνία σε ένα καθοριστικό σημείο για τις αποφάσεις που αφορούν το μέλλον της. Από την μία πλευρά, η άνθηση της κοινωνικά ευεργετικής καινοτομίας της τεχνητής νοημοσύνης υπόσχεται, μεταξύ άλλων, να συμβάλλει σε σημαντικές εξελίξεις για την ανθρωπότητα όπως την αντιμετώπιση της αλλαγής του κλίματος και την απώλεια της βιοποικιλότητας, της βελτίωσης της ιατρικής περίθαλψης, του

βιοτικού επιπέδου, των μεταφορών και της γεωργικής παραγωγής καθώς επίσης και την αντιμετώπιση πολλών από τις κοινωνικές αδικίες και τις υλικές ανισότητες που πλήττουν τον σημερινό κόσμο. Από την άλλη πλευρά, ο πολλαπλασιασμός των ανεύθυνων καινοτομιών της τεχνητής νοημοσύνης αποκαλύπτει προειδοποιητικά σημάδια για τα πιθανά προβλήματα που ενδέχεται να προκύψουν, εάν η πρόοδος αυτών των τεχνολογιών συνεχίσει. Τέτοιου είδους προειδοποιητικά σημάδια εντοπίζονται για παράδειγμα, στους αυξανόμενους κινδύνους για τα δικαιώματα στην ιδιωτική ζωή, την αυτο-έκφραση, τη σύνδεση και τη συγκατάθεση, καθώς και σε άλλες πολιτικές ελευθερίες και κοινωνικές ελευθερίες.

Η χρήση αλγοριθμικής λήψης αποφάσεων έχει γίνει κοινή πρακτική σε ένα ευρύ φάσμα τομέων. Χρησιμοποιούνται αλγοριθμικά συστήματα για το φιλτράρισμα ανεπιθύμητων μηνυμάτων, το σχεδιασμό της κυκλοφορίας, τη διαχείριση logistics, τη διάγνωση ασθενειών, την αναγνώριση ομιλίας και πολλά άλλα. Αν και η αλγοριθμική λήψη αποφάσεων μπορεί να φαίνεται λογική, ουδέτερη και αμερόληπτη, μπορεί επίσης να οδηγήσει σε άδικες και παράνομες διακρίσεις.

Παρόλο που δεν υπάρχει συναίνεση για τον ορισμό της αλγοριθμικής λήψης αποφάσεων και της τεχνητής νοημοσύνης, ορισμένες περιγραφές μπορεί να είναι χρήσιμες. Ένας αλγόριθμος είναι μια αφηρημένη, τυποποιημένη περιγραφή μιας υπολογιστικής διαδικασίας. Χαπόφαση αναφέρεται στην έξοδο αυτής της διαδικασίας. Σε γενικές γραμμές, ένας αλγόριθμος μπορεί να θεωρηθεί ως ένα πρόγραμμα υπολογιστή. Η αλγοριθμική λήψη αποφάσεων αναφέρεται έτσι στη διαδικασία με την οποία ένας αλγόριθμος παράγει αποτέλεσμα (Dourish, 2016).



Μερικές φορές, ένας αλγόριθμος αποφασίζει με έναν πλήρως αυτοματοποιημένο τρόπο. Για παράδειγμα, ένα φίλτρο ανεπιθύμητης αλληλογραφίας μπορεί να φιλτράρει αυτόματα τα ανεπιθύμητα μηνύματα από τον λογαριασμό ηλεκτρονικού ταχυδρομείου κάποιου. Μερικές φορές, οι αποφάσεις είναι μερικώς αυτοματοποιημένες: οι άνθρωποι λαμβάνουν αποφάσεις υποβοηθούμενοι από αλγόριθμους. Για παράδειγμα, ένας υπάλληλος τράπεζας μπορεί να αποφασίσει εάν ένας πελάτης μπορεί να δανειστεί χρήματα από την τράπεζα, αφού ένα αλγοριθμικό σύστημα αξιολόγησε την πιστοληπτική ικανότητα του. Ωστόσο, όταν συζητάμε για διακρίσεις, πολλοί κίνδυνοι είναι παρόμοιοι για τις πλήρως και εν μέρει αυτοματοποιημένες αποφάσεις. Οι άνθρωποι ενδέχεται να ακολουθούν συστάσεις από υπολογιστές, επειδή αυτές οι προτάσεις φαίνονται λογικές ή αλάνθαστες, ή επειδή οι άνθρωποι προσπαθούν να ελαχιστοποιήσουν τη δική τους ευθύνη (Zarsky, 2017).

Η τεχνητή νοημοσύνη (TN) μπορεί να περιγραφεί ως «η μελέτη του σχεδιασμού ευφυών παραγόντων που είναι σε θέση να δρουν, όπως οι υπολογιστές. Αυτό οφείλεται στην μηχανική μάθηση που έχει επιτευχθεί μέσω της TN. Όπως εξηγούν οι Lehr&Ohm (2017) «η μηχανική μάθηση αναφέρεται σε μια αυτοματοποιημένη διαδικασία εύρεσης συσχετίσεων (μερικές φορές εναλλακτικά αναφέρονται ως σχέσεις ή μοτίβα) μεταξύ μεταβλητών σε ένα σύνολο δεδομένων, συχνά για να γίνουν προβλέψεις ή εκτιμήσεις κάποιου αποτελέσματος(Lehr&Ohm, 2017). Λόγω κυρίως της διαθεσιμότητας τεράστιων ποσοτήτων δεδομένων, η μηχανική μάθηση έχει χρησιμοποιηθεί ευρέως κατά την τελευταία δεκαετία. Η μηχανική μάθηση είναι τόσο επιτυχημένη, που σήμερα πολλοί άνθρωποι

χρησιμοποιούν τις φράσεις τεχνητή νοημοσύνη και μηχανική μάθηση εναλλακτικά.

Τα αλγοριθμικά συστήματα μπορούν επίσης να χρησιμοποιηθούν για την προβλέψιμη αστυνόμευση, την εφαρμογή αναλυτικών τεχνικών - ιδιαίτερα ποσοτικών τεχνικών - για τον εντοπισμό πιθανών στόχων για αστυνομική παρέμβαση και την πρόληψη του εγκλήματος ή την επίλυση προηγούμενων εγκλημάτων κάνοντας στατιστικές προβλέψεις. Ωστόσο, η προγνωστική αστυνόμευση μπορεί να αναπαραγάγει και ακόμη και να ενισχύσει τις υπάρχουσες διακρίσεις. Ας πούμε ότι η αστυνομία δίνει ιδιαίτερη προσοχή σε μια γειτονιά με πολλούς μετανάστες, ενώ αυτή η γειτονιά έχει μέσο επίπεδο εγκληματικότητας. Η αστυνομία καταγράφει περισσότερο έγκλημα σε αυτήν τη γειτονιά από ότι αλλού. Επειδή οι αριθμοί δείχνουν ότι καταγράφεται περισσότερο έγκλημα (και έτσι φαίνεται να συμβαίνει) σε αυτήν τη γειτονιά, ακόμη περισσότερη αστυνομία αποστέλλεται εκεί. Με αυτόν τον τρόπο, η αστυνόμευση βάσει στατιστικών εγκλημάτων μπορεί να προκαλέσει πρόβλημα στην ανατροφοδότηση.

Και στον ιδιωτικό τομέα, η αλγοριθμική λήψη αποφάσεων μπορεί να έχει διακρίσεις. Για παράδειγμα, η TN μπορεί να χρησιμοποιηθεί από εταιρείες για την επιλογή υπαλλήλων ή από σχολεία για την επιλογή μαθητών. Ωστόσο, τα μεροληπτικά δεδομένα θα μπορούσαν να οδηγήσουν σε διακρίσεις. Τα δεδομένα μπορούν να μεροληπτούν επειδή αντιπροσωπεύουν ανθρώπινες αποφάσεις που εισάγουν διακρίσεις. Ο κίνδυνος μπορεί να επεξηγηθεί με ένα παράδειγμα από τη δεκαετία του 1980 στο Ηνωμένο Βασίλειο (Barocas&Selbst, 2016). Μια ιατρική σχολή χρησιμοποίησε ένα αλγοριθμικό σύστημα για την επιλογή φοιτητών.

Το σύστημα χρησιμοποίησε τα αρχεία εισαγωγής από προηγούμενα χρόνια, όταν οι υπάλληλοι του σχολείου επέλεγαν ποιοι υποψήφιοι θα μπορούσαν να μπουν στην ιατρική σχολή. Τα δεδομένα έδειξαν στο σύστημα ποια χαρακτηριστικά (η είσοδος) συσχετιζόνταν με την επιθυμητή έξοδο (εισαγωγή στην ιατρική σχολή). Το αλγοριθμικό σύστημα αναπαρήγαγε αυτή την μέθοδο επιλογής. Το σύστημα έκανε διακρίσεις εις βάρος γυναικών και ατόμων με μεταναστευτικό υπόβαθρο. Στα χρόνια που αφορούσαν τα δεδομένα, τα άτομα που επέλεγαν τους μαθητές ήταν προκατειλημμένα έναντι των γυναικών και των ατόμων με μεταναστευτικό υπόβαθρο. Έτσι, το πρόγραμμα δεν εισήγαγε μία νέα προκατάληψη αλλά απλώς αναπαρήγαγε αυτή που ήδη υπήρχε στο σύστημα (Lowry&Macpherson, 1988). Συνοπτικά, εάν ένα αλγοριθμικό σύστημα δέχεται προκατειλημμένα δεδομένα, τότε κινδυνεύει να αναπαραγάγει αυτή την προκατάληψη.

Η στοχευμένη διαδικτυακή διαφήμιση βασίζεται σε μεγάλο βαθμό στη λήψη αλγοριθμικών αποφάσεων. Αυτή η διαφήμιση είναι ένας κερδοφόρος τομέας για ορισμένες εταιρείες. Για παράδειγμα, το Facebook και η Google κερδίζουν το μεγαλύτερο μέρος των χρημάτων τους από διαδικτυακές διαφημίσεις. Ωστόσο, η διαδικτυακή διαφήμιση μπορεί να έχει διακρίσεις.

Οι Dattaetal. (2014) προσομοίωσαν τους χρήστες του Διαδικτύου και τους έκαναν να αυτο-δηλωθούν ως άνδρες ή γυναίκες. Οι ερευνητές ανέλυσαν τις διαφημίσεις που παρουσίασε η Google στους προσομοιωμένους χρήστες του Διαδικτύου. Η Google έδειξε διαφημίσεις προσομοίωσης ανδρών από ένα συγκεκριμένο γραφείο επαγγελματικής καθοδήγησης που υποσχέθηκε μεγάλους μισθούς πιο συχνά από τις προσομοιωμένες γυναίκες, ένα εύρημα που υποδηλώνει διακρίσεις. Η έλλειψη διαφάνειας της διαδικτυακής

διαφήμισης, δεν ήταν σαφής γιατί στις γυναίκες εμφανίστηκαν λιγότερες διαφημίσεις για θέσεις εργασίας με υψηλές αποδοχές. Η έρευνά έδειξε ότι η αδιαφάνεια της αλγοριθμικής λήψης αποφάσεων μπορεί να δυσκολέψει να ανακαλύψει τις διακρίσεις και την αιτία τους.

Τα συστήματα αναζήτησης εικόνων μπορούν επίσης να έχουν διακρίσεις. Το 2016, οι εικόνες της Google έδειξαν πολλές εικόνες συμμοριών όταν οι χρήστες έψαχναν για τρεις μαύρους εφήβους. Αντίθετα, οι εικόνες της Google έδειξαν εικόνες χαρούμενων λευκών παιδιών όταν οι άνθρωποι έψαχναν για τρεις λευκούς εφήβους. Η Google υποστήριξε ότι τα αποτελέσματα αναζήτησης των εικόνων της αντικατοπτρίζουν περιεχόμενο από ολόκληρο τον ιστό, συμπεριλαμβανομένης της συχνότητας εμφάνισης των τύπων εικόνων και του τρόπου με τον οποίο περιγράφονται στο Διαδίκτυο (Allen, 2016). Ωστόσο, ακόμη και αν το σφάλμα έγκειται στην κοινωνία και όχι στο αλγοριθμικό σύστημα, αυτά τα αποτελέσματα αναζήτησης εικόνων θα μπορούσαν να επηρεάσουν τις πεποιθήσεις των ανθρώπων.

Η έρευνα των Kayetal. (2015) έδειξε ότι τα αποτελέσματα αναζήτησης εικόνων για επαγγέλματα υπερβάλλουν ελαφρώς τα στερεότυπα του φύλου και απεικονίζουν το φύλο της μειονότητας ως λιγότερο επαγγελματικό. Υπάρχει επίσης μια μικρή υποεκπροσώπηση των γυναικών. Συνοπτικά, στο δημόσιο και τον ιδιωτικό τομέα, η αλγοριθμική λήψη αποφάσεων μπορεί να οδηγήσει σε διακρίσεις. Ενώ οι αποφάσεις από αλγόριθμους μπορεί να έχουν διακριτικά αποτελέσματα, οι αλγόριθμοι δεν είναι εγγενώς διακριτικοί. Οι αλγόριθμοι ενδέχεται να εξακολουθούν να αποδίδουν καλύτερα από τους υπεύθυνους λήψης αποφάσεων. Πολλοί

άνθρωποι κάνουν επίσης διακρίσεις. Πράγματι, μερικές φορές τα αλγοριθμικά συστήματα κάνουν διακρίσεις επειδή αναπαράγουν τις διακρίσεις από τον άνθρωπο.

Η αλγοριθμική λήψη αποφάσεων μπορεί επίσης να χρησιμοποιηθεί για την καταπολέμηση των διακρίσεων. Ας υποθέσουμε ότι ένα αλγοριθμικό σύστημα δείχνει ότι μια συλλογή φωτογραφιών που περιέχει στερεότυπα φύλου. Μία ερμηνεία είναι ότι το αλγοριθμικό σύστημα απεικονίζει στερεότυπη συμπεριφορά που υπάρχει ήδη. Ως εκ τούτου, ένα αλγοριθμικό σύστημα θα μπορούσε να βοηθήσει στην ανακάλυψη υφιστάμενων διακρίσεων που διαφορετικά θα παρέμεναν κρυμμένες. Υπάρχει ένα ζωντανό νέο υποπεδίο στην επιστήμη των υπολογιστών, με επίκεντρο τη δικαιοσύνη, την υπευθυνότητα και τη διαφάνεια στο πλαίσιο της αλγοριθμικής λήψης αποφάσεων. Οι επιστήμονες των υπολογιστών διερευνούν, για παράδειγμα, τρόπους για να ανακαλύψουν και να αποτρέψουν τις διακρίσεις και τρόπους για την οικοδόμηση κανόνων μη διάκρισης σε αλγοριθμικά συστήματα.

Ο νόμος περί μη διάκρισης και ο νόμος περί προστασίας δεδομένων είναι τα κύρια νομικά μέσα που θα μπορούσαν να προστατεύσουν το δικαίωμα μη διάκρισης στο πλαίσιο της αλγοριθμικής λήψης αποφάσεων. Πολλά συντάγματα και συνθήκες ανθρωπίνων δικαιωμάτων απαγορεύουν τις διακρίσεις. Για παράδειγμα, η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα αναφέρει στο άρθρο 14 ότι η απόλαυση των δικαιωμάτων και των ελευθεριών που ορίζονται στην Σύμβαση διασφαλίζεται χωρίς διακρίσεις για οποιοδήποτε λόγο όπως φύλο, φυλή, χρώμα, γλώσσα, θρησκεία, πολιτική ή άλλη γνώμη, εθνική ή κοινωνική προέλευση,

σύνδεση με μια εθνική μειονότητα, περιουσία, γέννηση ή άλλη κατάσταση.

Σύμφωνα με την νομολογία, η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα απαγορεύει τόσο τις άμεσες όσο και τις έμμεσες διακρίσεις. Εν συντομία, η άμεση διάκριση σημαίνει διάκριση βάσει προστατευόμενου εδάφους, όπως η εθνική καταγωγή. Η άμεση διάκριση περιγράφεται από το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων ως την ύπαρξη διαφοράς στη μεταχείριση προσώπων σε ανάλογες ή σχετικές παρόμοιες καταστάσεις, η οποία βασίζεται σε ένα αναγνωρίσιμο χαρακτηριστικό. Ένας παρόμοιος ορισμός χρησιμοποιείται στο δίκαιο της ΕΕ για την απαγόρευση των διακρίσεων.

Έμμεσες διακρίσεις σημαίνει ότι μια πρακτική που φαίνεται ουδέτερη με την πρώτη ματιά καταλήγει σε διακρίσεις εις βάρος ατόμων συγκεκριμένης εθνοτικής καταγωγής ή άλλου προστατευόμενου χαρακτηριστικού. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων περιγράφει την έμμεση διάκριση ως μια διαφορά στη μεταχείριση που μπορεί να έχει τη μορφή δυσανάλογα επιζήμιων επιπτώσεων μιας γενικής πολιτικής ή μέτρου το οποίο, αν και υπόκειται σε ουδέτερους όρους, εισάγει διακρίσεις εις βάρος μιας ομάδας. Μια τέτοια κατάσταση μπορεί να ισοδυναμεί με έμμεση διάκριση, η οποία δεν απαιτεί απαραίτητως πρόθεση διάκρισης. Η νομοθεσία της ΕΕ χρησιμοποιεί παρόμοιο ορισμό των έμμεσων διακρίσεων. Όσον αφορά τις έμμεσες διακρίσεις, δεν έχει σημασία αν υπάρχει ο σκοπός να γίνουν διακρίσεις. Είναι το αποτέλεσμα μιας πρακτικής που μετράει.

Τα αλγοριθμικά συστήματα μπορούν να προκαλέσουν διακρίσεις. Για παράδειγμα, η αλγοριθμική λήψη αποφάσεων θα

μπορούσε να παραβιάσει την απαγόρευση έμμεσης διάκρισης εάν ένα αλγοριθμικό σύστημα απορρίψει επιστολές αιτήσεων εργασίας από δυσανάλογο αριθμό ατόμων με συγκεκριμένη εθνικότητα. Επιπλέον, οι οργανισμοί θα μπορούσαν να χρησιμοποιήσουν αλγόριθμους για να κάνουν διάκριση με σκοπό. Για παράδειγμα, μια εταιρεία που ήθελε να κάνει διακρίσεις εις βάρος ατόμων μιας συγκεκριμένης εθνικότητας θα μπορούσε να κάνει διακρίσεις βάσει ενός πληρεξουσίου που σχετίζεται με αυτήν την εθνικότητα, όπως ο ταχυδρομικός κώδικας: ένας τύπος αλγοριθμικού κόκκινου επιπέδου.

Ο νόμος περί μη διάκρισης θα μπορούσε να βοηθήσει στην προστασία των ανθρώπων από τις αλγοριθμικές διακρίσεις. Ωστόσο, ο νόμος περί μη διάκρισης έχει πολλές αδυναμίες όταν εφαρμόζεται σε αλγοριθμικές διακρίσεις. Για παράδειγμα, ένα θύμα πρέπει να δείξει ότι ένας φαινομενικά ουδέτερος κανόνας, πρακτική ή απόφαση επηρεάζει δυσανάλογα μια προστατευόμενη τάξη και, ως εκ τούτου, εκ πρώτης όψεως εισάγει διακρίσεις.

Ωστόσο, οι έμμεσες διακρίσεις μπορούν να παραμείνουν κρυμμένες τόσο στον οργανισμό όσο και στο θύμα. Ας υποθέσουμε ότι κάποιος υποβάλλει αίτηση για δάνειο στον ιστότοπο μιας τράπεζας. Η τράπεζα χρησιμοποιεί ένα αλγοριθμικό σύστημα για να αποφασίσει σχετικά με αυτά τα αιτήματα. Εάν η τράπεζα αρνηθεί αυτόματα ένα δάνειο σε έναν πελάτη στον ιστότοπό της, ο πελάτης δεν βλέπει γιατί απορρίφθηκε το δάνειο. Και ο πελάτης δεν μπορεί να δει εάν το αλγοριθμικό σύστημα της τράπεζας αρνείται τα δάνεια σε ένα δυσανάλογο ποσοστό, για παράδειγμα, γυναικών. Ως εκ τούτου, ακόμη και αν οι πελάτες γνώριζαν ότι ένας αλγόριθμος παρά ένας υπάλληλος της τράπεζας αποφάσισε, θα ήταν δύσκολο για αυτούς να ανακαλύψουν εάν ο αλγόριθμος εισάγει διακρίσεις.

Τα αλγοριθμικά συστήματα είναι συχνά «μαύρα κουτιά», για διάφορους λόγους (Pasquale, 2015). Για παράδειγμα, οι περισσότεροι άνθρωποι δεν διαθέτουν την τεχνική εμπειρογνωμοσύνη για να καταλάβουν πώς αυτά τα συστήματα λαμβάνουν αποφάσεις. Ακόμη και οι ειδικοί που έχουν δημιουργήσει ένα αλγοριθμικό σύστημα μπορεί να μην γνωρίζουν πώς θα συμπεριφέρεται αυτό το σύστημα όταν χρησιμοποιείται στην πράξη και τροφοδοτούνται ορισμένα δεδομένα. Επιπλέον, τα εμπορικά ή κρατικά μυστικά ενδέχεται να εμποδίσουν την απόκτηση πληροφοριών σχετικά με τα αλγοριθμικά συστήματα (Burrell, 2016). Λόγω της έλλειψης διαφάνειας των αλγοριθμικών αποφάσεων, είναι δύσκολο για τους ανθρώπους να εκτιμήσουν εάν υφίσταντο διακρίσεις.

Ένα άλλο πρόβλημα με τη νομοθεσία περί μη διακρίσεων είναι ότι η απαγόρευση των έμμεσων διακρίσεων δεν παρέχει σαφή κανόνα. Η έννοια των έμμεσων διακρίσεων οδηγεί σε μάλλον ανοιχτού τύπου πρότυπα, τα οποία συχνά είναι δύσκολο να εφαρμοστούν στην πράξη. Η απαγόρευση των έμμεσων διακρίσεων δεν ισχύει εάν ο φερόμενος που τις πράττει επικαλεστεί με επιτυχία αντικειμενική αιτιολόγηση. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων υποστηρίζει ότι μια γενική πολιτική ή ένα μέτρο που έχει δυσανάλογα επιζήμια αποτελέσματα σε μια συγκεκριμένη ομάδα μπορεί να θεωρηθεί ότι εισάγει διακρίσεις ακόμη και όταν δεν στοχεύει συγκεκριμένα σε αυτήν την ομάδα και δεν υπάρχει καμία διάκριση. Αυτό συμβαίνει, ωστόσο, εάν μια τέτοια πολιτική ή μέτρο δεν έχει αντικειμενική και λογική αιτιολόγηση.

Ωστόσο, η αιτιολόγηση πρέπει να είναι αντικειμενική και λογική. Επιπλέον, η πρακτική (μέτρο ή πολιτική) πρέπει να είναι



ανάλογη με αυτόν τον στόχο. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων δηλώνει ότι μια πρακτική δεν πληροί αυτές τις προϋποθέσεις εάν η πρακτική αυτή δεν έχει αντικειμενική και εύλογη δικαιολογία, δηλαδή εάν δεν επιδιώκει θεμιτό σκοπό ή εάν δεν υπάρχει εύλογη σχέση αναλογικότητας μεταξύ των χρησιμοποιούμενων μέσων και του στόχου που επιδιώκεται να επιτευχθεί.

Εξαρτάται από όλες τις περιστάσεις μιας υπόθεσης εάν ένας κάποιος που κάνει διακρίσεις μπορεί να επικαλεστεί μια τέτοια αντικειμενική αιτιολόγηση. Επομένως, δεν είναι πάντοτε σαφές εάν μια συγκεκριμένη πρακτική παραβιάζει την απαγόρευση έμμεσης διάκρισης. Εν ολίγοις, ο νόμος περί μη διακρίσεων απαγορεύει πολλές διακρίσεις των αλγοριθμικών αποφάσεων, ιδίως μέσω της έννοιας της έμμεσης διάκρισης. Η επιβολή είναι δύσκολη, ωστόσο, και ο νόμος περί μη διάκρισης έχει αδυναμίες.

Η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα (1950) παρέχει στους ανθρώπους δικαίωμα στην ιδιωτική ζωή. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων συνήψε τις αρχές προστασίας δεδομένων από το δικαίωμα της ιδιωτικής ζωής στη Σύμβαση. Έτσι, το δικαστήριο δίνει σε ορισμένες αρχές προστασίας δεδομένων ένα καθεστώς που μοιάζει με τα ανθρώπινα δικαιώματα.

Στην Ευρωπαϊκή Ένωση, το δικαίωμα στην προστασία των προσωπικών δεδομένων έχει την ιδιότητα του ανθρώπινου δικαιώματος. Όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης είναι μέλη του Συμβουλίου της Ευρώπης και υπόκεινται στην Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα (1953). Ωστόσο, η ΕΕ έχει επίσης τον δικό της Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000, νομικά δεσμευτικός από το 2009). Ο

Χάρτης παρέχει στους ανθρώπους, εκτός από το δικαίωμα στην ιδιωτική ζωή, ένα ξεχωριστό δικαίωμα στην προστασία των προσωπικών δεδομένων.

Αναλυτικότεροι κανόνες μπορούν να βρεθούν στη Σύμβαση για την προστασία δεδομένων του Συμβουλίου της Ευρώπης και στον Γενικό Κανονισμό για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR, από το 2016). Οι βασικοί κανόνες και στα δύο μέσα είναι παρόμοιοι. Ο νόμος περί προστασίας δεδομένων στοχεύει στην υπεράσπιση της δικαιοσύνης και των ανθρωπίνων δικαιωμάτων όταν οι οργανισμοί χρησιμοποιούν προσωπικά δεδομένα. Ο νόμος περί προστασίας δεδομένων παρέχει δικαιώματα σε άτομα των οποίων τα δεδομένα χρησιμοποιούνται (υποκείμενα δεδομένων), και επιβάλλει υποχρεώσεις σε οργανισμούς που χρησιμοποιούν προσωπικά δεδομένα (υπεύθυνοι επεξεργασίας δεδομένων).

Ο πυρήνας του νόμου για την προστασία των δεδομένων αποτελείται από οκτώ αρχές, οι οποίες μπορούν να συνοψιστούν ως εξής:

(α) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο με νόμιμο, δίκαιο και διαφανή τρόπο.

(β) Τέτοια δεδομένα μπορούν να συλλεχθούν μόνο για έναν σκοπό που καθορίζεται εκ των προτέρων και πρέπει να χρησιμοποιούνται μόνο για σκοπούς που είναι συμβατοί με τον αρχικό σκοπό.

(γ) Οι οργανισμοί δεν πρέπει να συλλέγουν ή να χρησιμοποιούν περισσότερα δεδομένα από ό, τι είναι απαραίτητο.

(δ) Οι οργανισμοί πρέπει να διασφαλίζουν ότι αυτά τα δεδομένα είναι επαρκώς ακριβή και ενημερωμένα.

(ε) Οι οργανισμοί δεν πρέπει να αποθηκεύουν τα δεδομένα για υπερβολικά μεγάλο χρονικό διάστημα.

(στ) Οι οργανισμοί πρέπει να διασφαλίζουν την ασφάλεια των δεδομένων.

(ζ) Ο οργανισμός που καθορίζει τους σκοπούς και τα μέσα για την επεξεργασία (ο υπεύθυνος επεξεργασίας) είναι υπεύθυνος για τη συμμόρφωση.

Ο νόμος περί προστασίας δεδομένων θα μπορούσε να χρησιμοποιηθεί για να μετριάσει την ασυμμετρία των πληροφοριών και τους κινδύνους αθέμιτων και παράνομων διακρίσεων. Για παράδειγμα, ο νόμος περί προστασίας δεδομένων απαιτεί από τους οργανισμούς να είναι ανοιχτοί και διαφανείς σχετικά με τη χρήση των προσωπικών δεδομένων. Επομένως, οι οργανισμοί πρέπει να παρέχουν πληροφορίες, για παράδειγμα σε μια ειδοποίηση απορρήτου, για όλα τα στάδια της αλγοριθμικής λήψης αποφάσεων που περιλαμβάνουν προσωπικά δεδομένα. Παρόλο που οι περισσότεροι άνθρωποι αγνοούν τις ειδοποιήσεις απορρήτου, τέτοιες ειδοποιήσεις θα μπορούσαν να είναι χρήσιμες για ερευνητές, δημοσιογράφους και εποπτικές αρχές, για τη λήψη πληροφοριών σχετικά με τις πρακτικές ενός οργανισμού.

Σε ορισμένες περιπτώσεις, οι οργανισμοί υποχρεούνται να διενεργούν μια αξιολόγηση αντικτύπου προστασίας δεδομένων βάσει του GDPR και της Σύμβασης Προστασίας Δεδομένων. Μια αξιολόγηση μπορεί να περιγραφεί ως μια διαδικασία για συστηματική ανάλυση, αναγνώριση και ελαχιστοποίηση των κινδύνων προστασίας δεδομένων ενός έργου ή σχεδίου. Οι μελετητές όπως οι Kaminski&Malgieri(2019) υπογραμμίζουν τις

δυνατότητες των αξιολογήσεων να προστατεύουν τους ανθρώπους από αλγοριθμικές διακρίσεις.

Σύμφωνα με το GDPR, ένας οργανισμός πρέπει να διεξάγει αξιολόγηση όταν μια πρακτική είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ειδικά όταν χρησιμοποιεί νέες τεχνολογίες. Σε ορισμένες περιπτώσεις, ο GDPR αναλαμβάνει υψηλό κίνδυνο όπως για παράδειγμα, όταν οι οργανισμοί λαμβάνουν πλήρως αυτοματοποιημένες αποφάσεις που επηρεάζουν σοβαρά τους ανθρώπους. Για πολλά αλγοριθμικά συστήματα που λαμβάνουν αποφάσεις για άτομα, ο GDPR απαιτεί επομένως αξιολόγηση. Κατά τη διεξαγωγή της αξιολόγησης, οι οργανισμοί πρέπει επίσης να λάβουν υπόψη τον κίνδυνο αθέμιτων ή παράνομων διακρίσεων (Edwards&Veale, 2017).

Το Συμβούλιο της Ευρώπης και η ΕΕ απαιτούν από κάθε κράτος μέλος να διαθέτει ανεξάρτητη Αρχή Προστασίας Δεδομένων. Αυτές οι Αρχές Προστασίας Δεδομένων πρέπει να έχουν εξουσίες έρευνας. Σύμφωνα με το GDPR, μια Αρχή Προστασίας Δεδομένων μπορεί, για παράδειγμα, να έχει πρόσβαση στις εγκαταστάσεις ενός οργανισμού χρησιμοποιώντας προσωπικά δεδομένα και να ζητήσει από έναν οργανισμό να παρέχει πρόσβαση στους υπολογιστές του. Ο GDPR και η Σύμβαση περιέχουν συγκεκριμένους κανόνες για συγκεκριμένους τύπους αυτοματοποιημένης ατομικής λήψης αποφάσεων. Αυτοί οι κανόνες έχουν διάφορους στόχους, συμπεριλαμβανομένης της προστασίας των ανθρώπων από αθέμιτες ή παράνομες διακρίσεις.

Το άρθρο 22 του GDPR καλείται μερικές φορές η διάταξη Κάφκα. Κατ' αρχήν, το άρθρο 22 απαγορεύει ορισμένες πλήρως αυτοματοποιημένες αποφάσεις με νομικά ή παρόμοια σημαντικά

αποτελέσματα. Το άρθρο 22 ισχύει, για παράδειγμα, για την πλήρως αυτοματοποιημένη βαθμολογία πίστωσης και την ηλεκτρονική πρόσληψη. Ο κύριος κανόνας του άρθρου 22 αναφέρει ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένου του προφίλ, η οποία παράγει έννομα αποτελέσματα που τον αφορούν ή τον επηρεάζουν σημαντικά.

Ο κανόνας αυτός θα μπορούσε να συνοψιστεί ως εξής: οι οργανισμοί ενδέχεται να μην υποβάλλουν τους ανθρώπους σε συγκεκριμένους τύπους πλήρως αυτοματοποιημένων αποφάσεων με εκτεταμένα αποτελέσματα. Το άρθρο 22 ορίζει ότι οι άνθρωποι έχουν δικαίωμα να μην υπόκεινται σε ορισμένες αποφάσεις. Αυτό το δικαίωμα μπορεί να ερμηνευθεί ως απαγόρευση τέτοιων αποφάσεων (Wachteretal., 2017).

Η απαγόρευση ορισμένων αυτοματοποιημένων αποφάσεων δεν είναι απόλυτη αλλά υπάρχουν εξαιρέσεις. Εν συντομία, η απαγόρευση δεν ισχύει (i) εάν το άτομο έδωσε τη συγκατάθεσή του για την αυτοματοποιημένη απόφαση ή εάν η απόφαση είναι (ii) απαραίτητη για μια σύμβαση μεταξύ του ατόμου και του υπευθύνου επεξεργασίας δεδομένων ή (iii) έχει εγκριθεί από το νόμο.

Ένας διαφορετικός κανόνας ενεργοποιείται εάν ένας ελεγκτής μπορεί να βασιστεί στην εξαίρεση της σύμβασης (i) ή (ii) της σύμβασης. Αυτός ο κανόνας λέει ότι ο υπεύθυνος επεξεργασίας δεδομένων εφαρμόζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των νόμιμων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος

ανθρώπινης παρέμβασης εκ μέρους του υπευθύνου επεξεργασίας, να εκφράσει την άποψή του και να αμφισβητήσει την απόφαση.

Έτσι, σε ορισμένες περιπτώσεις, οι άνθρωποι μπορούν να απαιτήσουν από τον οργανισμό να κάνει έναν υπάλληλο να επανεξετάσει την αυτοματοποιημένη απόφαση. Για παράδειγμα, μια τράπεζα θα μπορούσε να διασφαλίσει ότι οι πελάτες μπορούν να καλέσουν την τράπεζα για να επανεξετάσει την απόφαση, εάν η τράπεζα τους αρνηθεί αυτόματα δάνειο μέσω του ιστότοπου της τράπεζας.

Υπάρχει μια ζωντανή επιστημονική συζήτηση σχετικά με το βαθμό στον οποίο ο GDPR δημιουργεί ένα δικαίωμα στην εξήγηση μεμονωμένων αποφάσεων. Αφενός, μελετητές όπως οι Wachteretal. (2017) αμφιβάλλουν για την αποτελεσματικότητα αυτού του δικαιώματος και επισημαίνουν ότι πολλές αλγοριθμικές αποφάσεις παραμένουν εκτός του πεδίου εφαρμογής των κανόνων του GDPR. Όπως σημειώνουν οι Veale&Edwards (2018), οι κανόνες για τις αυτοματοποιημένες αποφάσεις στη Σύμβαση είναι πιο γενναιόδωροι για τα άτομα. Σύμφωνα με τη Σύμβαση, οι άνθρωποι έχουν το δικαίωμα να αποκτήσουν, κατόπιν αιτήσεως, γνώση του σκεπτικού της υποκείμενης επεξεργασίας δεδομένων όταν τα αποτελέσματα αυτής της επεξεργασίας εφαρμόζονται σε αυτούς. Επομένως, η Σύμβαση δεν περιορίζει το δικαίωμα αυτό σε αποφάσεις με νομικά ή σημαντικά αποτελέσματα.

Ο νόμος περί προστασίας δεδομένων δεν αποτελεί κανόνα για την προστασία των ανθρώπων από αλγοριθμικές διακρίσεις. Απαιτούνται αρκετές προειδοποιήσεις. Πρώτον, υπάρχει έλλειμμα συμμόρφωσης και επιβολής. Πολλοί οργανισμοί δεν έλαβαν σοβαρά υπόψη τη συμμόρφωση με τη νομοθεσία περί προστασίας

δεδομένων. Φαίνεται ότι η συμμόρφωση βελτιώθηκε με την άφιξη του GDPR (που ισχύει από το 2018), αλλά είναι πολύ νωρίς για να εκτιμηθεί εάν βελτιώθηκε η συμμόρφωση. Ένα άλλο πρόβλημα είναι ότι οι αρχές προστασίας δεδομένων επιβαρύνονται υπερβολικά. Επιπλέον, πολλές Αρχές Προστασίας Δεδομένων δεν έχουν την εξουσία να επιβάλλουν σοβαρές κυρώσεις. Στην ΕΕ, ο GDPR παραχώρησε σε αυτές τις αρχές νέες εξουσίες, αλλά είναι πολύ νωρίς για δεδομένα που αφορούν το αποτέλεσμα αυτών των εξουσιών.

Δεύτερον, καθώς ο νόμος περί προστασίας δεδομένων εφαρμόζεται μόνο στα προσωπικά δεδομένα, οι αλγοριθμικές διαδικασίες λήψης αποφάσεων είναι εν μέρει εκτός του πεδίου εφαρμογής του νόμου περί προστασίας δεδομένων. Ο νόμος περί προστασίας δεδομένων δεν ισχύει για μοντέλα πρόβλεψης, επειδή δεν σχετίζονται με αναγνωρίσιμα άτομα. Για παράδειγμα, ένα μοντέλο πρόβλεψης που λέει ότι το 80% των ανθρώπων που ζουν στον ταχυδρομικό κώδικα 10017 πληρώνουν τους λογαριασμούς τους αργά δεν αναφέρεται σε ένα άτομο. Επομένως, το μοντέλο δεν είναι προσωπικό δεδομένο. Ο νόμος περί προστασίας δεδομένων ισχύει όταν ένα τέτοιο μοντέλο πρόβλεψης εφαρμόζεται σε ένα άτομο (Wachter&Mittelstadt, 2019).

Τρίτον, ο νόμος περί προστασίας δεδομένων χρησιμοποιεί πολλούς ανοιχτούς και αφηρημένους κανόνες, παρά σαφείς και συγκεκριμένους. Ο νόμος περί προστασίας δεδομένων πρέπει να χρησιμοποιεί ανοιχτούς κανόνες, διότι οι διατάξεις του ισχύουν σε πολλές διαφορετικές καταστάσεις, στον ιδιωτικό και στο δημόσιο τομέα. Αυτή η κανονιστική προσέγγιση, έχει πολλά πλεονεκτήματα. Για παράδειγμα, οι ανοιχτοί κανόνες δεν χρειάζεται να προσαρμόζονται κάθε φορά που αναπτύσσεται μια νέα τεχνολογία.

Ένα μειονέκτημα της προσέγγισης του νόμου περί προστασίας δεδομένων είναι ότι οι ανοιχτοί κανόνες μπορεί να είναι δύσκολο να εφαρμοστούν στην πράξη.

Μια τέταρτη προειδοποίηση αφορά τους αυστηρούς κανόνες του νόμου περί προστασίας δεδομένων σχετικά με τις «ειδικές κατηγορίες δεδομένων» (μερικές φορές ονομάζονται «ευαίσθητα δεδομένα»), όπως δεδομένα σχετικά με την εθνική καταγωγή ή την κατάσταση της υγείας. Όπως σημειώνουν οι De Schutter & Ringelheim (2008), αυτό το αυστηρότερο καθεστώς δημιουργεί προκλήσεις στην αξιολόγηση και μετριάσμο των διακρίσεων. Πολλές από τις μεθόδους για την καταπολέμηση των διακρίσεων σε αλγοριθμικά συστήματα υποθέτουν σιωπηρά ότι οι οργανισμοί κατέχουν αυτά τα ευαίσθητα δεδομένα. Υπάρχει σύγχυση μεταξύ του σεβασμού του νόμου περί προστασίας δεδομένων και της συλλογής ευαίσθητων δεδομένων για την καταπολέμηση των διακρίσεων.

Ακόμη και όταν υποθέτουμε ότι οι άνθρωποι έχουν δικαίωμα εξήγησης σχετικά με αλγοριθμικές αποφάσεις, είναι συχνά δύσκολο, αν όχι αδύνατο, να εξηγηθεί η λογική πίσω από μια απόφαση, όταν ένα αλγοριθμικό σύστημα φτάνει σε αυτήν την απόφαση μετά από ανάλυση μεγάλων ποσοτήτων δεδομένων (Edwards & Veale, 2017). Ωστόσο, θα ήταν καλό εάν οι οργανισμοί προσέφεραν περισσότερη διαφάνεια και εξηγήσεις σχετικά με τις αλγοριθμικές αποφάσεις τους. Απαιτείται περισσότερη διαφάνεια σχετικά με την αυτοματοποιημένη λήψη αποφάσεων. Οι επιστήμονες υπολογιστών διερευνούν διάφορους τρόπους βελτίωσης της διαφάνειας και της επεξήγησης των αλγοριθμικών αποφάσεων.

Είναι πολύ νωρίς για να εκτιμηθούν τα αποτελέσματα της Σύμβασης και του GDPR. Απαιτείται περισσότερη νομική έρευνα



σχετικά με τον τρόπο με τον οποίο ο νόμος για την προστασία των δεδομένων θα μπορούσε να συμβάλει στον μετριασμό των κινδύνων διάκρισης. Ενώ το δικαίωμα στην προστασία των προσωπικών δεδομένων και ο νόμος περί προστασίας των δεδομένων είναι σε μεγάλο βαθμό μη δοκιμασμένα ως εργαλείο μη διάκρισης, προσφέρουν δυνατότητες καταπολέμησης της παράνομης διάκρισης.

Άλλα νομικά μέσα θα μπορούσαν επίσης να βοηθήσουν στην προστασία των ανθρώπων από τις αλγοριθμικές διακρίσεις. Για παράδειγμα, η νομοθεσία για τους καταναλωτές θα μπορούσε να βοηθήσει στην υπεράσπιση των ανθρώπων από τη χειραγώγηση της αλγοριθμικής διαφήμισης. Ο νόμος περί ανταγωνισμού θα μπορούσε επίσης να είναι χρήσιμος. Η διακριτική συμπεριφορά μιας εταιρείας προκαλεί περισσότερα προβλήματα όταν η εταιρεία κατέχει μονοπωλιακή θέση. Στον δημόσιο τομέα, το ποινικό δίκαιο και το διοικητικό δίκαιο θα μπορούσαν να βοηθήσουν στη διασφάλιση της δικαιοσύνης των διαδικασιών. Ωστόσο, η εφαρμογή αυτών των τομέων δικαίου για την προστασία των ανθρώπων στον τομέα της αλγοριθμικής λήψης αποφάσεων είναι σε μεγάλο βαθμό ανεξερεύνητη.

Αρκετοί οργανισμοί δημοσίευσαν αρχές για δίκαιη, υπεύθυνη ή ηθική τεχνητή νοημοσύνη. Για παράδειγμα: ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) δημοσίευσε μια σύσταση για την τεχνητή νοημοσύνη και το Συμβούλιο της Ευρώπης δημοσίευσε ένα σχέδιο σύστασης για τις επιπτώσεις των αλγοριθμικών συστημάτων στα ανθρώπινα δικαιώματα. Η Ευρωπαϊκή Επιτροπή συνέστησε μίαςομάδα εμπειρογνομόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη, η οποία πρότεινε τις

κατευθυντήριες γραμμές για τη δεοντολογία της τεχνητής νοημοσύνης.

Άλλοι οργανισμοί δημοσίευσαν αρχές αυτορρύθμισης σχετικά με την ηθική και την τεχνητή νοημοσύνη. Από τη μία πλευρά, η αυτορρύθμιση είναι αξιόπαινη. Δεν μπορεί να αμφισβητηθεί ότι η ηθική ΤΝ είναι προτιμότερη από την ανήθικη ΤΝ. Η αυτορρύθμιση θα μπορούσε να βοηθήσει στον μετριασμό των διακρίσεων και θα μπορούσε να αποτελέσει έμπνευση για τους νομοθέτες. Από την άλλη πλευρά, υπάρχουν σοβαρά προβλήματα με την αυτορρύθμιση. Το πιο σημαντικό είναι ότι η αυτορρύθμιση είναι μη δεσμευτική. Η προστασία των ανθρωπίνων δικαιωμάτων δεν μπορεί να αφεθεί σε εθελοντικά μέτρα. Η εφαρμογή συνήθως στερείται τέτοιων κωδικών δεοντολογίας. Εκτός από αυτό, πολλές αρχές αυτορρύθμισης της ΤΝ είναι μάλλον ασαφείς και δεν παρέχουν λεπτομερείς οδηγίες. η αυτορρύθμιση δεν πρέπει να αποσπά την προσοχή των νομοθετών από την πιθανή ανάγκη νέων νόμων.

Μπορεί να υπάρχει ανάγκη για πρόσθετη ρύθμιση για την προστασία των ανθρώπων από τις αλγοριθμικές διακρίσεις. Οι γενικοί κανόνες είναι λογικά σαφείς σχετικά με την αλγοριθμική διάκριση. Οι κοινωνίες μας δεν αποδέχονται, και δεν πρέπει, να δέχονται διακρίσεις βάσει χαρακτηριστικών όπως η εθνοτική καταγωγή. Όπως ήδη αναφέρθηκε, ένα από τα προβλήματα με τα αλγοριθμικά συστήματα είναι ο χαρακτήρας του «μαύρου κουτιού». Αυτή η αδιαφάνεια μπορεί να θεωρηθεί ως πρόβλημα από μόνη της - αλλά η αδιαφάνεια εμποδίζει επίσης την ανακάλυψη διακρίσεων.

Η ρύθμιση θα μπορούσε να συμβάλει στη διαφάνεια της αλγοριθμικής λήψης αποφάσεων. Ο κανονισμός θα μπορούσε, για παράδειγμα, να απαιτεί τα αλγοριθμικά συστήματα που

χρησιμοποιούνται στο δημόσιο τομέα να αναπτύσσονται με τέτοιο τρόπο ώστε να επιτρέπουν τον έλεγχο και την επεξήγηση. Τέτοιες απαιτήσεις θα μπορούσαν επίσης να ληφθούν υπόψη για τον ιδιωτικό τομέα. Ως εκ τούτου, υπάρχει προηγούμενο για απαιτήσεις διαφάνειας στον ιδιωτικό τομέα. Στην ΕΕ, υπάρχει νομική απαίτηση για ερμηνεία για ορισμένα συστήματα αλγοριθμικών συναλλαγών που χρησιμοποιούνται από εταιρείες επενδύσεων.

Μερικές φορές, οι φορείς του δημόσιου τομέα θα μπορούσαν να απελευθερώσουν τον υποκείμενο κώδικα (λογισμικό) αλγοριθμικών συστημάτων. Σε ορισμένες περιπτώσεις, η εξέταση του κώδικα μπορεί να παρέχει πληροφορίες σχετικά με τον τρόπο λειτουργίας ενός συστήματος. Οι έλεγχοι κώδικα είναι πιθανότερο να είναι χρήσιμοι όταν υπάρχει μια σαφώς καθορισμένη ερώτηση σχετικά με το πώς λειτουργεί ένα πρόγραμμα λογισμικού σε ρυθμιζόμενο χώρο και συγκεκριμένα πρότυπα βάσει των οποίων μπορεί να μετρηθεί η συμπεριφορά ή η απόδοση ενός συστήματος. Θα μπορούσαν να προσαρμοστούν οι νόμοι περί ελευθερίας της πληροφόρησης, έτσι ώστε ο κώδικας σε αλγοριθμικά συστήματα να υπόκειται σε αυτούς τους νόμους. Μια τέτοια τροποποίηση θα επέτρεπε σε δημοσιογράφους, ερευνητές και άλλους να αποκτήσουν και να εξετάσουν αυτόν τον κώδικα.

Σε πολλές περιπτώσεις, η εξέταση του κώδικα ενός αλγοριθμικού συστήματος δεν παρέχει πολύ χρήσιμες πληροφορίες, καθώς το σύστημα μπορεί να εκτιμηθεί μόνο όταν χρησιμοποιείται στην πράξη. Τα αλγοριθμικά συστήματα προστατεύονται συχνά από εμπορικά μυστικά, δικαιώματα πνευματικής ιδιοκτησίας ή από τους όρους και τις προϋποθέσεις μιας εταιρείας. Αυτή η προστασία καθιστά δυσκολότερο για τους ρυθμιστικούς φορείς, τους

δημοσιογράφους και τους ερευνητές να διερευνήσουν τέτοια συστήματα. Ίσως ο νόμος πρέπει να προσαρμοστεί για να βελτιώσει τις εξαιρέσεις της έρευνας. Και ίσως ο νόμος θα πρέπει να απαιτεί από ιδιωτικούς οργανισμούς να αποκαλύπτουν συγκεκριμένες πληροφορίες στους ερευνητές, κατόπιν αιτήματος.

Ο νόμος θα μπορούσε να απαιτεί ο δημόσιος τομέας να χρησιμοποιεί μόνο αλγοριθμικά συστήματα που επιτρέπουν την εποπτεία και τον έλεγχο και τα οποία εκτιμήθηκαν σωστά για κινδύνους. Μια παρόμοια απαίτηση θα μπορούσε να ληφθεί υπόψη για τον ιδιωτικό τομέα, όταν τα αλγοριθμικά συστήματα χρησιμοποιούνται για συγκεκριμένους τύπους αποφάσεων, σχετικά με την επιλεξιμότητα για ασφάλιση, πίστωση ή εργασία. Απαιτείται σημαντική εμπειρογνωμοσύνη για τον έλεγχο αλγοριθμικών συστημάτων. Απαιτείται περισσότερη έρευνα και συζήτηση σχετικά με το ποιος πρέπει να διενεργεί αυτούς τους ελέγχους.

Οι Φορείς Ισότητας και οι Αρχές Προστασίας Δεδομένων θα πρέπει να διαθέτουν επαρκείς εξουσίες διερεύνησης και επιβολής, και θα πρέπει να λαμβάνουν επαρκή χρηματοδότηση, για παράδειγμα για την πρόσληψη τεχνικής εμπειρογνωμοσύνης. Συμπερασματικά, ο νέος κανονισμός θα πρέπει να στοχεύει στην καλύτερη επιβολή των σημερινών κανόνων μη διάκρισης στον τομέα της αλγοριθμικής λήψης αποφάσεων. Ωστόσο, η αλγοριθμική λήψη αποφάσεων επιτρέπει επίσης νέους τύπους διακρίσεων και διαφοροποιήσεων που θα μπορούσαν να αποφύγουν τους ισχύοντες διακρίσεις και άλλους νόμους.

Οι αλγοριθμικές αποφάσεις μπορεί να είναι άδικες ή να έχουν και άλλα μειονεκτήματα, ακόμη και αν οι αποφάσεις παραμένουν εκτός του πεδίου εφαρμογής του νόμου περί μη διάκρισης. Για

παράδειγμα, οι ασφαλιστικές εταιρείες θα μπορούσαν να χρησιμοποιήσουν αλγοριθμικά συστήματα για να καθορίσουν ασφάλιστρα για μεμονωμένους καταναλωτές ή να τους αρνηθούν την ασφάλιση. Σε κάποιο βαθμό, είναι απαραίτητη η διαφοροποίηση του κινδύνου και μια αποδεκτή πρακτική για την ασφάλιση. Και σε κάποιο βαθμό είναι δίκαιο όταν οι πελάτες υψηλού κινδύνου πληρώνουν υψηλότερα ασφάλιστρα. Ωστόσο, η ασφάλιση θα μπορούσε να καταστεί προσιτή για ορισμένους καταναλωτές εάν οι ασφαλιστικές εταιρείες εμπλέκονται σε υπερβολική ταξινόμηση κινδύνων. Ως εκ τούτου, η αλγοριθμική ταξινόμηση θα μπορούσε να απειλήσει τη λειτουργία συγκέντρωσης κινδύνων της ασφάλισης.

Επιπλέον, η αλγοριθμική λήψη αποφάσεων θα μπορούσε να ενισχύσει την κοινωνική ανισότητα. Κάποιος που ζει σε μια φτωχή γειτονιά με πολλές διαρρήξεις μπορεί να πληρώσει περισσότερα για την ασφάλιση κατοικίας, επειδή ο κίνδυνος διάρρηξης είναι υψηλότερος. Εάν οι γειτονιές όπου ζουν πολλοί φτωχοί άνθρωποι έχουν υψηλότερους κινδύνους, τότε οι φτωχοί πληρώνουν, κατά μέσο όρο, περισσότερο. Ωστόσο, η οικονομική κατάσταση κάποιου δεν είναι προστατευμένο χαρακτηριστικό, οπότε ο νόμος περί μη διάκρισης δεν ρυθμίζει μια τέτοια πρακτική (υποθέτοντας ότι η πρακτική δεν οδηγεί σε έμμεση διάκριση βάσει προστατευόμενου χαρακτηριστικού).

Πρέπει να εξεταστεί πρόσθετος κανονισμός για την υπεράσπιση των ανθρωπίνων δικαιωμάτων και της δικαιοσύνης στον τομέα της αλγοριθμικής λήψης αποφάσεων. Ωστόσο, δεν θα ήταν χρήσιμο να ρυθμιστεί γενικά η αλγοριθμική λήψη αποφάσεων. Η χρήση αλγορίθμων είναι πολύ διαφορετική για ένα σύνολο κανόνων. Η αλγοριθμική λήψη αποφάσεων χρησιμοποιείται σε πολλούς

διαφορετικούς τομείς, για πολλούς διαφορετικούς σκοπούς και στις περισσότερες περιπτώσεις, η αλγοριθμική λήψη αποφάσεων δεν απειλεί τα ανθρώπινα δικαιώματα. Ένα αλγοριθμικό σύστημα ενός υπολογιστή σκακιού φέρνει διαφορετικούς κινδύνους, εάν υπάρχουν, από ένα αλγοριθμικό σύστημα για πιστοληπτική ικανότητα ή προγνωστική αστυνόμευση.

Ακόμα και για αλγοριθμικά συστήματα που λαμβάνουν αποφάσεις για τον άνθρωπο, οι κίνδυνοι είναι διαφορετικοί σε διαφορετικούς τομείς και πρέπει να ισχύουν διαφορετικοί κανόνες. Δεν μπορούμε να αξιολογήσουμε την ορθότητα των αλγοριθμικών αποφάσεων γενικά. Ανάλογα με τον τομέα ή την περιοχή εφαρμογής, διαφορετικά επιχειρήματα έχουν διατυπωθεί. Για παράδειγμα, στον τομέα του ποινικού δικαίου, το δικαίωμα σε δίκαιη δίκη και το τεκμήριο αθωότητας είναι σημαντικά. Στις συναλλαγές καταναλωτών, η ελευθερία της σύμβασης είναι μια σημαντική αρχή. Επομένως, οι νέοι κανόνες θα πρέπει να επικεντρώνονται σε συγκεκριμένους τομείς.

Μπορούμε να επωφεληθούμε από την αλγοριθμική λήψη αποφάσεων. Ωστόσο, η αλγοριθμική λήψη αποφάσεων συνεπάγεται και κινδύνους. Οι επιστήμονες υπολογιστών έχουν δείξει πώς τα αλγοριθμικά συστήματα μπορούν να κάνουν διακρίσεις, για παράδειγμα όταν ένα τέτοιο σύστημα αναπαράγει διακρίσεις που έμαθε από διακριτικές ανθρώπινες αποφάσεις.

Τα αποτελέσματα των αλγοριθμικών αποφάσεων μπορεί να είναι εκτεταμένα. Στο δημόσιο τομέα, οι αλγόριθμοι μπορούν να χρησιμοποιηθούν για προβλέψεις αστυνόμευσης ή καταδίκης και για αποφάσεις σχετικά με, για παράδειγμα, συντάξεις, στέγαση ή παροχές ανεργίας. Και στον ιδιωτικό τομέα, οι αλγοριθμικές

αποφάσεις μπορούν να επηρεάσουν σοβαρά τους ανθρώπους, για παράδειγμα όταν οι αποφάσεις αφορούν απασχόληση, στέγαση ή πίστωση.

Ο νόμος περί μη διάκρισης και ο νόμος περί προστασίας των δεδομένων είναι τα πιο κατάλληλα νομικά μέσα για την καταπολέμηση της παράνομης διάκρισης από αλγοριθμικά συστήματα. Εάν επιβληθούν αποτελεσματικά, και τα δύο νομικά μέσα μπορούν να βοηθήσουν στην προστασία των ανθρώπων.

Ωστόσο, ορισμένοι τύποι αλγοριθμικών αποφάσεων αποφεύγουν τους ισχύοντες νόμους, ενώ μπορούν να οδηγήσουν σε αθέμιτη διαφοροποίηση ή διάκριση. Για παράδειγμα, πολλά καταστατικά κατά των διακρίσεων ισχύουν μόνο για διακρίσεις βάσει ορισμένων προστατευόμενων λόγων, όπως η εθνική καταγωγή. Τέτοια καταστατικά δεν ισχύουν εάν οι οργανισμοί διαφοροποιούνται με βάση τις νέες εφευρέσεις τάξεων που δεν συσχετίζονται με προστατευόμενους λόγους. Μια τέτοια διαφοροποίηση θα μπορούσε ακόμη να είναι άδικη, για παράδειγμα, όταν ενισχύει την κοινωνική ανισότητα.

Χρειαζόμαστε πιθανώς πρόσθετες ρυθμίσεις για την προστασία της δικαιοσύνης και των ανθρωπίνων δικαιωμάτων στον τομέα της αλγοριθμικής λήψης αποφάσεων. Ωστόσο, πιθανώς δεν είναι χρήσιμο να υιοθετηθούν κανόνες για τη λήψη αλγοριθμικών αποφάσεων γενικά. Ακριβώς όπως δεν υιοθετήσαμε και δεν μπορούσαμε να υιοθετήσουμε ένα καταστατικό για τη ρύθμιση της βιομηχανικής επανάστασης, δεν μπορούμε να υιοθετήσουμε ένα καταστατικό για τη ρύθμιση της αλγοριθμικής λήψης αποφάσεων. Για να μετριάσουμε τα προβλήματα που προκαλούνται από τη βιομηχανική επανάσταση, χρειαζόμασταν διαφορετικούς νόμους για

την ασφάλεια της εργασίας, την προστασία των καταναλωτών, το περιβάλλον κ.λπ. Σε διαφορετικούς τομείς, οι κίνδυνοι είναι διαφορετικοί και διακυβεύονται διαφορετικοί κανόνες και αξίες. Επομένως, οι νέοι κανόνες για τη λήψη αλγοριθμικών αποφάσεων πρέπει να είναι ειδικοί ανά τομέα.

## **2.2. Τεχνητή νοημοσύνη και δημοκρατία**

Μια πιθανή χρήση της τεχνητής νοημοσύνης είναι η μοντελοποίηση συγκεκριμένων προφίλ εγκληματιών. Η αρχή αυτής της προσέγγισης συνίσταται στην αξιολόγηση των δυνατοτήτων που σχετίζει έναν ύποπτο εκ των προτέρων με μία πράξη. Η πρόοδος της τεχνητής νοημοσύνης είναι να εκπαιδεύσει το μοντέλο από την εγκληματολογική θεωρία και από τις πραγματικές αναφορές περιπτώσεων. Αυτού του είδους οι εφαρμογές θα μπορούσαν να υλοποιηθούν για να δημιουργήσουν ένα μοντέλο τάξης για συγκεκριμένους εγκληματίες αλλά και για θύματα. Η ανάλυση των προτύπων που διαμορφώνονται από τους παραγωγικούς παραβάτες θα μπορούσε να βασιστεί σε πολλά στοιχεία, όπως οι κινήσεις τους, η περιοχή διαβίωσής τους, η διαφήμιση ή η εργασία τους, οι συνήθειες τους, το είδος του εγκλήματός τους, οι προηγούμενες καταδίκες τους, το σπίτι τους, οι καθημερινές τους δραστηριότητες, τα κοινωνικά τους δίκτυα, τους τόπους παραβάσεων, κ.λπ. (Perrot, 2017).

Με βάση την ίδια αρχή ένα προφίλ βασισμένο στην κοινωνική μηχανική θα μπορούσε να καθορίσει τον κίνδυνο αξιολόγησης επιθέσεων και εγκληματικών πράξεων. Απαραίτητο είναι να αποκτηθεί ένα ιστορικό προηγούμενων περιπτώσεων για να δημιουργηθεί ένα σύνολο δεδομένων θυμάτων και ένα άλλο μη



θυμάτων. Αυτό το είδος ανάλυσης αρχίζει να χρησιμοποιείται για να βρεθεί η πιο δυνατή πιθανότητα (Perrot, 2017).

Σε πολλές περιπτώσεις, η διαδικασία έρευνας είναι μια λογική επιχείρηση σε ένα περιβάλλον που σχηματίζεται από τη νομική διαδικασία. Επιπλέον, ένας ερευνητής χρησιμοποιεί τη δική του εμπειρία για να αυξήσει τη συνάφεια του. Αυτές οι διαφορετικές πτυχές μπορούν να διαμορφωθούν από ένα σύστημα εμπειρογνωμόνων που βασίζεται στην αρχή της εκπαίδευσης. Μια πηγή συλλογισμού του ερευνητή είναι τα αποτελέσματα των συνεντεύξεων που πραγματοποιήθηκαν με τους πράκτορες που θα μπορούσαν να χρησιμοποιηθούν για την εκπαίδευση ενός μοντέλου. Ένας αστυνομικός σε μία περίπτωση χρησιμοποιεί πιθανότατα τον παραγωγικό συλλογισμό και μαθαίνει τα πάντα με εμπειρία. Έτσι, η πρόκληση για ένα σύστημα εμπειρογνωμόνων είναι να μπορεί να είναι σε θέση να ενσωματώσει εμπειρία και έναν τρόπο συλλογισμού. Ωστόσο, η γνώση και η διαίσθηση του αστυνομικού παίζουν κεντρικό ρόλο. Όλη η διαδικασία δεν είναι λογική και ένας ερευνητής μπροστά σε μια κατάσταση πρέπει να διατηρήσει μια ανοιχτή και προσαρμοστική στάση. Η τεχνική και λογική γνώση, αν και απαραίτητη, δεν αρκεί για να εξηγήσει την παγκόσμια διαδικασία της έρευνας (Perrot, 2017).

Ένας εικονικός πράκτορας που μπορεί να παρέχει αντικειμενική βοήθεια σε έναν πραγματικό έλεγχο δεν φαίνεται ρεαλιστικός λόγω της ετερογένειας και της πολυπλοκότητας των καταστάσεων. Η τυπική ή ανεπίσημη αντίληψη παίζει σημαντικό ρόλο στη σύλληψη της πραγματικότητας για τους ερευνητές. Επειδή ο ανθρώπινος εγκέφαλος δεν είναι ένα πρόγραμμα σκακιού, η τεχνητή νοημοσύνη δεν είναι πλήρως έτοιμη σήμερα να τον μιμηθεί.

Η κατανόηση των ποινικών ερευνών απαιτεί επίσης να συναχθεί ένας κρυφός παράγοντας, δηλαδή η πρόθεση του αστυνομικού. Δεν μπορεί όμως να αποκλειστεί ότι στο μέλλον η επέκταση της τεχνητής νοημοσύνης σε αυτόν τον τομέα θα βασίζεται στην ανάλυση των προτύπων των αστυνομικών. Οι αναλύσεις θα μπορούσαν για παράδειγμα να περιλαμβάνουν την εμπειρία, την ηλικία των ερευνητών, τις τροχιές, τον τρόπο λειτουργίας των ερευνών, τον τύπο του εγκλήματος, κ.ο.κ. (Perrot, 2017).

Για σκοπούς πρόβλεψης, ο τύπος τεχνητής νοημοσύνης που επιτρέπει την εξαγωγή γνώσεων και προβλέψεων από μεγάλα ποικίλα ψηφιακά δεδομένα είναι πιο σχετικός. Αυτό σχετίζεται, αλλά διαφέρει από το πεδίο της ανάλυσης των μεγάλων δεδομένων (bigdata). Τα μεγάλα δεδομένα αναφέρονται σε σύνολα δεδομένων των οποίων το μέγεθος είναι πέρα από την ικανότητα των τυπικών εργαλείων βάσης δεδομένων να συλλαμβάνουν, να αποθηκεύουν διαχειρίζονται και να αναλύουν. Ένας δημοφιλής χαρακτηρισμός ορίζει τα μεγάλα δεδομένα σύμφωνα με τα ακόλουθα χαρακτηριστικά: ταχύτητα, αλήθεια, ποικιλία και όγκο. Συγκεκριμένα, οι χαρακτηρισμοί των μεγάλων δεδομένων είναι τεχνικοί, με βάση τη φύση των δεδομένων (McKendrick, 2019).

Οι επικαλυπτόμενες μέθοδοι ενδιαφέροντος είναι κυρίως εκείνες που χρησιμοποιούν τη μηχανική μάθηση για να δημιουργήσουν μοντέλα με βάση τα δεδομένα και στη συνέχεια κάνουν συμπεράσματα από αυτά τα μοντέλα. Αυτές οι μέθοδοι είναι κατά κάποιο τρόπο μια στενότερη περιοχή ενδιαφέροντος από τα μεγάλα δεδομένα, η οποία μπορεί επίσης να περιλαμβάνει τη χρήση μεγάλων συνόλων δεδομένων για αναζήτηση και ανάλυση από

ανθρώπινους χειριστές που δομούν συγκεκριμένα ερωτήματα. Τα δεδομένα που αναλύονται και ο τύπος των αναλύσεων είναι σε κάποιο βαθμό άρρηκτα συνδεδεμένα και αυτό συχνά προκαλεί σύγχυση μεταξύ της τεχνητής νοημοσύνης και των αναλυτικών στοιχείων μεγάλων δεδομένων. Οι αλγόριθμοι που υποστηρίζουν προγνωστικά μοντέλα αυτοπρογραμματίζονται με βάση την έκθεση σε δεδομένα. Σε πολλές περιπτώσεις, θα ήταν αδύνατο να αναλυθούν τα δεδομένα χωρίς μια τέτοια προσέγγιση, όσο θα ήταν αδύνατο να κατασκευαστούν τα μοντέλα χωρίς τα δεδομένα. Τα μεγάλα δεδομένα χρειάζονται την τεχνητή νοημοσύνη για να ερμηνευτούν ενώ η τεχνητή νοημοσύνη χρειάζεται συχνά μεγάλα δεδομένα για να δημιουργηθεί και να βελτιωθεί (McKendrick, 2019).

Οι εξελίξεις σε άλλους τομείς της τεχνητής νοημοσύνης σημαίνουν ότι η βελτίωση της ακρίβειας των προβλέψεων μπορεί να γίνει όλο και πιο σημαντική, τόσο για την αποτελεσματική αντιτρομοκρατική πρόληψη όσο και για να σταματήσει η διάβρωση της ιδιωτικής ζωής. Η μείωση του κόστους της τεχνολογίας και της αποθήκευσης δεδομένων έχει εξαλείψει οικονομικά ή πρακτικά αντικίνητρα για τη διενέργεια επιτήρησης. Η τεχνολογία αναγνώρισης προσώπου, για παράδειγμα, μπορεί να επιτρέψει την πλήρη αυτοματοποίηση της παρακολούθησης με χρήση CCTV σε δημόσιους χώρους στο εγγύς μέλλον. Η ανάλυση κειμένου που βασίζεται στην τεχνητή νοημοσύνη θα μπορούσε να χρησιμοποιηθεί για την κατανόηση του περιεχομένου των ιδιωτικών μηνυμάτων χωρίς να απαιτείται η προσοχή ενός ανθρώπινου αναλυτή (McKendrick, 2019).

Κατ' αρχήν, το επίπεδο αιτιολόγησης που απαιτείται για την έγκριση της δραστηριότητας επιτήρησης πρέπει να παραμένει το

ίδιο, ανεξάρτητα από τις πρακτικές δυνατότητες ή τις τεχνικές δυνατότητες. Παρά το γεγονός αυτό, δεν είναι σωστό να μην αναγνωρίζεται ότι η δυνατότητα επέκτασης της επιτήρησης μπορεί να οδηγήσει σε πολλά προβλήματα. Η ανυπαρξία πρακτικών περιορισμών στη διεξαγωγή της επιτήρησης σημαίνει ότι το ζήτημα του τρόπου με τον οποίο η επιτήρηση απευθύνεται σε άτομα με νόμιμο ενδιαφέρον πληροφοριών, αντί να εφαρμόζεται αδιάκριτα, μπορεί να γίνει όλο και πιο επίκαιρο. Στο εγγύς μέλλον, επομένως, η καλή πρόβλεψη σχετικά με το ποιος ή τι πρέπει να παρακολουθείται θα μπορούσε να έχει κεντρικό ρόλο στον περιορισμό της κατάχρησης των τεχνικών μέσων επιτήρησης.

Ο τρόπος με τον οποίο χρησιμοποιείται σήμερα η τεχνητή νοημοσύνη στην πρόληψη και στην αντιμετώπιση της τρομοκρατίας δείχνει ότι η ευθύνη βαρύνει ένα ευρύ φάσμα φορέων, κυρίως με βάση τον ρόλο τους ως θεματοφύλακες δεδομένων. Οι κυβερνήσεις ενδέχεται να αγοράσουν δεδομένα που τις βοηθούν να διατηρήσουν την ασφάλεια εάν δεν είναι σε θέση να τα λάβουν νόμιμα με άλλα μέσα, όπως η παρακολούθηση τηλεπικοινωνιών. Ενώ ορισμένες εταιρείες τεχνολογίας έχουν αποκλείσει ρητά τις κυβερνήσεις από τη χρήση δεδομένων από τις πλατφόρμες τους, αυτά τα ίδια δεδομένα παραμένουν διαθέσιμα σε τρίτες εταιρείες. Ως εκ τούτου, τέτοιες ρυθμίσεις έχουν κυρίως ρητορική αξία. Ο πραγματισμός σχετικά με την πρόσβαση σε μεγάλες αγορές οδηγεί τις εταιρείες τεχνολογίας να εγκαταλείψουν τις δηλωμένες αρχές τους σε ορισμένα κράτη όπου η ιδιωτικότητα και η ελευθερία των χρηστών κινδυνεύουν περισσότερο. Επιπλέον, υπάρχει περιορισμένη διαφάνεια ως προς το πού και πότε το κάνουν αυτό. Σε χώρες όπου υπάρχει μεγαλύτερος κυβερνητικός έλεγχος της ιδιωτικής βιομηχανίας, υπάρχουν απεριόριστες ευκαιρίες για τις κυβερνήσεις να συλλέγουν και να

αναλύουν προσωπικές ή ευαίσθητες πληροφορίες σχετικά με τα θέματα τους (McKendrick, 2019).

### **Κεφάλαιο 3. Μελέτες περίπτωσης**

#### **3.1. Αμερική**

Οι αιτήσεις για Ποινική Δικαιοσύνη και Δημόσια Ασφάλεια μέσω της τεχνητής νοημοσύνης διερευνώνται ως πόροι δημόσιας ασφάλειας με πολλούς τρόπους. Μία συγκεκριμένη εφαρμογή τεχνητής νοημοσύνης - αναγνώριση προσώπου - μπορεί να βρεθεί παντού τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Αναλυτές για παράδειγμα, συχνά βασίζονται σε εικόνες προσώπου που βοηθούν στον προσδιορισμό της ταυτότητας ενός ατόμου. Η εξέταση του τεράστιου όγκου πιθανώς σχετικών εικόνων και βίντεο με ακριβή και έγκαιρο τρόπο είναι μια χρονοβόρα, επίπονη εργασία, με πιθανότητα ανθρώπινου λάθους λόγω κόπωσης και άλλων παραγόντων. Σε αντίθεση με τους ανθρώπους, οι μηχανές δεν κουράζονται. Μέσα από πρωτοβουλίες όπως το έργο IntelligenceAdvancedResearchProjectsActivity'sJanuscomputer-visionproject, οι αναλυτές πραγματοποιούν δοκιμές στη χρήση αλγορίθμων και μπορούν να μάθουν πώς να διακρίνουν ένα άτομο

από ένα άλλο χρησιμοποιώντας τα χαρακτηριστικά του προσώπου με τον ίδιο τρόπο όπως ένας άνθρωπος αναλυτής. Το Υπουργείο Μεταφορών των ΗΠΑ επιδιώκει επίσης να αυξήσει τη δημόσια ασφάλεια μέσω της έρευνας, της ανάπτυξης και της δοκιμής αυτόματης ανίχνευσης τροχαίων ατυχημάτων με βάση τα βίντεο για τη διατήρηση της ασφαλούς και αποτελεσματικής κυκλοφορίας των επιβατών σε διάφορες τοποθεσίες και καιρικές συνθήκες, φωτισμό και συνθήκες κυκλοφορίας (Rigano, 2019).

Χρησιμοποιούνται αλγόριθμοι τεχνητής νοημοσύνης στην ιατρική για την ερμηνεία ακτινολογικών εικόνων, οι οποίες θα μπορούσαν να έχουν σημαντικές επιπτώσεις στην κοινότητα της ποινικής δικαιοσύνης και των ιατρικών εξεταστών κατά τον προσδιορισμό της αιτίας και του τρόπου θανάτου. Αλγόριθμοι τεχνητής νοημοσύνης έχουν επίσης διερευνηθεί σε διάφορους κλάδους της ιατροδικαστικής επιστήμης, συμπεριλαμβανομένης της ανάλυσης DNA. Η τεχνητή νοημοσύνη είναι επίσης γίνεται γρήγορα μια σημαντική τεχνολογία στον εντοπισμό απάτης. Στο διαδίκτυο εταιρείες όπως το PayPal γλιτώνουν από προσπάθειες απάτης χρησιμοποιώντας όγκους δεδομένων για να εκπαιδεύουν συνεχώς τους αλγόριθμους ανίχνευσης απάτης για να προβλέπουν και να αναγνωρίζουν μη φυσιολογικά πρότυπα και να μαθαίνουν να αναγνωρίζουν νέα μοτίβα (Rigano, 2019).

Η ανάλυση βίντεο και εικόνας χρησιμοποιείται στην ποινική δικαιοσύνη και τις κοινότητες επιβολής του νόμου για τη λήψη πληροφοριών σχετικά με άτομα, αντικείμενα και ενέργειες για την υποστήριξη ποινικών ερευνών. Ωστόσο, η ανάλυση των πληροφοριών βίντεο και εικόνας είναι πολύ απαιτητική και απαιτεί σημαντική επένδυση σε προσωπικό με εξειδίκευση σε θέματα. Η

ανάλυση βίντεο και εικόνας είναι επίσης επιρρεπής στο ανθρώπινο λάθος λόγω του τεράστιου όγκου πληροφοριών, του γρήγορου ρυθμού αλλαγής τεχνολογιών όπως τα smartphone και τα λειτουργικά συστήματα και ενός περιορισμένου αριθμού εξειδικευμένου προσωπικού με τη γνώση να επεξεργάζεται τέτοιες πληροφορίες. Οι τεχνολογίες τεχνητής νοημοσύνης παρέχουν την ικανότητα να ξεπερνούν τέτοια ανθρώπινα λάθη και να λειτουργούν ως ειδικοί. Οι παραδοσιακοί αλγόριθμοι λογισμικού βοηθούν τους ανθρώπους να περιορίζονται σε προκαθορισμένα χαρακτηριστικά όπως το σχήμα των ματιών, το χρώμα των ματιών και η απόσταση μεταξύ των ματιών για αναγνώριση προσώπου ή δημογραφικά στοιχεία για ανάλυση προτύπων. Οι αλγόριθμοι βίντεο και εικόνας τεχνητής νοημοσύνης όχι μόνο μαθαίνουν πολύπλοκες εργασίες αλλά επίσης αναπτύσσουν και καθορίζουν τις δικές τους ανεξάρτητες σύνθετες δυνατότητες/ παραμέτρους αναγνώρισης προσώπου για την επίτευξη αυτών των εργασιών, πέρα από αυτό που οι άνθρωποι μπορούν να κάνουν. Αυτοί οι αλγόριθμοι έχουν τη δυνατότητα να ταιριάζουν πρόσωπα, να εντοπίζουν όπλα και άλλα αντικείμενα και να ανιχνεύουν πολύπλοκα γεγονότα όπως ατυχήματα και εγκλήματα (σε εξέλιξη ή μετά από αυτό) (Rigano, 2019).

Ανταποκρινόμενη στις ανάγκες των κοινοτήτων ποινικής δικαιοσύνης και επιβολής του νόμου, οι ΗΠΑ έχουν επενδύσει σε διάφορους τομείς για τη βελτίωση της ταχύτητας, της ποιότητας και της ιδιαιτερότητας της συλλογής δεδομένων, της απεικόνισης και της ανάλυσης για τη βελτίωση των πληροφοριών. Για παράδειγμα, για να κατανοήσουν τα πιθανά οφέλη της τεχνητής νοημοσύνης από την άποψη της ταχύτητας, οι ερευνητές στο Πανεπιστήμιο του Τέξας στο Ντάλας, με χρηματοδότηση από την NIJ και σε συνεργασία με το FBI και το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας, αξιολογούν

την αναγνώριση προσώπου από ανθρώπους και εξετάζουν μεθόδους για αποτελεσματική σύγκριση αλγορίθμων τεχνητής νοημοσύνης και ειδικών εξεταστών προσώπου. Τα προκαταρκτικά αποτελέσματα δείχνουν ότι όταν οι ερευνητές περιορίζουν τον χρόνο αναγνώρισης στα 30 δευτερόλεπτα, οι αλγόριθμοι αναγνώρισης προσώπου που βασίζονται στην τεχνητή νοημοσύνη αναπτύχθηκαν το 2017 και συγκρίνονται με τους εξεταστές προσώπου (Rigano, 2019).

Επιπλέον, σε απάντηση της ανάγκης για πληροφορίες υψηλότερης ποιότητας και τη δυνατότητα αποτελεσματικότερης χρήσης εικόνων χαμηλότερης ποιότητας, το Πανεπιστήμιο CarnegieMellon χρησιμοποιεί χρηματοδότηση από την NIJ για την ανάπτυξη αλγορίθμων τεχνητής νοημοσύνης για τη βελτίωση της ανίχνευσης και αναγνώρισης. Μια ιδιαίτερα σημαντική πτυχή είναι η εργασία του πανεπιστημίου σε εικόνες στις οποίες το πρόσωπο ενός ατόμου είναι τραβηγμένο σε διαφορετικές γωνίες ή εν μέρει στο πλάι, και όταν το άτομο κοιτάζει μακριά από την κάμερα, καλύπτεται από μάσκες ή κράνη ή είναι μπλοκαρισμένο από φωτισμό. Οι ερευνητές εργάζονται επίσης με την κατασκευή εικόνας προσώπου χαμηλής ποιότητας, συμπεριλαμβανομένων εικόνων με κακή ανάλυση και χαμηλά επίπεδα φωτισμού περιβάλλοντος, όπου η ποιότητα της εικόνας καθιστά δύσκολη την αντιστοίχιση του προσώπου. Το κέντρο δοκιμών και αξιολόγησης της NIJ δοκιμάζει και αξιολογεί αυτούς τους αλγόριθμους (Rigano, 2019).

Τέλος, για να αποκρυπτογραφήσουν μια πινακίδα κυκλοφορίας (που θα μπορούσε να βοηθήσει στον εντοπισμό ενός υπόπτου ή να βοηθήσει σε μια έρευνα) ή να αναγνωρίσουν ένα άτομο σε εικόνες ή βίντεο εξαιρετικά χαμηλής ποιότητας, οι ερευνητές στο DartmouthCollege χρησιμοποιούν αλγόριθμους



τεχνητής νοημοσύνης που υποβαθμίζουν συστηματικά εικόνες υψηλής ποιότητας και συγκρίνουν με χαμηλής ποιότητας για καλύτερη αναγνώριση εικόνας και βίντεο χαμηλότερης ποιότητας. Για παράδειγμα, οι καθαρές εικόνες αριθμών και γραμμάτων υποβαθμίζονται αργά για να μιμηθούν εικόνες χαμηλής ποιότητας. Οι υποβαθμισμένες εικόνες στη συνέχεια εκφράζονται και καταλογίζονται ως μαθηματικές αναπαραστάσεις. Αυτές οι υποβαθμισμένες μαθηματικές αναπαραστάσεις μπορούν στη συνέχεια να συγκριθούν με εικόνες πινακίδων χαμηλής ποιότητας για να βοηθήσουν στην αναγνώριση της πινακίδας κυκλοφορίας (Rigano, 2019).

Οι αλγοριθμικές αποφάσεις όμως μπορούν να δημιουργούν διακρίσεις, για παράδειγμα όταν το σύστημα αναπτύσσεται από ανθρώπινες αποφάσεις που εισάγουν διακρίσεις. Ένα διαβόητο παράδειγμα ενός αλγοριθμικού συστήματος με διακριτικά αποτελέσματα είναι το COMPAS, το οποίο σημαίνει το "CorrectionalOffendManagementProfiling for Alternativesections". Το COMPAS χρησιμοποιείται στις ΗΠΑ για να προβλέψει εάν οι κατηγορούμενοι θα διαπράξουν ξανά έγκλημα. Το COMPAS έχει σκοπό να βοηθήσει τους δικαστές να καθορίσουν εάν πρέπει να επιτραπεί σε κάποιον να εκτίσει την ποινή του με επίβλεψη εκτός φυλακής. Το COMPAS δεν χρησιμοποιεί εθνοτική προέλευση ή χρώμα δέρματος ως δεδομένα. Ωστόσο, η έρευνα των Angwinetal. (2016) έδειξε ότι το COMPAS είναι προκατειλημμένο κατά των μαύρων. Οι μαύροι έχουν σχεδόν τη διπλάσια πιθανότητα από τους λευκούς να χαρακτηριστούν υψηλότερος κίνδυνος ενώ οι λευκοί είναι πολύ πιο πιθανό από τους μαύρους να χαρακτηρίζονται με χαμηλότερο κίνδυνο, αλλά συνεχίζουν να διαπράττουν και άλλα εγκλήματα.

### 3.2. Βρετανία

Στο Ηνωμένο Βασίλειο, οι εκτιμήσεις έθεσαν τον ετήσιο αντίκτυπο του οργανωμένου εγκλήματος σε 37 δισεκατομμύρια λίρες (Fell et al., 2019), ενώ στην Αυστραλία μελέτες κατέληξαν στο συμπέρασμα ότι οι εκτιμήσεις μπορούν να κυμαίνονται μεταξύ 23,8 δισεκατομμυρίων δολαρίων έως 47,4 δισεκατομμύρια δολαρίων, ανάλογα με τον τρόπο υπολογισμού τους. Αυτά τα υψηλότερα κόστη περιλαμβάνουν εκτιμήσεις του κόστους για την επιβολή του νόμου, το σύστημα ποινικής δικαιοσύνης, άλλες κυβερνητικές υπηρεσίες, τον ιδιωτικό τομέα και τις κοινότητες. Φυσικά, αυτές οι εκτιμήσεις είναι μόνο εκτιμήσεις, δεδομένου ότι η ίδια η φύση του οργανωμένου εγκλήματος είναι να κρύβει τις δραστηριότητες και τα οικονομικά του. Ωστόσο, παρόλο που οι ορισμοί της έννοιας, το εύρος των δραστηριοτήτων και η μέθοδος υπολογισμού του κόστους και των ζημιών ποικίλλουν, υπάρχουν ολοένα και περισσότερα στοιχεία ότι το οργανωμένο έγκλημα είναι ένα σημαντικό οικονομικό, πολιτικό και κοινωνικό πρόβλημα.

Στον κόσμο της επιβολής του νόμου, το Durham Constabulary έγινε η πρώτη αστυνομική δύναμη στο Ηνωμένο Βασίλειο που εφάρμοσε ένα σύστημα μηχανικής μάθησης για να εκτιμήσει τον κίνδυνο εκ νέου παράβασης ατόμων. Αλγοριθμικά εργαλεία χρησιμοποιούνται εδώ και αρκετά χρόνια αλλού στο σύστημα ποινικής δικαιοσύνης, όπως το σύστημα αξιολόγησης των παραβατών, ένα στατιστικό μοντέλο που χρησιμοποιείται από το Υπουργείο Δικαιοσύνης για την πρόβλεψη κινδύνου εκ νέου παράβασης. Ωστόσο, αυτή είναι η πρώτη φορά που εφαρμόζονται μέθοδοι μηχανικής μάθησης σε τέτοια μοντέλα προκειμένου να

βοηθήσουν τη λήψη αποφάσεων από την αστυνομία, αντιπροσωπεύοντας μια σημαντική εξέλιξη στη χρήση δεδομένων από την αστυνομία. Η εκτίμηση του κινδύνου εκ νέου παράβασης αποτελεί βασική ευθύνη των αστυνομικών καθώς αυτή η απόφαση καθορίζει ποιες περαιτέρω ενέργειες θα ληφθούν εναντίον ενός συλληφθέντος. Προς το παρόν, αυτές οι αποφάσεις βασίζονται σε ένα κλινικό μοντέλο πρόβλεψης κινδύνου, βασισμένο στην επαγγελματική κρίση του ανθρώπου αστυνομικού (Babuta, 2018).

Η ενσωμάτωση στατιστικών μεθόδων στη διαδικασία εκτίμησης κινδύνου έχει τη δυνατότητα να βελτιώσει την ακρίβεια αυτών των κρίσεων: η έρευνα σε ένα ευρύ φάσμα τομέων έχει δείξει με συνέπεια ότι οι στατιστικές προβλέψεις είναι τυπικά πιο ακριβείς στην πρόβλεψη του μελλοντικού κινδύνου από ό, τι η κλινική κρίση και μόνο. Σύμφωνα με στατιστικά στοιχεία του Υπουργείου Δικαιοσύνης, το 2016 το συνολικό ποσοστό παραβάσεων στην Αγγλία και την Ουαλία ήταν 29,6% (42,3% για ανήλικους). Καθώς τα επαναλαμβανόμενα αδικήματα αντιπροσωπεύουν ένα μεγάλο μέρος όλων των εγκλημάτων, η ανάπτυξη ενός συστήματος για τον ακριβέστερο προσδιορισμό αυτών που είναι πιο πιθανό να γίνουν ξανά στο μέλλον θα επέτρεπε στις αστυνομικές δυνάμεις να λαμβάνουν με συνέπεια τις κατάλληλες αποφάσεις κράτησης, με αποτέλεσμα τη απτή μείωση των συνολικών ποσοστών εγκληματικότητας (Babuta, 2018).

Το εργαλείο κινδύνου εκτίμησης βλαβών του Durham Constabulary (HART) προβλέπει τον κίνδυνο εκ νέου παράβασης ενός ατόμου με βάση 34 μεταβλητές, οι περισσότερες από τις οποίες σχετίζονται με προηγούμενο εγκληματικό ιστορικό. Το μοντέλο χρησιμοποιεί τυχαία πρόβλεψη (μια κοινή τεχνική

μηχανικής μάθησης) για να εκτιμήσει την πιθανότητα ενός ατόμου να διαπράξει σοβαρό αδίκημα, μη σοβαρό αδίκημα ή κανένα αδίκημα κατά τους επόμενους 24 μήνες. Με βάση αυτήν την πρόβλεψη, τα άτομα ταξινομούνται στη συνέχεια σε ομάδες υψηλού, μέτριου ή χαμηλού κινδύνου. Εάν συγκεκριμένες μειονότητες έχουν στοχοποιηθεί δυσανάλογα από αστυνομικές ενέργειες στο παρελθόν, ο αλγόριθμος μπορεί να εκτιμήσει εσφαλμένα τα άτομα αυτά ότι ενέχουν αυξημένο κίνδυνο στο μέλλον. Οι στατιστικές μέθοδοι που βασίζονται στη μηχανική μάθηση είναι σε θέση να λαμβάνουν υπόψη τον τεράστιο όγκο δεδομένων ενός παραβάτη που διατηρεί η αστυνομία παράγοντας πολύ περισσότερες πληροφορίες από όσες θα μπορούσε ποτέ να επεξεργαστεί ένας αστυνομικός. Ο αλγόριθμος HART, για παράδειγμα, εκπαιδεύτηκε χρησιμοποιώντας δεδομένα πενταετούς φύλαξης, συνολικά περίπου 104.000 ατόμων. Μέθοδοι όπως η τυχαία πρόβλεψη μπορούν να εξισορροπήσουν το διαφορετικό κόστος των σφαλμάτων με τρόπο που οι παραδοσιακές μέθοδοι πρόβλεψης δεν το κάνουν, και ως εκ τούτου είναι ιδιαίτερα επιθυμητές στο αστυνομικό περιβάλλον, όπου οι συνέπειες των σφαλμάτων μπορεί να είναι πολύ σοβαρές (Babuta, 2018).

Σύμφωνα με τα γραπτά στοιχεία που υποβλήθηκαν στην Επιτροπή Επιστήμης και Τεχνολογίας της Βουλής των Κοινοτήτων, το μοντέλο HART είναι προδιατεθειμένο να ευνοήσει τα ψευδώς θετικά έναντι των ψευδώς αρνητικών- δηλαδή είναι πιο πιθανό να ταξινομήσει εσφαλμένα ένα άτομο χαμηλού κινδύνου ως υψηλό κίνδυνο, καθώς αυτό το σφάλμα θεωρείται λιγότερο επιβλαβές από την εσφαλμένη ταξινόμηση ατόμων υψηλού κινδύνου ως χαμηλού κινδύνου. Οι προγραμματιστές του HART τονίζουν ότι ο αλγόριθμος χρησιμοποιείται μόνο για να υποστηρίξει τη διαδικασία λήψης

αποφάσεων των υπαλλήλων επιτήρησης ανθρώπων αλλά ο αξιωματικός διατηρεί την τελική ευθύνη για να αποφασίσει ποιες περαιτέρω ενέργειες πρέπει να γίνουν βάσει της αξιολόγησης. Τα μηχανήματα δεν θα αντικαταστήσουν τους αστυνομικούς σύντομα, τουλάχιστον όχι στο Ηνωμένο Βασίλειο. Ωστόσο, η εφαρμογή αλγοριθμικών εργαλείων αξιολόγησης κινδύνου για την αστυνόμευση έχει εκτεταμένες νομικές και ηθικές επιπτώσεις, ιδιαίτερα όταν λάβουμε υπόψη τον τρόπο με τον οποίο αυτή η τεχνολογία είναι πιθανό να αναπτυχθεί τα επόμενα χρόνια. Ιδιαίτερα ανησυχητικό από την άποψη αυτή είναι ο κίνδυνος μεροληψίας, η διαφάνεια της διαδικασίας λήψης αποφάσεων και η λογοδοσία του λήπτη αποφάσεων (Babuta, 2018).

Αυτή η επιλογή μπορεί τελικά να καταλήξει στη νομιμότητα. Στο Ηνωμένο Βασίλειο, ο νόμος για την ισότητα του 2010 και το άρθρο 14 του νόμου για τα ανθρώπινα δικαιώματα του 1998 καθιστούν παράνομη τη διάκριση σε βάρος ενός ατόμου για ευρύ φάσμα λόγων, συμπεριλαμβανομένου του φύλου, της φυλής, της θρησκείας και του σεξουαλικού προσανατολισμού. Εάν μπορεί να αποδειχθεί ότι οι αλγόριθμοι αστυνόμευσης παράγουν αποτελέσματα που δεν ευνοούν ορισμένες ομάδες ατόμων λόγω φυλής οι προγραμματιστές δεν έχουν άλλη επιλογή παρά να αφαιρέσουν όλες τις μεταβλητές που συμβάλλουν σε αυτήν την προκατάληψη. Για πολλούς, το γεγονός ότι τέτοια συστήματα μπορούν να ενισχύσουν τη φυλετική προκατάληψη είναι αρκετός λόγος για να αποκλείσει τη χρήση τους στην αστυνόμευση και ποινική δικαιοσύνη. Αλλά αντί να απορρίψουμε τον αλγόριθμο εντελώς, μια πιο κατάλληλη απάντηση μπορεί να είναι η αμφισβήτηση των πρακτικών που στηρίζουν τη συλλογή δεδομένων. Άλλωστε, ο αλγόριθμος δεν είναι η πηγή της προκατάληψης. Είναι τα

δεδομένα που είναι προκατειλημμένα και ο αλγόριθμος απλώς αντικατοπτρίζει τις εγγενείς προκαταλήψεις στο σύνολο δεδομένων. Αυτές οι νέες δυνατότητες θα μπορούσαν επομένως να δώσουν μια εικόνα για τους περιορισμούς των υφιστάμενων πρακτικών αστυνόμευσης, φωτίζοντας τις μεθόδους που ενδέχεται να εισάγουν διακρίσεις, οι οποίες θα ενθάρρυναν τις αστυνομικές δυνάμεις να επανεκτιμήσουν εάν οι ενέργειές τους στοχεύουν κατά λάθος σε μειονοτικές ομάδες. Συνεπώς, η ανησυχία δεν πρέπει να είναι ο κίνδυνος προκατειλημμένων αλγορίθμων που οδηγούν τους αστυνομικούς στη λήψη ακατάλληλων αποφάσεων, αλλά μάλλον ο κίνδυνος ακατάλληλων πρακτικών αστυνόμευσης που οδηγούν τους αλγόριθμους να κάνουν προκατειλημμένες προβλέψεις (Babuta, 2018).

### **3.3. Ευρώπη**

Το 2014, η έκθεση του Γραφείου της Ύπατης Αρμοστείας των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα (OHCHR) σχετικά με το δικαίωμα στην ιδιωτικότητα στην ψηφιακή εποχή παρατήρησε ότι τα παραδείγματα της ανοιχτής και κρυφής ψηφιακής επιτήρησης σε δικαιοδοσίες σε όλο τον κόσμο έχουν πολλαπλασιαστεί και η επιτήρηση αναδύεται ως επικίνδυνη συνήθεια και όχι ως έκτακτο μέτρο. Η τεχνητή νοημοσύνη θα μπορούσε να χρησιμοποιηθεί για τη διευκόλυνση της μαζικής επιτήρησης. Οι πρόσφατες εξελίξεις στην ανάλυση βίντεο και την επεξεργασία δείχνουν ότι οι μελλοντικές τεχνολογίες είναι πιθανό να το καταστήσουν αυτό ακόμη πιο δυνατό με δυνητικά χαμηλότερο κόστος. Όσον αφορά τους ειδικούς τομεακούς κανονισμούς σχετικά με τη χρήση της τεχνητής νοημοσύνης για τη δημόσια ασφάλεια, δεν έχει βρεθεί ακόμη

συναίνεση σχετικά με το πού θα πρέπει να ληφθεί υπόψη η χρήση αυτών των τεχνολογιών, είτε πρόκειται για υπηρεσίες πληροφοριών και ασφάλειας, την επιβολή του νόμου ή τον ιδιωτικό τομέα(McKendrick, 2019).

Ορισμένα από τα δικαιώματα και τις ελευθερίες που διακυβεύονται αναπτύσσονται στην Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων και παγιώνονται σε συνθήκες όπως το Διεθνές Σύμφωνο για τα Πολιτικά και Πολιτικά Δικαιώματα (ICCPR) που υιοθετήθηκε το 1966 και ισχύει από το 1976. Το ICCPR έχει παγκόσμια εμβέλεια. Προστατεύει τα δικαιώματα στην ιδιωτικότητα, την ελευθερία της σκέψης και της θρησκείας, της έκφρασης και της σύνδεσης μετά από ψήφισμα της Γενικής Συνέλευσης των Ηνωμένων Εθνών για το δικαίωμα στην ιδιωτικότητα στην ψηφιακή εποχή. Αυτό το ψήφισμα βάζει το βάρος στα κράτη να διασφαλίσουν ότι οι δραστηριότητές τους συμμορφώνονται με το διεθνές δίκαιο, αλλά οι διαφορετικές ερμηνείες εννοιών όπως η αυθαίρετη ή ακόμη και παράνομη παρέμβαση στην ιδιωτική ζωή ενός ατόμου σημαίνει ότι το ψήφισμα είναι σχετικά αδύναμο ως δεσμευτικός κανόνας (McKendrick, 2019).

Οι περιφερειακές συνθήκες προστασίας των δικαιωμάτων χρησιμεύουν για την ενίσχυση αυτών σε ορισμένους τομείς, ιδίως σε περιπτώσεις όπου διέπουν την εξουσία υπερεθνικών δικαστηρίων. Εκτός από τους τομείς που καλύπτονται από τη δικαιοδοσία των δικαστηρίων με υπερεθνική εξουσία, υπάρχουν έλεγχοι κατά της κατάχρησης της τεχνητής νοημοσύνης και των τεράστιων αποθεμάτων δεδομένων στα οποία βασίζεται. Υπάρχουν μεγάλες παραλλαγές σε όλον τον κόσμο σε ό, τι θεωρείται αποδεκτή χρήση της τεχνητής νοημοσύνης, τόσο ως προς τις μεθόδους όσο και ως

προς τον σκοπό. Η μαζική συλλογή και διατήρηση μόνο των εγχώριων δεδομένων, για κάποια μορφή των οποίων η χρήση προγνωστικής τεχνητής νοημοσύνης πιθανόν να ήταν ενδεχόμενη, παραμένει ένα έντονα αμφισβητούμενο σημείο. Στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ), για παράδειγμα, υπάρχουν διάφορες εκκρεμείς υποθέσεις που υποστηρίζουν ότι κράτη όπως η Γερμανία, η Σουηδία και το Ηνωμένο Βασίλειο παραβιάζουν την Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα μέσω της υποκλοπής, της διατήρησης και της χρήσης μαζικών δεδομένων (McKendrick, 2019).

Διάφορα τα κράτη είχαν επίσης εξουσίες διατήρησης δεδομένων που καταργήθηκαν με αποφάσεις του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ). Για παράδειγμα, τον Δεκέμβριο του 2016 το ΔΕΕ αποφάσισε κατά του Νόμου του Ηνωμένου Βασιλείου για τη διατήρηση δεδομένων και τις εξουσίες διερεύνησης του 2014, δηλώνοντας ότι δεν πληρούν τα θεμελιώδη δικαιώματα που εγγυάται ο Χάρτης της ΕΕ. Νομικές προκλήσεις στη νομοθεσία για την αντικατάσταση - ο νόμος για τις ερευνητικές δυνάμεις 2016 - βρίσκονται ήδη σε εξέλιξη και οι αρχικές αντιρρήσεις έγιναν δεκτές από το εθνικό Ανώτατο Δικαστήριο που οδήγησε σε τροποποίηση της πράξης.

Η εξουσία πρόσβασης, συλλογής και αποθήκευσης των δεδομένων των πολιτών από την εποχή της πληροφορίας μπορεί να αντιπροσωπεύει μια αλλαγή στη σχέση μεταξύ κρατών και πολιτών και απαιτεί αναθεώρηση των μέτρων που αποσκοπούν στη διαφύλαξη όχι μόνο της ιδιωτικής ζωής, αλλά άλλων ελευθεριών κρίσιμων για τη δημοκρατική λειτουργία, όπως αυτές της έκφρασης και της σύνδεσης. Οι περαιτέρω εξελίξεις της ψηφιακής εποχής,



όπως η δυνατότητα αυτοματοποίησης μεγάλων τμημάτων της ανάλυσης αυτών των δεδομένων, επαναλαμβάνουν αυτήν την απαίτηση (McKendrick, 2019).

Η προγνωστική τεχνητή νοημοσύνη θα βασιστεί στην ανάλυση δεδομένων που ανήκουν στο ευρύ κοινό για να διακρίνει την ύποπτη από την κανονική συμπεριφορά ή για να διακρίνει τάσεις που θα μπορούσαν να βοηθήσουν στην πρόβλεψη επιθέσεων. Η συντριπτική πλειοψηφία των δεδομένων που αναλύονται θα δημιουργηθούν από άτομα που δεν ενδιαφέρουν τις υπηρεσίες πληροφοριών. Εξαιτίας αυτού, ένας από τους συγκεκριμένους τομείς ανησυχίας που συνδέονται με την τεχνολογία πρόβλεψης τεχνητής νοημοσύνης θα ήταν ότι αποτελεί ένα μέτρο επιτήρησης που εφαρμόζεται σε ολόκληρο τον πληθυσμό και ότι θα το καθιστούσε αδιάκριτο και ως εκ τούτου εγγενώς δυσανάλογο. Αυτό ήταν επίσης ένα επίκεντρο αντιρρήσεων για τα προγράμματα μαζικής συλλογής και ανάλυσης δεδομένων των κρατών. Παρόλο που τέτοια προγράμματα δεν συνδέονται άμεσα με τη χρήση τεχνητής νοημοσύνης, η χρήση προγνωστικής τεχνητής νοημοσύνης για την αντιμετώπιση της τρομοκρατίας είναι πιθανό να βασίζεται στην ικανότητα συλλογής και ανάλυσης δεδομένων μαζικά. Ακόμη και η συλλογή και ανάλυση φαινομενικά μη ευαίσθητων δεδομένων μπορεί να δημιουργήσει σημαντική παρέμβαση στο απόρρητο (McKendrick, 2019).

Το ψήφισμα 68/167 της Γενικής Συνέλευσης των Ηνωμένων Εθνών για το δικαίωμα στην ιδιωτικότητα στην ψηφιακή εποχή περιγράφει την παράνομη ή αυθαίρετη συλλογή δεδομένων προσωπικού χαρακτήρα ως μια εξαιρετικά παρεμβατική πράξη που θα μπορούσε να παραβιάσει τα δικαιώματα στην ιδιωτικότητα και την ελευθερία της έκφρασης και μπορεί να έρχεται σε αντίθεση με

τις αρχές μιας δημοκρατικής κοινωνίας. Αυτό οφείλεται στη μακροχρόνια αναγνώριση ότι από αυτές τις μορφές δεδομένων μπορούν να συναχθούν σημαντικές προσωπικές πληροφορίες, και ότι η συγκέντρωση και ανάλυση δεδομένων συνιστά παραβίαση της ιδιωτικής ζωής, ακόμη και αν οι ενέργειες γίνονται δημόσια. Συνεπώς, η διαμάχη παραμένει, ακόμη και αν τα σχετικά δεδομένα συλλέγονται από ανοιχτές πηγές (McKendrick, 2019).

Ορισμένα καταστατικά του διεθνούς δικαίου παρέχουν κατευθυντήριες γραμμές για την αξιολόγηση του εάν η παραβίαση της ιδιωτικής ζωής των δεδομένων είναι δικαιολογημένη. Το δικαίωμα στην προστασία της ιδιωτικής ζωής των δεδομένων προστατεύεται πιο συγκεκριμένα βάσει του άρθρου 8 του Χάρτη της ΕΕ και καλύπτεται επίσης από το δικαίωμα στην ιδιωτική ζωή γενικά στο άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα. Εξαιτίας αυτού, το ΔΕΕ και το ΕΔΔΑ έχουν εκδώσει και οι δύο σχετικές αποφάσεις. Και για τα δύο θεσμικά όργανα, η παρέμβαση πρέπει να πληροί ένα τριπλό κριτήριο για την εκπλήρωση ενός νόμιμου σκοπού, που υλοποιείται εντός νομικού πλαισίου και ικανοποιεί προϋποθέσεις αναγκαιότητας και αναλογικότητας και ότι δεν περιορίζει περισσότερα δικαιώματα από ό, τι είναι αναγκαίο, δεδομένης της εναλλακτικής επιλογής (McKendrick, 2019).

Μια επιχείρηση διαλογής που διεξήχθη στη Γερμανία σε μια προσπάθεια αναγνώρισης τρομοκρατικών κυττάρων παρέχει ένα παράδειγμα όπου μια μέθοδος που περιλαμβάνει την ανάλυση μαζικών δεδομένων υπολείπεται σε έλεγχο σχετικά με την ικανότητά της να επιτύχει έναν νόμιμο στόχο. Η λειτουργία διαλογής περιλάμβανε τη διασταύρωση μιας ομάδας ατόμων που

προσδιορίστηκαν χρησιμοποιώντας χαρακτηριστικά-όπως η θρησκευτική σχέση-με άλλες βάσεις δεδομένων. Θεωρήθηκε αντισυνταγματικό από το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας με την αιτιολογία ότι παρεμβαίνει στον πληροφοριακό αυτοπροσδιορισμό των ανθρώπων έναντι των οποίων δεν υπάρχει καμία υποψία ελλείψει συγκεκριμένης απειλής. Τα χαρακτηριστικά που χρησιμοποιήθηκαν για τον διαχωρισμό αυτών των ατόμων επιλέχθηκαν με βάση τις εντυπώσεις από τις τάσεις των προηγούμενων επιθέσεων, η οποία δεν ήταν μια αρκετά αυστηρή βάση τεκμηρίων (McKendrick, 2019).

Πιο πρόσφατες κρίσεις του ΕΔΔΑ ρίχνουν περαιτέρω φως στη νομιμότητα των συστημάτων μαζικής συλλογής και διατήρησης δεδομένων. Τον Σεπτέμβριο του 2018 το δικαστήριο διαπίστωσε ότι το Ηνωμένο Βασίλειο παραβίαζε το δικαίωμα στην ιδιωτική ζωή λόγω των ανεπαρκών εγγυήσεων και εποπτείας στο καθεστώς μαζικής συλλογής δεδομένων. Τον Ιούνιο του 2018 το ΕΔΔΑ έκρινε ότι η μαζική υποκλοπή ηλεκτρονικών σημάτων από τη Σουηδία δεν παρεμβαίνει υπερβολικά στο δικαίωμα των πολιτών στην ιδιωτικότητα, εν μέρει επειδή περιορίζεται στην επικοινωνία που διέρχεται τα σουηδικά σύνορα. Σε αυτή την περίπτωση, μια σχετικά ευρεία προϋπόθεση έγινε δεκτή ως αρκετά περιοριστική παρουσία ανεξάρτητων φορέων εποπτείας και σαφούς νομικού ορισμού (McKendrick, 2019).

Τα πλαίσια νομοθεσίας και διακυβέρνησης για τη χρήση των μαζικών δεδομένων τείνουν να επικεντρώνονται κυρίως στις εξουσίες πρόσβασης σε δεδομένα, με περιορισμένη περιγραφή του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν τα δεδομένα, ή τις συνακόλουθες εκτιμήσεις για το πώς προστατεύονται σωστά από

κακή χρήση. Χωρίς να δοθούν περισσότερες λεπτομέρειες σχετικά με τη χρήση δεδομένων, είναι δύσκολο να αποδειχθεί η αναγκαιότητα συνδέοντας σαφώς τη διατήρηση δεδομένων με κάτι που μπορεί να αποδειχθεί ότι είναι θεμιτός στόχος. Εάν η τεχνητή νοημοσύνη χρησιμοποιείται σε μεγαλύτερο βαθμό, το πλαίσιο στο οποίο χρησιμοποιείται πρέπει να αποδεικνύει - ή να εγγυάται διαφορετικά - τη συμβολή της σε έναν νόμιμο στόχο (McKendrick, 2019).

#### **Κεφάλαιο 4. Συμπεράσματα**

Η ανθρωπότητα βρίσκεται εν μέσω μιας τεχνολογικής επανάστασης, όχι λιγότερο σημαντικής από τη βιομηχανική επανάσταση του δέκατου όγδοου και του δέκατου ένατου αιώνα - της επανάστασης της τεχνητής νοημοσύνης. Η ανάπτυξη της τεχνητής νοημοσύνης σε συνδυασμό με άλλες τεχνολογικές εξελίξεις, στον τομέα της ρομποτικής, για παράδειγμα, πιθανότατα θα οδηγήσει στην εξάλειψη διαφόρων επαγγελμαμάτων. Η τεχνολογική επανάσταση της τεχνητής νοημοσύνης είχε σημαντικό και άμεσο αντίκτυπο (το οποίο είναι βέβαιο ότι θα αυξηθεί στο μέλλον) σε πολλούς τομείς ασφάλειας και πληροφόρησης, ιδίως όσον αφορά τη χρήση πληροφοριών με σκοπό την αποτροπή της τρομοκρατίας. Η χρήση μεγάλων δεδομένων στην αντιτρομοκρατική ξεκίνησε μετά τις επιθέσεις της 11ης Σεπτεμβρίου 2001 και έχει πάρει δυναμική τα τελευταία χρόνια ως αποτέλεσμα συνδυασμού πολλών διαδικασιών: τον ρυθμό τεχνολογικής ανάπτυξης και προόδου, την τεράστια εμπειρία που έχει συσσωρευτεί στη χρήση των μεγάλων δεδομένων για πολιτικούς σκοπούς και τα επιτεύγματα που έχει επιτύχει η

χρήση των μεγάλων δεδομένων στην προληπτική αστυνόμευση και την πρόληψη μελλοντικών εγκλημάτων (Ganor, 2021).

Καθώς οι αστυνομικές υπηρεσίες υιοθετούν πρακτικές όπως η ILP και στρέφονται στις τεχνικές της επιστήμης δεδομένων ως τρόπο μέτρησης, διαχείρισης και ελέγχου του εγκλήματος, βλέπουμε την ανάπτυξη της πληροφόρησης και του ρόλου του αναλυτή πληροφοριών για το έγκλημα (Belur & Johnson, 2018; Manning, 2008; Ratcliffe, 2016). Η ILP, και οι σχετικές πρακτικές που βασίζονται σε δεδομένα, επιδιώκουν να οδηγήσουν την αστυνόμευση στη χρήση προληπτικών και στρατηγικών προσεγγίσεων (Burcher & Whelan, 2018). Κεντρικό σημείο αυτής της τάσεως είναι η χρήση της εγκληματικής πληροφόρησης για την καθοδήγηση των οργανωτικών αποφάσεων (Guidette & Martinelli, 2009). Ως αποτέλεσμα της αυξανόμενης εξάρτησης από δεδομένα πληροφοριών σχετικά με το έγκλημα, έχουμε δει την επέκταση της απασχόλησης και την επαγγελματικοποίηση των αναλυτών εγκληματικών πληροφοριών (Cope, 2004; Innes et al., 2005; Sanders & Condon, 2017; Taylore et al., 2007).

Η γνώση έχει τη δυνατότητα να εξομοιωθεί με τη δύναμη. Η ιδέα της συλλογής και της χρήσης πληροφοριών για την υποστήριξη της λήψης αποφάσεων με κάποιο επίσημο, δομημένο τρόπο δεν είναι κάτι νέο. Για να αποκτηθεί πλεονέκτημα έναντι των αντιπάλων, είναι επιτακτική ανάγκη να υπάρχουν οι πιο ενημερωμένες, ακριβείς πληροφορίες σχετικά με τις προθέσεις των άλλων και τις δυνατότητές τους. Επιπλέον, είναι μια διαδικασία που εξακολουθεί να αναπτύσσεται και εξελίσσεται, ως απάντηση σε αλλαγές στους κοινωνικούς / πολιτιστικούς παράγοντες, στην τεχνολογία, στις

οργανωτικές ανάγκες και στα νέα / υψηλότερα επίπεδα αναλυτικής ικανότητας.

Η ανασκόπηση του ιστορικού υποβάθρου, οι «ρίζες» της πληροφόρησης και της ανάλυσης ως διαδικασία και ως επάγγελμα είναι μια χρήσιμη και σημαντική άσκηση. Η αύξηση της κατανόησής για την προέλευση της πληροφόρησης και της ανάλυσης μας βοηθά να κατανοήσουμε τόσο πού είμαστε τώρα όσο και πώς / γιατί φτάσαμε σε αυτό το σημείο. Αυξάνει επίσης την επίγνωση για το πώς η ανάλυση πληροφοριών είναι μία συνεχώς μεταβαλλόμενη, εξελισσόμενη πρακτική, η οποία αν θέλει να παραμείνει σχετική και χρήσιμη με πρακτική έννοια χρειάζεται συνεχώς μια νέα, ευέλικτη προσέγγιση, νέες ιδέες, νέες δεξιότητες, νέες τεχνικές.

Η συλλογή πληροφοριών από μόνη της δεν οδηγεί στην απόκτηση πληροφοριών. Οι πληροφορίες πρέπει να αξιολογούνται σωστά προτού μπορέσουν να χρησιμοποιηθούν. Η αξία της εγκληματικής πληροφόρησης μπορεί να ενισχυθεί περαιτέρω με ανάλυση. Όταν η διαθέσιμη πληροφόρηση είναι πολύ περίπλοκη και με μεγάλη ένταση για την απλή δράση, πρέπει να αναλυθεί για να επιτευχθούν ουσιαστικά αποτελέσματα.

Η έλευση της ανάλυσης εγκληματικών πληροφοριών σχετίζεται άμεσα με τη μετατροπή του ατομικού εγκλήματος σε οργανωμένο ή ομαδικό έγκλημα. Η αποτελεσματική χρήση πληροφοριών είναι ζωτικής σημασίας για την ικανότητα μιας υπηρεσίας επιβολής του νόμου να καταπολεμά εγκληματικές ομάδες. Η ανάλυση πληροφοριών παρέχει επίσης στον οργανισμό τις γνώσεις που απαιτούνται για την αποτελεσματική διαχείριση των πόρων του. Με την κατάλληλη εργασία, τα προϊόντα της ανάλυσης πληροφοριών μπορούν να βοηθήσουν στην ανάπτυξη στρατηγικών σχεδίων για την

αντιμετώπιση των τρεχόντων προβλημάτων και την προετοιμασία για μελλοντικά αναμενόμενα.

Η ανάλυση της εγκληματικής πληροφόρησης επιτρέπει στις αρχές επιβολής του νόμου να καθιερώσουν μια προληπτική αντίδραση στο έγκλημα. Τους επιτρέπει να εντοπίζουν και να κατανοούν εγκληματικές ομάδες που δραστηριοποιούνται στις περιοχές τους. Μόλις εντοπιστούν εγκληματικές ομάδες και γίνουν γνωστές οι συνήθειες τους, οι αρχές επιβολής του νόμου ενδέχεται να αρχίσουν να αξιολογούν τις τρέχουσες τάσεις του εγκλήματος στις προβλέψεις και να παρεμποδίσουν την ανάπτυξη αντιληπτών μελλοντικών εγκληματικών δραστηριοτήτων. Η πληροφόρηση παρέχει τη γνώση πάνω στην οποία βασίζονται οι αποφάσεις και επιλέγονται κατάλληλοι στόχοι για διερεύνηση. Ενώ η χρήση ανάλυσης εγκληματικών πληροφοριών είναι κατάλληλη για την υποστήριξη ερευνών, επιχειρήσεων επιτήρησης και δίωξης υποθέσεων, παρέχει επίσης στις υπηρεσίες επιβολής του νόμου τη δυνατότητα να διαχειρίζονται αποτελεσματικά τους πόρους, τον προϋπολογισμό και να ανταποκρίνονται στην ευθύνη τους για την πρόληψη του εγκλήματος.

Πολλοί ακαδημαϊκοί έχουν εξετάσει τον τρόπο με τον οποίο η ευρεία ψηφιακή επιτήρηση θα μπορούσε να προκαλέσει ζητήματα σε σχέση με ευαίσθητα πολιτικά ζητήματα ή δραστηριότητες, αντίθετη γνώμη και κριτική σκέψη, καθώς τα άτομα συμμορφώνονται με τα συλλογικά πρότυπα. Το ζήτημα απασχόλησε ομάδες κοινωνίας των πολιτών, ιδιαίτερα μετά τις αποκαλύψεις (που συνήθως αναφέρονται ως αποκαλύψεις του Σνόουντεν) το 2013 σχετικά με την κλίμακα των εθνικών προγραμμάτων επιτήρησης. Ενώ η αυτοματοποιημένη ανάλυση μπορεί να μειώσει την εισβολή της

ιδιωτικής ζωής σε ατομικό επίπεδο, δημιουργεί επίσης την πιθανότητα όλοι να αισθάνονται σαν να παρακολουθούνται ανά πάσα στιγμή. Εξαιτίας αυτού, η αυτοματοποιημένη ανάλυση θα μπορούσε να έχει υψηλότερο κόστος για άλλα δικαιώματα, όπως τα δικαιώματα έκφρασης και σύνδεσης.

Εξακολουθεί να υπάρχει σκεπτικισμός ως προς τις επιπτώσεις της παρακολούθησης στη διαδικτυακή δραστηριότητα, αν και μια σειρά από μελέτες έχουν επιχειρήσει να τα τεκμηριώσουν ως εμπειρικά παρατηρήσιμο φαινόμενο. Είναι αδύνατο να διαχωριστεί ο αντίκτυπος της παρακολούθησης κάθε αυτής με αυτόν των άλλων μέτρων που έχουν σχεδιαστεί για να προκαλούν φόβο και να επιβάλλουν αλλαγές στη συμπεριφορά των ανθρώπων. Οι υποστηρικτές της επίδρασης της επιτήρησης αναγνωρίζουν ότι δεν είναι δυνατό να προβλεφθεί ποια ακριβώς θα είναι η φύση αυτού του αποτελέσματος ή να μετρηθεί. Θα εναπόκειται στις κυβερνήσεις να προλάβουν αυτές τις πιθανές επιπτώσεις όταν σχεδιάσουν κατάλληλους νομικούς ελέγχους στη δραστηριότητα της επιτήρησης. Η αντιμετώπιση αυτής της μελλοντικής ανησυχίας μπορεί να απαιτήσει την ανάπτυξη μοντέλων που αξιολογούν τις ευρύτερες βλάβες των παραβιάσεων της ιδιωτικής ζωής με βάση τον κοινωνικό τους αντίκτυπο.



## Βιβλιογραφία

- Adam, B. & van Loon, J. (2000). Introduction. In Adam, B. & van Loon, J. (eds.). *Risk society and beyond: Critical issues for social theory*. New York: Prentice-Hall.
- Allen, A. (2016). The 'three black teenagers' search shows it is society, not Google, that is racist. *The Guardian*, 10.
- Angwin, J., Larson, J., Mattu, S. & Kirchner, L. (2016). Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. In <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner,
- Ayling, J., & Broadhurst, R. (2014). Organized crime control in Australia and New Zealand. *The Oxford handbook of organized crime*, 612-633.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *Calif. L. Rev.*, 104, 671.
- Babuta, A. (2018). Innocent until predicted guilty. *Artificial Intelligence and Police Decision-Making. Royal United Services Institute*, 38(2), 1-4.
- Bartels, L. (2010). A review of confiscation schemes in Australia. Canberra, ACT: Commonwealth of Australia.
- Barton, A., & Evans, R. (1999). Proactive policing on Merseyside: briefing note. Police Research Group: Police Research Series, 105, 1-2.

- Behlendorf, B., & Jacome, M. (2015). Failure points in smuggling networks: Final report. College Park, MD: START.
- Belur, J., & Johnson, S. (2018). Is crime analysis at the heart of policing practice? A case study. *Policing and society*, 28(7), 768-786.
- Borgatti, S. P. (2003, October). Identifying sets of key players in a network. In IEMC'03 Proceedings. Managing Technologically Driven Organizations: The Human Side of Innovation and Change (IEEE Cat. No. 03CH37502) (pp. 127-131). IEEE.
- Bouchard, M. (2007). On the resilience of illegal drug markets. *Global crime*, 8(4), 325-344.
- Bouchard, M. (2020). Collaboration and boundaries in organized crime: A network perspective. *Crime and Justice*, 49(1), 425-469.
- Bright, D. A. (2015). Disrupting and dismantling dark networks: Lessons from social network analysis and law enforcement simulations. In L. M. Gerdes (ed.). *Illuminating dark networks: The study of clandestine groups and organizations* (pp. 39-51). New York: Cambridge University Press.
- Bright, D. A., Greenhill, C., & Levenkova, N. (2010). Attack of the nodes: Scale-free criminal networks and vulnerability to targeted law enforcement interventions. In 2nd Illicit Networks Workshop, Wollongong, Australia.
- Bright, D. A., Greenhill, C., Reynolds, M., Ritter, A., & Morselli, C. (2015). The use of actor-level attributes and centrality measures to identify key actors: A case study of an Australian drug trafficking network. *Journal of contemporary criminal justice*, 31(3), 262-278.

- Bright, D., Greenhill, C., Britz, T., Ritter, A., & Morselli, C. (2017). Criminal network vulnerabilities and adaptations. *Global Crime*, 18(4), 424-441.
- Brodeur, J. P., & Dupont, B. (2006). Knowledge workers or “knowledge” workers?. *Policing & Society*, 16(1), 7-26.
- Bullock, K. (2013). Community, intelligence-led policing and crime control. *Policing and society*, 23(2), 125-144.
- Burcher, M., & Whelan, C. (2015). Social network analysis and small group ‘dark’ networks: an analysis of the London bombers and the problem of ‘fuzzy’ boundaries. *Global crime*, 16(2), 104-122.
- Burcher, M., & Whelan, C. (2018). Social network analysis as a tool for criminal intelligence: Understanding its potential from the perspectives of intelligence analysts. *Trends in Organized Crime*, 21(3), 278-294.
- Burcher, M., & Whelan, C. (2019). Intelligence-led policing in practice: Reflections from intelligence analysts. *Police quarterly*, 22(2), 139-160.
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 2053951715622512.
- Carley, K. M. (2006). Destabilization of covert networks. *Computational & Mathematical Organization Theory*, 12(1), 51-66.
- Carter, J. G. (2016). Institutional pressures and isomorphism: The impact on intelligence-led policing adoption. *Police quarterly*, 19(4), 435-460.

- Carter, D. L., & Carter, J. G. (2009). Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal justice policy review*, 20(3), 310-325.
- Carter, J. G., & Phillips, S. W. (2015). Intelligence-led policing and forces of organisational change in the USA. *Policing and society*, 25(4), 333-357.
- Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., ... & Liotta, A. (2020). Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia. *Plos one*, 15(8), e0236476.
- Chan, J., & Bennett Moses, L. (2017). Making sense of big data for security. *The British journal of criminology*, 57(2), 299-319.
- Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology*, 51(2), 355-374.
- Clarke, C. (2006). Proactive policing: Standing on the shoulders of community-based policing. *Police Practice and Research*, 7(1), 3-17.
- Cope, N. (2004). 'Intelligence Led Policing or Policing Led Intelligence?' *Integrating Volume Crime Analysis into Policing*. *British journal of criminology*, 44(2), 188-203.
- Coyne, J. W., & Bell, P. (2011). Strategic intelligence in law enforcement: a review. *Journal of Policing, Intelligence and Counter Terrorism*, 6(1), 23-39.

- Cukier, K., & Mayer-Schoenberger, V. (2014). The rise of big data: How it's changing the way we think about the world (pp. 20-32). Princeton University Press.
- Darroch, S., & Mazerolle, L. (2013). Intelligence-led policing: A comparative analysis of organizational factors influencing innovation uptake. *Police quarterly*, 16(1), 3-37.
- Datta, A., Tschantz, M. C., & Datta, A. (2014). Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. arXiv preprint arXiv:1408.6491.
- Decary-Hetu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, 13(3), 160-175.
- De Lint, W. (2006). Intelligence in policing and security: reflections on scholarship. *Policing and Society*, 16(1), 1-6.
- De Schutter, O., & Ringelheim, J. (2008). Ethnic profiling: A rising challenge for European Human Rights law. *The Modern Law Review*, 71(3), 358-384.
- Deukmedjian, J. E., & Lint, W. D. (2007). Community into intelligence: Resolving information uptake in the RCMP. *Policing & Society*, 17(3), 239-256.
- Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. *Big Data & Society*, 3(2), 2053951716665128.
- Duijn, P. A., Kashirin, V., & Sloot, P. M. (2014). The relative ineffectiveness of criminal network disruption. *Scientific reports*, 4(1), 1-15.

- Duxbury, S. W., & Haynie, D. L. (2019). Criminal network security: An agent-based approach to evaluating network resilience. *Criminology*, 57(2), 314-342.
- Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, 16, 18.
- Evans, J. M., & Kebbell, M. R. (2012). The effective analyst: a study of what makes an effective crime and intelligence analyst. *Policing and society*, 22(2), 204-219.
- Everton, S. F. (2012). *Disrupting dark networks*. New York: Cambridge University Press.
- Fell, E., James, O., Dienes, H., Shah, N., & Grimshaw, J. (2019). *Understanding Organized Crime 2015/16: Estimating the Scale and the Social and Economic Costs*. Research Report 103. London: Home Office.
- Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police research series, paper*, 98(1-36), 10.
- Fyfe, N. R., Gundhus, H. O. I., & Ronn, K. V. (2017). Introduction: What is ILP? In N. R. Fyfe, H. O. I. Gundhus, & K. V. Ronn (eds.). *Moral issues in intelligence-led policing* (pp. 1-2). Abingdon, England: Routledge.
- Ganor, B. (2021). Artificial or Human: A New Era of Counterterrorism Intelligence?. *Studies in Conflict & Terrorism*, 44(7), 605-624.
- Giacomantonio, C. (2014). A typology of police organizational boundaries. *Policing and society*, 24(5), 545-565.

- Gill, P. & Phythian, M. (2006). *Intelligence in an insecure world*. Cambridge: Polity.
- Gill, P., & Phythian, M. (2013). From intelligence cycle to web of intelligence: Complexity and the conceptualisation of intelligence. In *Understanding the intelligence cycle* (pp. 35-56). Routledge.
- Gill, C., Weisburd, D., Telep, C. W., Vitter, Z., & Bennett, T. (2014). Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: A systematic review. *Journal of experimental criminology*, 10(4), 399-428.
- Gottschalk, P. (2010). *Policing organized crime. Intelligence strategy implementation*. New York: Taylor & Francis Group.
- Guidetti, R., & Martinelli, T. (2009). Intelligence-led policing: A strategic framework. *The Police Chief*, 76(10), 132.
- Hale, C., Heaton, R., & Uglow, S. (2004). Uniform styles? Aspects of police centralization in England and Wales. *Policing & Society*, 14(4), 291-312.
- Hashimi, S., & Bouchard, M. (2017). On to the next one? Using social network data to inform police target prioritization. *Policing: An International Journal of Police Strategies & Management*, 40(4), 768-782.
- Hauck, R. V., Atabakhsh, H., Ongvasith, P., Gupta, H., & Chen, H. (2002). COPLINK concept space: An application for criminal intelligence analysis. *IEEE Computer Digital Government Special Issue*, 35(3), 30-37.

- Innes, M. (2006). Policing uncertainty: Countering terror through community intelligence and democratic policing. *The Annals of the American Academy of Political and Social Science*, 605(1), 222-241.
- Innes, M., & Sheptycki, J. W. (2004). From detection to disruption. *International criminal justice review*, 14(1), 1-24.
- Innes, M., Fielding, N., & Cope, N. (2005). 'The Appliance of Science?' The Theory and Practice of Crime Intelligence Analysis. *British Journal of Criminology*, 45(1), 39-57.
- Innes, M., Abbott, L., Lowe, T., & Roberts, C. (2009). Seeing like a citizen: field experiments in 'community intelligence-led policing'. *Police practice and research: An international journal*, 10(2), 99-114.
- James, A. (2014). Forward to the past: reinventing intelligence-led policing in Britain. *Police practice and research*, 15(1), 75-88.
- Joh, E. E. (2017). Artificial intelligence and policing: First questions. *Seattle UL Rev.*, 41, 1139.
- Johnston, L. & Shearing, C. (2003). *Governing security: Explorations in policing and justice*. London: Routledge.
- Kaminski, M. E., & Malgieri, G. (2019). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. U of Colorado Law Legal Studies Research Paper, 19-28.
- Kay, M., Matuszek, C., & Munson, S. A. (2015). Unequal representation and gender stereotypes in image search results for occupations. In *Proceedings of the 33rd Annual ACM*



Conference on Human Factors in Computing Systems (pp. 3819-3828).

Keegan, B., Ahmed, M. A., Williams, D., Srivastava, J., & Contractor, N. (2010, August). Dark gold: Statistical properties of clandestine networks in massively multiplayer online games. In 2010 IEEE Second International Conference on Social Computing (pp. 201-208). IEEE.

Kirby, S., & Penna, S. (2010). Policing mobile criminality: Towards a situational crime prevention approach to organised crime. In K. Bullock, R. V. Clarke, & N. Tilley (eds.). *Situational prevention of organised crime* (pp. 193-212). Cullompton, UK: Willan Publishing.

Kirby, S., & Nailer, L. (2013). Reducing the offending of a UK organized crime group using an opportunity-reducing framework—a three year case study. *Trends in organized crime*, 16(4), 397-412.

Kirby, S., & Snow, N. (2016). Praxis and the disruption of organized crime groups. *Trends in organized crime*, 19(2), 111-124.

Kleemans, E. R., Soudijn, M. R., & Weenink, A. W. (2012). Organized crime, situational crime prevention and routine activity theory. *Trends in Organized Crime*, 15(2), 87-92.

Lehr, D., & Ohm, P. (2017). Playing with the data: what legal scholars should learn about machine learning. *UCDL Rev.*, 51, 653.

Lewandowski, C., Carter, J. G., & Campbell, W. L. (2018). The utility of fusion centres to enhance intelligence-led policing: an exploration of end-users. *Policing: A Journal of Policy and Practice*, 12(2), 177-193.

- Lowry, S., & Macpherson, G. (1988). A blot on the profession. *British medical journal*, 296(6623), 657.
- Lyon, D., & Wood, D. M. (2012). Security, surveillance, and sociological analysis. *Canadian Review of Sociology/Revue canadienne de sociologie*, 49(4), 317-327.
- Maguire, M., & John, T. (2006). Intelligence led policing, managerialism and community engagement: Competing priorities and the role of the National Intelligence Model in the UK. *Policing & society*, 16(1), 67-85.
- Manning, P. (2008). *The technology of policing: Crime mapping, information technology, and the rationality of crime control*. New York, NY: New York University Press
- Mastrofski, S. D., Worden, R. E., & Snipes, J. B. (1995). Law enforcement in a time of community policing. *Criminology*, 33(4), 539-563.
- Mastrofski, S. D., Willis, J. J., & Kochel, T. R. (2007). The challenges of implementing community policing in the United States. *Policing: a journal of policy and practice*, 1(2), 223-234.
- McGarrell, E. F., Freilich, J. D., & Chermak, S. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice*, 23(2), 142-158.
- McKendrick, K. (2019). *Artificial intelligence prediction and counterterrorism*. Royal Institute of International Affairs.
- Monahan, C.T. (2006). Questioning surveillance and security. In T. Monahan (ed.). *Surveillance and society: Technological politics and power in everyday life*. London: Routledge.

- Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social networks*, 29(1), 143-153.
- Oakensen, D., Mockford, R., & Pascoe, C. (2002). Does there have to be blood on the carpet? Integrating partnership, problem-solving and the National Intelligence Model in strategic and tactical police decision-making processes. *Police Research and Management*, 5(4), 51-62.
- Oliver, W. M. (2006). The fourth era of policing: Homeland security. *International Review of Law Computers & Technology*, 20(1-2), 49-62.
- O'Shea, T. C., Nicholls, K., Archer, J., Hughes, E., & Tatum, J. (2002). *Crime analysis in America*. Center for Public Policy, University of South Alabama, Mobile, AL.
- Pasquale, F. (2015). *The black box society*. Harvard University Press.
- Perrot, P. (2017). What about AI in Criminal Intelligence: From Predictive Policing to AI Perspectives. *Eur. Police Sci. & Res. Bull.*, 16, 65.
- Phillips, S. W. (2012). The attitudes of police managers toward intelligence-led policing. *FBI L. Enforcement Bull.*, 81, 13.
- Pickering, S. (2004). Border terror: policing, forced migration and terrorism. *Global Change, Peace & Security*, 16(3), 211-226.
- Ratcliffe, J. (2005). The effectiveness of police intelligence management: A New Zealand case study. *Police practice and research*, 6(5), 435-451.
- Ratcliffe, J. H. (2016). *Intelligence-led policing*. London: Routledge.

- Ratcliffe, J. H., & Taniguchi, T. A. (2008). Is crime higher around drug-gang street corners? Two spatial approaches to the relationship between gang set spaces and local crime levels. *Crime Patterns and Analysis*, 1(1), 17-39.
- Reuter, P., & Tonry, M. (2020). Organised crime: Less than meets the eye. *Crime and Justice*, 49.
- Rigano, C. (2019). *Using artificial intelligence to address criminal justice needs*. National Institute of Justice. Issue, 280.
- Roberts, N., & Everton, S. (2016). Monitoring and disrupting dark networks: A bias toward the center and what it costs us. In Dawoody, A. R. (ed.). *Eradicating Terrorism from the Middle East: Policy and administrative approaches* (pp. 29-42). Springer, Cham.
- Rosenbaum, D. P., & Lurigio, A. J. (1994). An inside look at community policing reform: Definitions, organizational changes, and evaluation findings. *Crime & delinquency*, 40(3), 299-314.
- Rowe, E., Akman, T., Smith, R. G., & Tomison, A. M. (2013). Organised crime and public sector corruption: A crime script analysis of tactical displacement risks. Canberra: Australian Institute of Criminology.
- Sanders, C. B., & Henderson, S. (2013). Police 'empires' and information technologies: Uncovering material and organisational barriers to information sharing in Canadian police services. *Policing and society*, 23(2), 243-260.
- Sanders, C. B., Weston, C., & Schott, N. (2015). Police innovations, 'secret squirrels' and accountability: Empirically

- studying intelligence-led policing in Canada. *British journal of criminology*, 55(4), 711-729.
- Sanders, C., & Condon, C. (2017). Crime analysis and cognitive effects: the practice of policing through flows of data. *Global crime*, 18(3), 237-255.
- Sanders, C. B., & Sheptycki, J. (2017). Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. *Crime, law and social change*, 68(1), 1-15.
- Schafer, J. A. (2010). The ineffective police leader: Acts of commission and omission. *Journal of Criminal Justice*, 38(4), 737-746.
- Sheptycki, J. (2002). The 'drug war': Learning from the paradigm example of transnational policing. In J. Sheptycki (ed.). *Issues in transnational policing* (pp. 215-242). Oxfordshire: Routledge.
- Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European journal of criminology*, 1(3), 307-332.
- Sheptycki, J. (2017). Liquid modernity and the police métier; thinking about information flows in police organisation. *Global Crime*, 18(3), 286-302.
- Sheptycki, J. (2017). The police intelligence division-of-labour. *Policing and Society*, 27(6), 620-635.
- Taylor, B., Kowalyk, A., & Boba, R. (2007). The integration of crime analysis into law enforcement agencies: An exploratory study into the perceptions of crime analysts. *Police Quarterly*, 10(2), 154-169.

- Tsai, W. (2002). Social structure of “coopetition” within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization science*, 13(2), 179-190.
- Tsvetovat, M., & Carley, K. M. (2003). Bouncing back: Recovery mechanisms of covert networks. Paper presented at the NAACSOS Conference, Pittsburgh, PA.
- Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398-404.
- von Lampe, K. (2011). The application of the framework of situational crime prevention to ‘organized crime’. *Criminology & Criminal Justice*, 11(2), 145-163.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76-99.
- Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.
- Weisburd, D., McElroy, J., & Hardyman, P. (1988). Challenges to supervision in community policing: Observations on a pilot project. *Am. J. Police*, 7, 29.
- Weisburd, D., & Eck, J. E. (2004). What can police do to reduce crime, disorder, and fear?. *The annals of the American academy of political and social science*, 593(1), 42-65.

Whelan, C. (2017). Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal*, 30(1), 310-327.

Whelan, C., & Dupont, B. (2017). Taking stock of networks across the security field: A review, typology and research agenda. *Policing and society*, 27(6), 671-687.

Wood, J., & Shearing, C. (2007). *Imagining security*. Cullompton, Devon: Willan Publishing.

Zarsky, T. Z. (2017). An Analytic Challenge: Discrimination Theory in the Age of Predictive Analytics. *ISJLP*, 14, 11.