ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Κωνσταντίνας Μαστρογιάννη (Α.Μ.: ΜΔΙ2224)

Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΕΠΟΧΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΑΝΘΡΩΠΙΣΜΟΥ ΚΑΙ ΤΟΥ ΨΗΦΙΑΚΟΥ ΣΥΝΤΑΓΜΑΤΙΣΜΟΥ

PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE UNDER THE PRISM OF DIGITAL HUMANISM AND DIGITAL CONSTITUTIONALISM

Επιβλέπουσα:

Δρ. Αικατερίνα Παπανικολάου

Πειραιάς, Σεπτέμβριος 2024

Στον πατέρα μου που με δίδαξε την απλότητα και την υπομονή

I don't know why people are so keen to put the details of their private life in public; they forget that invisibility is a superpower.

(Banksy, allegedly)

Δεν ξέρω γιατί οι άνθρωποι είναι τόσο πρόθυμοι να δημοσιοποιήσουν τις λεπτομέρειες της ιδιωτικής τους ζωής- ξεχνούν ότι η αορατότητα είναι μια υπερδύναμη.

(αποδίδεται στον Banksy)

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

CCPA	California Consumer Privacy Act
DPA	Data Protection Act
DRD	Data Retention Directive
DSA	Digital Services Act
DSM	Digital Single Market
FRIA	Fundamental Rights Impact Assessment
GPAI	General-purpose AI
LGPD	Lei Geral de Proteção de Dados
PIPEDA	Personal Information Protection and Electronic Documents Act
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΕΕ	Δικαστήριο Ευρωπαϊκής Ένωσης
ΕΔΑΔ	Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
Κανονισμός ePR	Κανονισμός ePrivacy
Σ	Σύνταγμα
ΣΕΕ	Συνθήκη για την Ευρωπαϊκή Ένωση
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΤΝ	Τεχνητή Νοημοσύνη

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματεύεται το θέμα της ιδιωτικότητας στην εποχή της τεχνητής νοημοσύνης υπό το πρίσμα δύο αλληλένδετων πολιτικών και κοινωνικών κινημάτων, αυτών του ψηφιακού ανθρωπισμού και του ψηφιακού συνταγματισμού. Η ιδιωτικότητα στην εποχή της τεχνητής νοημοσύνης αναδεικνύεται ως κρίσιμο ζήτημα, καθώς η τεχνολογία διεισδύει βαθύτερα στην καθημερινή ζωή, συλλέγοντας και επεξεργαζόμενη τεράστιες ποσότητες προσωπικών δεδομένων. Υπό το πρίσμα του ψηφιακού ανθρωπισμού και του ψηφιακού συνταγματισμού, η προστασία της ιδιωτικότητας αποκτά διπλή διάσταση. Ο ψηφιακός ανθρωπισμός εστιάζει στην ανάγκη διατήρησης της ανθρώπινης αξιοπρέπειας και της αυτονομίας σε ένα περιβάλλον όπου οι αλγόριθμοι και τα συστήματα τεχνητής νοημοσύνης μπορούν να επηρεάσουν αποφάσεις και συμπεριφορές χωρίς τη γνώση ή τη συγκατάθεση των ατόμων. Παράλληλα, ο ψηφιακός συνταγματισμός προσπαθεί να θεσπίσει νέους κανόνες και πλαίσια διακυβέρνησης που θα περιορίζουν την ανεξέλεγκτη ισχύ των μεγάλων τεχνολογικών εταιρειών, διασφαλίζοντας την προστασία των θεμελιωδών δικαιωμάτων, όπως η ιδιωτικότητα, μέσω της νομοθετικής και δικαστικής παρέμβασης. Η συνέργεια αυτών των δύο κινημάτων στοχεύει στη διαμόρφωση ενός τεχνολογικού οικοσυστήματος που θα είναι συμβατό με τις αρχές της δικαιοσύνης και της προστασίας της ιδιωτικής ζωής στην ψηφιακή εποχή.

Η ανάλυσή μας ξεκινά από την ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων όπως κατοχυρώνονται σε ποικίλα νομικά πλαίσια τόσο σε διεθνές όσο και σε εθνικό επίπεδο και συνεχίζει με τον τρόπο που η ιδιωτικότητα διασφαλίζεται στην εποχή της τεχνητής νοημοσύνης. Αφού αναδεικνύεται η σχέση μεταξύ ψηφιακού ανθρωπισμού και ψηφιακού συνταγματισμού, το μεγαλύτερο μέρος της εργασίας αφιερώνεται στην προσέγγιση του ψηφιακού συνταγματισμού τόσο ως εννοιολογικό όσο και ως κανονιστικό πλαίσιο. Έμφαση δίδεται στον ρόλο των νομολογιακών αποφάσεων, των μεγάλων τεχνολογικών εταιρειών και της κοινωνίας των πολιτών στη συνταγματοποίηση της ψηφιακής κοινωνίας. Τέλος, μελετώνται δύο βασικά κείμενα, η πρόταση Κανονισμού ePrivacy και ο Κανονισμός για την Τεχνητή Νοημοσύνη με στόχο να αναδειχθεί ο τρόπος της σύγχρονης προσέγγισης στο θέμα της ιδιωτικότητας και της μαζικής επιτήρησης.

ABSTRACT

This dissertation deals with the issue of privacy in the era of artificial intelligence in the light of two interconnected political and social movements, those of digital humanism and digital constitutionalism. Privacy in the age of artificial intelligence emerges as a critical issue as technology penetrates deeper into everyday life, collecting and processing vast amounts of personal data. In the light of digital humanism and digital constitutionalism, the protection of privacy takes on a double dimension. Digital humanism focuses on the need to preserve human dignity and autonomy in an environment where algorithms and AI systems can influence decisions and behaviour without the knowledge or consent of individuals. At the same time, digital constitutionalism seeks to establish new rules and governance frameworks that will limit the rampant power of large technology companies, while ensuring the protection of fundamental rights, such as privacy, through legislative and judicial intervention. The synergy between these two movements aims to create a technological ecosystem that is compatible with the principles of justice and privacy in the digital age.

Our analysis begins with privacy and data protection as enshrined in a variety of legal frameworks both internationally and nationally and continues with how privacy is secured in the age of artificial intelligence. After highlighting the relationship between digital humanism and digital constitutionalism, the bulk of the paper is devoted to approaching digital constitutionalism as both a conceptual and normative framework. Emphasis is placed on the role of judicial activism, large technology companies and civil society in the constitutionalisation of the digital society. Finally, we study two key texts, the proposed ePrivacy Regulation and the AI Regulation to highlight the contemporary approach to the issue of privacy and mass surveillance.

ΠΡΟΛΟΓΟΣ

Τα προϊόντα της τεχνητής νοημοσύνης αποτελούν μεγάλη πρόκληση για το μέλλον, αλλά δημιουργούν και έντονες ανησυχίες για τους κινδύνους που διατρέχει ο ανθρώπινος πολιτισμός. Δυσοίωνες προβλέψεις για τον ρόλο που θα αποκτήσουν τα δημιουργήματα της τεχνητής νοημοσύνης σε ποικίλες πτυχές της ζωής μας με αποτέλεσμα να απειλείται η κουλτούρα μας, η ατομικότητα και η ιδιωτικότητά μας, φόβοι σχετικά με την καταστρατήγηση των θεμελιωδών δικαιωμάτων του ανθρώπου λόγω της αλόγιστης χρήσης των προσωπικών δεδομένων και την εξάπλωση της ψηφιακής επιτήρησης, ανησυχίες για την υιοθέτηση διακρίσεων λόγω της μη δυνατότητας κατανοήσεως του τρόπου με τον οποίον αποφασίζουν οι «έξυπνες» μηχανές[1], .συνθέτουν ένα δυστοπικό σκηνικό που για πολλούς δεν απέχει πολύ από το άμεσο μέλλον.

Το δικαίωμα στην προσωπικότητα και τον πληροφοριακό αυτοκαθορισμό του ατόμου κάμπτεται όχι μόνο μπροστά στην αυτοματοποιημένη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα που είναι αλόγιστη, αλλά και στη χαμηλή ποιοτική στάθμη αυτών που πολύ συχνά υπάρχει. Η απουσία κριτηρίων καταλληλόλητας στη συλλογή των δεδομένων για την επίτευξη του επιδιωκόμενου σκοπού, τα λάθη και οι ανακρίβειες μπορούν να οδηγήσουν σε μεροληπτική κρίση, σε διακρίσεις, ειδικά όταν υπάρχουν περιορισμοί στο επιλεγέν δείγμα.

Επιπρόσθετα, η άκριτη εξόρυξη τεράστιου όγκου δεδομένων, χωρίς ανθρώπινη παρέμβαση, οι αυτοματοποιημένοι συσχετισμοί στην επαναχρησιμοποίηση της

[1] Η αδυναμία ελέγχου των μηχανών από τον άνθρωπο θέτει επί τάπητος το δυσεπίλυτο ζήτημα της αποδόσεως τυχόν ευθυνών σε περίπτωση προκλήσεως ατυχήματος από την πλευρά της τεχνητής νοημοσύνης. Σε επίπεδο ΕΕ, το ζήτημα της ρομποτικής και της αστικής ευθύνης των αυτόνομων μηχανών έχει απασχολήσει σημαντικά ήδη από το 2017 με το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (Ευρωπαϊκό Κοινοβούλιο, 2018). Ένα από τα βασικά ερωτήματα προς συζήτηση που έθεσε το Ψήφισμα ήταν κατά πόσο τα ρομπότ μπορούν να έχουν ηλεκτρονικές προσωπικότητες. Υπέρ της νομικής προσωπικότητας τάχθηκαν κυρίως ορισμένοι κατασκευαστές και οι θυγατρικές τους κυρίως στη λογική ότι έτσι τα ρομπότ θα είχαν την ίδια αξία με τις εταιρείες οι οποίες έχουν ήδη καθεστώς νομικών προσώπων και αντιμετωπίζονται ως τέτοιες από δικαστήρια ανά τον κόσμο. Το βασικό επιχείρημα υπέρ της νομικής προσωπικότητας των ρομπότ ήταν ότι σε έναν κόσμο που χάνεται η αιτιώδης συνάφεια, θα καλυφθεί το κενό που δημιουργείται από τις ενέργειες αυτών και οι οποίες δεν μπορούν να καταλογιστούν μόνο στον ανθρώπινο παράγοντα (Turner, 2019). Η συζήτηση εγκαταλείφθηκε σύντομα με τα επιχειρήματα κατά της νομικής προσωπικότητας των ρομπότ να υπερισχύουν.

πληροφορίας, η αδιαφάνεια στον τρόπο λειτουργίας των υπολογιστικών συστημάτων, οι πολύπλοκες σχέσεις που αναπτύσσονται λόγω της διασύνδεσης με άλλα υπολογιστικά συστήματα μας φέρνει αντιμέτωπους με το φαινόμενο του μαύρου κουτιού (black box effect)[2] και της συνεπαγόμενης απομάκρυνσης από τη λογική της αιτιώδους συνάφειας και της επικράτησης του επιχειρήματος του συσχετισμού. Αποφάσεις που βασίζονται σε στατιστικές συσχετίσεις χωρίς ικανοποιητικό βαθμό επεξηγησιμότητας οι οποίες μπορούν να επηρεάσουν την ιδιωτική ζωή έρχονται σε αντίφαση με το γενικό πλαίσιο για την προστασία των προσωπικών δεδομένων όπως έχει καθιερωθεί σε ενωσιακό επίπεδο στον ΓΚΠΔ, ο οποίος κατέστη υποχρεωτικής και οριζόντιας εφαρμογής σε όλα τα κράτη μέλη της ΕΕ στις 25 Μαΐου 2018 (Μπακιρτζόγλου, 2022).

Οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, η αρχή του περιορισμού του σκοπού της επεξεργασίας, αλλά και οι αρχές της ελαχιστοποίησης των δεδομένων, της ακρίβειας, της ακεραιότητας και της εμπιστευτικότητας επιτάσσουν τα προσωπικά δεδομένα να συλλέγονται και να επεξεργάζονται με τρόπο που να προστατεύεται το δικαίωμα στην ιδιωτική ζωή καθώς και το δικαίωμα του πληροφοριακού αυτοκαθορισμού. Οι εν λόγω αρχές φαίνεται να κάμπτονται εκ προοιμίου από τα εγγενή χαρακτηριστικά της τεχνητής νοημοσύνης τα οποία περιορίζουν τη δυνατότητα του ατόμου να γνωρίζει, να αποφασίζει και να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που τον αφορούν.

Οι επιπτώσεις από την εξέλιξη της τεχνολογίας ή καλύτερα από τη συνεξέλιξη της τεχνολογίας και του ανθρώπου εξαπλώνονται σε κάθε πτυχή της ανθρώπινης καθημερινότητας μετατοπίζοντας τις δομές ισχύος και θέτοντας υπό αμφισβήτηση τη διαχωριστική γραμμή μεταξύ ανθρώπου και μηχανής. Οι ακόλουθοι του υπερανθρωπισμού μιλούν για τη γέννηση ενός αναβαθμισμένου ανθρώπινου είδους που θα υπερβεί ακόμη και την ανθρώπινη φθορά. Ο Τάσης (2019) στο βιβλίο του «Ψηφιακός ανθρωπισμός: Εικονιστικό υποκείμενο και τεχνητή νοημοσύνη» αναφέρεται στη «δυσήνια ανασφάλεια ενόψει της πρωτόγνωρης φθοράς βεβαιοτήτων και κανόνων τόσο στην εθνική δημόσια σφαίρα όσο επίσης και στη διεθνή γεωπολιτική τάξη». Η εικονιστική κοινωνία δοκιμάζει την

[2] Το τεχνητό νευρωνικό δίκτυο στο οποίο στηρίζεται η λειτουργία των αλγορίθμων δημιουργεί το φαινόμενο του μαύρου κουτιού (black box effect), μιας κρυφής περιοχής όπου και οι ίδιοι οι δημιουργοί των αλγορίθμων δεν μπορούν να εξηγήσουν τι συμβαίνει στο εσωτερικό της και τελικά τον τρόπο με τον οποίο έφτασε ο αλγόριθμος στο συγκεκριμένο αποτέλεσμα.

ανθεκτικότητα παραδοσιακών θεσμών όπως η δημόσια σφαίρα, η γλώσσα, το έθνος κράτος, η οικονομία και η πολιτική. Το εικονιστικό υποκείμενο αναδύεται ως μιας νέας μορφής ανθρωπότυπος, ένα μελλοντικά υβριδικότερο ανθρώπινο είδος που αναδιαμορφώνει τη σχέση προς τον εαυτό σε σχέσεις μεταξύ ψηφιακών εικόνων.

Καθώς η ΤΝ κερδίζει έδαφος, κάποιοι ίσως θεωρήσουν ότι η ανθρωπότητα είναι πλέον πιο ικανή από ποτέ να κατανοεί και να διαχειρίζεται το περιβάλλον της. Άλλοι, ωστόσο, μπορεί να υποστηρίξουν ότι οι δυνατότητές μας είναι λιγότερο ισχυρές από ό,τι αρχικά πιστεύαμε. Αυτό θέτει ένα βαθύ υπαρξιακό ερώτημα για το πώς θα κατανοούμε τον εαυτό μας και τον ρόλο μας στον κόσμο. Πώς θα μπορούμε να συμφιλιώσουμε τη χρήση της ΤΝ με θεμελιώδεις έννοιες όπως η ανθρώπινη αυτονομία και αξιοπρέπεια; Καθώς η ΤΝ επηρεάζει και ενσωματώνεται στις καθημερινές μας δραστηριότητες, είναι σημαντικό να αναστοχαστούμε πώς θα διατηρήσουμε την αίσθηση του ελέγχου πάνω στις ζωές μας και πώς θα διαφυλάξουμε τις ηθικές αξίες που θεωρούμε ουσιώδεις για την ανθρώπινη ύπαρξη.

Οι κοινωνίες έχουν δύο βασικές επιλογές: να αντιδράσουν παθητικά και να προσαρμοστούν σιγά σιγά στις αλλαγές που φέρνει η Τεχνητή Νοημοσύνη ή να αποφασίσουν ενεργά να ξεκινήσουν έναν ουσιαστικό διάλογο, αξιοποιώντας όλες τις πτυχές της ανθρώπινης γνώσης, για να καθορίσουν τον ρόλο της ΤΝ και, ταυτόχρονα, τον ρόλο των ανθρώπων σε αυτό το νέο πλαίσιο. Η πρώτη επιλογή θα συμβεί χωρίς ιδιαίτερη προσπάθεια, σχεδόν αυτόματα. Η δεύτερη, όμως, απαιτεί επίγνωση και συνεργασία, φέρνοντας μαζί ηγέτες, φιλοσόφους, επιστήμονες, ανθρωπιστές και άλλους, για να συνδιαμορφώσουν το μέλλον μας με υπευθυνότητα και όραμα (Σμιτ, Κίσινγκερ και Χούτενλοχερ, 2022).

Είναι αλήθεια ότι το διακύβευμα της ανθρώπινης ύπαρξης ενεργοποίησε μηχανισμούς προστασίας τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο με τη μορφή κανονισμών, κανόνων δεοντολογίας, νόμων και νομολογιακών αποφάσεων στην προσπάθεια να εξασφαλιστεί δικαιοσύνη, ισότητα, λογοδοσία και διαφάνεια στην ψηφιακή εποχή και στα προϊόντα τεχνολογικής καινοτομίας. Επίσης, δημιούργησε τις προϋποθέσεις για την ανάδειξη νέων κοινωνικών και πολιτικών κινημάτων, όπως αυτό του ψηφιακού ανθρωπισμού στον οποίο θα αναφερθούμε αναλυτικότερα σε επόμενη ενότητα.

Η προστασία της ιδιωτικότητας βρίσκεται στο επίκεντρο της συζήτησης που έχει ξεκινήσει. Η σημασία της μπορεί να γίνει πιο κατανοητή όταν εξετάσουμε τις επιπτώσεις που έχει η απώλειά της στο άτομο. Η έλλειψη ελέγχου επί της ιδιωτικότητας καθιστά το άτομο ευάλωτο και εκτεθειμένο, απειλώντας τον πυρήνα της αυτονομίας και της ταυτότητάς του (DeCew,1997). Πριν προχωρήσουμε στην περαιτέρω ανάλυση της επίδρασης των νέων τεχνολογιών στην ιδιωτική ζωή, στην επόμενη ενότητα θα ασχοληθούμε με τους βασικούς ορισμούς και τη σχέση του δικαιώματος με αυτό της προστασίας των προσωπικών δεδομένων.

1. ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Η ιδιωτική ζωή και τα προσωπικά δεδομένα θεωρούνται θεμελιώδη δικαιώματα, προστατευμένα από διάφορα νομικά πλαίσια σε διεθνή και εθνικά επίπεδα Η διάκριση μεταξύ των δύο εννοιών είναι ουσιαστική για την κατανόηση της νομικής προστασίας που παρέχεται σε κάθε περίπτωση.

Τα δεδομένα γενικά αναφέρονται σε πληροφορίες. Τα προσωπικά δεδομένα είναι συγκεκριμένες πληροφορίες που σχετίζονται με ένα αναγνωρίσιμο άτομο, είτε άμεσα είτε έμμεσα. Αυτές οι πληροφορίες μπορεί να αφορούν την ιδιωτική ή επαγγελματική και οικονομική δραστηριότητα του ατόμου, τις σχέσεις του με άλλα πρόσωπα ή αντικείμενα, τις ενέργειες, τις αντιδράσεις και τις συμπεριφορές του, ανεξαρτήτως αν αφορούν το παρόν ή το παρελθόν (Κίτσος, 2011).

Από την άλλη πλευρά, η «ιδιωτική ζωή» αναφέρεται γενικά στην κατάσταση του ατόμου να είναι μόνο του και απαλλαγμένο από την δημόσια προσοχή. Στην αγγλική γλώσσα, η λέξη «privacy» περιγράφεται ως «η κατάσταση του να μπορεί κάποιος να είναι μόνος και να μην μπορεί κάποιος να τον δει ή να τον ακούσει» καθώς και «η κατάσταση του να είναι κάποιος ελεύθερος από τη δημόσια προσοχή» (Longman, 2014).

Η διακεκριμένη Γερμανίδα φιλόσοφος Beate Rössler (2006) αναγνωρίζει στην ιδιωτικότητα τρεις βασικές και αλληλένδετες μεταξύ τους διαστάσεις. Αυτές οι διαστάσεις προσδιορίζουν διαφορετικούς τρόπους με τους οποίους η ιδιωτικότητα επηρεάζει τη ζωή των ατόμων και το πώς αυτή μπορεί να προστατευτεί ή να παραβιαστεί:

1. **Ιδιωτικότητα της Διαβίωσης** (Decisional Privacy): Αυτή η διάσταση αφορά την αυτονομία των ατόμων να λαμβάνουν αποφάσεις σχετικά με τη ζωή τους χωρίς εξωτερικές παρεμβάσεις. Περιλαμβάνει την ελευθερία να επιλέγουν τον τρόπο ζωής τους, να αποφασίζουν για τις προσωπικές σχέσεις, την υγεία τους και άλλες σημαντικές προσωπικές αποφάσεις.
2. **Ιδιωτικότητα της Προσωπικής Ζωής** (Informational Privacy): Αυτή η διάσταση σχετίζεται με τον έλεγχο της πληροφορίας που αφορά ένα άτομο. Η προστασία των προσωπικών δεδομένων και η ελευθερία από την παρακολούθηση ή την ανεπιθύμητη δημοσιοποίηση προσωπικών πληροφοριών εμπίπτουν σε αυτήν τη διάσταση.

3. **Ιδιωτικότητα του Χώρου** (Local Privacy): Αυτή η διάσταση επικεντρώνεται στον φυσικό χώρο και το δικαίωμα των ατόμων να έχουν έναν ιδιωτικό χώρο, όπως το σπίτι τους, όπου μπορούν να αποσύρονται και να προστατεύονται από εξωτερικές παρεμβάσεις.

Στην πραγματικότητα, ενώ τα προσωπικά δεδομένα είναι μια πιο περιορισμένη έννοια, η προστασία τους συμβάλλει στην προστασία της ιδιωτικής ζωής. Πιο συγκεκριμένα, η προστασία των προσωπικών δεδομένων διασφαλίζει ότι οι πληροφορίες που σχετίζονται με ένα άτομο δε χρησιμοποιούνται κατά τρόπο που να παραβιάζει την ιδιωτική του ζωή. Υπάρχει, επομένως, μια αλληλεξάρτηση μεταξύ των δύο εννοιών, με την προστασία των προσωπικών δεδομένων να αποτελεί ένα υποσύνολο της γενικότερης προστασίας της ιδιωτικής ζωής. Η ιδιωτική ζωή ως μια ευρύτερη έννοια περιλαμβάνει την προστασία της αυτονομίας και της προσωπικής ακεραιότητας του ατόμου. Ουσιαστικά, η ιδιωτική ζωή σχετίζεται με το δικαίωμα του ατόμου να ζει χωρίς αδικαιολόγητες παρεμβολές από την κρατική εξουσία ή άλλους τρίτους.

Η ανάλυση των δύο βασικών προσεγγίσεων–αμερικανικής και ευρωπαϊκής— που άσκησαν τη σημαντικότερη επιρροή στη διαμόρφωση της διεθνούς νομοθεσίας και των κανονιστικών πλαισίων γύρω από το θέμα αυτό προσφέρει μια συγκριτική θεώρηση, η οποία είναι ουσιώδης για την κατανόηση των διαφορετικών νομικών, κοινωνικών και πολιτισμικών αντιλήψεων περί ιδιωτικότητας και προστασίας δεδομένων (Κίτσος, ibid).

1.1. Η αμερικανική προσέγγιση

Η αμερικανική προσέγγιση στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων χαρακτηρίζεται από μια φιλελεύθερη θεώρηση, εστιάζοντας κυρίως στην έννοια της ιδιωτικότητας ως δικαίωμα του καταναλωτή και λιγότερο ως θεμελιώδες ανθρώπινο δικαίωμα. Η προσέγγιση αυτή αναδεικνύεται μέσω της έμφασης που δίνεται στην αυτορρύθμιση των επιχειρήσεων και στη χρήση τεχνολογικών λύσεων για την προστασία της ιδιωτικότητας.

Δεν είναι τυχαίο ότι στην αμερικανική νομική σκέψη δεν γίνεται σαφής διάκριση μεταξύ της ιδιωτικότητας και των προσωπικών δεδομένων. Και γι'αυτό, για θέματα που

αφορούν την προστασία των προσωπικών δεδομένων και την ιδιωτική ζωή, χρησιμοποιείται συνήθως ο όρος «ιδιωτικότητα» ή «ιδιωτική ζωή» (privacy)[3].

Στις Ηνωμένες Πολιτείες, η νομοθεσία για την προστασία της ιδιωτικότητας είναι κατακερματισμένη και τομεακή, με διαφορετικούς νόμους να εφαρμόζονται σε διαφορετικούς τομείς, όπως η υγεία, οι χρηματοοικονομικές υπηρεσίες και οι ηλεκτρονικές επικοινωνίες[4]. Η έλλειψη ενός ενιαίου, οριζόντιου νομικού πλαισίου επιτρέπει μεγαλύτερη ευελιξία, αλλά ταυτόχρονα οδηγεί σε κενά προστασίας και ασυνέπειες στην εφαρμογή των νόμων.

Επιπλέον,η αμερικανική νομοθεσία βασίζεται συχνά στην αρχή της ειδοποίησης και της συναίνεσης (notice and consent), όπου οι οργανισμοί υποχρεούνται να ενημερώνουν τα άτομα για τις πρακτικές συλλογής και επεξεργασίας δεδομένων και να εξασφαλίζουν τη συναίνεσή τους. Όμως και σε αυτή την περίπτωση, η αρχή της ειδοποίησης και συναίνεσης, εφαρμόζεται διαφορετικά ανάλογα με τον τομέα και τον τύπο των δεδομένων[5] .

Οι επικριτές της ανωτέρω πρακτικής υποστηρίζουν ότι η απλή ειδοποίηση και λήψη συναίνεσης δεν αρκεί για να διασφαλιστεί η προστασία των προσωπικών δεδομένων, καθώς οι όροι χρήσης και οι πολιτικές απορρήτου συχνά είναι πολύπλοκοι και δύσκολα κατανοητοί για τον μέσο χρήστη. Επιπλέον, οι καταναλωτές συχνά αισθάνονται ότι δεν έχουν άλλη επιλογή από το να αποδεχτούν τους όρους για να αποκτήσουν πρόσβαση σε μια υπηρεσία ή προϊόν, γεγονός που υπονομεύει την ελευθερία επιλογής τους.

Τέλος, η προσέγγιση της ιδιωτικότητας στις ΗΠΑ αντανακλάται και στη νομολογία, όπου δικαστικές αποφάσεις συχνά σταθμίζουν την προστασία της ιδιωτικότητας έναντι άλλων συμφερόντων, όπως η ελευθερία της έκφρασης και το επιχειρηματικό συμφέρον. Αυτή η προσέγγιση υποδηλώνει την επιδίωξη της ισορροπίας μεταξύ της προστασίας των

[3] Όπως θα δούμε και στη συνέχεια, ο όρος "personal data" (προσωπικά δεδομένα), χρησιμοποείται στην ευρωπαϊκή νομική ορολογία.
[4] Π.χ. Health Insurance Portability and Accountability Act (HIPAA) (1996), Gramm-Leach-Bliley Act (GLBA) (1999), Children's Online Privacy Protection Act (COPPA) (1998), Electronic Communications Privacy Act (ECPA) (1986), California Consumer Privacy Act (CCPA) (2018).
[5] COPPA (άρθρο 312.4), CCPA (Τμήμα 1798.100 b), GLBA (Τμήμα 6803).

ατομικών δικαιωμάτων και των οικονομικών αναγκών, αντανακλώντας τις ευρύτερες φιλοσοφικές και νομικές αξίες της αμερικανικής κοινωνίας[6].

1.2. Η ευρωπαϊκή προσέγγιση

Η ευρωπαϊκή προσέγγιση θεμελιώνεται πάνω στη θεωρία ότι η προστασία της ιδιωτικότητας είναι ένα θεμελιώδες ανθρώπινο δικαίωμα, κατοχυρωμένο τόσο σε εθνικά συνταγματικά πλαίσια όσο και μέσω της ΕΣΔΑ και του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Αυτή η προσέγγιση αναγνωρίζει την ιδιωτικότητα όχι μόνο ως ατομικό δικαίωμα, αλλά και ως κρατική υποχρέωση προστασίας.

Σε αντίθεση με τις ΗΠΑ, η προστασία της ιδιωτικότητας στον ευρωπαϊκό χώρο βασίζεται στην έννοια της «αξιοπρέπειας του ατόμου», και όχι μόνο στην «προσωπική ελευθερία», όπως συμβαίνει στις ΗΠΑ. Αυτή η προσέγγιση υπογραμμίζει τη σημασία της προστασίας των προσωπικών δεδομένων μέσα από αυστηρούς κανονισμούς και νομοθετικά πλαίσια, που αποσκοπούν στην προστασία της ιδιωτικής ζωής των πολιτών από την αυθαίρετη και καταχρηστική χρήση από το κράτος ή άλλες οντότητες. Σε αυτό συνετέλεσε η ιστορική εμπειρία της Ευρώπης από αυταρχικά καθεστώτα και η καταχρηστική χρήση των προσωπικών δεδομένων για τον έλεγχο και την καταστολή των πολιτών.

Η ΕΕ έχει αναπτύξει ένα σαφές κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων το οποίο περιλαμβάνει την προστασία της ιδιωτικής ζωής, αλλά επεκτείνεται και σε άλλες πτυχές, όπως το δικαίωμα στη μη διάκριση. Η Οδηγία 95/46/ΕΚ (Οδηγία για την Προστασία Δεδομένων) και ο Κανονισμός 2016/679 (ΓΚΠΔ) αποτελούν τις κεντρικές νομοθετικές πράξεις της ΕΕ που διασφαλίζουν την προστασία των προσωπικών δεδομένων. Ο τελευταίος καθιερώνει αυστηρούς κανόνες για τη συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων, ενώ παράλληλα επιβάλλει σοβαρές κυρώσεις για παραβιάσεις. Ο κανονισμός ενισχύει τα δικαιώματα των ατόμων, όπως το δικαίωμα πρόσβασης, το δικαίωμα στη διόρθωση και το δικαίωμα στη διαγραφή των δεδομένων τους, γνωστό και ως «δικαίωμα στη λήθη».

[6] Βλ. υποθέσεις Olmstead v. United States (1928), Katz v. United States (1967), Smith v. Maryland (1979), Florida v. Jardines (2013), Riley v. California (2014), Carpenter v. United States (2018).

Η ευρωπαϊκή προσέγγιση δίνει, επίσης, έμφαση στην ανεξαρτησία των εθνικών αρχών προστασίας δεδομένων, οι οποίες επιβλέπουν και διασφαλίζουν την εφαρμογή της νομοθεσίας. Ο ΓΚΠΔ απαιτεί από τις επιχειρήσεις και τους οργανισμούς να εφαρμόζουν τις βασικές αρχές προστασίας δεδομένων από τον σχεδιασμό (privacy by design) και από προεπιλογή (privacy by default), εξασφαλίζοντας ότι τα προσωπικά δεδομένα προστατεύονται σε κάθε στάδιο της επεξεργασίας τους.

Είναι ενδιαφέρον ότι η νομολογία των ευρωπαϊκών δικαστηρίων, όπως του ΕΔΑΔ [7], έχει επεκτείνει την έννοια της ιδιωτικής ζωής για να συμπεριλάβει όχι μόνο τον ιδιωτικό χώρο του ατόμου αλλά και τον επαγγελματικό και ψηφιακό χώρο, διασφαλίζοντας έτσι μια ευρεία προστασία της ιδιωτικότητας. Αυτή η προσέγγιση αντικατοπτρίζει τη δέσμευση της Ευρώπης για την προάσπιση των ατομικών δικαιωμάτων σε ένα περιβάλλον που σέβεται την ανθρώπινη αξιοπρέπεια και την προσωπική αυτονομία.

Συμπερασματικά, το ευρωπαϊκό κανονιστικό πλαίσιο αντανακλά μια βαθιά ριζωμένη κουλτούρα προστασίας της ιδιωτικότητας, όπου η προστασία των προσωπικών δεδομένων θεωρείται ζωτικής σημασίας για τη διατήρηση της ανθρώπινης αξιοπρέπειας και της ατομικής ελευθερίας, συστατικά στοιχεία της ιδιωτικότητας.

1.3. Η ανθρώπινη αξία, η προσωπική ελευθερία και το δικαίωμα στην ιδιωτική ζωή σύμφωνα με την ελληνική έννομη τάξη

Η έννοια της ανθρώπινης αξίας, όπως αναγνωρίζεται από το ελληνικό Σύνταγμα και το άρθρο 2 παρ. 1, θεμελιώνεται στην αρχή της αυτονομίας του ατόμου και της ακεραιότητας της προσωπικότητάς του. Ο σεβασμός προς την ανθρώπινη αξία αποτελεί όχι μόνο μια συνταγματική επιταγή αλλά και τη βάση πάνω στην οποία δομείται ολόκληρη η έννομη τάξη, καθιστώντας τον άνθρωπο το κεντρικό υποκείμενο των δικαιωμάτων και

[7] Βλ. Niemietz κατά Γερμανίας (1992), Amann κατά Ελβετίας (2000), K.U. κατά Φινλανδίας (2008), Klass κατά Γερμανίας (1978), Malone κατά Ηνωμένου Βασιλείου (1984), Copland κατά Ηνωμένου Βασιλείου (2007), Halford κατά Ηνωμένου Βασιλείου (1997), Niemietz κατά Γερμανίας (1992), Klass κατά Γερμανίας (1978), Amann κατά Ελβετίας (2000). Στις υποθέσεις **Klass κατά Γερμανίας (1978)**, **Malone κατά Ηνωμένου Βασιλείου (1984)**, και **Copland κατά Ηνωμένου Βασιλείου (2007)**, το ΕΔΑΔκαθόρισε ότι οι ηλεκτρονικές επικοινωνίες και η παρακολούθησή τους εμπίπτουν στην έννοια της ιδιωτικής ζωής και προστατεύονται από το άρθρο 8 της ΕΣΔΑ. Οι αποφάσεις αυτές υπογράμμισαν ότι οποιαδήποτε επέμβαση στην ιδιωτική ζωή, όπως παρακολουθήσεις τηλεφωνικών συνομιλιών ή ηλεκτρονικών μηνυμάτων, πρέπει να γίνεται με βάση το νόμο και να είναι αναλογική προς τον επιδιωκόμενο σκοπό.

υποχρεώσεων, και αναγνωρίζοντας την κρατική εξουσία ως θεματοφύλακα της ανθρώπινης αξιοπρέπειας. Για τον Häberle (1982), η ανθρώπινη αξία λειτουργεί ως «αφετηρία της κρατικής εξουσίας»[8], ενώ για τον Bleckmann (1988), η αξία του ανθρώπου του άρθρου 2 παρ.1 του Σ ορίζεται ως η σπονδυλική στήλη του συστήματος αξιών της συνταγματικής τάξης.

Συνολικά, η ελληνική έννομη τάξη έχει συνθέσει ένα πλαίσιο που όχι μόνο αναγνωρίζει την ανθρώπινη αξία και την ιδιωτική ζωή ως θεμελιώδη δικαιώματα, αλλά τα προστατεύει ενεργά από οποιαδήποτε μορφή εργαλειοποίησης ή καταπάτησης, διασφαλίζοντας έτσι την πλήρη ανάπτυξη και ελευθερία της προσωπικότητας κάθε ατόμου. Στην απόφαση 4701/2002, το Μονομελές Πρωτοδικείο Αθηνών αναγνωρίζει ότι «Η ιδιωτική ζωή συνιστά τον πυρήνα της ανθρώπινης προσωπικότητας, της αξίας του ανθρώπου. Με άλλα λόγια, η ιδιωτική ζωή τελεί σε εγγενή και μάλιστα κεντρική σχέση προς τη θεμελιώδη αξία της αξίας του ανθρώπου. Ο ιδιωτικός βίος, η ελευθερία και η αξία του ανθρώπου τελούν σε τέτοια σχέση ώστε η απουσία ή η διακινδύνευση ενός από τα τρία δικαιώματα πλήττει σοβαρά τα άλλα».

Συμπερασματικά, η ιδιωτικότητα θεωρείται θεμελιώδες και αναπαλλοτρίωτο στοιχείο της αξίας του ανθρώπου, καθώς συνδέεται άμεσα με τον πυρήνα της ατομικότητάς του. Αυτό σημαίνει ότι η ιδιωτικότητα δεν προστατεύει μόνο τις εξωτερικές εκφάνσεις της ανθρώπινης ζωής, όπως είναι οι κοινωνικές και επαγγελματικές σχέσεις, αλλά αγγίζει και τις εσωτερικές πλευρές, όπως τις προσωπικές σκέψεις, τις πεποιθήσεις και τα συναισθήματα. Η έννοια της ιδιωτικότητας περιλαμβάνει την ελευθερία του ατόμου να διατηρεί την εσωτερική του ζωή απαλλαγμένη από εξωτερικές παρεμβάσεις, καθώς και την αυτονομία να επιλέγει ποια στοιχεία της προσωπικής του ζωής θα μοιραστεί με τον ευρύτερο κόσμο.

Αυτή η προσέγγιση υποστηρίζεται από τους E. Hintz και M. Winterberg, οι οποίοι, στο άρθρο τους στη Zeitschrift fur Rechtpolitik (2001, σελ. 295), τονίζουν τη σημασία της ιδιωτικότητας ως έναν από τους ακρογωνιαίους λίθους που διαμορφώνουν την ατομικότητα και την αξία του ανθρώπου. Η προστασία της ιδιωτικότητας επιτρέπει στα άτομα να αναπτύξουν τη δική τους προσωπική ταυτότητα και να ακολουθήσουν τις δικές τους ηθικές

[8] Σύμφωνα με τον Häberle, το συνταγματικό κράτος έχει διπλό θεμέλιο, ήτοι την λαϊκή κυριαρχία και την ανθρώπινη αξιοπρέπεια.

και κοινωνικές επιλογές, χωρίς τον φόβο της αδικαιολόγητης παρακολούθησης ή της παρέμβασης από τρίτους, είτε αυτοί είναι κρατικές αρχές είτε ιδιωτικοί φορείς.

Όπως η ιδιωτικότητα αποτελεί έναν αδιαπραγμάτευτο πυλώνα της ανθρώπινης αξιοπρέπειας και της ελεύθερης ανάπτυξης της προσωπικότητας, αναγνωρίζοντας την ως κρίσιμο συστατικό της σύγχρονης αντίληψης για τα θεμελιώδη δικαιώματα και τις συνταγματικές ελευθερίες, έτσι και η ανθρώπινη αξία και το δικαίωμα στην ελεύθερη ανάπτυξη της προσωπικότητας (άρθρο 5, παράγραφος 1 του Σ)[9] συνυπάρχουν στο πλαίσιο της γενικότερης ελευθερίας του ανθρώπου να διαμορφώνει το περιεχόμενο της προσωπικότητάς του, αν και η έννοια της ανθρώπινης αξίας είναι ευρύτερη από αυτή της προσωπικής ελευθερίας.

Η Ακριβοπούλου (2011) στο πολύ ενδιαφέρον κείμενό της «Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από τον φακό του δικαιώματος στην ιδιωτική ζωή», εμβαθύνει στη διάκριση μεταξύ των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής. Παρόλο που τα δύο δικαιώματα δεν μπορούν να διαχωριστούν πλήρως, καθώς το ένα αποτελεί προέκταση του άλλου, η ιδιωτικότητα συχνά λειτουργεί ως προπαρασκευαστικό πεδίο για την έκφραση και την επικοινωνία, που το δικαίωμα στην προσωπικότητα προστατεύει και υλοποιεί. Αυτή η στενή σχέση δικαιώνει την κοινή τους αναπαράσταση στη θεωρία μέσω μεταφορών όπως το «κρεμμύδι» με τις πολλαπλές του στρώσεις ή τις επάλληλες «σφαίρες». Στην πράξη, αυτή η αλληλοσύνδεση εξηγεί γιατί σε ορισμένα νομικά συστήματα, όπως το γερμανικό ή το αμερικανικό, καθώς και στο κείμενο της ΕΣΔΑ,[10] η προστασία ενός εκ των δύο δικαιωμάτων αρκεί για την έμμεση προστασία και του άλλου.

Ωστόσο, παρά την αλληλεξάρτηση, τα δικαιώματα της προσωπικότητας και της ιδιωτικής ζωής διατηρούν διακριτές διαστάσεις. Το δικαίωμα στην ιδιωτική ζωή έχει εσωτερικό και ηθικό χαρακτήρα, επικεντρώνεται στην προστασία της ατομικότητας και της προσωπικής αυτονομίας του ατόμου. Αντίθετα, το δικαίωμα της προσωπικότητας εκτείνεται στην εξωτερική σφαίρα, καλύπτοντας τις κοινωνικές, οικονομικές και πολιτικές εκφράσεις

[9] «Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη».

[10] Για παράδειγμα, η προστασία που παρέχει το άρθρο 8 παρ. 1 της ΕΣΔΑ καλύπτει τόσο την προσωπικότητα όσο και την ιδιωτικότητα του ατόμου.

της ύπαρξης του ατόμου. Αποτελεί συνδυασμό ηθικών και υλικών στοιχείων, ενσωματώνοντας ποικίλα επιμέρους δικαιώματα, όπως η αξιοπρέπεια, η τιμή, η εικόνα, το όνομα και η πνευματική ιδιοκτησία.

Όπως θα δούμε και παρακάτω διεξοδικότερα, το δικαίωμα στην προστασία των προσωπικών δεδομένων τοποθετείται διακριτά στο ενδιάμεσο πεδίο μεταξύ των δικαιωμάτων της προσωπικότητας και της ιδιωτικότητας, αναλαμβάνοντας έναν κρίσιμο ρόλο στη διαχείριση και αντιμετώπιση των προσβολών που δύνανται να ανακύψουν από τη συλλογή, αποθήκευση, επεξεργασία ή χρήση των προσωπικών δεδομένων ενός ατόμου. Στην ουσία του, το δικαίωμα αυτό αναδεικνύει τις εν δυνάμει παραβιάσεις που τα δικαιώματα στην προσωπικότητα και την ιδιωτική ζωή μπορεί να υποστούν, ιδίως υπό το πρίσμα των σύγχρονων τεχνολογικών εξελίξεων και της εντατικής συλλογής πληροφοριών.

1.3.1. Το δικαίωμα στην προστασία των προσωπικών δεδομένων και η σχέση του με την ιδιωτικότητα

Στην Ελλάδα, το δικαίωμα στην προστασία των προσωπικών δεδομένων συνδέθηκε άρρηκτα με τα δικαιώματα της προσωπικότητας και της ιδιωτικής ζωής, με βάση τη διάκριση μεταξύ απλών και ευαίσθητων δεδομένων που εισήγαγε ο Νόμος 2472/1997. Η συνταγματική αναθεώρηση του 2001 αποτέλεσε σταθμό για την ελληνική νομική πραγματικότητα, καθώς το δικαίωμα αυτό αναγνωρίστηκε ρητά στο άρθρο 9^{α} Σ[11] το οποίο καθιερώνει ένα ισοδύναμο στο άρθρο 5^{α} δικαίωμα[12].

Σύμφωνα με την Παναγοπούλου-Κουτνατζή (2023), η προστασία που παρέχει το άρθρο 9^{α} δεν οδηγεί σε απόλυτο περιορισμό, αλλά απαιτεί την καθιέρωση ενός θεσμικού πλαισίου εντός του οποίου θεωρείται θεμιτή η συλλογή, επεξεργασία και χρήση των

[11] «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

[12] «1. Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων.2. Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19».

δεδομένων. Ειδικότερα, στην εποχή της ηλεκτρονικής διακινδύνευσης, η ανάγκη προστασίας της ιδιωτικής ζωής ως ατομικό, αμυντικό δικαίωμα, έγκειται α) στην απαγόρευση καταγραφής δεδομένων σε συγκεκριμένες περιπτώσεις, και β) στην άρνηση παροχής πληροφοριών για τον εαυτό μας.

Είναι σημαντικό να κατανοήσουμε ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων θεμελιώνεται στα δικαιώματα της προσωπικότητας και της ιδιωτικότητας, χωρίς ωστόσο να ταυτίζεται πλήρως με αυτά. Όπως παρατηρεί και η Ακριβοπούλου (ibid), το δικαίωμα στην προστασία των προσωπικών δεδομένων, όπως αναδεικνύεται μέσα από τη νομολογία και τη θεωρία, παρουσιάζει έναν ιδιόμορφο χαρακτήρα ετεροαναφορικότητας. Η ετεροαναφορικότητα του δικαιώματος έγκειται στο γεγονός ότι αντλεί την ηθική του θεμελίωση από άλλα δικαιώματα, ενώ ταυτόχρονα λειτουργεί ως εγγυητής και αμυντικός μηχανισμός για την προστασία τους.

Για παράδειγμα, υπάρχουν πληροφορίες που μπορεί να είναι απόρρητες χωρίς να είναι ιδιωτικές ή προσωπικές, όπως συμβαίνει με τα στρατιωτικά απόρρητα έγγραφα. Αντίστοιχα, υπάρχουν κατηγορίες δεδομένων που δεν προστατεύονται απαραίτητα από την έννοια της προσωπικότητας, καθώς υπερβαίνουν τα ατομικά όρια και διεισδύουν σε βαθύτερους τομείς που προστατεύονται από την ιδιωτικότητα, όπως τα δεδομένα που αφορούν τον σεξουαλικό προσανατολισμό, τη γενετική ταυτότητα ή την αναπαραγωγή. Αυτά τα δεδομένα, χαρακτηριζόμενα ως ευαίσθητα, συνδέονται με την ουσία της ύπαρξης του ατόμου και τη δυνατότητά του να καθορίζει ελεύθερα και αυτόνομα την ταυτότητά του.

Επίσης, ορισμένα δεδομένα, λόγω της ειδικής φύσης τους, μπορεί να μην εμπίπτουν στον στενό ορισμό της προσωπικότητας, όπως τα δεδομένα που σχετίζονται με το

θρήσκευμα, τα οποία προστατεύονται συνδυαστικά από τα άρθρα 9α και 13Σ[13] ή τα δεδομένα τηλεφωνικών συνδιαλέξεων, που καλύπτονται από τα άρθρα 9α και 19 παρ.1Σ[14].

Αυτός ο πλουραλισμός στην προστασία υπογραμμίζει τον ιδιαίτερο ρόλο της συνταγματικής αναγνώρισης των προσωπικών δεδομένων ως εργαλείο που ενισχύει την ακεραιότητα της προσωπικότητας και της ιδιωτικής ζωής, προσφέροντας ένα ευέλικτο και πολυδιάστατο πλαίσιο προστασίας απέναντι σε διαφορετικές μορφές παραβίασης.

1.3.2. Ιδιωτικότητα και απόρρητο

Η παραδοσιακή αντίληψη της ιδιωτικότητας ως χώρου προστασίας παρουσιάζει αξιοσημείωτες ομοιότητες και, σε ορισμένες περιπτώσεις, συγχέεται με τις έννοιες του απορρήτου και της εμπιστευτικότητας. Αν και αυτοί οι όροι συχνά χρησιμοποιούνται εναλλακτικά και αποσκοπούν στην προάσπιση παρεμφερών αξιώσεων προστασίας, είναι κρίσιμο να αναγνωριστεί ότι δεν είναι απολύτως ισοδύναμοι (Μήτρου, 2010).

Το άρθρο 19 Σ διασφαλίζει την προστασία του απορρήτου των επιστολών και κάθε μορφής επικοινωνίας, επισημαίνοντας δύο βασικές πτυχές που είναι στενά συνδεδεμένες: αφενός, την ελευθερία της επικοινωνίας και αφετέρου, το δικαίωμα στο απόρρητο αυτής της επικοινωνίας, εφόσον οι συμμετέχοντες επιθυμούν τη διατήρηση της μυστικότητας. Αυτή η συνταγματική διάταξη επεκτείνει την έννοια της προσωπικής ελευθερίας σε ευρεία έννοια, προστατεύοντας την επικοινωνία υπό συνθήκες ιδιωτικότητας, σε αντίθεση με το άρθρο 14, το οποίο επικεντρώνεται στην ελευθερία της επικοινωνίας σε δημόσιο πλαίσιο. Αυτή η

[13] «1. Η ελευθερία της θρησκευτικής συνείδησης είναι απαραβίαστη. Η απόλαυση των ατομικών και πολιτικών δικαιωμάτων δεν εξαρτάται από τις θρησκευτικές πεποιθήσεις καθενός.2. Κάθε γνωστή θρησκεία είναι ελεύθερη και τα σχετικά με τη λατρεία της τελούνται ανεμπόδιστα υπό την προστασία των νόμων. Η άσκηση της λατρείας δεν επιτρέπεται να προσβάλλει τη δημόσια τάξη ή τα χρηστά ήθη. Ο προσηλυτισμός απαγορεύεται.3. Οι λειτουργοί όλων των γνωστών θρησκειών υπόκεινται στην ίδια εποπτεία της Πολιτείας και στις ίδιες υποχρεώσεις απέναντί της, όπως και οι λειτουργοί της επικρατούσας θρησκείας.4. Κανένας δεν μπορεί, εξαιτίας των θρησκευτικών του πεποιθήσεων, να απαλλαγεί από την εκπλήρωση των υποχρεώσεων προς το Κράτος ή να αρνηθεί να συμμορφωθεί προς τους νόμους.5. Κανένας όρκος δεν επιβάλλεται χωρίς νόμο, που ορίζει και τον τύπο του».

[14] «1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων».

προστασία της ιδιωτικότητας προσδίδει στο δικαίωμα έναν έντονα «προσωπικό» χαρακτήρα, καθιστώντας το ουσιαστικά δικαίωμα προσωπικής ελευθερίας.

Το απόρρητο της επικοινωνίας λειτουργεί ως σημείο σύγκλισης διαφορετικών συνταγματικών δικαιωμάτων, τα οποία αλληλοεπικαλύπτονται και ενισχύουν το ένα το άλλο. Συγκεκριμένα, σχετίζεται άμεσα με την προσωπική ελευθερία, καθώς προστατεύει την ιδιωτική ζωή και αποτελεί ουσιαστικά προέκταση του ασύλου της κατοικίας. Επίσης, συνδέεται με την πνευματική ελευθερία και την ελευθερία της έκφρασης, διασφαλίζοντας την ελεύθερη διακίνηση ιδεών και πληροφοριών. Τέλος, έχει άμεση σχέση με το δικαίωμα στην ιδιοκτησία, και ειδικότερα στην πνευματική ιδιοκτησία, δεδομένου ότι οι επιστολές ή άλλες μορφές επικοινωνίας μπορούν να έχουν οικονομική ή πνευματική αξία και να θεωρούνται περιουσιακά στοιχεία του αποστολέα ή του παραλήπτη.

Η αντίληψη ότι το περιεχόμενο των επικοινωνιών πρέπει να παραμένει απροσπέλαστο και εμπιστευτικό υπερβαίνει την απλή ανάγκη για εχέμυθη επικοινωνία και στοχεύει στην ευρύτερη προστασία της ιδιωτικής ζωής του ατόμου. Η σύνδεση του δικαιώματος αυτού με την ιδιωτική ζωή είναι καθοριστικής σημασίας, καθώς το δικαίωμα ενός ατόμου να επικοινωνεί με επιλεγμένα άτομα σε κλίμα εχεμύθειας και εμπιστοσύνης ενισχύει την ανάπτυξη στενών και προσωπικών σχέσεων που διαφέρουν από τις γενικότερες κοινωνικές αλληλεπιδράσεις. Η προστασία αυτών των σχέσεων μέσω της διασφάλισης της εμπιστευτικότητας της επικοινωνίας συμβάλλει στην ενίσχυση της προσωπικής αυτονομίας και της κοινωνικής συνοχής (Κουφάκη, 2019).

Επομένως, το άρθρο 19 παρ. 1 Σ θέτει αυστηρές απαγορεύσεις: α) στην παρακολούθηση, τον έλεγχο και την καταγραφή επικοινωνιών, β) στη λογοκρισία ή οποιαδήποτε μορφή παρεμπόδισης της επικοινωνίας και γ) στη χρήση αποδεικτικών στοιχείων που αποκτήθηκαν κατά παράβαση της συνταγματικής προστασίας του απορρήτου, είτε από δημόσιες αρχές είτε ενώπιον τους. Αυτές οι απαγορεύσεις διασφαλίζουν ότι η προστασία του απορρήτου των επικοινωνιών παραμένει ακέραιη και αποτελεσματική, υποστηρίζοντας την ελευθερία της προσωπικής έκφρασης και τη διατήρηση της ιδιωτικής σφαίρας σε ένα περιβάλλον που σέβεται τα συνταγματικά δικαιώματα και τις ατομικές ελευθερίες.

2. ΨΗΦΙΑΚΟΣ ΑΝΘΡΩΠΙΣΜΟΣ

2.1. Εισαγωγή στον ψηφιακό ανθρωπισμό

Ο ψηφιακός ανθρωπισμός έκανε την εμφάνισή του ως κοινωνικό και πολιτικό κίνημα τον Μάιο του 2019 μετά από ένα διεθνές συνέδριο στο Τεχνολογικό Πανεπιστήμιο της Βιέννης το οποίο κατέληξε στο Μανιφέστο της Βιέννης ως «πρόσκληση για διαβούλευση και δράση σχετικά με την τεχνολογική ανάπτυξη» (Vienna Manifesto, 2019). Το μανιφέστο συντάχθηκε από 31 ακαδημαϊκούς συγγραφείς από διάφορα πανεπιστήμια της Αυστρίας, της Ιταλίας, των Κάτω Χωρών, της Ελβετίας, της Γερμανίας και των ΗΠΑ. Μετά τη δημοσίευσή του και μέχρι το τέλος 2023, το Μανιφέστο της Βιέννης για τον Ψηφιακό Ανθρωπισμό έχει υπογραφεί από περισσότερους από χίλιους εμπειρογνώμονες και οργανισμούς παγκοσμίως και έχει μεταφραστεί σε οκτώ γλώσσες.

Ο Prem (2024) αναφέρει για το Μανιφέστο ότι ξεκινώντας από μια διαγνωσμένη συνεξέλιξη της τεχνολογίας και της ανθρωπότητας, αποτελεί ευκαιρία για μια νέα «αναζήτηση του διαφωτισμού και του ανθρωπισμού» καθώς και αφορμή για κάλεσμα για να καθοδηγήσουμε την τεχνολογική ανάπτυξη προς μια ανθρωπιστική κατεύθυνση.

Το μανιφέστο της Βιέννης ξεκινά με το απόσπασμα του Tim Berners-Lee «Το σύστημα αποτυγχάνει» και ζητά δράση, συμπεριλαμβανομένης της ρύθμισης (Werthner et al., 2022). Απαριθμεί έντεκα βασικές αρχές για την ανάπτυξη ενός καλύτερου ψηφιακού μέλλοντος που δίνουν έμφαση στη δημοκρατία και τις δημοκρατικές αξίες όπως είναι η ελευθερία του λόγου ή της έκφρασης και η προστασία της ιδιωτικής ζωής. Τονίζει την αναγκαιότητα για αυστηρότερη ρύθμιση του ψηφιακού τομέα και των τεχνολογικών μονοπωλίων και πλατφορμών με βάση έναν ευρύ ακαδημαϊκό και δημόσιο διάλογο.

Οι ανωτέρω αρχές τάσσονται υπέρ ενός συνδυασμού τεχνικών δεξιοτήτων και ηθικής και κοινωνικής αφύπνισης. Τα πανεπιστήμια καλούνται να δημιουργήσουν την απαραίτητη γνώση μέσω της διαβούλευσης των ερευνητών με την ευρύτερη κοινωνία και την εισαγωγή νέων προγραμμάτων σπουδών στην επιστήμη της πληροφορικής, ενώ οι επαγγελματίες καλούνται, αντίστοιχα, να αναλάβουν την ευθύνη για τον αντίκτυπο των τεχνολογιών που αναπτύσσουν. Εκτός, από μια ακαδημαϊκή χροιά, υποβόσκει και μια έντονη πολιτική συνιστώσα καθώς η ακαδημαϊκή κοινότητα καλείται να διαμορφώσει ενεργά την τεχνολογική ανάπτυξη, δηλαδή την τεχνολογική πολιτική.

Ο ακόλουθος πίνακας (Πίνακας 1) παρέχει έναν κατάλογο των θεμάτων που θίγει το κίνημα, ομαδοποιημένων κατά μήκος τεσσάρων τομέων ενδιαφέροντος: ο άνθρωπος, η κοινωνία, η οικονομία και το κράτος.

Άνθρωπος	Οικονομία	Κοινωνία	Κράτος
Αυτοματοποίηση της εργασίας	Επιτήρηση	Οικονομία των πλατφορμών	Δημοκρατία
Ανθρώπινη ταυτότητα	Ηθική τεχνολογία	Τεχνολογικά μονοπώλια	Ψηφιακές πολιτικές και ρύθμιση
Ανθρώπινη αξιοπρέπεια	Δημόσιος διάλογος, Fake news	Ρύθμιση της τεχνολογίας και των τεχνολογικών εταιρειών	Κυριαρχία
Ιδιωτικότητα	Ελευθερία του λόγου	Δικαιώματα των καταναλωτών	Γεωπολιτική
Αλγοριθμικός έλεγχος και αποφάσεις	Ανθρώπινα δικαιώματα		
Εκπαίδευση	Προσαρμοστικότητα		

Πίνακας 1: Επισκόπηση των βασικών θεμάτων στον ψηφιακό ανθρωπισμό που ομαδοποιούνται σε τέσσερις τομείς ενδιαφέροντος (Prem, ibid)

Σε γενικές γραμμές, οι υπέρμαχοι του ψηφιακού ανθρωπισμού προωθούν μια προσέγγιση που είναι ευνοϊκή προς τον άνθρωπο (Nida-Rümelin & Weidenfeld, 2022) και επικεντρώνεται στην ανθρωποκεντρικότητα (Werthner et al., ibid) όσον αφορά τη χρήση της ψηφιακής τεχνολογίας και τη διαμόρφωση της κοινωνίας. Αυτή η προσέγγιση αντλεί έμπνευση εν μέρει από τις αρχές του αναγεννησιακού ανθρωπισμού και του Διαφωτισμού. Οι υποστηρικτές της θεωρίας αυτής υποστηρίζουν την ανάγκη για εναρμόνιση της τεχνολογίας με τις ανθρωπιστικές αξίες και αμφισβητούν αντιλήψεις και πρακτικές που ενδέχεται να παραγκωνίσουν τον άνθρωπο, να υπονομεύσουν την ανθρώπινη λογική, τις δεξιότητες και τη δημιουργικότητα (Scuotto et al., 2023), καθώς και να θυσιάσουν τις ανθρώπινες αξίες στον βωμό της τεχνολογικής προόδου. Για να αποσαφηνίσει την έννοια του ψηφιακού ανθρωπισμού, ο Coeckelbergh (2024) διακρίνει τις εξής συνιστώσες:

α) Η πρώτη συνιστώσα αφορά την εικόνα του ανθρώπου στην ψηφιακή εποχή. Οι ψηφιακοί ανθρωπιστές αμφισβητούν τη σύγχρονη αντίληψη περί μηχανοποίησης του

ανθρώπου. Απορρίπτουν την ιδέα του τεχνητού ανθρώπου με ό,τι αυτό συνεπάγεται για την ανθρώπινη φύση και προασπίζονται τον ανθρωπιστικό ορισμό του ανθρώπου.

β) Η δεύτερη συνιστώσα αναφέρεται στην ιδέα ότι οι άνθρωποι πρέπει να διατηρούν τον έλεγχο της ψηφιακής τεχνολογίας. Κρίσιμος στόχος του ψηφιακού ανθρωπισμού είναι να τεθεί υπό ανθρώπινο έλεγχο η τεχνητή νοημοσύνη και οι εφαρμογές της, κυρίως, μέσω της υιοθέτησης τεχνικών και οργανωτικών μέτρων που θα αναλυθούν σε επόμενη ενότητα.

γ) Η τρίτη συνιστώσα αφορά την ανθρωποκεντρική ηθική η οποία συνεπάγεται την ανθρώπινη παρέμβαση ήδη στο στάδιο του σχεδιασμού των τεχνολογικών προϊόντων έτσι ώστε οι ψηφιακές τεχνολογίες να υιοθετούν τις ανθρώπινες αξίες και αρχές, όπως είναι η ανθρώπινη αξιοπρέπεια, η δημοκρατία, η συμμετοχικότητα, η δικαιοσύνη, η λογοδοσία, τα ανθρώπινα δικαιώματα, και ούτω καθεξής.

δ) Η τέταρτη συνιστώσα αφορά τη διεπιστημονικότητα και τη συνεργασία της πληροφορικής με τους μελετητές των ανθρωπιστικών και κοινωνικών επιστημών έτσι ώστε να προχωρήσουμε σε μια πιο ολιστική κατανόηση των προβλημάτων της ανθρωπότητας. Η εισαγωγή προγραμμάτων σπουδών που διδάσκουν την τεχνολογική ηθική στους προγραμματιστές, τους μηχανικούς και τους επιστήμονες πληροφορικής αποτελεί βασική πρόταση των ψηφιακών ανθρωπιστών.

ε) Η πέμπτη συνιστώσα σχετίζεται με την άποψη ότι ο ψηφιακός ανθρωπισμός λόγω της σαφούς πολιτικής συνιστώσας, απαιτεί (περισσότερο ή λιγότερο) ριζοσπαστικές πολιτικές μεταρρυθμίσεις για την επίτευξη των άλλων συνιστωσών. Πολλοί από τους ακόλουθους αυτού του κινήματος αμφισβητούν το καπιταλιστικό σύστημα και υπερασπίζονται μια συγκεκριμένη μορφή κοινωνικής και πολιτικής οργάνωσης: τη δημοκρατία. Άλλωστε, η πρώτη αρχή του Μανιφέστου πρεσβεύει ότι οι ψηφιακές τεχνολογίες θα πρέπει να σχεδιάζονται για να προωθούν τη δημοκρατία και την ένταξη.

Είναι γεγονός ότι αυτή η πολιτική διάσταση δεν πρέπει να μας εκπλήσσει, εφόσον κάθε κίνημα που επιδιώκει να αλλάξει την τεχνολογία είναι εξ ορισμού πολιτικό. Και οι ψηφιακές τεχνολογίες, όπως όλες οι τεχνολογίες, είναι ήδη οι ίδιες πολιτικές καθώς εκτός από πολιτικούς σκοπούς εμπεριέχουν την εμπλοκή με ευρύτερα πολιτικά και κοινωνικά ζητήματα, όπως είναι οι διακρίσεις και ο κοινωνικός αποκλεισμός.

2.2. Ψηφιακός ανθρωπισμός και ιδιωτικότητα

Παρά τη δυναμική των σύγχρονων τεχνολογιών να βελτιώσουν την ανθρώπινη ευημερία, οι ίδιες τεχνολογίες μπορούν, επίσης, να προκαλέσουν σημαντικές αρνητικές συνέπειες. Ο διάλογος γύρω από τις επιπτώσεις των νέων τεχνολογιών εστιάζει κυρίως στους κινδύνους που ελλοχεύουν για την προστασία της ιδιωτικότητας των δεδομένων: πώς η κακή χρήση των δεδομένων των χρηστών μπορεί να προκαλέσει ψυχολογικές, κοινωνικές, οικονομικές επιπτώσεις ή θέματα ασφαλείας (Redmiles, 2022).

Είναι ενδιαφέρον ότι οι οπαδοί του ψηφιακού ανθρωπισμού πηγαίνουν τη συζήτηση για την προστασία της ιδιωτικής ζωής ένα βήμα παρακάτω μιλώντας για την ανάγκη καλλιέργειας τεχνολογιών που δε σέβονται απλά την ιδιωτικότητα των δεδομένων, αλλά και τις προσδοκίες των χρηστών για τη χρήση της τεχνολογίας και το πλαίσιο στο οποίο λαμβάνει χώρα αυτή η χρήση[15] (Redmiles, ibid).

Ως έννοια, η ιδιωτικότητα είναι σύνθετη και αφορά πολλούς τομείς της κοινωνίας. Είναι ενδιαφέρον ότι ο ορισμός της ιδιωτικής ζωής ως «το δικαίωμα να μείνει κανείς μόνος» πρωτοεμφανίστηκε σε ένα άρθρο της Νομικής Επιθεώρησης του 1890 (Brandeis & Warren,1890) και αφορμή ήταν η αυξημένη πώληση φωτογραφικών μηχανών. Έκτοτε, έχουν δημοσιευθεί πολυάριθμες εννοιολογικές αναλύσεις της ιδιωτικότητας, με τον ορισμό του Altman να είναι ένας από τους πιο σημαντικούς. Ο Altman (Palen and Dourish, 2003, σελ. 129)[16] ορίζει την ιδιωτικότητα ως τον «επιλεκτικό έλεγχο της πρόσβασης στον εαυτό ή στην ομάδα».

---

[15] Η Redmiles υποστηρίζει ότι η υιοθέτηση της τεχνολογίας καθοδηγείται από την αντίληψη των χρηστών για το αν η τεχνολογία θα σεβαστεί τις προσδοκίες τους σχετικά με τη χρήση των δεδομένων και την συνολική της επίδραση στη ζωή τους. Επίσης, κριτικάρει το «παράδοξο της ιδιωτικότητας», όπου οι πραγματικές συμπεριφορές των χρηστών συχνά δεν συμβαδίζουν με τις εκφρασμένες ανησυχίες τους για την ιδιωτικότητα, προτείνοντας να ξεφύγουμε από τη μονοδιάστατη εστίαση στην ιδιωτικότητα εξετάζοντας ένα ευρύτερο φάσμα παραγόντων που επηρεάζουν την υιοθέτηση και τον αντίκτυπο της τεχνολογίας, όπως η αποτελεσματικότητα, το κόστος και η ευχρηστία των τεχνολογιών.

[16] Η ιδιωτικότητα παραδοσιακά θεωρείται ως μια κατάσταση κοινωνικής απομόνωσης, δηλαδή αποφυγής των άλλων ανθρώπων. Ωστόσο, ο Altman την αντιλαμβάνεται ως μια διαλεκτική και δυναμική διαδικασία ρύθμισης των ορίων, όπου η ιδιωτικότητα δεν είναι στατική, αλλά αποτελεί έναν επιλεκτικό έλεγχο της πρόσβασης στον εαυτό μας ή στην ομάδα μας. Σύμφωνα με τον Altman, η «διαλεκτική» αναφέρεται στην αλληλεπίδραση μεταξύ του ανοιγόμενου εαυτού προς τους άλλους και της απομάκρυνσης από αυτούς, δηλαδή στην επιδίωξη ή την αποφυγή της κοινωνικής επαφής. Η «δυναμική» πλευρά της ιδιωτικότητας υποδηλώνει ότι το επιθυμητό επίπεδο ιδιωτικότητας,

Η τρέχουσα ερευνητική βιβλιογραφία διακρίνει τη φυσική, ψυχολογική, κοινωνική και πληροφοριακή ιδιωτικότητα και αγγίζει αντίστοιχα έννοιες, όπως ο προσωπικός χώρος και η φυσική πρόσβαση σε αυτόν, το δικαίωμα ελέγχου του με ποιον και υπό ποιες συνθήκες θα μοιραστεί κανείς τις σκέψεις του, τη δυνατότητα διατήρησης της ανωνυμίας και ελέγχου των κοινωνικών αλληλεπιδράσεων, καθώς και το πότε, πώς και σε ποιο βαθμό θα δοθούν πληροφορίες για τον εαυτό του σε άλλο πρόσωπο ή οργανισμό (Leino-Kilpi et al., 2001).

Τα τελευταία χρόνια, ιδίως μετά την εφαρμογή του ΓΚΠΔ, υπάρχει έντονη ανησυχία για τον όγκο των προσωπικών πληροφοριών που συλλέγονται από τις τεχνολογικές εφαρμογές και τις υπηρεσίες που χρησιμοποιούμε καθημερινά. Αυτή η εκτεταμένη συλλογή και εμπορευματοποίηση προσωπικών δεδομένων είναι κυρίως αποτέλεσμα των εταιρειών που συλλέγουν, αναλύουν και πωλούν προφίλ χρηστών με σκοπό τη στοχευμένη διαφήμιση, μια πρακτική γνωστή ως «**καπιταλισμός της επιτήρησης**» (Zuboff, 2019).

Μέχρι πρόσφατα, υπήρχε η κοινή πεποίθηση ότι η επιτήρηση ήταν κυρίως χαρακτηριστικό των λιγότερο δημοκρατικών χωρών, όπου χρησιμοποιείται ως μέσο για την παρακολούθηση και τον έλεγχο των πολιτών. Ένα χαρακτηριστικό παράδειγμα αυτής της πρακτικής είναι η Κίνα, όπου μελέτες έχουν δείξει ότι το περιεχόμενο που διαμοιράζονται διεθνείς χρήστες στην πλατφόρμα κοινωνικής δικτύωσης WeChat αξιοποιείται για τη βελτίωση των μηχανισμών λογοκρισίας στη χώρα (Knockel et al., 2020). Ωστόσο, αυτή η αντίληψη άλλαξε δραματικά μετά τις αποκαλύψεις του Edward Snowden το 2013, ο οποίος αποκάλυψε πως η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA) συγκέντρωνε τεράστιες ποσότητες δεδομένων από επικοινωνίες σε παγκόσμια κλίμακα, όπως ηλεκτρονικά

δηλαδή το ιδανικό επίπεδο κοινωνικής επαφής σε μια συγκεκριμένη στιγμή, δεν είναι σταθερό αλλά αλλάζει διαρκώς. Αυτό το επίπεδο μεταβάλλεται ανάλογα με ατομικές και πολιτισμικές διαφορές και προσαρμόζεται στις διαφορετικές συνθήκες που προκύπτουν με την πάροδο του χρόνου.
Με άλλα λόγια, το επιθυμητό επίπεδο ιδιωτικότητας μεταβάλλεται ανάλογα με το περιβάλλον και τις συνθήκες. Μπορεί σε μια στιγμή να θέλουμε να αποφεύγουμε τους άλλους, ενώ σε μια άλλη στιγμή να επιθυμούμε κοινωνική επαφή. Ο Altman επίσης υποστηρίζει ότι ο στόχος της ρύθμισης της ιδιωτικότητας είναι να επιτευχθεί το βέλτιστο επίπεδο ιδιωτικότητας, δηλαδή το ιδανικό επίπεδο κοινωνικής αλληλεπίδρασης. Στην προσπάθεια αυτή, όλοι προσπαθούμε να εναρμονίσουμε την επιτευχθείσα ιδιωτικότητα, δηλαδή το πραγματικό επίπεδο επαφής σε μια συγκεκριμένη στιγμή, με την επιθυμητή ιδιωτικότητα. Όταν επιτυγχάνουμε το βέλτιστο επίπεδο ιδιωτικότητας, μπορούμε να βιώνουμε την επιθυμητή μοναξιά όταν θέλουμε να είμαστε μόνοι ή να απολαμβάνουμε την επιθυμητή κοινωνική επαφή όταν επιθυμούμε την παρέα. Ωστόσο, αν το πραγματικό επίπεδο ιδιωτικότητας είναι υψηλότερο από το επιθυμητό, μπορεί να νιώσουμε μοναξιά ή απομόνωση, ενώ αν είναι χαμηλότερο από το επιθυμητό, μπορεί να νιώσουμε ενόχληση ή πίεση από τον συνωστισμό.

μηνύματα και αρχεία συνομιλιών (Gellman and Lindeman, 2013, Gellman and Poitras, 2013, Greenwald & MacAskill, 2013). Αν και η κοινή πεποίθηση που επικρατούσε ήταν ότι αυτά τα δεδομένα συλλέγονταν για λόγους εθνικής ασφάλειας, η πραγματικότητα είναι ότι η συλλογή τους γινόταν χωρίς τα απαραίτητα εντάλματα, στοχεύοντας ακόμα και σε αθώους πολίτες.

Μια από τις αιτίες που η NSA και άλλες κρατικές υπηρεσίες, όπως το Κυβερνητικό Αρχηγείο Επικοινωνιών του Ηνωμένου Βασιλείου (GCHQ), μπόρεσαν να πραγματοποιούν μαζική συλλογή δεδομένων ήταν η πρόσβασή τους σε πληροφορίες από μεγάλες τεχνολογικές εταιρείες, όπως η Google, το Facebook, η Microsoft και η Apple. Η συνεργασία ανάμεσα σε κυβέρνηση και ιδιωτικές εταιρείες επιβεβαιώθηκε περαιτέρω από αναφορές που έδειχναν ότι ομοσπονδιακές υπηρεσίες των ΗΠΑ, όπως το Υπουργείο Εσωτερικής Ασφάλειας και η Υπηρεσία Εσωτερικών Εσόδων, αγόραζαν εμπορικά διαθέσιμα δεδομένα από «μεσίτες δεδομένων» (Whittaker, 2023).

Η εκμετάλλευση των δεδομένων χρηστών από τις τεχνολογικές εταιρείες παρέχει στις κυβερνήσεις και στις υπηρεσίες επιβολής του νόμου πρόσβαση σε πληροφορίες που κανονικά δεν θα μπορούσαν να αποκτήσουν νόμιμα (Hoofnagle, 2003), όπως μέσω της «προγνωστικής αστυνόμευσης»[17]. Καθώς οι συσκευές του Διαδικτύου των Πραγμάτων (IoT) γίνονται όλο και πιο δημοφιλείς, επιτρέπουμε την καταγραφή ολοένα και περισσότερων προσωπικών πληροφοριών σχετικά με την καθημερινή μας ζωή και τις συνήθειές μας, όπως στην περίπτωση ενός «έξυπνου» σπιτιού. Δεν είναι τυχαίο ότι νέα πρότυπα μετάδοσης, όπως το Hybrid Broadcast Broadband TV (HbbTV) που αναπτύσσεται στην Ευρώπη, επιτρέπουν την παρακολούθηση σε πραγματικό χρόνο των προτιμήσεων των τηλεθεατών και τη δημιουργία εξατομικευμένων προφίλ συνδυάζοντας πληροφορίες από διάφορες πηγές μέσω του διαδικτύου (Tagliaro et al., 2023).

Το πιο ανησυχητικό είναι ότι η παρακολούθηση των προτιμήσεων και της συμπεριφοράς δεν περιορίζεται μόνο στην προώθηση προϊόντων, αλλά χρησιμοποιείται και

[17] Η **προληπτική αστυνόμευση** (ή **proactive policing** στα αγγλικά) αναφέρεται σε στρατηγικές και πρακτικές της αστυνομίας που έχουν ως στόχο την πρόληψη του εγκλήματος πριν αυτό συμβεί, αντί της παραδοσιακής αντίδρασης μετά τη διάπραξη ενός εγκλήματος. Αυτός ο τύπος αστυνόμευσης εστιάζει στην πρόληψη και την αποτροπή των παραβάσεων μέσω διαφόρων μεθόδων, όπως η παρουσίαση της αστυνομίας σε σημεία υψηλού κινδύνου, η χρήση δεδομένων και ανάλυσης πληροφοριών, καθώς και η συνεργασία με την κοινότητα.

για σκοπούς όπως η χειραγώγηση των δημόσιων και πολιτικών απόψεων. Ένα χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση της Cambridge Analytica, η οποία χρησιμοποίησε δεδομένα που συνέλεξε από το Facebook για πολιτικές εκστρατείες (Rosenberg et al., 2018).

Στο πλαίσιο του ψηφιακού ανθρωπισμού, οι βασικές διαφορές ανάμεσα στην επιτήρηση και την ιδιωτικότητα προκύπτουν από το γεγονός ότι η επιτήρηση αφορά τη συλλογή δεδομένων, ενώ η ιδιωτικότητα επικεντρώνεται στην προστασία και στον έλεγχο της χρήσης αυτών των πληροφοριών. Η επιτήρηση μπορεί να παραβιάζει το δικαίωμα της ιδιωτικής ζωής, εάν γίνεται χωρίς τη γνώση ή τη συγκατάθεση του ατόμου ή αν περιλαμβάνει τη συλλογή ευαίσθητων ή προσωπικών δεδομένων. Ωστόσο, η επιτήρηση μπορεί (και πρέπει) να σχεδιάζεται με τέτοιο τρόπο ώστε να αποτρέπει την κατάχρηση εξουσίας, (Gerber at al., 2018), να περιορίζει τη συλλογή προσωπικών δεδομένων και να προστατεύει την ιδιωτική ζωή, προσφέροντας παράλληλα σημαντικά οφέλη για την ασφάλεια της κοινωνίας.

Αν και η επιτήρηση και η προστασία της ιδιωτικής ζωής θεωρούνται συνήθως αντίθετες έννοιες, η επιτήρηση από μόνη της δεν είναι ούτε εγγενώς καλή ούτε κακή και μπορεί να είναι αναγκαία για το ευρύτερο κοινωνικό καλό και για τη διασφάλιση της εθνικής ασφάλειας παρέχοντας στις αρχές επιβολής του νόμου τα μέσα για τη διερεύνηση του εγκλήματος. Για παράδειγμα, το υλικό από τις κάμερες παρακολούθησης συνέβαλε καθοριστικά στην εξεύρεση των ενόχων για τη βομβιστική επίθεση στον Μαραθώνιο της Βοστώνης το 2013 και τις επιθέσεις στο Καπιτώλιο των ΗΠΑ το 2021.

Η υπόσχεση της χρήσης της επιτήρησης και της συλλογής δεδομένων για την ενίσχυση της ασφάλειας και τη βελτίωση των διαδικασιών είναι τόσο μεγάλη που δεν προκαλεί έκπληξη το γεγονός ότι πολλές ιδιωτικές εταιρείες θέλουν να επωφεληθούν από αυτήν. Στο πλαίσιο της «επιτήρησης στο χώρο εργασίας», οι εταιρείες στοχεύουν στην αποτελεσματικότερη διαδικασία πρόσληψης, προαγωγής και απόλυσης υπαλλήλων (Peck, 2013- Kantor & Sundaram, 2022). Αυτό προφανώς προϋποθέτει την κρυφή παρακολούθηση της απόδοσης και της δραστηριότητας των εργαζομένων, διασφαλίζοντας ότι εκπληρώνουν τα καθήκοντά τους και εντοπίζοντας σημεία όπου μπορεί να βελτιωθεί η παραγωγικότητά τους. Η νομιμότητα αυτής της πρακτικής και κατά πόσο μπορεί να συμβαδίσει με την εργατική νομοθεσία (Calacci & Stein, 2023), παραμένει αμφισβητούμενη. Υπάρχουν, επίσης

ηθικά ζητήματα και ερωτήματα για το κατά πόσο αυτή η πρακτική αποδίδει πραγματικά, καθώς μπορεί να μειώνει την παραγωγικότητα δημιουργώντας ένα εργασιακό περιβάλλον με συνεχή τον φόβο της παρακολούθησης.

Οι Gerber et al. (ibid) ανακεφαλαιώνουν τις αρνητικές συνέπειες των τεχνολογιών παρακολούθησης και των επιδράσεών τους στην ιδιωτική ζωή και τη συμπεριφορά των χρηστών αναλύοντας τρία χαρακτηριστικά φαινόμενα:

- **το φαινόμενο ψυχρού αποτελέσματος** (Chilling Effect)[18]: Η χρήση τεχνολογιών παρακολούθησης, όπως η χρήση καμερών, μπορεί να αποθαρρύνει παράνομες ενέργειες, αλλά ταυτόχρονα μπορεί να περιορίσει τα νόμιμα δικαιώματα των χρηστών. Όταν έρχονται αντιμέτωποι με την ψηφιακή επιτήρηση, για παράδειγμα, οι χρήστες ενδέχεται να αλλάξουν τη διαδικτυακή τους συμπεριφορά και να αυτολογοκριθούν αντί να ασκήσουν το δικαίωμά τους στην ελεύθερη έκφραση.

- **το παράδοξο της ιδιωτικότητας**: Το 2007, οι Norberg et al. (2007) καθιέρωσαν τον όρο «ιδιωτικό παράδοξο» (privacy paradox) για να περιγράψουν τη διχοτόμηση ανάμεσα στην προθυμία των ατόμων να παραχωρήσουν πρόσβαση στα δεδομένα τους με σχεδόν μηδαμινά ανταλλάγματα και στις εκπεφρασμένες ανησυχίες τους για την παραβίαση της ιδιωτικότητάς τους (Kokolakis, 2017). Ουσιαστικά, η διαδικτυακή συμπεριφορά των χρηστών συχνά αποκλίνει από τις αξίες τους όσον αφορά την προστασία των προσωπικών τους πληροφοριών, μερικές φορές απλώς επειδή η επιλογή που παραβιάζει την ιδιωτικότητα, όπως για παράδειγμα η αποδοχή cookies όταν επισκέπτονται μια ιστοσελίδα ή τη συμμετοχή τους στα μέσα κοινωνικής δικτύωσης με τη συνακόλουθη παροχή προσωπικών πληροφοριών είναι πιο βολική.

[18] Σε νομικό πλαίσιο, το φαινόμενο του «ψυχρού αποτελέσματος» αναφέρεται στην αποθάρρυνση ή αναστολή της νόμιμης άσκησης δικαιωμάτων, είτε από φυσικά είτε από νομικά πρόσωπα, λόγω του φόβου νομικών κυρώσεων. Αυτό το αποτέλεσμα μπορεί να προκληθεί από διάφορες νομικές ενέργειες, όπως η ψήφιση ενός νέου νόμου, η έκδοση μιας δικαστικής απόφασης, ή ακόμη και η απειλή υποβολής αγωγής. Οποιαδήποτε νομική κίνηση που προκαλεί δισταγμό στην άσκηση νόμιμων δικαιωμάτων, όπως η ελευθερία της έκφρασης, λόγω φόβου για πιθανές νομικές συνέπειες, μπορεί να συμβάλει στο φαινόμενο αυτό. Στο πλαίσιο των ψηφιακών τεχνολογιών, το φαινόμενο του ψυχρού αποτελέσματος έχει πρόσφατα χρησιμοποιηθεί ως επιχείρημα κατά των πολιτικών περιορισμού περιεχομένου στις πλατφόρμες κοινωνικής δικτύωσης, όπως το Facebook και το Twitter. Οι πλατφόρμες αυτές διαθέτουν όρους και προϋποθέσεις που τους επιτρέπουν να αφαιρούν αναρτήσεις και φωτογραφίες που θεωρούνται προσβλητικές, ακόμα και χωρίς τη συναίνεση του ατόμου που τις δημοσίευσε. Ως αποτέλεσμα, οι ενδιάμεσοι αυτοί συχνά λειτουργούν ως λογοκριτές.

- **το θεώρημα του Υπολογισμού της Ιδιωτικότητας**: Η απόφαση των χρηστών να αποκαλύψουν προσωπικές πληροφορίες βασίζεται συχνά σε μια ανάλυση κινδύνου-οφέλους ως συμβιβασμός μεταξύ της λειτουργικότητας και της αποτελεσματικότητας μιας τεχνολογικής εφαρμογής και των δεδομένων που πρέπει να μοιραστούν.

Στο σημείο αυτό, για τις ανάγκες της ανάλυσής μας, είναι ζωτικής σημασίας να υπογραμμιστεί η ποικιλομορφία και οι τύποι των δεδομένων που περιγράφονται με τον όρο «προσωπικές πληροφορίες» (Lindorfer,2024):

- **Πληροφορίες ταυτοποίησης προσώπου**: Πρόκειται για στοιχεία που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ενός ατόμου. Τέτοιες πληροφορίες μπορεί να περιλαμβάνουν άμεσα αναγνωριστικά, π.χ. διαβατήρια ή αριθμούς κοινωνικής ασφάλισης, που μπορούν να ταυτοποιήσουν μοναδικά ένα άτομο, ή οιονεί αναγνωριστικά στοιχεία, όπως το φύλο ή η φυλή, που μπορούν να συνδυαστούν με άλλα στοιχεία για να ταυτοποιηθεί ένα άτομο. Τέτοιο παράδειγμα είναι οι φωτογραφίες (π.χ. selfies) που είναι πολύτιμες για την εκπαίδευση λογισμικού αναγνώρισης προσώπου.

- **Αναγνωριστικά υλικού και λογισμικού**: Αυτά μπορούν να λειτουργήσουν ως ψηφιακή «πινακίδα κυκλοφορίας» μιας συσκευής και αποτελούν έναν ειδικό τύπο δεδομένων που, αν και δεν εμπεριέχουν απαραίτητα προσωπικά στοιχεία του χρήστη, μπορεί να χρησιμοποιηθούν για την παρακολούθηση της διαδικτυακής του δραστηριότητας. Χαρακτηριστικά παραδείγματα είναι οι διευθύνσεις IP και MAC ή πληροφορίες από την κάρτα SIM ενός τηλεφώνου, αλλά και αναγνωριστικά που δημιουργούνται μέσω μιας διαδικασίας που ονομάζεται «αποτύπωμα του προγράμματος περιήγησης». Κανείς δεν αμφισβητεί ότι τα ψηφιακά δακτυλικά αποτυπώματα μπορούν να είναι χρήσιμα για λόγους ασφαλείας, όπως για την αναγνώριση ύποπτων συνδέσεων σε έναν τραπεζικό ιστότοπο και την αποτροπή παραβίασης λογαριασμών. Ωστόσο, από την άποψη της προστασίας της ιδιωτικής ζωής, πρέπει να εξετάσουμε κατά πόσο ο χρήστης έχει την ελευθερία επέμβασης ή ρύθμισης αυτών των αναγνωριστικών.

- **Μεταδεδομένα**: Ακόμα και αν δεν υπάρχουν όλες οι λεπτομέρειες μιας επικοινωνίας, όπως το περιεχόμενο των emails και των συνομιλιών, το γεγονός ότι δύο άτομα επικοινωνούν (πότε και για πόσο) μπορεί να είναι ένα ευαίσθητο στοιχείο που μπορεί να οδηγήσει στην αναγνώριση ενός προσώπου.

Ειδικότερα, ως προς τη διασφάλιση της ιδιωτικότητας, ο ψηφιακός ανθρωπισμός πρεσβεύει ότι αυτή προϋποθέτει απαντήσεις σε ερωτήματα σχετικά με (1) ποιος τύπος δεδομένων πρέπει να προστατεύεται, (2) πόσο ευαίσθητα είναι αυτά τα δεδομένα (π.χ., οι πληροφορίες για την υγεία θεωρούνται πιο κρίσιμες από τη φυσική τοποθεσία ή τον αριθμό τηλεφώνου ενός χρήστη) και (3) από ποιον πρέπει να προστατεύονται τα δεδομένα. Επιπλέον, τονίζουν ότι ενώ όλοι έχουν το δικαίωμα στην ιδιωτική ζωή και θα πρέπει να μπορούν να λαμβάνουν μέτρα για την προστασία των προσωπικών τους πληροφοριών και των διαδικτυακών τους δραστηριοτήτων, ευάλωτες κοινωνικά ομάδες διατρέχουν μεγαλύτερο κίνδυνο παρακολούθησης και παραβίασης της ιδιωτικής ζωής, όπως οι πολιτικοί ακτιβιστές, οι δημοσιογράφοι και οι πληροφοριοδότες, τα άτομα με ψυχική ασθένεια, θύματα ενδοοικογενειακής βίας, τα παιδιά και οι νεαροί έφηβοι (Lindorfer, ibid).

Ζητήματα απορρήτου ανακύπτουν κυρίως όταν οι χρήστες συναινούν στον διαμοιρασμό των πληροφοριών τους, αλλά δεν γνωρίζουν ή δεν ελέγχουν αν αυτά τα δεδομένα μεταβιβάζονται σε τρίτα μέρη όπως είναι οι διαφημιστές και μεσίτες δεδομένων. Παράλληλα, ακόμα και αν οι χρήστες πιστεύουν ότι δεν έχουν κάτι να κρύψουν, ο συνδυασμός δεδομένων από διάφορες πηγές μπορεί να αποκαλύψει προσωπικές πληροφορίες και χαρακτηριστικά που οι χρήστες δεν γνωρίζουν, κάτι που αποτυπώνεται στην έννοια του "data onion" (Szymielewicz, 2019). Έρευνες δείχνουν ότι οι χρήστες κατατάσσονται σε 650.000 κατηγορίες προφίλ, που μπορούν να χρησιμοποιηθούν για τη στοχευμένη προβολή διαφημίσεων (Keegan & Eastwood, 2023).

Για την αντιμετώπιση των αρνητικών συνεπειών από την τεχνολογική εισβολή στην ιδιωτική ζωή, οι υπερασπιστές του ψηφιακού ανθρωπισμού υποστηρίζουν ότι υπάρχει πλήθος στρατηγικών που μπορούν να υιοθετηθούν από άτομα, προγραμματιστές λογισμικού, επιχειρήσεις και κυβερνήσεις για την προστασία της ιδιωτικότητας, οι οποίες συνοψίζονται στις ακόλουθες κατευθύνσεις:

-**Ιδιωτικότητα από τον σχεδιασμό**: Το απόρρητο πρέπει να ενσωματώνεται ως βασική προϋπόθεση από την αρχή της ανάπτυξης ενός προϊόντος ή μιας υπηρεσίας.

-**Ιδιωτικότητα από προεπιλογή**: Οι διαμορφώσιμες ρυθμίσεις πρέπει να ενεργοποιούν εξ ορισμού τις πιο φιλικές προς την ιδιωτικότητα επιλογές, ακολουθώντας την αρχή του "opt-in" για τη συλλογή δεδομένων και όχι του "opt-out"[19].

-**Διατήρηση ή ενίσχυση της ιδιωτικότητας**: Η διαχείριση των προσωπικών δεδομένων των χρηστών μπορεί να γίνεται με τρόπο που τα προστατεύει, χωρίς να επηρεάζεται το επίπεδο λειτουργικότητας μιας εφαρμογής ή υπηρεσίας σε σύγκριση με μια εφαρμογή ή υπηρεσία με πλήρη και απροστάτευτη πρόσβαση στα προσωπικά δεδομένα.

Για την υλοποίηση των συγκεκριμένων στρατηγικών, προτείνεται η λήψη των ακόλουθων τεχνικών, οργανωτικών και πολιτικών μέτρων:

Τεχνικά μέτρα

-**Έλεγχοι πρόσβασης**: Μηχανισμοί που περιορίζουν την πρόσβαση σε ευαίσθητες πληροφορίες μόνο σε εξουσιοδοτημένα μέρη, όπως η προστασία με κωδικό πρόσβασης, ο έλεγχος ταυτότητας πολλαπλών παραγόντων ή άλλες μορφές επαλήθευσης ταυτότητας.

-**Κρυπτογράφηση**: Η διαδικασία κωδικοποίησης ή μετασχηματισμού πληροφοριών με τρόπο ώστε να μπορούν να διαβαστούν μόνο από εξουσιοδοτημένα μέρη που κατέχουν κλειδί ή κωδικό πρόσβασης. Με την κρυπτογράφηση των δεδομένων, οι χρήστες μπορούν να διασφαλίσουν ότι αυτά δεν μπορούν να υποκλαπούν ή να διαβαστούν από μη εξουσιοδοτημένα μέρη, από άτομα που χρησιμοποιούν το ίδιο δημόσιο Wi-Fi σε μια καφετέρια μέχρι παρόχους υπηρεσιών διαδικτύου (ISP) και κυβερνητικές υπηρεσίες[20].

[19] Το opt-in είναι η παροχή ρητής συγκατάθεσης από ένα άτομο πριν από την ανάληψη οποιασδήποτε δραστηριότητας, όπως η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου μάρκετινγκ. Ενώ η αποχώρηση (opt-out) είναι η διαδικασία που επιτρέπει στα άτομα να αρνηθούν ή να αποσυρθούν από τη συμμετοχή τους σε μια συγκεκριμένη δραστηριότητα, όπως η λήψη επικοινωνιών μάρκετινγκ.

[20] Ένα ευρέως καθιερωμένο πρότυπο για την προστασία των επικοινωνιών μέσω κρυπτογράφησης είναι η υιοθέτηση του πρωτοκόλλου ασφαλούς μεταφοράς υπερκειμένου (HTTPS) αντί του απλού HTTP κατά την πλοήγηση σε ιστοσελίδες. Πέρα από αυτό, υπάρχουν και άλλες μέθοδοι κρυπτογράφησης, όπως η κρυπτογράφηση των ηλεκτρονικών μηνυμάτων και η χρήση εφαρμογών ανταλλαγής μηνυμάτων με κρυπτογράφηση από άκρο σε άκρο, όπως η εφαρμογή Signal. Επιπρόσθετα, τα Εικονικά Ιδιωτικά Δίκτυα (VPN) παρέχουν μια ασφαλή και κρυπτογραφημένη σύνδεση, συνήθως γνωστή ως «σήραγγα», μεταξύ της συσκευής του χρήστη, όπως ένα κινητό τηλέφωνο, και του Διαδικτύου. Το λογισμικό Tor, από την άλλη πλευρά, διαχειρίζεται την διαδικτυακή κίνηση μέσω μιας σειράς κρυπτογραφημένων αναμεταδοτών, γεγονός που καθιστά

-**Ανωνυμοποίηση**: Η διαδικασία αφαίρεσης προσωπικών πληροφοριών από σύνολα δεδομένων για την προστασία της ιδιωτικής ζωής των ατόμων. Μια ασθενέστερη μορφή είναι η ψευδωνυμοποίηση, η οποία επεξεργάζεται τα προσωπικά δεδομένα με τρόπο ώστε να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο χρήστη.

-**Ελαχιστοποίηση των δεδομένων**: Από τεχνική άποψη εξετάζεται το είδος των δεδομένων που είναι πραγματικά απαραίτητα για την παροχή μιας υπηρεσίας ή μιας εφαρμογής. Για παράδειγμα, ένα ερώτημα που συχνά καλούμαστε να απαντήσουμε όταν ασχολούμαστε με την προστασία της ιδιωτικής ζωής είναι κατά πόσο είναι απαραίτητη η ακριβής τοποθεσία για να προτείνουμε ένα εστιατόριο ή αρκεί απλά η πόλη.

Οργανωτικά μέτρα

-**Πολιτικές απορρήτου**: Πρόκειται για κείμενα-δηλώσεις που περιγράφουν τις πρακτικές χειρισμού δεδομένων ενός οργανισμού και τα δικαιώματα των ατόμων των οποίων τα δεδομένα συλλέγονται. Μπορούν να παρέχουν διαφάνεια και λογοδοσία και να βοηθήσουν τα άτομα να λαμβάνουν ενημερωμένες αποφάσεις σχετικά με τα δεδομένα τους.

Πολλές έρευνες δείχνουν ότι οι πολιτικές απορρήτου είναι συχνά δύσκολο να κατανοηθούν από τους μη νομικούς και απαιτούν υψηλό επίπεδο αναγνωστικής ικανότητας (Litman-Navarro, 2019). Μια μελέτη του 2008 (McDonald & Cranor, 2008; Madrigal, 2012) εκτιμά ότι οι χρήστες θα ξόδευαν 76 εργάσιμες ημέρες ετησίως για να διαβάσουν όλες αυτές τις πολιτικές.

Μια ενδιαφέρουσα πρόταση για τη συμπύκνωση των πληροφοριών από τις πολιτικές απορρήτου και την παρουσίασή τους με τυποποιημένο και εύληπτο τρόπο είναι οι «ετικέτες απορρήτου» (Kelley et al., 2009, Emami-Naeini et al., 2020). Οι Apple και Google εισήγαγαν ήδη έναν τέτοιο μηχανισμό: η Apple εισήγαγε ετικέτες απορρήτου στο App Store το 2020 και η Google εισήγαγε το τμήμα ασφάλειας δεδομένων στο Google Play το 2021. Ωστόσο, μια αδυναμία της τακτικής αυτής είναι το γεγονός ότι οι πληροφορίες αυτές παρέχονται κυρίως από τους ίδιους τους προγραμματιστές. Η Google προσφέρει τη δυνατότητα επικύρωσης από

δύσκολο τον εντοπισμό των διαδικτυακών δραστηριοτήτων των χρηστών και επιτρέπει την σχεδόν ανώνυμη περιήγηση στο Διαδίκτυο.

τον χρήστη, αλλά αυτή εστιάζει κυρίως σε πρότυπα ασφαλείας και όχι στο πώς η εταιρεία χειρίζεται τα προσωπικά δεδομένα.

Εικόνα 1: Παράδειγμα συμπύκνωσης πληροφοριών από πολιτικές απορρήτου σε «ετικέτες απορρήτου» (Emami Naeini et al., ibid)

-Εκπαίδευση των εργαζομένων: Η ευαισθητοποίηση σχετικά με τους κινδύνους που ελλοχεύουν για την ιδιωτική ζωή και οι βέλτιστες πρακτικές εντός ενός οργανισμού μπορεί να συμβάλουν στην πρόληψη τυχαίων ή σκόπιμων παραβιάσεων της ιδιωτικής ζωής από τους υπαλλήλους.

-Μελέτες εκτίμησης αντικτύπου για την προστασία της ιδιωτικής ζωής: Οι συστηματικές αξιολογήσεις των δυνητικών κινδύνων για την προστασία της ιδιωτικής ζωής από νέες ή τροποποιημένες διαδικασίες, συστήματα ή τεχνολογίες μπορούν να βοηθήσουν τους οργανισμούς να εντοπίσουν και να αντιμετωπίσουν τους κινδύνους για την προστασία της ιδιωτικής ζωής πριν από την εμφάνισή τους.

Πολιτικά μέτρα

-**Νόμοι για την προστασία των δεδομένων**: Τα νομικά πλαίσια που ρυθμίζουν τη συλλογή, την αποθήκευση και τη χρήση δεδομένων προσωπικού χαρακτήρα μπορούν να παρέχουν στα άτομα νομικά δικαιώματα, όπως το δικαίωμα πρόσβασης, διόρθωσης ή διαγραφής των δεδομένων τους και να επιβάλλουν κυρώσεις για μη συμμόρφωση ή κακή χρήση.

-**Διεθνείς συμφωνίες**: Νομικά πλαίσια όπως ο ΓΚΠΔ (GDPR) στην Ευρωπαϊκή Ένωση (ΕΕ) και συνεργασίες όπως το πλαίσιο προστασίας δεδομένων ΕΕ-ΗΠΑ μπορούν να συμβάλουν στη θέσπιση παγκόσμιων προτύπων προστασίας της ιδιωτικής ζωής και να διευκολύνουν τη διασυνοριακή προστασία των δεδομένων.

Μία από τις κύριες διατάξεις του ΓΚΠΔ είναι η απαίτηση για σαφή και ρητή συγκατάθεση από τους χρήστες πριν τη συλλογή και επεξεργασία των δεδομένων τους. Παρέχει επίσης στους χρήστες δικαιώματα ενημέρωσης, ανάκλησης της συγκατάθεσης και διαγραφής των δεδομένων τους. Παρόμοιοι κανονισμοί υπάρχουν σε άλλες χώρες, όπως ο νόμος για την προστασία των καταναλωτών της Καλιφόρνιας (CCPA), ο γενικός νόμος για την προστασία δεδομένων της Βραζιλίας (LGPD), ο καναδικός νόμος για την προστασία προσωπικών πληροφοριών (PIPEDA) και ο νόμος του Ηνωμένου Βασιλείου για την προστασία δεδομένων του 2018 (DPA).

-**Ευαισθητοποίηση και ακτιβισμός**: Η ευαισθητοποίηση σχετικά με τους κινδύνους για την προστασία της ιδιωτικής ζωής είναι σημαντική για την απόδοση ευθυνών σε οργανισμούς και κυβερνήσεις για τις πρακτικές τους στον τομέα της προστασίας της ιδιωτικής ζωής, καθώς και για τη διαμόρφωση δημόσιας πολιτικής για την προώθηση των δικαιωμάτων και της προστασίας της ιδιωτικής ζωής.

2.3. Κριτικός Προβληματισμός

Όσοι προσεγγίζουν με κριτική σκέψη τα βασικά σημεία του ψηφιακού ανθρωπισμού, εντοπίζουν τις ακόλουθες αδυναμίες:

Πρώτον, εάν σήμερα οι άνθρωποι αντιμετωπίζονται σαν μηχανές, αυτό είναι αποτέλεσμα μιας συγκεκριμένης σχέσης μεταξύ ανθρώπου και μηχανής που βλέπει τους

δύο πρωταγωνιστές ως αντίθετες και ξεχωριστές οντότητες. Οι ψηφιακές τεχνολογίες, όπως και κάθε άλλη τεχνολογία, συνδέονται πάντα με τον άνθρωπο με διάφορους τρόπους: αναπτύσσονται, σχεδιάζονται από ανθρώπους και χρησιμοποιούνται από ανθρώπους. Η λύση στα προβλήματα που αναφέρουν οι ψηφιακοί ανθρωπιστές δεν είναι ο εννοιολογικός και πολιτικός διαχωρισμός ανθρώπων και μηχανών, αλλά η δημιουργία μιας καλύτερης σχέσης μεταξύ τους. Είναι σημαντικό να αναγνωρίσουμε ότι ο άνθρωπος και η τεχνολογία επηρεάζουν ο ένας τον άλλον.

Δεύτερον, το μοντέλο του τεχνολογικού ντετερμινισμού στο οποίο στηρίζεται η άποψη των ψηφιακών ανθρωπιστών σύμφωνα με την οποία οι άνθρωποι έχουν χάσει ή κινδυνεύουν να χάσουν τον έλεγχο των ψηφιακών τεχνολογιών λόγω της αυτονόμησης της τεχνολογίας θα πρέπει να αναθεωρηθεί. Πρέπει να αναγνωρίσουμε τη δυνατότητα ανθρώπινου ελέγχου και να εξετάσουμε τις σχέσεις εξουσίας που δημιουργούνται, προωθώντας έναν πραγματικό εκδημοκρατισμό των ψηφιακών τεχνολογιών και της κοινωνίας.

Τρίτον, η πρακτική εφαρμογή της ηθικής στην τεχνολογία παραμένει μέχρι σήμερα ένα ζήτημα ανοιχτό καθώς παραμένει ασαφές με ποιο τρόπο θα εφαρμοστούν οι ανθρωπιστικές αξίες στην τεχνολογία. Ως εκ τούτου, η ιδέα της εφαρμογής ανθρωπιστικών αξιών στην τεχνολογία είναι σημαντική, αλλά παραμένει ασαφές πώς θα επιτευχθεί. Είναι γεγονός ότι, παρά την εννοιολογική εργασία δεκαετιών, οι ψηφιακές τεχνολογίες αναπτύσσονται συχνά χωρίς να λαμβάνουν υπόψη την ηθική και αυτό συμβαίνει εν μέρει λόγω ζητημάτων εξουσίας ή άγνοιας.

Επιπλέον, η εφαρμογή αξιών στην ανάπτυξη ψηφιακών τεχνολογιών εγείρει το ζήτημα της κυρίαρχης Δύσης καθώς η επικρατούσα καινοτομία στην ψηφιακή τεχνολογία προέρχεται από τη Δύση. Συνεπώς, πρέπει να αναρωτηθούμε σχετικά με το ποιες και ποιων αξίες θα εφαρμοστούν, ειδικά εάν λάβουμε υπόψη ότι οι άνθρωποι με περισσότερη δύναμη μπορούν να επιβάλλουν τις αξίες τους στους άλλους. Σύμφωνα με τους Werthner et al. (2022,ibid), παρότι κάποιοι ψηφιακοί ανθρωπιστές απορρίπτουν την επιβολή συγκεκριμένων αξιών, παραμένει ασαφής ο τρόπος με τον οποίο θα αποφευχθεί αυτό.

Είναι βέβαιο ότι μια κριτική ματιά στον ψηφιακό ανθρωπισμό πηγαίνει το ζήτημα της ηθικής στην τεχνολογία ένα βήμα παρακάτω και θέτει το ερώτημα εάν πραγματικά

χρειαζόμαστε μια ανθρωποκεντρική ηθική. Είναι φανερό ότι οι ψηφιακοί ανθρωπιστές επιδιώκουν να προστατεύσουν τον άνθρωπο απέναντι σε μια απάνθρωπη ή αντι-ανθρώπινη ψηφιακή τεχνολογία. Γιατί θα πρέπει να μετράνε μόνο οι ανθρώπινες αξίες, δεδομένου ότι υπάρχουν επίσης τα ζώα και το φυσικό περιβάλλον; Η συζήτηση προφανώς περιλαμβάνει μια αναθεώρηση του οράματος του ψηφιακού ανθρωπισμού που δεν θα τοποθετεί τον άνθρωπο άκριτα στο επίκεντρο του ηθικού και του πολιτικού.

Τέταρτον, για να αναπτυχθεί πραγματικά η διεπιστημονικότητα, όπως υποστηρίζουν οι οπαδοί του ψηφιακού ανθρωπισμού απαιτούνται εκτεταμένες συστημικές αλλαγές και δεν αρκεί να προστεθούν διεπιστημονικά μαθήματα στα προγράμματα σπουδών πληροφορικής. Αυτό μπορεί να επιτευχθεί μέσω μιας εκπαιδευτικής προσέγγισης προσανατολισμένης στο πρόβλημα. Επίσης, παρόλο που σήμερα δίνεται περισσότερη προσοχή στα ζητήματα εξουσίας σχετικά με το ρόλο της τεχνητής νοημοσύνης και των πλατφορμών στην κοινωνία, είναι επίσης κρίσιμο να συζητηθούν τα ζητήματα εξουσίας στο πλαίσιο της εκπαίδευσης και της δημόσια χρηματοδοτούμενης έρευνας.

Πέμπτον, οι ψηφιακοί ανθρωπιστές πρέπει να συζητήσουν περαιτέρω τους πολιτικούς στόχους του κινήματος. Εφόσον θεωρούν ότι ο ψηφιακός ανθρωπισμός δεν είναι απλώς ένα ακαδημαϊκό εγχείρημα, ποιοι πρέπει να είναι οι πολιτικοί του στόχοι; Μικρές αλλαγές στη νομοθεσία και στα εκπαιδευτικά προγράμματα ή μια πιο ριζική και συστημική αλλαγή; Τι σημαίνει εκδημοκρατισμός των ψηφιακών τεχνολογιών και ποιο όραμα δημοκρατίας τον εμπνέει; Χρειάζεται το κίνημα πολιτική ηγεσία και πόσο δημοκρατικό μπορεί να είναι το ίδιο το κίνημα;

Συνοψίζοντας, ο ψηφιακός ανθρωπισμός είναι ένας όρος-ομπρέλα που καλύπτει βασικές κριτικές για τις ψηφιακές τεχνολογίες και προσφέρει μια κανονιστική κατεύθυνση για το μέλλον. Παρότι δεν είναι ακόμα πλήρως πειστικός, έχει μια ολιστική προοπτική και μπορεί να χρησιμοποιηθεί για τη διαφώτιση του κοινού και των οργάνων λήψης αποφάσεων. Ήδη η βιομηχανία έχει αρχίσει να αγκαλιάζει τις βασικές του αξίες, εστιάζοντας σε ανθρώπινους παράγοντες και περιβαλλοντικές επιδράσεις, αλλά είναι πιο δύσκολο να υιοθετήσει τις κοινωνικές του πτυχές και τους περιορισμούς που συνεπάγεται στη δύναμή της (Krause, 2023). Εάν τελικά αυτό επιτευχθεί, ο ψηφιακός ανθρωπισμός μπορεί να γίνει μια ισχυρή δύναμη για κοινωνικο-τεχνολογικές αλλαγές.

3. ΕΙΣΑΓΩΓΗ ΣΤΟΝ ΨΗΦΙΑΚΟ ΣΥΝΤΑΓΜΑΤΙΣΜΟ

3.1. Μια πρώτη ανάλυση

Κατά τις τελευταίες δεκαετίες, η ψηφιακή τεχνολογία έχει προκαλέσει μια ανισορροπία στο συνταγματικό οικοσύστημα, η οποία έχει οδηγήσει στην εμφάνιση κανονιστικών αντιδράσεων που σκοπεύουν να αντιμετωπίσουν τις νέες προκλήσεις και να αποκαταστήσουν αυτή την ισορροπία. Η συνταγματική ισορροπία μπορεί να θεωρηθεί ως η ιδανική κατάσταση που προκύπτει από την εφαρμογή των κανόνων του συνταγματικού δικαίου σε ένα δεδομένο νομικό πλαίσιο το οποίο περιλαμβάνει δύο βασικές πτυχές: την προστασία των θεμελιωδών δικαιωμάτων και την ισορροπία των εξουσιών.

Όπως υποστηρίζει ο Celeste (2022), η έλευση της ψηφιακής τεχνολογίας επιφέρει διάφορες αλλαγές :

α) Ενισχύει τις δυνατότητες των ατόμων να ασκούν τα θεμελιώδη δικαιώματά τους. Πιο συγκεκριμένα, η ψηφιακή τεχνολογία διευρύνει τη δυνατότητα μετάδοσης πληροφοριών, ενισχύοντας έτσι δικαιώματα όπως η ελευθερία της έκφρασης, η θρησκευτική ελευθερία, η ελευθερία του συνέρχεσθαι και η ελευθερία άσκησης επαγγέλματος.

β) Αυξάνει τους κινδύνους για τα θεμελιώδη δικαιώματα. Η ίδια δυνατότητα ανταλλαγής πληροφοριών που ενισχύει τα δικαιώματα μπορεί να αποτελέσει πηγή απειλών, όπως είναι η δυσφήμιση, ρητορική μίσους, κυβερνοεκφοβισμό και παιδική πορνογραφία. Επιπλέον, η ψηφιακή τεχνολογία μπορεί να επιτρέψει τον αποκλεισμό ή τον περιορισμό της μετάδοσης πληροφοριών, την παρακολούθηση του περιεχομένου και την καταγραφή πληροφοριών για τους χρήστες, παραβιάζοντας έτσι δικαιώματα όπως η ιδιωτικότητα και η προστασία προσωπικών δεδομένων.

γ) Επηρεάζει την ισορροπία των εξουσιών. Οι ιδιωτικές εταιρείες τεχνολογίας εμφανίζονται ως νέοι κυρίαρχοι δρώντες δίπλα στα κράτη. Το συνταγματικό δίκαιο ιστορικά στοχεύει στην ισορροπία της εξουσίας, με το κράτος ως κύριο κυρίαρχο να περιορίζει τη δράση του ώστε να εγγυάται την άσκηση των ατομικών δικαιωμάτων. Ωστόσο, οι ιδιωτικές εταιρείες, οι οποίες δεν δεσμεύονται άμεσα από τα συνταγματικά πρότυπα, ασκούν σημαντική επιρροή στον τρόπο άσκησης των δικαιωμάτων των ατόμων μέσω των ψηφιακών τεχνολογιών.

Ως εκ τούτου, ο σύγχρονος συνταγματισμός αποσκοπεί στην προστασία των θεμελιωδών δικαιωμάτων και στον περιορισμό της ανάδυσης εξουσιών εκτός οποιουδήποτε ελέγχου. Γι' αυτό, η συζήτηση πλέον επικεντρώνεται σε μια ψηφιακή συνταγματική οπτική γωνία. Όπως παρατηρεί ο Suzor (2019, σελ.173), «ο ψηφιακός συνταγματισμός απαιτεί από εμάς να αναπτύξουμε νέους τρόπους περιορισμού της κατάχρησης εξουσίας σε ένα πολύπλοκο σύστημα που περιλαμβάνει πολλές διαφορετικές κυβερνήσεις, επιχειρήσεις και οργανώσεις της κοινωνίας των πολιτών». Με άλλα λόγια, η νέα αυτή προσπάθεια συνταγματικής ρύθμισης έρχεται να ελέγξει μια νέα μορφή ψηφιακής ιδιωτικής εξουσίας η οποία έχει προκύψει λόγω της μαζικής ικανότητας παραγωγής - οργάνωσης περιεχομένου και επεξεργασίας δεδομένων. Ωστόσο, αυτή η νέα «συνταγματική στιγμή» δεν σημαίνει μια συνταγματική ανατροπή. Δεν αντιμετωπίζουμε μια «κοπερνίκεια» αλλαγή παραδείγματος που να αλλάζει τις βασικές αρχές που χαρακτηρίζουν την συνταγματική μας ταυτότητα (Celeste, 2019), αλλά σε μια δυναμική διαλεκτική μεταξύ του τρόπου με τον οποίο οι ψηφιακές τεχνολογίες επηρεάζουν την εξέλιξη του συνταγματισμού και την αντίδραση του συνταγματικού δικαίου απέναντι στη νέα ψηφιακή εξουσία, όπως ακριβώς εκφράζει η συγχώνευση των εκφράσεων «ψηφιακός» και «συνταγματισμός».

Η έννοια του ψηφιακού συνταγματισμού δεν είναι καινούργια. Αντιθέτως, οι βασικές πτυχές αυτής της έννοιας έχουν εμφανιστεί στις αναλύσεις ακαδημαϊκών από τις αρχές της δεκαετίας του 2000 και λόγω της ασαφούς σημασίας της, τα τελευταία είκοσι χρόνια η βιβλιογραφία την έχει χρησιμοποιήσει σε διάφορα πλαίσια και με διαφορετικές σημασίες. Για παράδειγμα, σύμφωνα με τον Fitzgerald (1999), η φύση της κοινωνίας της πληροφορίας, η οποία είναι διεθνής, άυλη, μη εδαφική και αποκεντρωμένη, απαιτεί μια μικτή δομή διακυβέρνησης που συνδυάζει την αυτορρύθμιση του ιδιωτικού τομέα με την εποπτεία των δημόσιων θεσμών. Η θεωρία του Fitzgerald περί «πληροφοριακού συνταγματισμού» ή «πληροφοριακού δικαίου» αναφέρεται στο δίκαιο του κράτους (ειδικά το δίκαιο πνευματικής ιδιοκτησίας, το δίκαιο των συμβάσεων, το δίκαιο του ανταγωνισμού και το δίκαιο της ιδιωτικότητας), που πρέπει να περιορίσει την αυτορρύθμιση των ιδιωτικών φορέων. Ωστόσο, υπάρχουν δύο βασικά ζητήματα που πρέπει να αντιμετωπιστούν: πρώτον, συχνά δεν είναι εύκολο να υπαχθούν οι ιδιωτικοί φορείς στη δικαιοδοσία ενός κράτους, και δεύτερον, η δραστηριότητα των ιδιωτικών φορέων στην κοινωνία της πληροφορίας είναι διακρατική, κάτι που μπορεί να προκαλέσει συγκρούσεις με τους νόμους άλλων κρατών.

Σε αντίθεση με τον Fitzgerald, ο οποίος αναγνώρισε τον ρόλο του ιδιωτικού δικαίου στον περιορισμό της εξουσίας των ιδιωτικών φορέων, ο Berman (2000) απέρριψε την ιδέα ότι το «κοινό δίκαιο» θα μπορούσε να επιτελέσει μια τέτοια συνταγματική λειτουργία. Υποστήριξε ότι το συνταγματικό δίκαιο είναι πιο κατάλληλο για την καθιέρωση γενικών αρχών, ενώ ο στόχος του κοινού δικαίου είναι περιορισμένος στην ρύθμιση καθημερινών προβλημάτων. Μέσω αυτής της προσέγγισης, τα δικαστήρια θα μπορούσαν να χρησιμοποιούν το σύνταγμα ως μέτρο για την ανάπτυξη θεμελιωδών αξιών, την επίλυση πολιτικά απαιτητικών ζητημάτων και την ενθάρρυνση της ενεργούς συμμετοχής του κοινού σε αυτά τα ζητήματα.

Αναφερόμενος τόσο στον Fitzgerald όσο και στον Berman, ο Suzor αναγνώρισε τον ρόλο της εξουσίας των ιδιωτικών φορέων στη ρύθμιση των εικονικών κοινοτήτων (Suzor, 2010). Υποστήριξε ότι η συνταγματική προοπτική είναι χρήσιμη για τον καθορισμό των κατάλληλων ορίων στην εξουσία των ιδιωτικών φορέων και χρησιμοποίησε τον όρο "ψηφιακός συνταγματισμός" για να περιγράψει το έργο που επιδιώκει να οριοθετήσει την εξουσία των ιδιωτικών φορέων, ειδικά στο πλαίσιο των εικονικών κοινοτήτων.

Σε αντίθεση με τον Berman, ο Suzor δεν υποστήριξε ότι ο έλεγχος της ιδιωτικής εξουσίας πρέπει να ασκείται από το συνταγματικό δίκαιο. Αντίθετα, υποστήριξε ότι το συνταγματικό δίκαιο παίζει διπλό ρόλο στον περιορισμό της ιδιωτικής εξουσίας: πρώτον, μπορεί να χρησιμοποιηθεί για να καθορίσει τον βαθμό συμμόρφωσης της αυτορρύθμισης των ιδιωτικών φορέων με τις αξίες που καθορίζονται από το κράτος και δεύτερον, έχει το καθήκον να καθοδηγεί την ανάπτυξη του δικαίου των συμβάσεων .

Από την άλλη πλευρά, ο Karavas (2010) εστιάζει στη ρύθμιση των εικονικών κοινοτήτων και υποστηρίζει ότι η διαδικασία συνταγματοποίησης δεν χρειάζεται να καθοδηγείται από το κράτος. Εξετάζοντας μια απόφαση γερμανικού δικαστηρίου σχετικά με την αποβολή ενός χρήστη από μια διαδικτυακή πλατφόρμα, ο Karavas διαπίστωσε ότι οι δικαστές υποστήριξαν εμμέσως την ιδέα μιας συνταγματοποίησης που προέρχεται από την κοινωνία, παρά από το κράτος (Karavas,ibid). Ουσιαστικά, ο Karavas υποστηρίζει ότι η κρατική πολιτική δεν μπορεί πλέον να ρυθμίσει πλήρως την πολυπλοκότητα μιας κατακερματισμένης και πλουραλιστικής κοινωνίας. Υιοθετεί τη θεωρία του Teubner για την εμφάνιση «αστικών συνταγμάτων», τα οποία αναδύονται από την ίδια την κοινωνία (Teubner, 2004). Σύμφωνα με τον Karavas, αυτή η μορφή συνταγματοποίησης προέρχεται

από τους ίδιους τους χρήστες και τους κοινωνικούς τομείς, χωρίς να απαιτείται η καθοδήγηση του κράτους. Τελικά, ο Karavas προτείνει έναν ενδιάμεσο δρόμο μεταξύ του κρατικά καθοδηγούμενου συνταγματισμού και της πλήρως αυτόνομης συνταγματοποίησης που προέρχεται από την κοινωνία. Υποστηρίζει ότι ενώ η αυτορρύθμιση των ιδιωτικών φορέων είναι δυνατή, οι κοινωνικοί τομείς έχουν πλέον τη δυνατότητα να προωθήσουν τη δική τους διαδικασία συνταγματοποίησης, χωρίς να βασίζονται στο κράτος.

Το 2015, οι Gill, Redeker και Gasser πρότειναν να χρησιμοποιηθεί ο όρος «ψηφιακός συνταγματισμός» ως ένας γενικός όρος για να συνδέσει μια σειρά από έγγραφα που επιδιώκουν να καθιερώσουν ένα χάρτη δικαιωμάτων για το Διαδίκτυο. Αυτά τα κείμενα, τα οποία έχουν αναδυθεί τα τελευταία είκοσι πέντε χρόνια, θεωρούνται ως μέρος ενός ευρύτερου «προ-συνταγματικού» λόγου, με τελικό στόχο να οριστεί ένα συνολικό σύνολο δικαιωμάτων, αρχών και κανόνων διακυβέρνησης για το Διαδίκτυο.

Ωστόσο, αυτά τα κείμενα δεν είναι συντάγματα με την κλασική έννοια, καθώς δεν κατέχουν κάποια πρωταρχική θέση στην ιεραρχία των νομικών πηγών. Παρόλα αυτά, μπορούν να συσχετιστούν με τα συντάγματα επειδή μοιράζονται τις βασικές ουσιαστικές πτυχές του συνταγματισμού, όπως οι αξίες, τα προβλήματα και οι αρχές του, καθώς και τις κύριες λειτουργίες του περιορισμού της κρατικής εξουσίας και της ενίσχυσης των θεσμών μέσα στην κοινωνία (Gill, Redeker, και Gasser, 2015) .

Οι εν λόγω ακαδημαϊκοί υποστήριξαν ότι η αντίληψη τους για τον ψηφιακό συνταγματισμό δεν είναι τόσο στενή όσο αυτή του Suzor, ο οποίος αναφέρεται στον περιορισμό της εξουσίας μόνο στο πλαίσιο των εικονικών κοινοτήτων. Για αυτούς, ο ψηφιακός συνταγματισμός στοχεύει στον περιορισμό της δημόσιας εξουσίας, ενώ για τον Suzor, στον περιορισμό της ιδιωτικής εξουσίας.

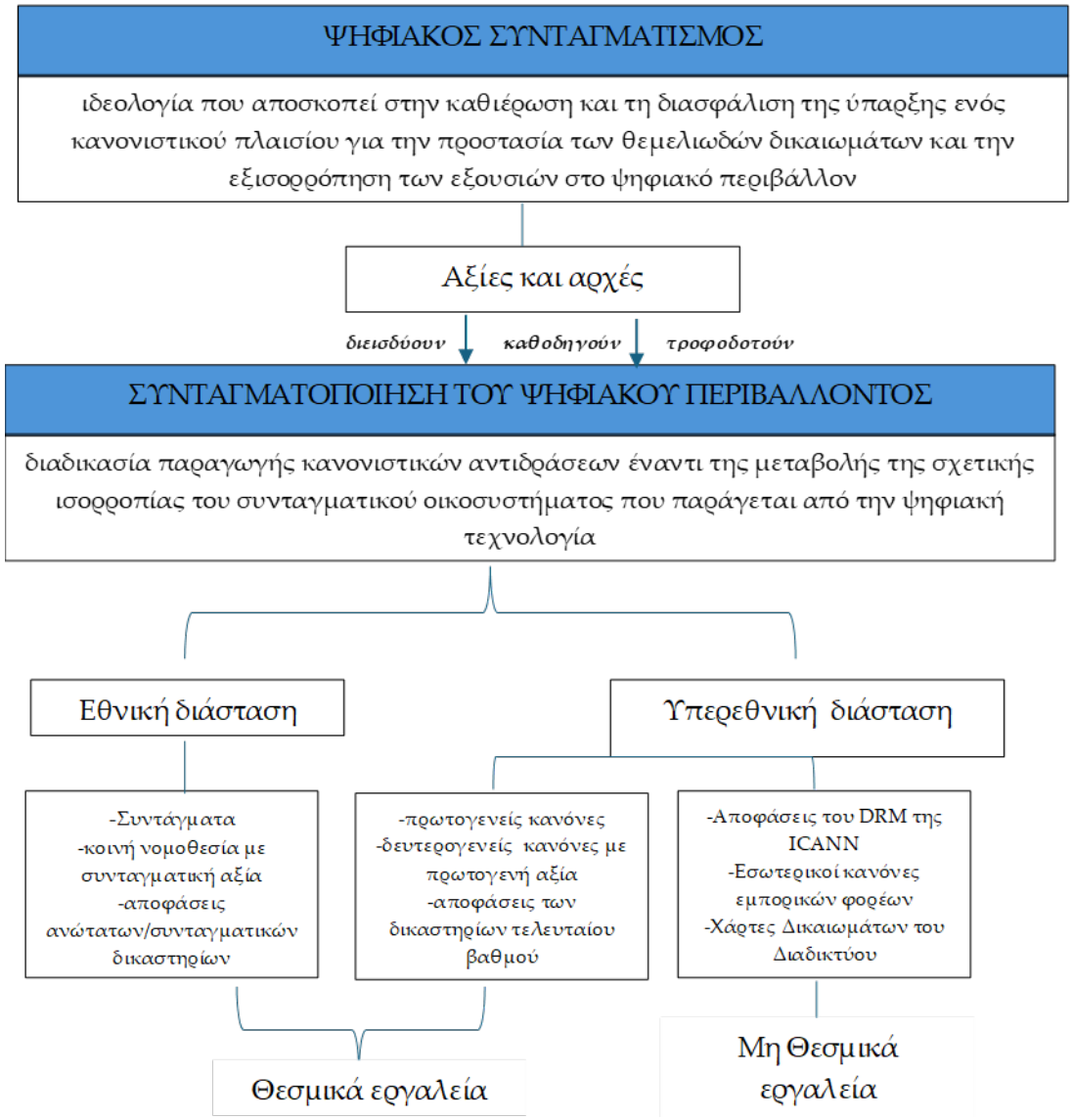
Όπως έγινε αντιληπτό, η υπάρχουσα βιβλιογραφία δεν παρέχει μια ενιαία εικόνα της έννοιας του ψηφιακού συνταγματισμού. Συγκεκριμένα, δεν υπάρχει συναίνεση σχετικά με δύο θεμελιώδη χαρακτηριστικά αυτής της έννοιας. Πρώτον, δεν είναι σαφές αν ο ψηφιακός συνταγματισμός στοχεύει στον περιορισμό της ιδιωτικής εξουσίας ή και της δημόσιας εξουσίας. Δεύτερον, δεν υπάρχει συμφωνία για το εργαλείο που θα πρέπει να υλοποιήσει τις αξίες του ψηφιακού συνταγματισμού.

Μπορούμε να υποστηρίξουμε ότι ο ψηφιακός συνταγματισμός αποτελεί μια νέα κατεύθυνση του σύγχρονου συνταγματισμού. Ωστόσο, δεν υποδηλώνει ένα νέο στάδιο εξέλιξης του συνταγματισμού, αλλά είναι μια από τις πρόσφατες κατευθύνσεις του. Ο όρος «ψηφιακός» δεν προσδιορίζει άμεσα τον όρο «συνταγματισμός», αλλά μεταφέρει την ιδέα ότι αναφέρεται στον συνταγματισμό που σχετίζεται με το ψηφιακό περιβάλλον. Ο Celeste (ibid) εξειδικεύει την αντίληψη αυτή κάνοντας τη διάκριση μεταξύ «συνταγματοποίησης» και «συνταγματισμού».

Από τη μια πλευρά, η έννοια της «συνταγματοποίησης του ψηφιακού περιβάλλοντος» αναφέρεται στη διαδικασία δημιουργίας κανόνων που στοχεύουν στην προστασία των θεμελιωδών δικαιωμάτων και στην ισορροπία των εξουσιών μέσα στο ψηφιακό πλαίσιο. Περιλαμβάνει την εθνική (Συντάγματα, κοινή νομοθεσία με συνταγματική αξία, αποφάσεις ανώτατων/συνταγματικών δικαστηρίων) και την υπερεθνική διάσταση (πρωτογενείς κανόνες, δευτερογενείς κανόνες με πρωτογενή αξία, αποφάσεις δικαστηρίων τελευταίου βαθμού και αποφάσεις μη κρατικών φορέων, όπως είναι οι αποφάσεις του DRM της ICANN[21], εσωτερικοί κανόνες και κώδικες δεοντολογίας εμπορικών φορέων και χάρτες δικαιωμάτων για το Διαδίκτυο[22]).

[21] Οι αποφάσεις του DRM (Dispute Resolution Mechanism) της ICANN (Internet Corporation for Assigned Names and Numbers) αφορούν τον μηχανισμό επίλυσης διαφορών που διαχειρίζεται η ICANN. Η ICANN είναι ένας μη κερδοσκοπικός οργανισμός που είναι υπεύθυνος για τη διαχείριση και τον συντονισμό του συστήματος ονομάτων τομέα (DNS) του Διαδικτύου. Οι αποφάσεις του DRM της ICANN αποτελούν σημαντικό κομμάτι της υπερεθνικής διάστασης του ψηφιακού συνταγματισμού, καθώς αναδεικνύουν την επιρροή και την εξουσία των μη κρατικών φορέων στη ρύθμιση του ψηφιακού περιβάλλοντος και την προστασία των δικαιωμάτων στο Διαδίκτυο. Αυτές οι αποφάσεις συμβάλλουν στην ανάπτυξη ενός κανονιστικού πλαισίου που διασφαλίζει τη δίκαιη και ισότιμη χρήση των ονομάτων τομέα, ενώ παράλληλα προστατεύει τα δικαιώματα των εμπλεκομένων μερών.

[22] Οι Χάρτες Δικαιωμάτων για το Διαδίκτυο είναι έγγραφα που προσπαθούν να καθορίσουν και να προστατεύσουν τα δικαιώματα των χρηστών του Διαδικτύου. Αυτά τα έγγραφα δημιουργούνται από διάφορους οργανισμούς, κυβερνήσεις, και φορείς της κοινωνίας των πολιτών και στοχεύουν στη διασφάλιση ενός ασφαλούς, ελεύθερου και ανοιχτού Διαδικτύου. Οι χάρτες αυτοί είναι κρίσιμοι για τη διαμόρφωση ενός δικαιότερου και πιο ασφαλούς ψηφιακού περιβάλλοντος. Παρέχουν ένα πλαίσιο για την ανάπτυξη πολιτικών και νομοθεσιών που προστατεύουν τα δικαιώματα των χρηστών, ενισχύουν τη διαφάνεια και προωθούν την ισότητα και τη δικαιοσύνη στο Διαδίκτυο. Επιπλέον, συμβάλλουν στη διαμόρφωση της παγκόσμιας διακυβέρνησης του Διαδικτύου, ενθαρρύνοντας τη συνεργασία μεταξύ κρατών, οργανισμών και χρηστών. Οι Χάρτες Δικαιωμάτων για το Διαδίκτυο περιλαμβάνουν συνήθως τις ακόλουθες αρχές και δικαιώματα: Ελευθερία της Έκφρασης, Ιδιωτικότητα και Προστασία Δεδομένων, Πρόσβαση και Συμμετοχή Ασφάλεια και Ανθρώπινα Δικαιώματα Διαφάνεια και Λογοδοσία.



Διάγραμμα 1: Απεικόνιση της διαδικασίας συνταγματοποίησης (Celeste, 2019)

Από την άλλη, ο ψηφιακός συνταγματισμός αποτελεί το σύνολο των αξιών και των ιδανικών που καθοδηγούν και διαπερνούν τη διαδικασία συνταγματοποίησης του ψηφιακού περιβάλλοντος. Δηλαδή, ο ψηφιακός συνταγματισμός παρέχει το θεωρητικό και αξιακό υπόβαθρο που καθιστά απαραίτητη την συνταγματοποίηση και τη δημιουργία κανονιστικών αντιδράσεων για την αντιμετώπιση των προκλήσεων που εγείρει η ψηφιακή τεχνολογία. Σε αυτό το πλαίσιο, η συνταγματοποίηση λειτουργεί ως ένας συνεχής διάλογος

Δημοφιλείς Χάρτες Χαρτών Δικαιωμάτων για το Διαδίκτυο είναι : η Χάρτα Δικαιωμάτων για το Διαδίκτυο του Συμβουλίου της Ευρώπης, η Χάρτα Δικαιωμάτων για το Διαδίκτυο της Βραζιλίας, η Αφρικανική Χάρτα Δικαιωμάτων για το Διαδίκτυο.

για την αναδιαμόρφωση των συνταγματικών αρχών και κανόνων προκειμένου να ανταποκριθούν στις εξελίξεις και τις απαιτήσεις της ψηφιακής εποχής. Αυτό σημαίνει ότι η διαδικασία συνταγματοποίησης δεν είναι στατική αλλά εξελίσσεται διαρκώς, αντικατοπτρίζοντας τις αλλαγές στην κοινωνία και την τεχνολογία.

3.2. Η άνοδος του ευρωπαϊκού ψηφιακού συνταγματισμού

Ο De Gregorio (2022) αναφέρεται ειδικότερα στην άνοδο και εδραίωση του ευρωπαϊκού ψηφιακού συνταγματισμού ως παράδειγμα για το πώς το συνταγματικό δίκαιο μπορεί να αντιδράσει απέναντι στις προκλήσεις της αλγοριθμικής κοινωνίας, με ιδιαίτερη έμφαση στο ρόλο των επιγραμμικών πλατφορμών. Οι ψηφιακές επιχειρήσεις φιλοδοξούν να αναλάβουν έναν νέο ρόλο, περισσότερο κυβερνητικό «αντικαθιστώντας τη λογική της εδαφικής κυριαρχίας με τη λειτουργική κυριαρχία». Ως gatekeepers της πληροφορίας και του περιεχομένου, οι επιγραμμικές πλατφόρμες μπορούν να αποφασίζουν αυτόνομα όχι μόνο για το πώς οι άνθρωποι αλληλεπιδρούν, αλλά και για το πώς μπορούν να διεκδικήσουν τα δικαιώματά τους. Θα λέγαμε ότι ελλείψει άλλης ρύθμισης, κάνει την εμφάνισή του το «δίκαιο των πλατφορμών» ως ένα μείγμα ιδιωτικού δικαίου και αυτοματοποιημένων τεχνολογιών.

Ειδικότερα, με τους όρους παροχής υπηρεσιών (Terms of Service – ToS), οι πλατφόρμες καθορίζουν μονομερώς τους κανόνες με τους οποίους οι χρήστες πρέπει να συμμορφώνονται για να έχουν πρόσβαση στις υπηρεσίες των παρόχων και με τους οποίους ενημερώνονται για τον τρόπο επεξεργασίας των δεδομένων τους. Κατά τον ίδιο τρόπο, οι δημόσιες διοικήσεις βασίζονται στις μεγάλες τεχνολογικές εταιρείες για να προσφέρουν νέες δημόσιες υπηρεσίες ή για να βελτιώσουν τις ήδη υπάρχουσες με αυτοματοποιημένες τεχνολογίες. Προφανώς, αυτή η συνεργασία αυξάνει τον βαθμό εξάρτησης του δημόσιου τομέα από αυτές τις εταιρείες οι οποίες επιβάλλουν τους όρους τους όταν προχωρούν σε σύμπραξη. Έτσι, σταδιακά, οι νομικοί κανόνες αντικαθίστανται από τεχνολογικά και συμβατικά πρότυπα που θεσπίζονται από ιδιωτικούς υπερεθνικούς φορείς. Παράλληλα, όμως, όπως θα αναλύσουμε σε επόμενο σημείο της ανάλυσης, η σύμπραξη ιδιωτικού και δημόσιου φορέα δημιουργεί ευκαιρία για ζυμώσεις στο πεδίο του ψηφιακού συνταγματισμού.

3.3. Οι φάσεις εξέλιξης του ευρωπαϊκού ψηφιακού συνταγματισμού

Ο De Gregorio (2021a) στο άρθρο του "The rise of digital constitutionalism in the European Union" διακρίνει τρεις φάσεις στην εξέλιξη του ευρωπαϊκού ψηφιακού συνταγματισμού.

3.3.1. Η πρώτη φάση: ψηφιακός φιλελευθερισμός

Η πρώτη φάση του ψηφιακού συνταγματισμού στην Ευρώπη, γνωστή ως Ψηφιακός Φιλελευθερισμός, ξεκινά με την υπογραφή της Συνθήκης της Ρώμης το 1957, η οποία επεδίωξε να δημιουργήσει μια κοινή αγορά και να προωθήσει την οικονομική σύγκλιση μεταξύ των κρατών μελών της ΕΕ. Κατά την περίοδο αυτή, η πολιτική της ΕΕ ήταν προσανατολισμένη προς έναν φιλελεύθερο οικονομικό μοντέλο, το οποίο στόχευε στην ανάπτυξη της ψηφιακής τεχνολογίας και των υπηρεσιών στο πλαίσιο της εσωτερικής αγοράς.

Μια από τις πρώτες σημαντικές πρωτοβουλίες ήταν η Οδηγία 95/46/ΕΚ, γνωστή και ως Οδηγία για την Προστασία Δεδομένων, η οποία υιοθετήθηκε το 1995. Αυτή η Οδηγία αποσκοπούσε στην προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών και στην εναρμόνιση των εθνικών νομοθεσιών για την προστασία της ιδιωτικότητας. Παράλληλα, η Οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο εισήχθη το 2000, με στόχο τη διευκόλυνση της παροχής ψηφιακών υπηρεσιών εντός της ΕΕ και την εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας.

Κατά τη διάρκεια αυτής της περιόδου, η πολιτική της ΕΕ εστίασε στην απορρύθμιση και την απελευθέρωση της αγοράς, πιστεύοντας ότι η τεχνολογική πρόοδος και η ανάπτυξη της ψηφιακής οικονομίας θα οδηγήσουν σε οικονομική ευημερία και καινοτομία. Οι νομοθετικές πρωτοβουλίες της εποχής είχαν ως στόχο να δημιουργήσουν ένα ευνοϊκό περιβάλλον για την ανάπτυξη της ψηφιακής τεχνολογίας, ενώ ταυτόχρονα προσπαθούσαν να διασφαλίσουν την προστασία των δεδομένων προσωπικού χαρακτήρα .

Ωστόσο, αυτή η φιλελεύθερη προσέγγιση δεν αντιμετώπισε επαρκώς τις προκλήσεις που συνδέονται με την προστασία των δικαιωμάτων των πολιτών στον ψηφιακό χώρο. Η εστίαση στην οικονομική ανάπτυξη και την ελευθερία της αγοράς συχνά άφηνε περιθώρια για παραβιάσεις της ιδιωτικότητας και την ανεπαρκή προστασία των προσωπικών

δεδομένων. Αυτή η αντίφαση αναδείχθηκε κατά τη διάρκεια της εξέλιξης της ψηφιακής τεχνολογίας και κατέδειξε την ανάγκη για πιο ολοκληρωμένες και αυστηρές ρυθμίσεις (De Gregorio, ibid).

3.3.2. Η δεύτερη φάση: η προστατευτική νομολογία των δικαστηρίων

Η δεύτερη φάση του ψηφιακού συνταγματισμού στην Ευρώπη χαρακτηρίζεται από μια σειρά νομολογιακών αποφάσεων, με σημαντικότερες αυτές του Δικαστηρίου του ΔΕΕ. Αυτή η φάση αναπτύχθηκε σημαντικά μετά την υιοθέτηση της Συνθήκης της Λισαβόνας το 2009, η οποία αναγνώρισε νομική ισχύ στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Κατά τη διάρκεια αυτής της περιόδου, το ΔΕΕ ανέλαβε πιο ενεργό ρόλο στην προστασία των θεμελιωδών δικαιωμάτων στον ψηφιακό χώρο. Μέσα από σημαντικές αποφάσεις, όπως η υπόθεση Google Spain (2014), η οποία θα αναλυθεί παρακάτω, το δικαστήριο καθόρισε τις υποχρεώσεις των διαδικτυακών πλατφορμών όσον αφορά την προστασία των δεδομένων των πολιτών και την ευθύνη για το περιεχόμενο που φιλοξενούν. Αυτές οι αποφάσεις τόνισαν τη σημασία της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων, υπογραμμίζοντας ότι οι ψηφιακές πλατφόρμες πρέπει να σέβονται τα θεμελιώδη δικαιώματα των χρηστών τους.

Ο προστατευτικός ρόλος των δικαστηρίων συνέβαλε στην ενίσχυση του ρυθμιστικού πλαισίου, επιβάλλοντας αυστηρότερους κανόνες και προσφέροντας μεγαλύτερη προστασία στους πολίτες. Η δικαστική παρέμβαση, μέσω του ΔΕΕ, έδειξε ότι η δικαιοσύνη μπορεί να λειτουργήσει ως μηχανισμός προστασίας των δικαιωμάτων των πολιτών στον ψηφιακό χώρο, ακόμη και όταν οι νομοθετικές πρωτοβουλίες υστερούν.

Συνολικά, η δεύτερη φάση του ψηφιακού συνταγματισμού στην Ευρώπη ενίσχυσε την προστασία των θεμελιωδών δικαιωμάτων και κατέστησε σαφές ότι τα δικαστήρια μπορούν να διαδραματίσουν καθοριστικό ρόλο στην αντιμετώπιση των προκλήσεων της ψηφιακής εποχής.

3.3.3. Η τρίτη φάση: ψηφιακός συνταγματισμός

Η τρίτη φάση του ψηφιακού συνταγματισμού στην Ευρώπη αναγνωρίζεται ως μια νέα εποχή που εστιάζει στην προστασία των θεμελιωδών δικαιωμάτων και στην ισορροπία

των εξουσιών στο ψηφιακό περιβάλλον. Αποσκοπεί στην ενίσχυση των δημοκρατικών αρχών στο ψηφιακό περιβάλλον μέσω της προστασίας της ελευθερίας της έκφρασης, της προώθησης της πρόσβασης στην πληροφορία και της ενίσχυσης της συμμετοχής των πολιτών στη διαδικασία λήψης αποφάσεων.

Αυτή η φάση χαρακτηρίζεται από την υιοθέτηση και εφαρμογή κανονισμών και πολιτικών που στοχεύουν στην αντιμετώπιση των προκλήσεων που επιφέρει η ψηφιακή τεχνολογία και οι διαδικτυακές πλατφόρμες. Οι κανονιστικές αυτές αντιδράσεις μπορούν να συστηματοποιηθούν ως εξής (Celeste, 2019, ibid):

α) Κανόνες που στοχεύουν στην ενίσχυση της ικανότητας άσκησης υφιστάμενων θεμελιωδών δικαιωμάτων. Ένα παράδειγμα αυτών των κανόνων είναι εκείνοι που αναγνωρίζουν το δικαίωμα στην πρόσβαση στο διαδίκτυο ως ουσιαστική προϋπόθεση για την άσκηση πολλών υφιστάμενων δικαιωμάτων, από την ελευθερία της έκφρασης μέχρι το δικαίωμα στην εργασία και την ελευθερία του επιχειρείν.

β) Κανόνες που στοχεύουν στον περιορισμό της αύξησης παραβιάσεων των θεμελιωδών δικαιωμάτων. Ένα αντιπροσωπευτικό παράδειγμα αυτών των κανόνων είναι η ανάπτυξη του δικαίου προστασίας των δεδομένων με καθοριστική την περίπτωση θέσπισης του ΓΚΠΔ.

γ) Κανόνες που στοχεύουν στην αποκατάσταση της ισορροπίας εξουσίας μεταξύ πολιτών και κράτους και εισάγουν νέες μορφές ελέγχου της κρατικής εξουσίας από τους πολίτες, επιτρέποντάς τους να αντιδρούν σε πιθανές καταχρήσεις Για παράδειγμα, κανόνες που απαιτούν από δημόσιους φορείς να δημοσιεύουν συγκεκριμένες πληροφορίες στους ιστότοπούς τους ή κανόνες που δίνουν στους πολίτες δικαίωμα πρόσβασης σε έγγραφα μέσω της ψηφιακής τεχνολογίας.

Σημαντικό στοιχείο αυτής της φάσης είναι η Στρατηγική για την Ψηφιακή Ενιαία Αγορά (Digital Single Market - DSM) της ΕΕ, η οποία, όπως θα αναλύσουμε και στη συνέχεια, στοχεύει στη δημιουργία μιας ενιαίας αγοράς για τις ψηφιακές υπηρεσίες και αγαθά. Η στρατηγική αυτή περιλαμβάνει νομοθετικά μέτρα που επιδιώκουν να εξασφαλίσουν την προστασία των δικαιωμάτων των χρηστών και την υπευθυνότητα των ψηφιακών πλατφορμών.

Συνολικά, η τρίτη φάση του ψηφιακού συνταγματισμού επιδιώκει να ενισχύσει την υπευθυνότητα και τη διαφάνεια των ψηφιακών πλατφορμών μέσω της επιβολής εφαρμογής μηχανισμών προκειμένου α) να παρέχουν σαφείς και διαφανείς πληροφορίες στους χρήστες σχετικά με τη συλλογή και τη χρήση των δεδομένων τους και β) να αντιμετωπίσουν φαινόμενα παραπληροφόρησης και μετάδοσης επιβλαβούς περιεχομένου.

3.4. Η σχέση του ψηφιακού συνταγματισμού με τον ψηφιακό ανθρωπισμό

Ο Celeste (2019) αν και δεν ορίζει ρητά τη σχέση μεταξύ ψηφιακού συνταγματισμού και ψηφιακού ανθρωπισμού, υποδεικνύει τη σύνδεση μεταξύ τους με βάση τις αρχές που περιγράφει στη μελέτη του. Ακολουθούν ορισμένα βασικά σημεία που απεικονίζουν αυτή τη σχέση:

- **Εννοιολογικά θεμέλια**: Ο ψηφιακός συνταγματισμός και ο ψηφιακός ανθρωπισμός προκύπτουν από την ανάγκη να αντιμετωπιστούν οι επιπτώσεις της ψηφιακής τεχνολογίας στην κοινωνία. Ο ψηφιακός συνταγματισμός επικεντρώνεται στα νομικά πλαίσια και τις αρχές που διέπουν τις ψηφιακές αλληλεπιδράσεις, ενώ ο ψηφιακός ανθρωπισμός δίνει έμφαση στις ανθρωποκεντρικές αξίες και τις ηθικές αξίες στο ψηφιακό πεδίο.

- **Προστασία των δικαιωμάτων**: Ο ψηφιακός συνταγματισμός στοχεύει στη θέσπιση ενός κανονιστικού πλαισίου που προστατεύει τα θεμελιώδη δικαιώματα στο ψηφιακό περιβάλλον. Αυτό ευθυγραμμίζεται με τους στόχους του ψηφιακού ανθρωπισμού, ο οποίος υπερασπίζεται την αξιοπρέπεια και τα δικαιώματα των ατόμων ενόψει των τεχνολογικών εξελίξεων. Και οι δύο έννοιες επιδιώκουν να διασφαλίσουν ότι η τεχνολογία υπηρετεί την ανθρωπότητα αντί να την υπονομεύει.

- **Εξισορρόπηση των εξουσιών**: Ο ψηφιακός συνταγματισμός ασχολείται με την ισορροπία των εξουσιών μεταξύ των δημόσιων αρχών και των ιδιωτικών επιχειρήσεων στον ψηφιακό χώρο. Ομοίως, ο ψηφιακός ανθρωπισμός απαιτεί μια ισορροπία που δίνει προτεραιότητα στην ανθρώπινη ευημερία έναντι των εταιρικών συμφερόντων. Αυτή η κοινή εστίαση στη δυναμική της εξουσίας αναδεικνύει τη σημασία της λογοδοσίας και της ηθικής διακυβέρνησης στην ψηφιακή εποχή.

- **Κανονιστικό πλαίσιο**: Ο ψηφιακός συνταγματισμός επιβάλλει την ανάγκη κανονιστικών αντιδράσεων απέναντι στις προκλήσεις που θέτει η ψηφιακή τεχνολογία. Ο

ψηφιακός ανθρωπισμός λειτουργεί συμπληρωματικά υποστηρίζοντας την υιοθέτηση ηθικών κατευθυντήριων γραμμών και πρακτικών που προάγουν την ανθρώπινη ευημερία, ενισχύοντας έτσι την ανάγκη για ένα ισχυρό νομικό πλαίσιο που ευθυγραμμίζεται με τις ανθρωπιστικές αξίες.

- **Προσαρμογή των αξιών**: Ο ψηφιακός συνταγματισμός περιγράφεται ως μια ιδεολογία που προσαρμόζει τις παραδοσιακές συνταγματικές αξίες στο ψηφιακό πλαίσιο. Ο ψηφιακός ανθρωπισμός επιδιώκει ομοίως να προσαρμόσει τις ανθρωπιστικές αρχές στις προκλήσεις του ψηφιακού κόσμου, τονίζοντας την ανάγκη για ένα πλαίσιο που σέβεται τα ανθρώπινα δικαιώματα, ενώ παράλληλα πλοηγείται στις τεχνολογικές αλλαγές.

- **Διεπιστημονική προσέγγιση**: Και οι δύο έννοιες επωφελούνται από μια διεπιστημονική προσέγγιση, που αντλεί από το δίκαιο, τη δεοντολογία, την τεχνολογία και τις κοινωνικές επιστήμες. Αυτή η συνεργασία είναι απαραίτητη για την ανάπτυξη ολοκληρωμένων στρατηγικών που αντιμετωπίζουν τις πολυπλοκότητες του ψηφιακού τοπίου, διασφαλίζοντας ότι λαμβάνονται υπόψη τόσο οι νομικές όσο και οι ανθρωπιστικές προοπτικές.

Συνοπτικά, ενώ ο ψηφιακός συνταγματισμός επικεντρώνεται στις νομικές πτυχές της διακυβέρνησης στην ψηφιακή εποχή, ο ψηφιακός ανθρωπισμός δίνει έμφαση στις ηθικές και ανθρωποκεντρικές διαστάσεις. Μαζί, αποτελούν ένα συμπληρωματικό πλαίσιο που επιδιώκει την προστασία των δικαιωμάτων και την προώθηση της ανθρώπινης αξιοπρέπειας σε έναν ολοένα και περισσότερο ψηφιακό κόσμο.

Πολύ ενδιαφέρουσα είναι η άποψη του De Gregorio (2022) ο οποίος αναλύει τη σχέση μεταξύ ψηφιακού συνταγματισμού και ανθρωπισμού, ειδικά στο πλαίσιο της αντιπαράθεσης με τον ψηφιακό καπιταλισμό, στον τομέα της ανάπτυξης τεχνολογιών τεχνητής νοημοσύνης. Ο De Gregorio τονίζει ότι η Ευρωπαϊκή Ένωση, μέσω του ψηφιακού συνταγματισμού, προσπαθεί να βρει μια ισορροπία μεταξύ των δύο αυτών κυρίαρχων ιδεολογιών, προωθώντας την ανθρωποκεντρική προσέγγιση στην ανάπτυξη τεχνολογικών προϊόντων. Ο συγγραφέας αναφέρεται στην έννοια της «τρίτης οδού» που επιδιώκει η Ευρωπαϊκή Ένωση στο πλαίσιο του ψηφιακού συνταγματισμού ως μια στρατηγική που επιδιώκει να συνδυάσει τα πλεονεκτήματα της τεχνολογικής καινοτομίας με τη διατήρηση των δημοκρατικών αξιών και της ανθρώπινης αξιοπρέπειας.

3.5. Το συνταγματικό μήνυμα του ΓΚΠΔ υπό το πρίσμα των αξιών του ψηφιακού ανθρωπισμού

Παρόλο που ο ΓΚΠΔ δεν έχει τυπικά συνταγματικό χαρακτήρα, μπορεί να ειπωθεί ότι διαδραματίζει «παρα-συνταγματικό ρόλο» (Celeste and De Gregorio, 2021) καθώς μεταφράζει και εφαρμόζει βασικές συνταγματικές αρχές στο πλαίσιο της αλγοριθμικής κοινωνίας. **Η ανθρώπινη αξιοπρέπεια**, **το κράτος δικαίου** και **το δικαίωμα στη δικαστική προστασία** είναι αρχές που διαπερνούν το σύνολο του κειμένου.

Ειδικότερα, το άρθρο 22 παρ. 1 του ΓΚΠΔ θεσπίζει μια γενική απαγόρευση όλων των αποφάσεων που α) βασίζονται αποκλειστικά σε μια μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και β) παράγουν νομικά ή τουλάχιστον σημαντικά αποτελέσματα για το υποκείμενο των δεδομένων. Αν και με μια απλή ανάγνωση του ΓΚΠΔ δεν μπορεί κανείς να κατανοήσει τις αξίες τις οποίες επιδιώκει να προστατεύσει αυτή η γενική απαγόρευση, εν τέλει, όπως θα δούμε μέσα από την ανάλυσή μας, το άρθρο 22 αποσκοπεί περισσότερο στη συνταγματική προστασία του δικαιώματος στην **ανθρώπινη αξιοπρέπεια** παρά στην απόλυτη προστασία του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Όπως υποστηρίζουν και οι Dreyer and Schulz (2019, σελ.29) στην ανάλυσή τους "The General Data Protection Regulation and Automated Decision-making: Will it deliver?", «Οι κίνδυνοι που εγκυμονεί η αυτοματοποιημένη λήψη αποφάσεων - εάν κάποιος αγνοήσει την αναγκαία επεξεργασία δεδομένων που αυτή συνεπάγεται - δεν θίγουν άμεσα τις εγγυήσεις προστασίας των δεδομένων, αλλά συνήθως πτυχές των ανθρωπίνων δικαιωμάτων που συνδέονται με την προσωπική αυτονομία και την ανθρώπινη αξιοπρέπεια, μεταξύ άλλων».

Στο σημείο αυτό, αξίζει να αναφερθούμε στην πολύ ενδιαφέρουσα μελέτη της Meg Letta Jones (2017) με τίτλο "The right to a human in the loop: Political construction of computer automation and personhood" στην οποία αποκαλύπτεται ότι η ρύθμιση των αλγορίθμων έχει ένα πλούσιο, πολιτισμικά ενσωματωμένο και πολιτικά σημαντικό ιστορικό υπόβαθρο. Εξετάζοντας τις ιστορικές ρίζες των σύγχρονων διαφωνιών μεταξύ των κοινωνιών πληροφορίας, ιδιαίτερα των χωρών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε αντίθεση με τις Ηνωμένες Πολιτείες, η Jones αναφέρεται στους ενσαρκωτές της ευρωπαϊκής πολιτικής κουλτούρας. Σύμφωνα με τους τελευταίους, η πλήρης

αυτοματοποίηση ή η παροχή αποκλειστικά αυτοματοποιημένης αντιμετώπισης μειώνει την ανθρώπινη υπόσταση του ατόμου, διότι μια μηχανή μπορεί να αλληλεπιδράσει με τον άνθρωπο μόνο υπολογιστικά. Έτσι, η αντιμετώπιση ενός ανθρώπου με πλήρως αυτοματοποιημένο τρόπο μειώνει την αξιοπρέπεια του ατόμου και η αποκατάσταση της αξιοπρέπειας μπορεί να επιτευχθεί μέσω της εμπλοκής ενός ανθρώπου στη διαδικασία.

Εν αντιθέσει και παρά το γεγονός ότι μερικοί Αμερικανοί μελετητές, τεχνικοί ειδικοί, επιχειρηματίες και υπεύθυνοι χάραξης πολιτικής έχουν εκφράσει παρόμοιες ανησυχίες σχετικά με τη μετατροπή των ατόμων και των ομάδων σε δεδομένα μέσω της αυτοματοποίησης, οι νομοθετικές λύσεις στις ΗΠΑ έχουν ακολουθήσει μια διαφορετική προσέγγιση. Αντί να εστιάζουν στη συμμετοχή του ανθρώπου στη διαδικασία (όπως συμβαίνει στην Ευρώπη), οι Αμερικανικές προσεγγίσεις έχουν επικεντρωθεί σε τρεις βασικές αρχές: διαφάνεια, πρόσβαση και ακρίβεια, έννοιες ουδέτερες που θεωρούν ότι μπορούν να διατηρήσουν την ακεραιότητα της προσωπικότητας.

Οι οδηγίες που εξέδωσε η Ομάδα Εργασίας του άρθρου 29 [23] για την εφαρμογή του Άρθρου 22 επιβεβαιώνουν τον εξισορροπητικό σκοπό του Άρθρου. Το Άρθρο 22 εφαρμόζεται σε περιπτώσεις «σοβαρών επιπτώσεων» και όταν η αυτοματοποιημένη απόφαση μπορεί «να επηρεάσει σημαντικά τις συνθήκες, τη συμπεριφορά ή τις επιλογές των ενδιαφερομένων ατόμων· να έχει παρατεταμένη ή μόνιμη επίδραση στο υποκείμενο των δεδομένων· ή στο πιο ακραίο, να οδηγήσει στον αποκλεισμό ή τη διάκριση των ατόμων». Σε αυτές τις περιπτώσεις, δηλ. όταν η αυτοματοποιημένη λήψη αποφάσεων επηρεάζει την νομική κατάσταση του ατόμου ή έχει σημαντικές επιπτώσεις στη ζωή του, το οικονομικό όφελος από τη χρήση των «έξυπνων μηχανών» θα πρέπει να θυσιαστεί. Το Άρθρο 22 εμμέσως αποτάσσεται το μοντέλο του τεχνολογικού ντετερμινισμού, όπως αναλυτικά περιγράφεται σε αυτό που η Rouvroy (2011) αποκαλεί ως «στατιστική διακυβέρνηση του πραγματικού»[24].

[23] Η Ομάδα Εργασίας του Άρθρου 29 (Article 29 Working Party - WP29) ήταν ένα ανεξάρτητο συμβουλευτικό σώμα της Ευρωπαϊκής Ένωσης για θέματα προστασίας δεδομένων και ιδιωτικότητας. Ιδρύθηκε βάσει του Άρθρου 29 της Οδηγίας 95/46/ΕΚ (Οδηγία για την Προστασία Δεδομένων) του 1995. Η WP29 έπαιξε καθοριστικό ρόλο στη διαμόρφωση των πολιτικών προστασίας δεδομένων στην ΕΕ μέχρι το 2018.

[24] Η φράση «στατιστική διακυβέρνηση του πραγματικού» αναφέρεται στον τρόπο με τον οποίο τα δεδομένα και οι στατιστικές αναλύσεις χρησιμοποιούνται για τη λήψη αποφάσεων και τη διαχείριση της κοινωνίας. Αυτή η μορφή διακυβέρνησης βασίζεται σε μεγάλες ποσότητες δεδομένων που συλλέγονται από διάφορες πηγές και αναλύονται για να προβλέψουν και να διαχειριστούν τις συμπεριφορές και τις ανάγκες των ανθρώπων.

Ο αναγνώστης μπορεί να εντοπίσει στη συζήτηση αυτή και διαστάσεις θεολογικού περιεχομένου περί του αυτεξούσιου του ανθρώπου που συνδέεται με τη μοναδικότητά του ως προσώπου[25]. Ουσιαστικά, ο ΓΚΠΔ επαναλαμβάνει την αρχή που θεσπίστηκε στην Οδηγία Προστασίας Δεδομένων του 1995, η οποία τόνιζε ότι τα συστήματα επεξεργασίας δεδομένων πρέπει να εξυπηρετούν τον άνθρωπο και να εξασφαλίζουν την ευημερία του.

Όπως ήδη έχουμε επισημάνει, το Άρθρο 22 του ΓΚΠΔ δεν επιβάλλει απόλυτη απαγόρευση στην αυτοματοποιημένη λήψη αποφάσεων. Και για το λόγο αυτό, προβλέπει τρεις εξαιρέσεις[26], οι οποίες καθορίζονται στην παρ.2 του εν λόγω άρθρου καθώς στον ευρωπαϊκό συνταγματισμό υπόκεινται σε ένα πλέγμα περιορισμών σύμφωνα με τις διατάξεις του Άρθρου 52[27] του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ (Celeste and De Gregorio, ibid). Καθώς δικαιολογημένα κάποιος θα μπορούσε να διερωτηθεί κατά πόσο μπορεί να υπάρχουν περιορισμοί στην αρχή του σεβασμού της ανθρώπινης αξιοπρέπειας, ο ΓΚΠΔ θεσπίζει επιπρόσθετες εγγυήσεις που λειτουργούν ως δικλίδες ασφαλείας ex-ante και ex-post, εν προκειμένω στα άρθρα 13 και 15 ΓΚΠΔ.

Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει το υποκείμενο των δεδομένων, κατά τη φάση συλλογής των δεδομένων, για την ύπαρξη διαδικασίας αυτοματοποιημένης λήψης αποφάσεων, τη λογική της, τη σημασία και τις συνέπειές της (άρθρο 13). Επιπρόσθετα, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει πρόσβαση στα

---

[25] Στη χριστιανική διδασκαλία, με τον όρο πρόσωπο θεωρείται «κάθε έλλογο ον που υπερβαίνει τις αναγκαιότητες της φύσεως, που κατακτά την ιδιαιτερότητά του, αλλά συγχρόνως κινείται αγαπητικά για να συναντήσει τα υπόλοιπα έλλογα όντα και κατ' επέκταση όλο το έμβιο περιβάλλον του». (Νικολάου , 2013). Βασικό στοιχείο του προσώπου είναι η ελευθερία του αυτοπροσδιορισμού του, η αυτονομία του και ο τρόπος με τον οποίο χρησιμοποιεί το αυτεξούσιο του ανάλογα με τις επιθυμίες του.

[26] Οι εξαιρέσεις που καθορίζονται στο Άρθρο 22 παρ.2 του GDPR επιτρέπουν την αυτοματοποιημένη λήψη αποφάσεων όταν ισχύει ένα από τα ακόλουθα:

1. **Αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης**: Όταν η αυτοματοποιημένη επεξεργασία είναι απαραίτητη για τη σύναψη ή την εκτέλεση μιας σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας.
2. **Εξουσιοδοτημένη από το δίκαιο της ΕΕ ή κράτους μέλους**: Όταν η αυτοματοποιημένη λήψη αποφάσεων επιτρέπεται από τη νομοθεσία της Ευρωπαϊκής Ένωσης ή κράτους μέλους, που επίσης προβλέπει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, ελευθεριών και έννομων συμφερόντων του υποκειμένου των δεδομένων.
3. **Ρητή συγκατάθεση**: Όταν το υποκείμενο των δεδομένων έχει δώσει τη ρητή συγκατάθεσή του για την επεξεργασία των δεδομένων του με αυτόν τον τρόπο.

[27] Αυτό το άρθρο καθορίζει τις αρχές βάσει των οποίων μπορούν να επιβάλλονται περιορισμοί στα θεμελιώδη δικαιώματα και τις ελευθερίες που κατοχυρώνονται στον Χάρτη, διασφαλίζοντας ότι οι περιορισμοί αυτοί είναι αναγκαίοι, ανάλογοι και δεν παραβιάζουν την ουσία των δικαιωμάτων.

προσωπικά του δεδομένα από τον υπεύθυνο επεξεργασίας (άρθρο 15). Ουσιαστικά, οι ex-post εγγυήσεις εφαρμόζονται αφού έχει ληφθεί μια αυτοματοποιημένη απόφαση και επιτρέπουν στο υποκείμενο των δεδομένων να ζητήσει την επανεξέταση και τον εκ νέου «εξανθρωπισμό» της απόφασης.

Με την υιοθέτηση αυτών των άρθρων, ο ΓΚΠΔ γίνεται ένα αντιπροσωπευτικό κείμενο ψηφιακού συνταγματισμού καθώς μεταφέρει τις **αρχές του κράτους δικαίου** στον ιδιωτικό χώρο. Αφενός, με το να εξασφαλίζει τη διαφάνεια στη διαδικασία, ενισχύει το δικαίωμα του υποκειμένου στην ελευθερία διαμόρφωσης της ψηφιακής του ταυτότητας και, συνεπώς, το δικαίωμα στον πληροφοριακό αυτοκαθορισμό. Αφετέρου, καθώς ο υπεύθυνος επεξεργασίας δεδομένων υποχρεούται να εξηγεί τη λογική που διέπει την εν λόγω διαδικασία, μέσω μιας σειράς προκαθορισμένων, λογικών και μη αυθαίρετων κριτηρίων, ο ΓΚΠΔ επαναφέρει την ισορροπία ανάμεσα στις ισχυρές ιδιωτικές εταιρείες και τα αδύναμα υποκείμενα δεδομένων.

Τέλος, το Άρθρο 22 παρ.3 συμπληρώνει τις προαναφερθείσες συνταγματικές αξίες με το να προβλέπει το δικαίωμα του υποκειμένου των δεδομένων να ζητήσει ανθρώπινη παρέμβαση, να εκφράσει την άποψή του και να αμφισβητήσει την αυτοματοποιημένη απόφαση αντιμετωπίζοντας κατ' αυτόν τον τρόπο την «πλάνη της διαφάνειας» (transparency fallacy)[28] (Edwards and Veale, 2017). Όπως αναφέρουν οι Celeste και De Gregorio (ibid), ο ΓΚΠΔ με τη συγκεκριμένη ρύθμιση, εισάγει ένα δικαίωμα πλήρως

[28] Ο όρος "transparency fallacy" εμφανίζεται στο άρθρο "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For" των Lilian Edwards και Michael Veale. Ο όρος χρησιμοποιείται για να περιγράψει την εσφαλμένη αντίληψη ότι η απλή διαφάνεια των αλγορίθμων ή των διαδικασιών λήψης αποφάσεων είναι επαρκής για να εξασφαλίσει τη δικαιοσύνη, την υπευθυνότητα και την αξιοπιστία τους.
Στο κείμενο, οι συγγραφείς αναλύουν ότι η διαφάνεια μπορεί να δημιουργήσει μια ψευδή αίσθηση ασφάλειας ή εμπιστοσύνης, κάνοντας τους χρήστες να πιστεύουν ότι επειδή ένας αλγόριθμος είναι διαφανής, είναι επίσης δίκαιος και ακριβής, ενώ στην πραγματικότητα, η διαφάνεια από μόνη της δεν αντιμετωπίζει τις εγγενείς προκαταλήψεις που μπορεί να υπάρχουν στα δεδομένα ή στο ίδιο το μοντέλο. Επιπλέον, η διαφάνεια δεν εξασφαλίζει πάντα ότι οι χρήστες θα μπορέσουν να κατανοήσουν ή να ερμηνεύσουν τις πληροφορίες που παρέχονται.
Οι συγγραφείς υποστηρίζουν ότι η αναζήτηση ενός «δικαιώματος στην εξήγηση» όπως προβλέπεται από τον ΓΚΠΔ μπορεί να αποδειχθεί αποπροσανατολιστική και να καλλιεργήσει μια νέα μορφή της «απάτης της διαφάνειας». Προτείνουν ότι άλλες διατάξεις του ΓΚΠΔ, όπως το δικαίωμα στη διαγραφή («δικαίωμα στη λήθη») και το δικαίωμα στη φορητότητα των δεδομένων, καθώς και η προστασία της ιδιωτικότητας μέσω του σχεδιασμού και των αξιολογήσεων επιπτώσεων της προστασίας δεδομένων μπορούν να κάνουν τους αλγορίθμους πιο υπεύθυνους, εξηγήσιμους και ανθρωποκεντρικούς.

διαδεδομένο στον αναλογικό κόσμο, το δικαίωμα της προσφυγής και της δίκαιης κρίσης από ανθρώπινο παράγοντα. Όπως ανέφερε η Ευρωπαϊκή Επιτροπή το 1992, η επεξεργασία δεδομένων μπορεί να είναι σημαντική για τη λήψη αποφάσεων. Ωστόσο, τόνισε ότι «η ανθρώπινη κρίση πρέπει να έχει τη θέση της». Εν τέλει, η αρχή που υπογραμμίζει την αναγκαιότητα της ανθρώπινης κρίσης στις διαδικασίες λήψης αποφάσεων συμπληρώνει τη γενική απαγόρευση της αυτοματοποιημένης λήψης αποφάσεων που θεσπίζεται στο άρθρο 22 παράγραφος 1 του ΓΚΠΔ. Και οι δύο αυτές διατάξεις στοχεύουν στη διατήρηση της ανθρώπινης αξιοπρέπειας. Καθώς η ανθρώπινη ζωή είναι τόσο πολύπλευρη και απρόβλεπτη που δεν μπορεί να κατανοηθεί πλήρως από μια μηχανή, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτεί την τελική λήψη απόφασης από έναν άνθρωπο.

Αν και κάποιος μπορεί να ισχυριστεί ότι η παρουσία ενός ανθρώπου δεν εξαλείφει αυτόματα τους κινδύνους της μεροληπτικής λήψης αποφάσεων, ωστόσο λειτουργεί ως αντίβαρο στην αυξανόμενη επιρροή των ιδιωτικών αλγοριθμικών συστημάτων, διασφαλίζοντας τη διαφάνεια και την τήρηση των δημοκρατικών αξιών.

Συμπερασματικά, η ανάλυσή μας ανέδειξε ότι ο περιορισμός της αυτοματοποιημένης λήψης αποφάσεων στον ΓΚΠΔ ενισχύει τις συνταγματικές αξίες, προωθώντας μια νέα μορφή ανθρωπισμού - ψηφιακό ανθρωπισμό. Σε αυτό το πλαίσιο, η ελεύθερη ανάπτυξη του ατόμου και η προστασία της ψηφιακής του ταυτότητας τοποθετούνται πάνω από την τεχνολογία και την οικονομική αποτελεσματικότητα. Ο ΓΚΠΔ ενσωματώνει και επικαιροποιεί ένα παλιό συνταγματικό μήνυμα, προσαρμοσμένο στις προκλήσεις της ψηφιακής εποχής, τονίζοντας ότι η τεχνολογία πρέπει να εξυπηρετεί την ανθρωπότητα και όχι να την ελέγχει.

4. ΨΗΦΙΑΚΟΣ ΣΥΝΤΑΓΜΑΤΙΣΜΟΣ, ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Όπως αναφέραμε προηγουμένως, ο ψηφιακός συνταγματισμός στην Ευρώπη είναι αποτέλεσμα των κοινωνικών και πολιτικών ζυμώσεων και συντίθεται από ένα κράμα κανονιστικών πλαισίων, δικαστικών επιρροών και επανατροφοδότησης εκ μέρους της κοινωνίας των πολιτών. Στη συνέχεια, αναλύονται τα βασικότερα κείμενα ψηφιακού συνταγματισμού και ο ρόλος που διαδραμάτισαν οι αποφάσεις του ΔΕΕ στην αλλαγή του

παραδείγματος, ενώ στο επόμενο κεφάλαιο θα εξειδικεύσουμε την ανάλυσή μας στην προστασία της ιδιωτικότητας αναφορικά με τη μαζική επιτήρηση.

4.1. Κείμενα ψηφιακού συνταγματισμού

Η πρόσφατη προσπάθεια της ΕΕ να ρυθμίσει τη χρήση των δεδομένων και των τεχνολογιών που βασίζονται σε αυτά έχει οδηγήσει σε ένα συνεκτικό πλαίσιο κανόνων προστασίας. Εκτός από τον ΓΚΠΔ για τον οποίο αναφερθήκαμε ξεχωριστά, η Οδηγία για τα πνευματικά δικαιώματα (DSM), ο Κανονισμός σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο και η Πράξη για τις ψηφιακές υπηρεσίες αποτελούν τρία παραδείγματα που δείχνουν πώς η ευρωπαϊκή συνταγματική προσέγγιση επιδιώκει να προστατεύσει τα θεμελιώδη δικαιώματα και τις δημοκρατικές αξίες, περιορίζοντας ταυτόχρονα την ιδιωτική εξουσία των διαδικτυακών πλατφορμών.

Η **Οδηγία για τα πνευματικά δικαιώματα** εισάγει ένα νέο πλαίσιο ευθύνης για τους παρόχους υπηρεσιών επιγραμμικού διαμοιρασμού περιεχομένου, αναγνωρίζοντας τον ενεργό ρόλο τους στη διανομή περιεχομένου. Επιβάλλει ένα σύστημα αδειοδότησης μεταξύ των εν λόγω πλατφορμών και των κατόχων δικαιωμάτων για την αντιμετώπιση των οικονομικών απωλειών από μη εξουσιοδοτημένες μεταφορτώσεις έργων που προστατεύονται από πνευματικά δικαιώματα. Ειδικότερα, το άρθρο 17 απαιτεί από τις πλατφόρμες να αποκτούν άδειες για τη φιλοξενία περιεχομένου τρίτων, καθιστώντας τις υπεύθυνες για μη εξουσιοδοτημένη δημόσια κοινοποίηση τέτοιου περιεχομένου, εκτός εάν εμπίπτουν στο πλαίσιο εξαιρέσεων του άρθρου. Η Οδηγία αυτή σηματοδοτεί ένα σημαντικό βήμα για την απόδοση ευθυνών στις διαδικτυακές πλατφόρμες και την ενίσχυση της προστασίας των κατόχων πνευματικών δικαιωμάτων.

Παρομοίως, ο **Κανονισμός σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο (TERREG)** αποσκοπεί στη δημιουργία ενός σαφούς και ενιαίου νομικού πλαισίου για την πρόληψη της κατάχρησης από παρόχους υπηρεσιών φιλοξενίας στην περίπτωση διάδοσης τρομοκρατικού περιεχομένου. Ορίζει νομικά το τρομοκρατικό περιεχόμενο, περιορίζοντας τη διακριτική ευχέρεια των διαδικτυακών πλατφορμών όσον αφορά το συγκεκριμένο θέμα. Επιπλέον, επιβάλλει στους παρόχους υπηρεσιών φιλοξενίας να ενεργούν επιμελώς, αναλογικά και χωρίς διακρίσεις,

λαμβάνοντας πάντα υπόψη τα θεμελιώδη δικαιώματα των χρηστών, ιδίως την ελευθερία της έκφρασης.

Παρόλο που η κύρια εστίασή του είναι η πρόληψη της διάδοσης επιβλαβούς περιεχομένου, οι διαδικαστικές εγγυήσεις που επιβάλλει ο Κανονισμός, όπως η διαφάνεια στις διαδικασίες αφαίρεσης περιεχομένου και η δυνατότητα προσφυγής των χρηστών κατά των αποφάσεων αυτών, ενισχύουν την προστασία της ιδιωτικότητας των χρηστών καθώς διασφαλίζεται ότι τα δεδομένα των χρηστών και οι ενέργειές τους στο διαδίκτυο δεν θα υποβάλλονται σε αδικαιολόγητες ή υπερβολικές παρεμβάσεις από τις πλατφόρμες ή τις αρχές.

Επιπλέον, ο Κανονισμός επιδιώκει να ελαχιστοποιήσει την αδιάκριτη παρακολούθηση και τον υπερβολικό έλεγχο του διαδικτυακού περιεχομένου, κάτι που θα μπορούσε να οδηγήσει σε παραβιάσεις της ιδιωτικότητας των χρηστών. Με τον καθορισμό σαφών κανόνων και διαδικασιών, ο Κανονισμός επιτρέπει την προστασία των προσωπικών δεδομένων των χρηστών και της ιδιωτικότητάς τους, διασφαλίζοντας ότι οποιαδήποτε παρέμβαση γίνεται με σεβασμό στα θεμελιώδη δικαιώματα.

Η Πράξη για τις Ψηφιακές Υπηρεσίες (DSA) αποτελεί επίσης παράδειγμα των προσπαθειών της Ευρωπαϊκής Ένωσης να δημιουργήσει ένα δικαιότερο και πιο υπεύθυνο ψηφιακό περιβάλλον. Μέσω της DSA, η ΕΕ επιδιώκει να προωθήσει τη συνταγματοποίηση της διακυβέρνησης του Διαδικτύου, αναδεικνύοντάς την ως σημαντικό βήμα προς τον ψηφιακό συνταγματισμό. Αυτή η προσπάθεια στοχεύει στη δημιουργία ενός ενιαίου πλαισίου δικαιωμάτων, αρχών και κανόνων διακυβέρνησης για τον ψηφιακό χώρο, ενώ παράλληλα συμβάλλει στην ανάπτυξη νέων δομών διακυβέρνησης[29] και ρυθμιστικών

[29] Κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης θα πρέπει να ορίσει μία ή περισσότερες εθνικές αρχές ψηφιακών υπηρεσιών (Digital Services Coordinators). Αυτές οι αρχές θα είναι υπεύθυνες για την παρακολούθηση της συμμόρφωσης των διαδικτυακών πλατφορμών με τους κανόνες της DSA σε εθνικό επίπεδο. Οι εθνικές αρχές θα έχουν την εξουσία να εποπτεύουν τη λειτουργία των πλατφορμών εντός της δικαιοδοσίας τους, να διεξάγουν έρευνες και να ζητούν πληροφορίες από τις πλατφόρμες για να διασφαλίσουν ότι τηρούνται οι κανονισμοί καθώς και να επιβάλλουν κυρώσεις σε περιπτώσεις μη συμμόρφωσης, που μπορεί να περιλαμβάνουν πρόστιμα, περιορισμούς στη λειτουργία ή άλλες κυρώσεις ανάλογα με τη σοβαρότητα της παραβίασης. Ταυτόχρονα, η **Ευρωπαϊκή Επιτροπή** θα διαδραματίσει κεντρικό ρόλο στην επιβολή των κανόνων της DSA, ιδιαίτερα όταν πρόκειται για μεγάλες διαδικτυακές πλατφόρμες που έχουν σημαντικό αντίκτυπο σε περισσότερα από ένα κράτη μέλη. Η Επιτροπή θα έχει τις εξής αρμοδιότητες: 1)**Συντονισμός των Εθνικών Αρχών**: Η Ευρωπαϊκή Επιτροπή θα διασφαλίζει ότι οι εθνικές αρχές ψηφιακών υπηρεσιών συνεργάζονται αποτελεσματικά και ότι υπάρχει συνοχή στην εφαρμογή των κανόνων σε όλη την

φορέων που θα επικεντρώνονται στην αποτελεσματική προστασία των θεμελιωδών δικαιωμάτων στο διαδίκτυο (De Gregorio, 2021b).

4.2. Ο ρόλος της νομολογίας του ΔΕΕ προς μια ψηφιακή συνταγματική προσέγγιση

Οι αποφάσεις του ΔΕΕ έχουν διαδραματίσει καθοριστικό ρόλο στην υπογράμμιση των νέων προκλήσεων της κοινωνίας της πληροφορίας, ανοίγοντας έτσι το δρόμο για μια νέα ευρωπαϊκή συνταγματική φάση. Η εφαρμογή νομικών κανόνων που αποσκοπούν στην αύξηση του βαθμού διαφάνειας και λογοδοσίας στον έλεγχο του διαδικτυακού περιεχομένου και στην επεξεργασία δεδομένων συμβάλλει στην αποτροπή της «συνταγματοποίησης των αυτόνομων υποσυστημάτων της παγκόσμιας κοινωνίας» (De Gregorio, 2021). Στη συνέχεια, αναλύονται οι σημαντικότερες αποφάσεις με αναφορά στην επίδρασή τους στην καλλιέργεια του ψηφιακού συνταγματισμού και τη μετάβαση από τα οικονομικά συμφέροντα προς τον σεβασμό στον χρήστη και τον πληροφοριακό αυτοκαθορισμό του. Σημειώνεται ότι κάποιες εξ αυτών θα σχολιαστούν και σε επόμενη ενότητα με μεγαλύτερη λεπτομέρεια ως προς την εισφορά τους στον περιορισμό της αδιάκριτης μαζικής παρακολούθησης.

Lindqvist (2003), Promusicae (2008): Οι πρώτες δικαστικές αποφάσεις που λειτούργησαν ως προπομποί της μεταστροφής του ΔΕΕ από την οικονομική διάσταση της Οδηγίας για την προστασία των προσωπικών δεδομένων σε μια πιο συνταγματική προσέγγιση στο ψηφιακό περιβάλλον ήταν οι υποθέσεις Lindqvist και Promusicae. Στην υπόθεση Lindqvist, το ΔΕΕ έκρινε ότι η δημοσίευση πληροφοριών στο Διαδίκτυο σχετικά με την υγεία και άλλων προσωπικών δεδομένων χωρίς τη συγκατάθεση των ατόμων παραβιάζει την προστασία των δεδομένων προσωπικού χαρακτήρα και το δικαίωμα στην ιδιωτική ζωή, όπως αυτά προστατεύονται από την Οδηγία. Το ΔΕΕ τόνισε την ανάγκη εξισορρόπησης μεταξύ της προστασίας των προσωπικών δεδομένων και της ελευθερίας της έκφρασης. Ωστόσο, έδωσε προτεραιότητα στην προστασία της ιδιωτικής ζωής. Αργότερα, στην υπόθεση Promusicae, το ΔΕΕ διεύρυνε την ερμηνεία του για το δικαίωμα στην

ΕΕ. 2)**Άμεση παρέμβαση** σε περιπτώσεις όπου η παραβίαση των κανονισμών από μια πλατφόρμα έχει διακρατική διάσταση ή όταν οι εθνικές αρχές δεν μπορούν να επιλύσουν το ζήτημα αποτελεσματικά. 3)**Επιβολή κυρώσεων** σε πολύ μεγάλες διαδικτυακές πλατφόρμες (VLOPs), οι οποίες λόγω του μεγέθους και της επιρροής τους, απαιτούν ιδιαίτερα αυστηρή εποπτεία.

προστασία των δεδομένων. Εξετάζοντας το θέμα της αποκάλυψης ταυτότητας και διεύθυνσης χρηστών διαδικτύου, το ΔΕΕ αναγνώρισε τη σημασία της προστασίας των δεδομένων για τη διασφάλιση της ιδιωτικής ζωής, ακόμα και αν αυτά τα δύο δικαιώματα είναι στενά συνδεδεμένα.

Google France (2010): Το ΔΕΕ έκρινε ότι οι μηχανές αναζήτησης δεν ευθύνονται για τα δεδομένα που αποθηκεύουν κατόπιν αιτήματος των διαφημιστών, εφόσον δεν έχουν γνώση της παρανομίας τους. Η υπόθεση αυτή υπογράμμισε τη σημασία των οικονομικών συμφερόντων, αλλά ανέδειξε επίσης τον αναδυόμενο ρόλο της αυτοματοποιημένης λήψης αποφάσεων στη διαχείριση περιεχομένου. Αν και το ΔΕΕ δεν αναγνώρισε ενεργό ρόλο της Google σε αυτή την υπόθεση, επεσήμανε την επιρροή των αλγόριθμων και των αυτοματοποιημένων διαδικασιών στον καθορισμό της εμφάνισης του διαδικτυακού περιεχομένου.

L'Oréal κατά eBay (2011): Το δικαστήριο αναγνώρισε ότι διαδικτυακές πλατφόρμες όπως το eBay, οι οποίες βοηθούν στη βελτιστοποίηση των πωλήσεων, επιτελούν πιο ενεργό ρόλο από την απλή παροχή παθητικής υπηρεσίας. Η αναγνώριση του γεγονότος ότι οι αυτοματοποιημένες τεχνολογίες μπορούν να κάνουν έναν πάροχο να διαδραματίσει ενεργό ρόλο σημαίνει ότι η ευθύνη τους μπορεί να επεκταθεί πέρα από την απλή αποθήκευση ή διαβίβαση περιεχομένου. Η απόφαση αυτή αποτελεί σημαντική εξέλιξη στο νομικό πλαίσιο ευθύνης των διαδικτυακών μεσαζόντων, υπογραμμίζοντας τη σημασία του διαχωρισμού μεταξύ παθητικών και ενεργών ρόλων των παρόχων υπηρεσιών στο διαδίκτυο.

Scarlet Extended και Netlog (2011-2012): Η υιοθέτηση μιας πιο συνταγματικής προσέγγισης προέκυψε από δύο υποθέσεις που αφορούσαν διαδικτυακούς μεσάζοντες και την απαγόρευση της γενικής παρακολούθησης. Στις υποθέσεις Scarlet και Netlog, τα εθνικά δικαστήρια εξέτασαν αν τα κράτη μέλη μπορούν να επιτρέψουν στα δικαστήρια να επιβάλουν στις διαδικτυακές πλατφόρμες την υποχρέωση εγκατάστασης συστημάτων φιλτραρίσματος όλων των ηλεκτρονικών επικοινωνιών για την πρόληψη παράνομου περιεχομένου. Υπενθυμίζουμε ότι η Οδηγία για το ηλεκτρονικό εμπόριο απαγορεύει τη γενική παρακολούθηση. Το ΔΕΕ έκρινε ότι τέτοια επιβολή θα παραβίαζε την επιχειρηματική ελευθερία των πλατφορμών και τα θεμελιώδη δικαιώματα των χρηστών, όπως την ιδιωτική ζωή και την ελευθερία της έκφρασης. Ως εκ τούτου, το ΔΕΕ αποφάσισε ότι η βελγική απαίτηση για γενικό φιλτράρισμα περιεχομένου ήταν ασύμβατη με την απαγόρευση της

γενικής υποχρέωσης παρακολούθησης χρησιμοποιώντας εφεξής τον Χάρτη για την αξιολόγηση του πλαισίου της Οδηγίας για το ηλεκτρονικό εμπόριο.

Telekabel (2014) και McFadden (2016). Στις υποθέσεις Telekabel και McFadden, το ΔΕΕ εξέτασε διαταγές ασφαλιστικών μέτρων που αφορούσαν διαδικτυακούς διαμεσολαβητές. Το ΔΕΕ επικύρωσε την ερμηνεία των εθνικών δικαστηρίων, όπως στις υποθέσεις Scarlet και Netlog, αποφασίζοντας ότι τα θεμελιώδη δικαιώματα δεν αποκλείουν τέτοιες δικαστικές εντολές. Και στις δύο υποθέσεις, το ΔΕΕ επιβεβαίωσε την αρχή ότι οι διαδικτυακοί διαμεσολαβητές μπορούν να διατάσσονται να λαμβάνουν μέτρα για την πρόληψη παραβιάσεων πνευματικών δικαιωμάτων, αλλά τέτοια μέτρα πρέπει να είναι αναλογικά και να μην παραβιάζουν τα θεμελιώδη δικαιώματα των χρηστών.

4.3. Ο δικαστικός δρόμος προς την ψηφιακή ιδιωτικότητα

Digital Rights Ireland (2014): Η πρώτη σημαντική απόφαση, μετά την έναρξη ισχύος της Συνθήκης της Λισαβόνας, που αποδεικνύει ότι το ΔΕΕ σταδιακά αρχίζει να εφαρμόζει τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, αναγνωρίζοντας ένα νέο θεμελιώδες δικαίωμα—της προστασίας των προσωπικών δεδομένων— είναι η υπόθεση **Digital Rights Ireland.** Το δικαστήριο ακύρωσε την Οδηγία για τη διατήρηση δεδομένων λόγω των δυσανάλογων επιπτώσεων στα θεμελιώδη δικαιώματα, τονίζοντας την ανάγκη για εγγυήσεις κατά της κατάχρησης δεδομένων προσωπικού χαρακτήρα. Πιο συγκεκριμένα, το ΔΕΕ διαπίστωσε ότι η γενική και χωρίς διάκριση διατήρηση δεδομένων ήταν δυσανάλογη και δεν τηρούσε την αρχή της αναλογικότητας, καθώς δεν περιείχε επαρκείς εγγυήσεις για την προστασία των δικαιωμάτων των χρηστών. Σε σχέση με τις αυτοματοποιημένες τεχνολογίες, το ΔΕΕ τόνισε ότι η ανάγκη για τέτοιου είδους εγγυήσεις είναι ακόμη μεγαλύτερη όταν τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε αυτοματοποιημένη επεξεργασία και όταν υπάρχει σημαντικός κίνδυνος παράνομης πρόσβασης στα δεδομένα αυτά. Η προσέγγιση αυτή σχετικά με τη διατήρηση των δεδομένων υιοθετήθηκε και σε μεταγενέστερες αποφάσεις, όπως στην Tele2 (2016) και La Quadrature du Net (2020), οι οποίες θα αναλυθούν στο επόμενο κεφάλαιο.

Google Spain (2014): Αυτή η υπόθεση-ορόσημο καθιέρωσε το «δικαίωμα στη λήθη», επιτρέποντας στα άτομα να ζητούν την αφαίρεση προσωπικών δεδομένων από τα αποτελέσματα των μηχανών αναζήτησης. Αποτελεί την πρώτη δικαστική προσπάθεια να

αντιμετωπιστεί η ισχύς των διαδικτυακών πλατφορμών και να δοθεί απάντηση στη νομοθετική αδράνεια της Ένωσης, θέτοντας έτσι τα θεμέλια του ψηφιακού συνταγματισμού. Το δικαστήριο έκρινε ότι οι μηχανές αναζήτησης είναι υπεύθυνοι επεξεργασίας δεδομένων και πρέπει να συμμορφώνονται με τις αρχές προστασίας δεδομένων, ενισχύοντας έτσι την προστασία της ιδιωτικής ζωής και των δικαιωμάτων των δεδομένων.

Schrems I (2015): Η υπόθεση Schrems I ήταν καθοριστική για την προστασία των δεδομένων στην ΕΕ και επηρέασε σημαντικά τον τρόπο με τον οποίο ρυθμίζονται οι διασυνοριακές μεταφορές δεδομένων. Το Δικαστήριο ακύρωσε τη συμφωνία Safe Harbour[30] καθώς έκρινε δεν παρείχε επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ όταν αυτά μεταφέρονται στις ΗΠΑ. Συγκεκριμένα, το ΔΕΕ διαπίστωσε ότι το πλαίσιο δεν προστάτευε επαρκώς τα δεδομένα από την πρόσβαση των αμερικανικών αρχών ασφαλείας. Ουσιαστικά, το ΔΕΕ θεώρησε ότι ένα υπερθενικό πλαίσιο προστασίας ταυτίζεται με την ύπαρξη ενός ουσιαστικά ισοδύναμου με αυτό της ΕΕ[31].

---

[30] Ο όρος "Safe Harbour" (Ασφαλές Λιμάνι) αναφέρεται σε ένα νομικό πλαίσιο που είχε αρχικά δημιουργηθεί για να διευκολύνει τη μεταφορά προσωπικών δεδομένων από την ΕΕ προς τις Ηνωμένες Πολιτείες. Το πλαίσιο αυτό υιοθετήθηκε το 2000 και προέβλεπε ότι οι εταιρείες στις ΗΠΑ που συμμορφώνονταν με τις αρχές του Safe Harbour (Αρχή της Ενημέρωσης (Notice Principle), Αρχή της Επιλογής (Choice Principle), Αρχή της Επικοινωνίας (Onward Transfer Principle), Αρχή της Ασφάλειας (Security Principle), Αρχή της Ακεραιότητας των Δεδομένων (Data Integrity Principle), Αρχή της Πρόσβασης (Access Principle), Αρχή της Επιβολής (Enforcement Principle) μπορούσαν να μεταφέρουν και να επεξεργάζονται προσωπικά δεδομένα πολιτών της ΕΕ χωρίς να παραβιάζουν την αυστηρή νομοθεσία της ΕΕ περί προστασίας δεδομένων.

[31] Μετά την ακύρωση του Safe Harbour, οι ΕΕ και οι ΗΠΑ διαπραγματεύτηκαν και καθιέρωσαν το Privacy Shield ως νέο πλαίσιο για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ στις ΗΠΑ. Το Privacy Shield εισήγαγε αρκετές βελτιώσεις σε σχέση με το προηγούμενο πλαίσιο, προκειμένου να ανταποκριθεί στις ανησυχίες που εκφράστηκαν από το ΔΕΕ και να προσφέρει καλύτερη προστασία των προσωπικών δεδομένων των Ευρωπαίων πολιτών. Σε αντίθεση με το Safe Harbour, το Privacy Shield εισήγαγε αυστηρότερους μηχανισμούς επιβολής, με το Υπουργείο Εμπορίου των ΗΠΑ να αναλαμβάνει ενεργό ρόλο στην επιτήρηση της συμμόρφωσης των αμερικανικών εταιρειών και την επιβολή αυστηρών κυρώσεων σε περιπτώσεις παραβίασης. Περιελάμβανε πιο συγκεκριμένες και αυστηρές διατάξεις σχετικά με την πρόσβαση των αμερικανικών κυβερνητικών αρχών στα προσωπικά δεδομένα για λόγους εθνικής ασφάλειας, επιβεβαιώνοντας ότι η πρόσβαση αυτή θα γινόταν μόνο όταν ήταν απαραίτητο και αναλογικό. Επιπλέον, εισήγαγε τον ανεξάρτητο μηχανισμό Ombudsman για την εξέταση καταγγελιών των Ευρωπαίων πολιτών και την επιβεβαίωση της συμμόρφωσης με τους νόμους των ΗΠΑ. Οι μηχανισμοί επίλυσης διαφορών ενισχύθηκαν, δίνοντας στους πολίτες τη δυνατότητα προσφυγής σε ανεξάρτητους φορείς στις ΗΠΑ, ενώ οι εταιρείες υποχρεώθηκαν να απαντούν άμεσα στις καταγγελίες. Το πλαίσιο απαιτούσε επίσης μεγαλύτερη διαφάνεια και λογοδοσία, με τις εταιρείες να δημοσιεύουν τις πολιτικές απορρήτου τους και να υποβάλλονται σε τακτικές αναθεωρήσεις. Τέλος, το Privacy Shield ενίσχυσε τη συνεργασία με τις ευρωπαϊκές αρχές προστασίας δεδομένων,

5. ΨΗΦΙΑΚΟΣ ΣΥΝΤΑΓΜΑΤΙΣΜΟΣ, ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΜΑΖΙΚΗ ΕΠΙΤΗΡΗΣΗ

Οι αποκαλύψεις του Edward Snowden το 2013, ανέδειξαν ότι, σε περιόδους έντασης, όπως κατά τη διάρκεια τρομοκρατικών επιθέσεων και διεθνών εγκλημάτων, οι δημόσιες αρχές καταφεύγουν όλο και περισσότερο σε συστήματα παρακολούθησης για να εγγυηθούν την εθνική και δημόσια ασφάλεια. Παρά την αποτελεσματικότητά της στην καταπολέμηση της τρομοκρατίας και του παγκόσμιου εγκλήματος, η μαζική παρακολούθηση προκαλεί σοβαρές επεμβάσεις στην ιδιωτική ζωή πολλών ανθρώπων, απειλώντας το δικαίωμα προστασίας των δεδομένων και άλλα θεμελιώδη δικαιώματα, όπως η ελευθερία της έκφρασης και η αρχή του τεκμηρίου αθωότητας. Στην ΕΕ, αυτή η πρόκληση έχει γίνει το επίκεντρο έντονης συζήτησης μεταξύ της κοινωνίας των πολιτών, των δικαστηρίων, των νομοθετών και των αρχών επιβολής του νόμου σε εθνικό και υπερεθνικό επίπεδο. Πολίτες και ΜΚΟ επιδιώκουν την απαγόρευση ή τουλάχιστον αυστηρότερους κανόνες για τη χρήση επεμβατικών μέτρων παρακολούθησης, προκειμένου να προστατεύσουν τα θεμελιώδη δικαιώματα και τις ελευθερίες από τον προληπτικό έλεγχο δεδομένων από τις δημόσιες αρχές. Οι ομάδες της κοινωνίας των πολιτών έχουν διαδραματίσει κρίσιμο ρόλο, προωθώντας δικαστικές συζητήσεις για την ανάγκη θέσπισης εγγυήσεων για τις τεχνικές μαζικής παρακολούθησης και συμμετέχοντας σε δημόσιες συζητήσεις για την προσαρμογή των συνταγματικών δικαιωμάτων στις σύγχρονες προκλήσεις που προκύπτουν από την ψηφιακή τεχνολογία και την εθνική ασφάλεια.

Οι Celeste και Formici (2024) στη μελέτη τους "Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia" χαρτογραφούν τη σταδιακή προσπάθεια συνταγματικής αντιμετώπισης των πρακτικών μαζικής παρακολούθησης, εστιάζοντας σε τρεις βασικούς παράγοντες: την κοινωνία των πολιτών, το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) και τους εθνικούς νομοθέτες.

επιτρέποντάς τους να παραπέμπουν υποθέσεις στις αμερικανικές αρχές και να συνεργάζονται για την επίλυση διαφορών. Παρά τις βελτιώσεις αυτές, το Privacy Shield ακυρώθηκε τελικά στην υπόθεση Schrems II (C-311/18) καθώς κρίθηκε ότι δεν παρείχε επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων από τις ευρείες εξουσίες παρακολούθησης των αμερικανικών αρχών.

5.1. Ο ρόλος της κοινωνίας των πολιτών

Οι ανωτέρω συγγραφείς διαπιστώνουν ότι οι πρακτικές επιτήρησης αναπτύχθηκαν λόγω της ύπαρξης ενός συνταγματικού κενού, καθώς τα υπάρχοντα συνταγματικά κείμενα σπάνια αναφέρονται ρητά σε αυτές. Χαρακτηριστικό είναι ότι ο όρος «επιτήρηση» περιλαμβάνεται ρητά μόνο στα συντάγματα της Σουηδίας και της Γερμανίας. Στη Σουηδία, η νομοθεσία προστατεύει τον πολίτη κατά της παρακολούθησης της αλληλογραφίας και οποιασδήποτε άλλης μορφής εμπιστευτικής επικοινωνίας και της εν γένει παρακολούθησης χωρίς συγκατάθεση, ενώ στη Γερμανία η επιτήρηση επιτρέπεται υπό αυστηρές προϋποθέσεις (δικαστική έγκριση και χρονικός περιορισμός) για την αντιμετώπιση σοβαρών εγκλημάτων ή κινδύνων για τη δημόσια ασφάλεια.

Η προστασία της ιδιωτικής ζωής γενικά αναγνωρίζεται στα σύγχρονα συντάγματα, ωστόσο, δεν υπάρχουν σαφείς διατάξεις που να περιορίζουν αυστηρά τη χρήση πρακτικών μαζικής παρακολούθησης, ακόμα και σε συνταγματικά κείμενα που αναφέρονται συγκεκριμένα στην παρακολούθηση. Αντιθέτως, τα εθνικά συντάγματα συχνά περιλαμβάνουν διατάξεις που μπορεί να περιορίζουν το απόρρητο της αλληλογραφίας, το δικαίωμα στην ιδιωτική ζωή και το δικαίωμα στην προστασία των δεδομένων. Αυτά τα δικαιώματα δεν θεωρούνται απόλυτα και σχετικοποιούνται από περιορισμούς για λόγους δημόσιας και εθνικής ασφάλειας, επιτρέποντας έτσι την εγκαθίδρυση συστημάτων μαζικής παρακολούθησης.

Ελλείψει σαφούς και λεπτομερούς ρύθμισης της επιτήρησης στα εθνικά και υπερεθνικά συντάγματα, η κοινωνία των πολιτών έπαιξε καταλυτικό ρόλο στην προσπάθεια «συνταγματοποίησης» της μαζικής επιτήρησης. Οι οργανώσεις της κοινωνίας των πολιτών έχουν λειτουργήσει ως καταλύτες για σημαντικές δικαστικές υποθέσεις που αμφισβητούν τις κρατικές πρακτικές παρακολούθησης. Ακτιβιστές, όπως ο Max Schrems, και οργανώσεις όπως οι Digital Rights Ireland , Quadrature du Net, Privacy International και Big Brother Watch[32] στο πλαίσιο της στρατηγικής τους ενάντια στις καταχρήσεις των νομοθετών

[32] Οι υποθέσεις Big Brother Watch και άλλοι κατά Ηνωμένου Βασιλείου και Privacy International κατά Ηνωμένου Βασιλείου ξεκίνησαν μετά τις αποκαλύψεις του Edward Snowden το 2013, οι οποίες έδειξαν ότι η GCHQ (Government Communications Headquarters) εμπλέκεται σε εκτεταμένες πρακτικές μαζικής παρακολούθησης τόσο εντός όσο και εκτός του Ηνωμένου Βασιλείου. Και οι δύο περιπτώσεις αμφισβήτησαν τη νομιμότητα αυτών των πρακτικών υπό το πρίσμα της ΕΣΔΑ, επικεντρώνοντας στην παραβίαση των άρθρων 8 (δικαίωμα στην ιδιωτική ζωή) και 10 (δικαίωμα

και των κυβερνητικών υπηρεσιών προσέφυγαν δικαστικά και οδήγησαν σε σημαντικές νομοθετικές μεταρρυθμίσεις τόσο σε επίπεδο ΕΕ όσο και σε εθνικό επίπεδο.

Ακαδημαϊκοί, ακτιβιστές και ΜΚΟ έχουν, επίσης, διαδραματίσει σημαντικό ρόλο στην ανάπτυξη νέων συνταγματικών αρχών που στοχεύουν ειδικά στις πρακτικές επιτήρησης. Εμπειρικές μελέτες καταγράφουν πάνω από 200 δηλώσεις που εκδόθηκαν από φορείς της κοινωνίας των πολιτών για τη διατύπωση αρχών και αξιών για την ψηφιακή κοινωνία. Αυτά τα κείμενα, γνωστά ως "Internet Bill of Rights", δεν είναι νομικά δεσμευτικά, αλλά προσφέρουν καινοτόμες κανονιστικές λύσεις στις προκλήσεις της μαζικής επιτήρησης. Από κοινωνικο-νομική σκοπιά, αυτά τα έγγραφα έχουν ανεκτίμητη αξία για την κατανόηση των αιτημάτων της κοινωνίας των πολιτών στην ψηφιακή εποχή και του βαθμού στον οποίο αυτά τα αιτήματα ενσωματώνονται στην έννομη τάξη. Αν και δεν είναι προϊόντα δημοκρατικής διαβούλευσης, τα κείμενα αυτά έχουν στοιχεία που τα καθιστούν παρόμοια με εθνικά και υπερεθνικά συντάγματα (Celeste, Internet Bill of Rights) Στα κείμενα αυτά μπορεί κανείς να βρει τρεις βασικούς κανόνες:

Πρώτα απ' όλα, οι τίτλοι αυτών των εγγράφων αναφέρονται ξεκάθαρα σε μια συνταγματική διάσταση. Μερικά παραδείγματα είναι ο «Χάρτης των Θεμελιωδών Ψηφιακών Δικαιωμάτων της ΕΕ», η «Μάγκνα Κάρτα για την Ψηφιακή Εποχή» και η «Διακήρυξη των Δικαιωμάτων του Διαδικτύου».

Δεύτερον, χρησιμοποιούν ορολογία που απαντάται σε συνταγματικά κείμενα. Για παράδειγμα, περιλαμβάνουν «προοίμιο» και προτάσεις που αναφέρονται σε «όλους» ή «όλους τους ανθρώπους», καθώς και ρήματα όπως «πρέπει».

Τρίτον, αναφέρονται σε δικαιώματα και υποχρεώσεις, όπως ακριβώς γίνεται στα εθνικά συντάγματα. Για παράδειγμα, ο Χάρτης Δικαιωμάτων του Διαδικτύου της APC (Association for progressive communications), προβλέπει το δικαίωμα στην ψηφιακή πληροφόρηση υποχρεώνοντας τις κυβερνήσεις να διασφαλίζουν τη διαφάνεια και τη λογοδοσία με ανοικτές και προσβάσιμες μορφές δεδομένων. Κατά παρόμοιο τρόπο, οι Αρχές της Σάντα Κλάρα σχετικά με τη διαφάνεια και τη λογοδοσία στον έλεγχο του περιεχομένου

στην ελευθερία της έκφρασης). Οι αποφάσεις του ΕΔΑΔ ανάγκασαν το Ηνωμένο Βασίλειο να επανεξετάσει και να αναθεωρήσει τις πρακτικές του για τη μαζική παρακολούθηση, εισάγοντας αυστηρότερες εγγυήσεις για την προστασία της ιδιωτικής ζωής και της ελευθερίας της έκφρασης.

στο Διαδίκτυο θεμελιώνουν το δικαίωμα της δίκαιης δίκης, όταν ορίζουν ότι «οι εταιρείες θα πρέπει να παρέχουν μια ουσιαστική ευκαιρία για έγκαιρη προσφυγή κατά οποιασδήποτε αφαίρεσης περιεχομένου ή αναστολής λογαριασμού». Επίσης, το άρθρο 2 της Διακήρυξης των Δικαιωμάτων στο Διαδίκτυο δομεί το δικαίωμα πρόσβασης στο Διαδίκτυο ως εξής:

1.Η πρόσβαση στο Διαδίκτυο αποτελεί θεμελιώδες δικαίωμα όλων των ατόμων και προϋπόθεση για την ατομική και κοινωνική τους ανάπτυξη. 2. Κάθε πρόσωπο έχει το ίδιο δικαίωμα πρόσβασης στο Διαδίκτυο με ίσους όρους, χρησιμοποιώντας κατάλληλες και σύγχρονες τεχνολογίες που αίρουν όλους τους οικονομικούς και κοινωνικούς φραγμούς.3. Το θεμελιώδες δικαίωμα πρόσβασης στο Διαδίκτυο πρέπει να διασφαλίζεται ως προς τις ουσιαστικές προϋποθέσεις του και όχι μόνο ως απλή δυνατότητα σύνδεσης στο Διαδίκτυο. 4. Η πρόσβαση πρέπει να περιλαμβάνει την ελευθερία επιλογής όσον αφορά τις συσκευές, τα λειτουργικά συστήματα και τις εφαρμογές, συμπεριλαμβανομένου του κατανεμημένου λογισμικού. 5.Οι δημόσιοι οργανισμοί λαμβάνουν τα αναγκαία μέτρα για την υπέρβαση όλων των μορφών ψηφιακού χάσματος, συμπεριλαμβανομένων εκείνων που δημιουργούνται από το φύλο, την οικονομική κατάσταση, την προσωπική ευπάθεια ή την αναπηρία.

Τέλος, ο Χάρτης Ανθρωπίνων Δικαιωμάτων και Αρχών για το Διαδίκτυο αναγνωρίζει το δικαίωμα προστασίας των προσωπικών δεδομένων που υποβάλλονται σε ειδική επεξεργασία στο διαδίκτυο, ως ακολούθως: *Καθένας έχει δικαίωμα στην ιδιωτική ζωή στο διαδίκτυο. Αυτό περιλαμβάνει την ελευθερία από την παρακολούθηση, το δικαίωμα χρήσης κρυπτογράφησης και το δικαίωμα στην ανωνυμία στο διαδίκτυο. Καθένας έχει επίσης το δικαίωμα στην προστασία των δεδομένων, συμπεριλαμβανομένου του ελέγχου της συλλογής, διατήρησης, επεξεργασίας, διάθεσης και κοινοποίησης προσωπικών δεδομένων.*

Σύμφωνα με μια επιστημονική άποψη (Teubner, 2004), ο ρόλος αυτών των κειμένων δεν είναι απλά να μεταφέρουν τις ανθρώπινες αξίες και αρχές στον ψηφιακό κόσμο. Αναγνωρίζοντας ότι μια σειρά από θεμελιώδη δικαιώματα σχεδιασμένα να υπάρχουν στον αναλογικό κόσμο, παλεύουν για να διαπεράσουν στον εικονικό κόσμο, ο Teubner υποστηρίζει ότι τα ιδιωτικά αυτά κείμενα επιτελούν μια διπλή λειτουργία—αυτή της «γενίκευσης» και του «επαναπροσδιορισμού». Ο συνταγματικός κανόνας δεν μπορεί απλώς να εφαρμοστεί αυτούσια σε ένα διαφορετικό κοινωνικό πλαίσιο. Είναι απαραίτητο να κατανοηθεί ο βασικός του σκοπός, να γενικευθούν οι θεμελιώδεις αρχές του, να απαλλαγεί από τις αρχικές επιρροές του περιβάλλοντος και στη συνέχεια να επαναπροσδιοριστεί

σύμφωνα με τα χαρακτηριστικά της νέας κοινωνικής πραγματικότητας. Ένα παράδειγμα θεμελιώδους αξίας είναι ο σεβασμός της ιδιωτικής ζωής. Ο σεβασμός της ιδιωτικής ζωής του ατόμου είναι ένα απτό παράδειγμα γενίκευσης και επαναπροσδιορισμού καθώς στις διακηρύξεις δικαιωμάτων στο Διαδίκτυο όχι μόνο επαναδιατυπώνεται με αναφορά στην ψηφιακή τεχνολογία, αλλά και γενικεύεται και επαναπροσδιορίζεται λαμβάνοντας υπόψη τις προκλήσεις της ψηφιακής κοινωνίας

Τα περισσότερα από αυτά τα κείμενα δικαιωμάτων γενικά επιβεβαιώνουν ότι οποιαδήποτε μορφή παρακολούθησης επηρεάζει την ιδιωτική ζωή του ατόμου. Ωστόσο, ορισμένα από αυτά εισάγουν νέες αρχές που περιορίζουν τις πρακτικές μαζικής παρακολούθησης. Για παράδειγμα, η Αφρικανική Διακήρυξη για τα Δικαιώματα και τις Ελευθερίες του Διαδικτύου αναφέρει:

Η μαζική ή αδιάκριτη παρακολούθηση ατόμων ή η παρακολούθηση των επικοινωνιών τους συνιστά δυσανάλογη παρέμβαση και, συνεπώς, παραβίαση του δικαιώματος στην ιδιωτική ζωή, της ελευθερίας της έκφρασης και άλλων ανθρωπίνων δικαιωμάτων. Η μαζική παρακολούθηση απαγορεύεται με νόμο. [...] Προκειμένου να πληρούνται οι απαιτήσεις του διεθνούς δικαίου των ανθρωπίνων δικαιωμάτων, η στοχευμένη επιτήρηση των επιγραμμικών επικοινωνιών πρέπει να διέπεται από σαφείς και διαφανείς νόμους οι οποίοι, κατ' ελάχιστον, συμμορφώνονται με τις ακόλουθες βασικές αρχές: πρώτον, η παρακολούθηση των επικοινωνιών πρέπει να είναι τόσο στοχευμένη όσο και να βασίζεται σε εύλογη υποψία διάπραξης ή εμπλοκής στη διάπραξη σοβαρού εγκλήματος- δεύτερον, η παρακολούθηση των επικοινωνιών πρέπει να είναι δικαστικά εξουσιοδοτημένη και τα άτομα που έχουν τεθεί υπό παρακολούθηση πρέπει να ενημερώνονται για την παρακολούθηση της επικοινωνίας τους, το συντομότερο δυνατό μετά την ολοκλήρωση της επιχείρησης παρακολούθησης- τρίτον, η εφαρμογή των νόμων περί παρακολούθησης πρέπει να υπόκειται σε ισχυρή κοινοβουλευτική εποπτεία για την πρόληψη της κατάχρησης και τη διασφάλιση της λογοδοσίας των υπηρεσιών πληροφοριών και των υπηρεσιών επιβολής του νόμου.

Εν κατακλείδι, οι ιδιωτικές διακηρύξεις για τα δικαιώματα στο Διαδίκτυο δηλώνουν ότι η μαζική και αδιάκριτη παρακολούθηση αποτελεί ανεπίτρεπτη παραβίαση του δικαιώματος στην ιδιωτική ζωή, η οποία δεν μπορεί να θεωρηθεί αναλογική σε καμία περίπτωση. Μόνο στοχευμένες μορφές παρακολούθησης, οι οποίες υπόκεινται σε συγκεκριμένες εγγυήσεις, μπορούν να γίνουν αποδεκτές ως λογικοί περιορισμοί αυτού του

δικαιώματος. Είναι ενδιαφέρον ότι οι εγγυήσεις αυτές όπως η ανάγκη για αντιμετώπιση σοβαρών εγκλημάτων, η προηγούμενη δικαστική άδεια και η ενημέρωση των ατόμων που υπόκεινται σε καθεστώς παρακολούθησης ευθυγραμμίζονται με τις πρακτικές που καθιερώνει σταδιακά η νομολογία του ΔΕΕ, όπως θα εξεταστεί στην επόμενη ενότητα.

5.2. Ο ρόλος των μεγάλων ιδιωτικών εταιρειών

Στο πλαίσιο της ψηφιακής εποχής, οι ιδιωτικές εταιρείες τεχνολογίας έχουν αναλάβει έναν σημαντικό ρόλο στη ρύθμιση και διαχείριση των ψηφιακών δικαιωμάτων και της διαδικτυακής δραστηριότητας. Οι ιδιωτικές εταιρείες τεχνολογίας, όπως η Facebook, η Google και άλλες μεγάλες πλατφόρμες, έχουν δημιουργήσει τους δικούς τους κανονισμούς και πολιτικές (lex digitalis) για τη διαχείριση του περιεχομένου και της συμπεριφοράς των χρηστών στις πλατφόρμες τους. Αυτές οι πολιτικές συχνά περιλαμβάνουν όρους χρήσης και πολιτικές απορρήτου που καθορίζουν τι επιτρέπεται και τι όχι στην πλατφόρμα (Platform law), καθώς και πώς συλλέγονται, αποθηκεύονται και χρησιμοποιούνται τα δεδομένα των χρηστών.

Ένα παράδειγμα αυτής της ιδιωτικής ρύθμισης είναι η "Lex Facebook", ένας όρος που χρησιμοποιείται για να περιγράψει τους κανονισμούς και τις πολιτικές που εφαρμόζει η Facebook για τη διαχείριση του περιεχομένου και της συμπεριφοράς των χρηστών της πλατφόρμας της. Η Facebook έχει αναπτύξει ένα σύνολο κανόνων και διαδικασιών για την αντιμετώπιση ζητημάτων όπως η ρητορική μίσους, η παραπληροφόρηση και το βίαιο περιεχόμενο. Επιπλέον, έχει δημιουργήσει και εφαρμόζει δικούς της μηχανισμούς επιβολής των κανόνων της, συμπεριλαμβανομένων αλγορίθμων που εντοπίζουν και αφαιρούν περιεχόμενο που παραβιάζει τις πολιτικές της, καθώς και ομάδες ανθρώπων που εξετάζουν περιπτώσεις πιο περίπλοκες ή αμφιλεγόμενες.

Στο σημείο αυτό είναι ενδιαφέρον να αναφερθούμε στους όρους του "Lex Facebook" στην εποχή πριν τη θέσπιση του ΓΚΠΔ καθώς το συνταγματικό ύφος αυτών προκαλεί εντύπωση. Παρά το γεγονός ότι κάποιος μπορεί να ισχυριστεί ότι «η Δήλωση Δικαιωμάτων και Υποχρεώσεων» (Statement of Rights and Responsibilities) που υιοθέτησε το Facebook για να περιγράψει τους εσωτερικούς κανόνες, έγινε για λόγους στρατηγικής μάρκετινγκ, η μοναδικότητα του όρου στο τοπίο των όρων υπηρεσίας των κύριων ιστοσελίδων κοινωνικής δικτύωσης παραμένει γεγονός. Το Facebook, επίσης, δημιούργησε ένα ξεχωριστό έγγραφο

που τιτλοφορήθηκε οι «Αρχές του Facebook» στο οποίο απαριθμεί τις βασικές αξίες (π.χ. διαφάνεια, έλεγχος, προσβασιμότητα).

Είναι προφανές ότι η αυξανόμενη επιρροή των ιδιωτών νομοθετών εγείρει ερωτήματα σχετικά με τη λογοδοσία και τη διαφάνεια. Σε αντίθεση με τα κρατικά όργανα, οι ιδιωτικές εταιρείες δεν υπόκεινται στην ίδια βαθμίδα ελέγχου και εποπτείας. Οι αποφάσεις τους συχνά λαμβάνονται χωρίς τη διαφάνεια που απαιτείται από τα δημόσια όργανα και οι χρήστες μπορεί να μην έχουν την ίδια δυνατότητα να προσβάλουν ή να ελέγξουν αυτές τις αποφάσεις καθώς δεν έχουν πλήρη εικόνα των κριτηρίων που χρησιμοποιούνται.

Ωστόσο, κανείς δεν μπορεί να αμφισβητήσει το γεγονός ότι η ύπαρξη εσωτερικών κανόνων ιδιωτικών φορέων μπορεί να λειτουργήσει αφενός ως αντίβαρο σε ενδεχόμενη κυβερνητική απάθεια και αφετέρου ως πεδίο διάδρασης που αποκαλύπτει και την πολύπλοκη ισορροπία μεταξύ ιδιωτικής εξουσίας και δημόσιου συμφέροντος. Για παράδειγμα, με την έναρξη ισχύος του ΓΚΠΔ, το Facebook αναπροσάρμοσε τους όρους χρήσης του, περιλαμβάνοντας και αλλαγή στον επίσημο τίτλο τους ("Terms of Service"). Σύμφωνα με τον ΓΚΠΔ, οι υπεύθυνοι για την επεξεργασία δεδομένων οφείλουν να παρουσιάζουν τις πληροφορίες με τρόπο που είναι ξεκάθαρος, κατανοητός και εύκολα προσβάσιμος. Αυτή η απαίτηση πιθανώς οδήγησε το Facebook να κρίνει ότι ο προηγούμενος τίτλος θα μπορούσε να δημιουργήσει παρανοήσεις στους χρήστες.

Στο σημείο αυτό αξίζει να γίνει μια σύντομη αναφορά και στο Lex informatica, όρο που χρησιμοποίησε ο Reidenberg (1998), για να περιγράψει τη δυνατότητα που έχουν οι ιδιωτικές εταιρείες να καθιερώνουν νομικούς κανόνες μέσω της τεχνικής αρχιτεκτονικής του λογισμικού τους. Αυτή η ιδέα συνοψίζεται στο διάσημο σύνθημα του Lawrence Lessig «ο κώδικας είναι νόμος». Συνεπώς, αν και ο νομικός κανόνας δεν είναι ρητά διατυπωμένος, είναι ενσωματωμένος στον τρόπο που οι προγραμματιστές σχεδιάζουν ένα πρόγραμμα. Όπως αναφέρει ο Karavas (2009), ο κώδικας έχει ισχυρή ρυθμιστική δύναμη και αποτελεσματικότητα σε σύγκριση με τους παραδοσιακούς νόμους. Στον ψηφιακό κόσμο, ο κώδικας μπορεί να ρυθμίζει τη συμπεριφορά των χρηστών πιο αποτελεσματικά από τους νόμους, καθώς μπορεί να αποτρέπει άμεσα τις παραβάσεις μέσω της τεχνολογικής του δομής.

Χαρακτηριστική περίπτωση του τρόπου με τον οποίο ο κώδικας υπολογιστών ενσαρκώνει στον ψηφιακό κόσμο τους νομικούς κανόνες είναι η διαχείριση προσωπικών δεδομένων στις κοινωνικές πλατφόρμες. Π.χ. μια κοινωνική πλατφόρμα μπορεί να ενσωματώσει τη νομοθεσία για την προστασία των προσωπικών δεδομένων ενσωματώνοντας τεχνικούς περιορισμούς που περιορίζουν την ποσότητα των προσωπικών δεδομένων που συλλέγονται κατά την εγγραφή ενός νέου χρήστη. Μπορεί επίσης να προσφέρει εργαλεία διαχείρισης απορρήτου που επιτρέπουν στους χρήστες να ελέγχουν ποια δεδομένα μοιράζονται και με ποιον. Ο Karavas (ibid) καταλήγει ότι οι τεχνολογικές εταιρείες χρησιμοποιούν τόσο τους ρητά διατυπωμένους νομικούς κανόνες τους (όρους χρήσης) όσο και τους εφαρμοσμένους κανόνες τους (κώδικα) για να αυτορρυθμίσουν την εξουσία τους και να ρυθμίσουν τη συμπεριφορά των χρηστών, καθιστώντας το νομικό πεδίο πιο τεχνο-κεντρικό και λιγότερο εξαρτώμενο από τους παραδοσιακούς νομικούς κανόνες.

5.3. Η συνταγματοποίηση της μαζικής επιτήρησης μέσα από τις δικαστικές απαγορεύσεις

Μελετώντας τη νομολογία που αναπτύχθηκε τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, μπορούμε να κατανοήσουμε καλύτερα τη συμβολή των δικαστικών αρχών στη συζήτηση για τα όρια της παρακολούθησης και τις συνταγματικές επιπτώσεις. Μέσα από την ανάλυσή μας θα αναδείξουμε ότι η συνταγματοποίηση της μαζικής επιτήρησης στην ΕΕ περιλαμβάνει την ενσωμάτωση των αρχών της αναλογικότητας και της απόλυτης αναγκαιότητας στη νομοθεσία, καθώς και την εισαγωγή εγγυήσεων όπως η προηγούμενη έγκριση και ο έλεγχος από ανεξάρτητες αρχές. Αυτή η διαδικασία δεν αποσκοπεί στην απόλυτη απαγόρευση της μαζικής παρακολούθησης, αλλά στην προσαρμογή της στα συνταγματικά πλαίσια, διασφαλίζοντας την προστασία των θεμελιωδών δικαιωμάτων. Άλλωστε, κατά την άποψή μας, η συνταγματική κωδικοποίηση μιας απόλυτης απαγόρευσης θα αποτύγχανε τελικά να επιτύχει ισορροπία μεταξύ της προστασίας της κρατικής ασφάλειας και της συμπίεσης των θεμελιωδών δικαιωμάτων.

Οι νομοθετικές συζητήσεις στην ΕΕ, καθώς και οι ανησυχίες που εξέφρασαν τόσο η Ομάδα Εργασίας του Άρθρου 29 και διάφορες ΜΚΟ (Privacy International, European Digital Rights (EDRi), Amnesty International, Human Rights Watch, Reporters Without Borders) είχαν σημαντική επίδραση στη συνταγματική συζήτηση σχετικά με τα συστήματα διατήρησης δεδομένων στην ΕΕ. Αν και σε εθνικό επίπεδο, οι αποφάσεις των δικαστηρίων έθιγαν ακόμη

και την ίδια τη νομιμότητα της Οδηγίας ePrivacy [33], καμία δεν έφτασε στο σημείο να την ακυρώσει. Ζητήματα νομιμότητας τόσο της Οδηγίας ePrivacy όσο και της DRD τέθηκαν για πρώτη φορά σε ευρωπαϊκό επίπεδο στην απόφαση Digital Rights Ireland η οποία ήταν και το έναυσμα για τη δημιουργία μιας μακράς και σύνθετης ιστορίας νομοθετικών, δικαστικών και πολιτικών αντιπαραθέσεων γύρω από την υποχρεωτική διατήρηση δεδομένων επικοινωνίας στην ΕΕ.

Η εμβληματική αυτή απόφαση έθεσε τις ακόλουθες αρχές για τα συστήματα μαζικής επιτήρησης οι οποίες εν τέλει οδήγησαν στην ακύρωση της DRD. Πρώτον, το ΔΕΕ έκρινε ότι η γενικευμένη και αδιάκριτη διατήρηση μεταδεδομένων, ανεξάρτητα από την ενδεχόμενη μετέπειτα πρόσβαση σε αυτά από τις κρατικές αρχές, θεωρείται από μόνη της παραβίαση της ιδιωτικής ζωής των χρηστών. Επίσης, το Δικαστήριο αναγνώρισε ότι τα δεδομένα επικοινωνιών, ανεξάρτητα από το περιεχόμενο της επικοινωνίας, μπορούν να οδηγήσουν σε ακριβή συμπεράσματα για τις συνήθειες των χρηστών, την καθημερινή τους ζωή, τον τόπο κατοικίας, τις κινήσεις, τις δραστηριότητες, τις σχέσεις και τα κοινωνικά τους περιβάλλοντα. Αυτό μπορεί να δημιουργήσει στους ανθρώπους «την αίσθηση ότι οι ιδιωτικές τους ζωές βρίσκονται υπό καθεστώς διαρκούς παρακολούθησης» (παράγραφος 37). Δεύτερον, υπογράμμισε ότι η μαζική και γενικευμένη διατήρηση, που καλύπτει όλες τις υπηρεσίες ηλεκτρονικών επικοινωνιών και το σύνολο των χρηστών και των δεδομένων επικοινωνίας τους, δεν μπορεί να θεωρηθεί ως αναγκαίο μέτρο.

Τρίτον, το ΔΕΕ τόνισε ότι μια μορφή νόμιμης και αναλογικής διατήρησης μπορεί να υφίσταται μόνο σε ένα «στοχευμένο σύστημα». Αυτό σημαίνει ότι η διατήρηση πρέπει να περιορίζεται σε άτομα για τα οποία υπάρχουν αποδείξεις ότι μπορεί να έχουν σχέση, έστω και έμμεσα, με σοβαρά εγκλήματα (παράγραφος 58), ή να είναι περιορισμένη σε μια

[33] Η πρώτη διάταξη που υιοθετήθηκε για τη διατήρηση δεδομένων είναι το Άρθρο 15 της Οδηγίας ePrivacy (2002/58) το οποίο εισάγει μια σημαντική εξαίρεση από τον γενικό κανόνα διαγραφής ή ανωνυμοποίησης των μεταδεδομένων. Αυτό σημαίνει ότι τα κράτη μέλη μπορούν να θεσπίσουν νόμους που επιτρέπουν την προσωρινή διατήρηση δεδομένων επικοινωνίας, εάν θεωρηθεί ότι αυτό είναι απαραίτητο, κατάλληλο και αναλογικό μέτρο για την προστασία της εθνικής ασφάλειας, της άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, ανίχνευση και δίωξη εγκλημάτων ή την αποτροπή μη εξουσιοδοτημένης χρήσης των συστημάτων ηλεκτρονικών επικοινωνιών. Η Οδηγία για τη Διατήρηση Δεδομένων (DRD) συμπλήρωσε τις ασαφείς διατάξεις του Άρθρου 15 της Οδηγίας 2002/58, ζητώντας από τα κράτη μέλη να θεσπίσουν νόμους που απαιτούν από τους παρόχους υπηρεσιών να διατηρούν εκτεταμένα δεδομένα επικοινωνίας για έξι μήνες έως δύο χρόνια.

συγκεκριμένη γεωγραφική περιοχή ή χρονικό διάστημα και να έχει μοναδικό σκοπό την πρόληψη ή καταπολέμηση σοβαρών εγκλημάτων.

Μετά την ακύρωση της DRD, πολλά προκαταρκτικά ερωτήματα υποβλήθηκαν από τα σουηδικά, βρετανικά και ισπανικά δικαστήρια, ζητώντας διευκρινίσεις σχετικά με την ερμηνεία του Άρθρου 15 της Οδηγίας ePrivacy. Το ΔΕΕ στις υποθέσεις Tele2 (2016) και Ministerio Fiscal (2018), επανέλαβε τις αρχές που είχε ήδη διατυπώσει στην υπόθεση Digital Rights Ireland, δίδοντας σαφείς οδηγίες στα εθνικά δικαστήρια για την ενσωμάτωση βασικών συνταγματικών αξιών, όπως το κράτος δικαίου, τις εγγυήσεις της δίκαιης δίκης και το τεκμήριο αθωότητας, στους εθνικούς νομικούς κανόνες για τη διατήρηση δεδομένων. Τέλος, διευκρίνισε ότι το άρθρο 15 πρέπει να ερμηνεύεται έχοντας ως νομική βάση τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Παρά τις σημαντικές συνταγματικές αλλαγές στον τομέα της παρακολούθησης και αποθήκευσης δεδομένων από τους τηλεπικοινωνιακούς παρόχους που προωθήθηκαν από την προαναφερόμενη νομολογία του ΔΕΕ, τα κράτη-μέλη αντέδρασαν αρνητικά υιοθετώντας μια αμυντική στάση απέναντι στο μοντέλο της στοχευμένης παρακολούθησης αρνούμενα να εγκαταλείψουν τα γενικευμένα καθεστώτα που θεωρούνταν αναντικατάστατα εργαλεία στην καταπολέμηση των εθνικών και διακρατικών απειλών ασφαλείας. Μάλιστα, αντιπρότειναν ως λειτουργικότερο μοντέλο, αυτό του «καθεστώτος περιορισμένης διατήρησης δεδομένων». Η έντονη κριτική που εκφράστηκε από τις κυβερνητικές αρχές οδήγησε τα εθνικά δικαστήρια να απευθυνθούν εκ νέου στο ΔΕΕ ζητώντας «να αποσαφηνίσει, να βελτιώσει ή ακόμη και να επανεξετάσει διάφορες πτυχές της νομολογίας του» (Case C-520/18, La Quadrature du Net et al. v. Premier Ministre et al. (Jan. 15, 2020). Το ΔΕΕ στις υποθέσεις La Quadrature du Net, Συνεκδικασθείσες υποθέσεις C-511/18, C-512/18 and C-520/18 επιβεβαίωσε εκ νέου τη σημασία εφαρμογής των αρχών του κράτους δικαίου όταν οι αρχές επιβολής του νόμου διατάσσουν τη μαζική παρακολούθηση.

Μια απόδειξη της συνεχιζόμενης και εξελισσόμενης φύσης της διαδικασίας συνταγματοποίησης στον τομέα της παρακολούθησης των δεδομένων επικοινωνίας, υπήρξε η στάση του ΔΕΕ απέναντι στα ζητήματα εθνικής ασφάλειας. Στις ίδιες υποθέσεις, το Δικαστήριο έκρινε ότι η προστασία της εθνικής ασφάλειας από σοβαρές απειλές, όπως η τρομοκρατία ή άλλες δραστηριότητες που μπορούν να αποσταθεροποιήσουν ένα κράτος και τις δομές του παρέχει στα κράτη μέλη μεγαλύτερο περιθώριο ελιγμών και δικαιολογεί τον

περιορισμό των θεμελιωδών δικαιωμάτων. Ωστόσο, το Δικαστήριο έσπευσε να καθορίσει συνταγματικές εγγυήσεις και όρια προχωρώντας ένα βήμα παρακάτω την προσπάθεια συνταγματοποίησης και απαιτώντας από τους εθνικούς νομοθέτες να καθορίσουν: (i) ένα σαφές νομοθετικό πλαίσιο που καθορίζει τους όρους για την υιοθέτηση συστημάτων μαζικής αποθήκευσης δεδομένων, (ii) έναν καθορισμένο χρονικό περιορισμό στη χρήση αυτού του μέσου, (iii) αυστηρές εγγυήσεις ασφάλειας δεδομένων για την προστασία από τον κίνδυνο καταχρήσεων και (iv) εποπτεία από δικαστικά σώματα ή ανεξάρτητες διοικητικές αρχές (La Quadrature du Net, Συνεκδικασθείσες υποθέσεις C-511/18, C-512/18 and C-520/18 , παρ. 138).

Ειδικά για το θέμα των πρόσθετων εγγυήσεων, η απόφαση του ΔΕΕ στην υπόθεση H.K. (2021) δημιούργησε δικαστικό προηγούμενο. Ενώ στις αποφάσεις Privacy International και La Quadrature du Net, το Δικαστήριο εξέτασε τη νομιμότητα της επιβολής γενικής υποχρέωσης διατήρησης δεδομένων για λόγους εθνικής ασφάλειας, στην υπόθεση H.K., διευκρίνισε τις προϋποθέσεις για στοχευμένη διατήρηση δεδομένων και ανέλυσε τις επιπτώσεις της παραβίασης θεμελιωδών δικαιωμάτων στο πλαίσιο της ποινικής διαδικασίας. Συγκεκριμένα, το ΔΕΕ αποφάνθηκε ότι ο έλεγχος που ασκεί ο εισαγγελέας στα μέτρα επιτήρησης μεταδεδομένων δεν διαθέτει την απαραίτητη ανεξαρτησία καθώς ο εισαγγελέας είναι μέρος της ποινικής διαδικασίας και όχι ανεξάρτητος διαιτητής και, επομένως, δεν μπορεί να αντικαταστήσει την εποπτεία που θα έπρεπε να γίνεται από ένα δικαστήριο. Επιπλέον, το Δικαστήριο σημείωσε ότι αυτή η έλλειψη ανεξάρτητου ελέγχου δεν μπορεί να διορθωθεί εκ των υστέρων με εποπτεία κατά τη διάρκεια της δικαστικής διαδικασίας καθώς δεν θα μπορούσε να διασφαλίσει ότι η πρόσβαση στα δεδομένα περιορίζεται μόνο στο απολύτως αναγκαίο.

Ένας άλλος λόγος που η απόφαση στην υπόθεση H.K. είναι σημαντική είναι γιατί έθεσε προηγούμενο σχετικά με το πώς πρέπει να αντιμετωπίζονται τα αποδεικτικά στοιχεία σε ποινικές υποθέσεις όταν αυτά αποκτώνται με τρόπο που δεν τηρεί τις νόμιμες διαδικασίες. Το Δικαστήριο επισήμανε ότι, επειδή το δίκαιο της ΕΕ δεν έχει συγκεκριμένους κανόνες για το πώς να αντιμετωπίζονται τα αποδεικτικά στοιχεία που προέρχονται από γενικευμένη και αδιάκριτη διατήρηση δεδομένων, κάθε χώρα της ΕΕ μπορεί να ορίσει τους δικούς της κανόνες. Ωστόσο, αυτοί οι κανόνες πρέπει να διασφαλίζουν ότι τα αποδεικτικά

στοιχεία που έχουν συλλεχθεί παράνομα δεν προκαλούν αδικαιολόγητη βλάβη σε κάποιον κατηγορούμενο.

Το Δικαστήριο τόνισε ότι ένας τρόπος για να επιτευχθεί αυτός ο στόχος είναι να μην επιτρέπεται η χρήση τέτοιων παράνομων αποδεικτικών στοιχείων στα δικαστήρια, ή να λαμβάνεται υπόψη η βαρύτητα αυτών των ελαττωματικών στοιχείων κατά τη διάρκεια της δίκης και της απόφασης. Είναι επίσης σημαντικό, σύμφωνα με το Δικαστήριο, ότι τα εθνικά ποινικά δικαστήρια δεν πρέπει να λαμβάνουν υπόψη αποδεικτικά στοιχεία που έχουν αποκτηθεί μέσω γενικής και αδιάκριτης διατήρησης δεδομένων ή μέσω παράνομης πρόσβασης σε αυτά τα δεδομένα, αν δεν δίνεται στους υπόπτους η δυνατότητα να αμφισβητήσουν τη νομιμότητα αυτών των αποδεικτικών στοιχείων. Με απλά λόγια, το δικαστήριο πρέπει να εξασφαλίσει ότι οι κατηγορούμενοι έχουν το δικαίωμα σε δίκαιη δίκη και ότι δεν χρησιμοποιούνται εναντίον τους αποδεικτικά στοιχεία που έχουν αποκτηθεί παράνομα.

Εκτός συνόρων ΕΕ (υποθέσεις Schrems I και II), το ΔΕΕ αντιμετώπισε την πρόκληση να διασφαλίσει ότι οι συνταγματικές αρχές και οι εγγυήσεις που προστατεύουν τα θεμελιώδη δικαιώματα των πολιτών εντός της ΕΕ, ισχύουν και εκτός αυτής ελέγχοντας εμμέσως τα αμερικανικά συστήματα μαζικής παρακολούθησης όπως το Prism και το Upstream και ακυρώνοντας δύο φορές τις αποφάσεις σχετικά με τις μεταφορές δεδομένων στις ΗΠΑ. Παρόμοια στάση επέδειξε και στη Γνώμη 1/15 [34] ακυρώνοντας το σχέδιο συμφωνίας PNR με τον Καναδά σχετικά με τη διαβίβαση και επεξεργασία δεδομένων PNR επιβατών της ΕΕ στις καναδικές αρχές επιβολής του νόμου και ασφάλειας.

Όπως έγινε αντιληπτό, η πορεία προς τη συνταγματοποίηση των εργαλείων μαζικής παρακολούθησης στην Ευρωπαϊκή Ένωση αποτελεί ένα περίπλοκο και πολυεπίπεδο ζήτημα που αντανακλάται σε διάφορες νομοθετικές και δικαστικές αντιδράσεις των κρατών μελών. Και αυτό αποδεικνύεται από το γεγονός ότι τα κράτη μέλη αντέδρασαν με πολύ

[34] Η Γνώμη 1/15, που εκδόθηκε από το ΔΕΕ στις 26 Ιουλίου 2017, αφορά τη νομιμότητα του σχεδίου συμφωνίας μεταξύ της ΕΕ και του Καναδά σχετικά με τη διαβίβαση και επεξεργασία δεδομένων PNR (Passenger Name Record) των επιβατών της ΕΕ από τις καναδικές αρχές. Η γνωμοδότηση αυτή εκδόθηκε μετά από αίτημα του Ευρωπαϊκού Κοινοβουλίου, το οποίο ζήτησε από το Δικαστήριο να αξιολογήσει αν το σχέδιο συμφωνίας ήταν συμβατό με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, με έμφαση στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων.

διαφορετικούς τρόπους στη συνεχιζόμενη πορεία συνταγματοποίησης που δρομολόγησαν οι δικαστές της ΕΕ, δημιουργώντας ένα κατακερματισμένο τοπίο λύσεων και προσεγγίσεων.

Από τις πιο χαρακτηριστικές περιπτώσεις είναι η ακύρωση της εθνικής νομοθεσίας διατήρησης δεδομένων από το βελγικό Συνταγματικό Δικαστήριο, το οποίο έκρινε ότι η μαζική διατήρηση δεδομένων παραβιάζει τις αρχές της αναλογικότητας. Αντίθετα, η Γαλλία υιοθέτησε μια διαφορετική προσέγγιση, διατηρώντας ένα γενικευμένο σύστημα διατήρησης δεδομένων για λόγους εθνικής ασφάλειας, το οποίο κρίθηκε ότι συμμορφώνεται με τις αρχές της ΕΕ, υπό ορισμένες προϋποθέσεις. Η Ιταλία, αν και αρχικά δεν επηρεάστηκε σημαντικά από τη νομολογία του ΔΕΕ, προχώρησε σε μεταρρυθμίσεις μετά την απόφαση του ΔΕΕ στην υπόθεση H.K. κατά Prokuratuur[35]. Η μεταρρύθμιση εισήγαγε αυστηρότερες εγγυήσεις για την πρόσβαση στα δεδομένα, αλλά διατήρησε το μαζικό και γενικευμένο σύστημα διατήρησης δεδομένων. Στην Πορτογαλία, το Συνταγματικό Δικαστήριο κήρυξε αντισυνταγματικά πολλά άρθρα του νόμου για τα μεταδεδομένα, αναδεικνύοντας την ανάγκη για μια πιο προσεκτική και αναλογική προσέγγιση στην μαζική παρακολούθηση.

Εν κατακλείδι, μπορούμε να υποστηρίξουμε ότι η διαδικασία συνταγματοποίησης που έχει προωθηθεί από τη νομολογία του ΔΕΕ σχετικά με τη διατήρηση δεδομένων προσωπικού χαρακτήρα έχει δημιουργήσει ένα σημαντικό πλαίσιο με αρχές που πρέπει να εφαρμοστεί και σε άλλα μέσα μαζικής παρακολούθησης, όπως αυτά που βασίζονται στην τεχνητή νοημοσύνη. Προφανώς, η ενσωμάτωση αυτών των αρχών στις νομοθετικές διαδικασίες αποτελεί πρόκληση για τους νομοθέτες, καθώς πρέπει να εξισορροπήσουν την ανάγκη για ασφάλεια με την προστασία των θεμελιωδών δικαιωμάτων. Οι νομοθέτες καλούνται να δημιουργήσουν ένα συνεκτικό και σαφές νομικό πλαίσιο που θα προστατεύει τα δικαιώματα των ατόμων, ενώ ταυτόχρονα θα επιτρέπει τη χρήση προηγμένων τεχνολογιών για τη διασφάλιση της δημόσιας ασφάλειας. Η διαδικασία αυτή απαιτεί τη συνεργασία μεταξύ των εθνικών και υπερεθνικών αρχών, καθώς και την ενεργή συμμετοχή

[35] Σύμφωνα με την απόφαση του ΔΕΕ στις 2 Μαρτίου 2021, η πρόσβαση στα προσωπικά δεδομένα από τις αρμόδιες αρχές χωρίς προηγούμενη έγκριση από δικαστική ή άλλη ανεξάρτητη αρχή συνιστά παραβίαση των δικαιωμάτων για σεβασμό της ιδιωτικής ζωής και προστασία των προσωπικών δεδομένων, όπως αυτά προστατεύονται από τα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Επιπλέον, το Δικαστήριο υπογράμμισε τη σημασία της τήρησης της αρχής της αναλογικότητας κατά την πρόσβαση σε προσωπικά δεδομένα.

της κοινωνίας των πολιτών για την εξασφάλιση μιας ισορροπημένης και δίκαιης προσέγγισης.

6. Ο ΚΑΝΟΝΙΣΜΟΣ EPRIVACY ΚΑΙ Η ΣΥΜΒΟΛΗ ΤΟΥ ΣΤΗΝ ΚΑΤΟΧΥΡΩΣΗ ΤΗΣ ΨΗΦΙΑΚΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Υπό το πρίσμα της σταδιακής συνταγματοποίησης της ψηφιακής επικοινωνίας, όπως αναπτύχθηκε παραπάνω και στη σκιά του παράδοξου της ιδιωτικότητας[36], προτάθηκε από την Ευρωπαϊκή Επιτροπή στις 10.1.2017 (Ευρωπαϊκή Επιτροπή, 2017), ο Κανονισμός «για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες» γνωστός ως Κανονισμός ePrivacy. Στόχος της εν λόγω πρότασης ήταν η εναρμόνιση των κανόνων που διέπουν τις ηλεκτρονικές επικοινωνίες στην Ευρωπαϊκή Ένωση και απώτερος σκοπός η ενίσχυση της εμπιστοσύνης των πολιτών στις ψηφιακές υπηρεσίες.

Ως lex specialis, στοχεύει να αντικαταστήσει την προηγούμενη Οδηγία 2002/58 (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο Ε.Ε., 2002) για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και να εξειδικεύσει τον ΓΚΠΔ.

Τα βασικά πεδία του προτεινόμενου κανονισμού είναι η εμπιστευτικότητα των επικοινωνιών, η ηλεκτρονική συγκατάθεση, τα στοιχεία ελέγχου απορρήτου μέσω προγραμμάτων περιήγησης καθώς και η χρήση των cookies τα οποία και θα αναλυθούν στα επόμενα κεφάλαια.

6.1. Βασικά σημεία του Κανονισμού ePR και οι σημαντικότερες διατάξεις του

1. Ο Κανονισμός υπόσχεται να ενισχύσει την προστασία της ιδιωτικότητας των χρηστών στις ηλεκτρονικές επικοινωνίες. Στο περιεχόμενο αυτών περιλαμβάνονται τα δεδομένα κατά τη χρήση των επιγραμμικών υπηρεσιών (π.χ. επικοινωνία μέσω της εφαρμογής WhatsApp και βιντεοκλήσεις με τις παλτφόρμες Zoom και Skype) από τον τελικό χρήστη, που βρίσκεται εντός και εκτός των γεωγραφικών ορίων της ΕΕ, καθώς και των

[36] Το παράδοξο της ιδιωτικότητας αναφέρεται στο χάσμα μεταξύ των προθέσεων των ανθρώπων σχετικά με την πρόσβαση στα δεδομένα τους και τη συμπεριφορά τους στην πράξη. Μελέτες έχουν δείξει ότι παρά τον ισχυρισμό ότι για τους περισσότερους ανθρώπους το δικαίωμα στην ιδιωτική ζωή είναι σημαντικό, οι περισσότεροι άνθρωποι όταν έρχονται αντιμέτωποι με μια παραβίαση της ιδιωτικής τους ζωής, επιλέγουν να μην την αναφέρουν σε κάποιο θεσμικό φορέα (Kokolakis, 2017).

παραγόμενων μεταδεδομένων, όπως είναι η θέση, ο χρόνος και ο αποδέκτης της επικοινωνίας.

2. Ενίσχυση της ασφάλειας και της εμπιστοσύνης των χρηστών στο διαδίκτυο και στις ηλεκτρονικές επικοινωνίες, περιλαμβανομένων των διαδικτυακών εφαρμογών και των IoT συσκευών. Οι εταιρείες θα πρέπει να λαμβάνουν συγκατάθεση από τους χρήστες πριν από τη συλλογή και τη χρήση δεδομένων τους και να προσφέρουν τη δυνατότητα αποδοχής ή απόρριψης των cookies.

3. Η καταπολέμηση των ανεπιθύμητων μηνυμάτων (spam) είναι άλλη μία βασική πτυχή του νέου νομοθετήματος ePR. Σύμφωνα με τους νέους κανόνες, οι εταιρείες θα πρέπει να έχουν τη συγκατάθεση των ατόμων πριν αποστείλουν ηλεκτρονικά διαφημιστικά μηνύματα ή μηνύματα οποιασδήποτε άλλης φύσης. Επιπλέον, οι επιχειρήσεις θα πρέπει να διασφαλίζουν ότι οι αποδέκτες των μηνυμάτων έχουν τη δυνατότητα εύκολης απεγγραφής από τη λίστα αλληλογραφίας τους, ενώ τα μηνύματα πρέπει να περιλαμβάνουν σαφείς οδηγίες για τη διαγραφή από τη λίστα και τον τρόπο με τον οποίο μπορεί να επαληθευθεί η απεγγραφή.

4. Ο Κανονισμός θα περιορίσει τα στοιχεία που μπορούν να συλλέγονται από τους παρόχους επιφυών υπηρεσιών [37] για τη συλλογή πληροφοριών από τους χρήστες. Συγκεκριμένα, θα ενισχύσει τα δικαιώματα των χρηστών όσον αφορά την προστασία της ανωνυμίας τους, συμπεριλαμβανομένου του δικαιώματός τους να ζητήσουν πληροφορίες σχετικά με τη συλλογή και τη χρήση των δεδομένων τους και να επιλέξουν τις προτιμήσεις τους όσον αφορά τις επικοινωνίες που λαμβάνουν.

5. Ένα άλλο σημαντικό στοιχείο του Κανονισμού είναι ο αυξημένος έλεγχος που θα διαθέτουν οι εποπτικές αρχές. Οι αρχές αυτές θα έχουν τη δυνατότητα να επιβάλλουν πρόστιμα σε εταιρείες που δεν συμμορφώνονται με τους κανόνες της προστασίας δεδομένων και να επιβάλλουν αποτελεσματικές κυρώσεις για τις παραβιάσεις. Επιπλέον, οι εταιρείες θα πρέπει να αναφέρουν στις εποπτικές αρχές οποιαδήποτε παραβίαση έχει συμβεί στα

[37] Σύμφωνα με τους πρώτους ορισμούς, ως επιφυείς υπηρεσίες νοούνται αυτές που μεταδίδονται πάνω από το δίκτυο (over the top services), αποδίδοντας προστιθέμενη αξία στους πελάτες, χωρίς να μετέχει κάποιος φορέας εκμετάλλευσης του δικτύου στον σχεδιασμό, τις πωλήσεις, ή την παροχή αυτών και φυσικά χωρίς την άμεση αποκόμιση κέρδους των παραδοσιακών παρόχων από αυτές (Green and Lancaster, 2006).

συστήματά τους, ενώ οι αρχές θα έχουν το δικαίωμα να προσπελάσουν τα συστήματα αυτά για επιθεώρηση και έλεγχο.

6. Το νέο ePR θα προσπαθήσει να απλοποιήσει τους κανόνες που διέπουν την επεξεργασία προσωπικών δεδομένων στον τομέα των επικοινωνιών και να εναρμονίσει τους κανόνες σε όλη την ΕΕ, προκειμένου να διευκολυνθεί η συμμόρφωση για τις εταιρείες που δραστηριοποιούνται σε πολλά κράτη μέλη. Επίσης, θα διευκολύνει τις εταιρείες να αντιληφθούν τα δικαιώματα και τις υποχρεώσεις τους σε σχέση με την επεξεργασία προσωπικών δεδομένων στον τομέα των επικοινωνιών.

6.2. Γενικός Κανονισμός Προστασίας Δεδομένων και ePR

Ο αναγνώστης της παρούσας εργασίας θα μπορέσει να κατανοήσει καλύτερα το πεδίο ρύθμισης του ePR μέσα από μια σύντομη σύγκριση μεταξύ του ΓΚΠΔ, της προηγούμενης Οδηγίας 2002/58 και του προτεινόμενου Κανονισμού.

1. Ο Κανονισμός καλύπτει κυρίως τις ηλεκτρονικές τηλεπικοινωνίες ρυθμίζοντας τη χρήση των δεδομένων και των μεταδεδομένων των ηλεκτρονικών επικοινωνιών των χρηστών του διαδικτύου σε αντίθεση με την παλαιότερη Οδηγία η οποία εστίαζε κυρίως στις παραδοσιακές τηλεπικοινωνίες όπως οι φωνητικές κλήσεις, οι ανταλλαγές ηλεκτρονικών μηνυμάτων (text-messaging) και οι βιντεοκλήσεις (video chats).

2. Επικεντρώνεται κυρίως στην εμπιστευτικότητα των επικοινωνιών στις οποίες περιλαμβάνονται τόσο τα προσωπικά όσο και τα μη-προσωπικά δεδομένα καθώς και τα δεδομένα σχετικά με νομικά πρόσωπα και όχι μόνο φυσικά, όπως συμβαίνει στην περίπτωση της Οδηγίας. Σύμφωνα με τον "cookies law"[38] της Οδηγίας, ήταν απαραίτητη η εξασφάλιση της προηγούμενης συναινετικής συγκατάθεσης προκειμένου μια εταιρεία να μπορεί να παρακολουθεί έναν χρήστη με cookies[39]. Ο Κανονισμός υπόσχεται απλούστευση

[38] Αναφέρεται στην υποχρέωση των ιστοσελίδων να ενημερώνουν τους χρήστες για τη χρήση των cookies και να εξασφαλίζουν τη συγκατάθεσή τους πριν προχωρήσουν στην αποθήκευση ή ανάκτηση πληροφοριών από τον υπολογιστή ή τη συσκευή τους

[39] Σύμφωνα με την Αρχή Προστασίας Δεδομένων, ως cookies νοούνται τα μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστοτόπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτόν. Ο ιστοτόπος ανακτά τις εν λόγω πληροφορίες(π.χ. αναζητήσεις) σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες.

της εν λόγω διαδικασίας, αλλά και νέους τρόπους για την προστασία από την ανεπιθύμητη παρακολούθηση των ηλεκτρονικών επικοινωνιών.

3. Η νομιμοποιητική βάση των δύο κανονιστικών κειμένων—ΓΚΠΔ και Κανονισμού—είναι διαφορετική αντιμετωπίζοντας την ιδιωτικότητα από άλλη οπτική γωνία. Ο ΓΚΠΔ βασίζεται στο Άρθρο 8 του Ευρωπαϊκού χάρτη για τα Θεμελιώδη Δικαιώματα το οποίο για τους νομοθέτες του ΓΚΠΔ σκοπεύει στον σεβασμό της προσωπικής και οικογενειακής ζωής των χρηστών. Η βάση για τον ePR είναι το Άρθρο 16 και το Άρθρο 114 της Συνθήκης για την Λειτουργία της ΕΕ. Ωστόσο, περιλαμβάνει και μέρος του Άρθρου 7 του Κεφαλαίου για τα Θεμελιώδη Δικαιώματα (Τσίτσιρας, 2018).

6.3. Η επίδραση του ePR στον ψηφιακό συνταγματισμό

Περισσότερο από δεκαπέντε χρόνια μετά την έκδοση της Οδηγίας 2006/24 σχετικά με τη διατήρηση δεδομένων και επτά χρόνια μετά την ακύρωσή της ως ασυμβίβαστη με το δίκαιο της ΕΕ, το θέμα της γενικής υποχρέωσης διατήρησης δεδομένων και η συμβατότητά της με τα ανθρώπινα δικαιώματα παραμένει ανοιχτό για συζήτηση και αντιπαράθεση.

Η μακροχρόνια αυτή διαμάχη αποτυπώνεται και στις ατέρμονες συζητήσεις για την τροποποίηση της Οδηγίας 2002/58 και την υιοθέτηση του νέου Κανονισμού ePR. Παρόλο που η προαναφερόμενη Οδηγία είναι 20 ετών –γεγονός που, στην πράξη, δημιουργεί πρόσθετη δυσκολία[40] στην ανάλυση του νομικού πλαισίου της ΕΕ για τη διατήρηση δεδομένων, οι εργασίες για έναν νέο κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (EPR) που θα αντικαταστήσει την ePD απέκτησαν δυναμική μόλις το 2016, αφού συμφωνήθηκε το περιεχόμενο του ΓΚΠΔ και εν τέλει τον Φεβρουάριο του 2021 επιτεύχθηκε συναίνεση στο Συμβούλιο σχετικά με το σχέδιο κανονισμού.

Στη συνέχεια, θα παρατεθούν οι αλλαγές που προτάθηκαν στο σχέδιο κανονισμού ePR και συμφωνήθηκαν από το Συμβούλιο με κύριο στόχο να αναδείξουμε α) την αντίσταση που προβάλλουν ακόμη τα κράτη στην ευρωπαϊκή προσπάθεια κατοχύρωσης της ψηφιακής ιδιωτικότητας που προέρχεται από τη συνεργασία των δικαστηρίων και της κοινωνίας των πολιτών και β) κατά πόσον η πρόταση του Συμβουλίου μπορεί όντως να επηρεάσει

[40] Η Οδηγία δεν έχει λάβει υπόψη τις αλλαγές που προέκυψαν από τη μεταρρύθμιση της Λισαβόνας και, ως εκ τούτου, δεν έχει προσαρμοστεί στο σημερινό ρυθμιστικό μοντέλο της αγοράς τηλεπικοινωνιών.

σημαντικά το εύρος εφαρμογής του δικαίου της ΕΕ και τη συνάφεια της αξιολόγησης των εθνικών νόμων για τη διατήρηση δεδομένων από το Δικαστήριο (Rojszczak, 2021).

α) Ένα στοιχείο του ePR είναι οι συγκεκριμένες προϋποθέσεις για τη θέσπιση εθνικών νόμων περί διατήρησης δεδομένων. Η διατήρηση δεδομένων, ως μέτρο που επηρεάζει το δικαίωμα στην ιδιωτική ζωή, συνιστά εξαίρεση από το τηλεπικοινωνιακό απόρρητο. Στο σχέδιο της Επιτροπής του 2017, αυτή η πτυχή του κανονισμού δεν διαφοροποιήθηκε ιδιαίτερα σε σχέση με το κείμενο της Οδηγίας 2002/58. Η Επιτροπή, στην αιτιολογική έκθεση του σχεδίου, υπογράμμισε ότι η προτεινόμενη μορφή του άρθρου 11 του ePR βασίζεται στο άρθρο 15 της ePD και, ως εκ τούτου, δημιουργεί ένα γενικό νομικό πλαίσιο για τη θέσπιση εθνικών κανόνων διατήρησης δεδομένων. Έτσι, το σχέδιο της Επιτροπής αναπαρήγαγε το ρυθμιστικό μοντέλο της Οδηγίας και προέβλεπε ότι οι εθνικοί κανόνες διατήρησης δεδομένων θα μπορούσαν να θεσπίζονται υπό την προϋπόθεση ότι θα ήταν σύμφωνοι με το δίκαιο της ΕΕ και λαμβάνοντας υπόψη τη νομολογία του ΔΕΕ. Συνεπώς, το νομικό πλαίσιο για τη διατήρηση δεδομένων που περιέχεται στο σχέδιο του νέου κανονισμού της Επιτροπής ήταν σχεδόν ταυτόσημο με το ισχύον βάσει της Οδηγίας 2002/58.

Βέβαια, αξίζει να σημειωθεί ότι, ήδη σε αυτό το αρχικό στάδιο των νομοθετικών εργασιών, το σχέδιο της Επιτροπής αναφερόταν στο άρθρο 23 παράγραφος 1 του ΓΚΠΔ για τον καθορισμό γενικών στόχων ασφαλείας που δικαιολογούν την εισαγωγή περιορισμών στα δικαιώματα και τις υποχρεώσεις των υπηρεσιών ηλεκτρονικών επικοινωνιών. Οι περιορισμοί αυτοί θα μπορούσαν να επιβληθούν στον τομέα της καταπολέμησης του εγκλήματος (άρθρο 23 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ), της επιδίωξης στόχων εθνικής ασφάλειας (άρθρο 23 παράγραφος 1 στοιχείο α) του ΓΚΠΔ) και της άμυνας (άρθρο 23 παράγραφος 1 στοιχείο β) του ΓΚΠΔ).

Κατά την αρχική συζήτηση στο Συμβούλιο, κάποια κράτη μέλη εξέφρασαν ανησυχίες ότι οι προτεινόμενοι κανόνες διατήρησης δεδομένων ήταν υπερβολικά περιοριστικοί. Αναφέρθηκε συγκεκριμένα ότι το νέο σχέδιο κανονισμού επαναλάμβανε ασαφείς διατάξεις της τότε ισχύουσας Οδηγίας, ειδικά όσον αφορά την ερμηνεία της ρήτρας παρέκκλισης που περιλαμβανόταν στο άρθρο 11 του ePR. Η ρήτρα αυτή επέτρεπε τη θέσπιση κανόνων διατήρησης δεδομένων για λόγους εθνικής ασφάλειας, παρόλο που το άρθρο 2 του ePR εξαιρούσε τους λόγους εθνικής ασφάλειας από το πεδίο εφαρμογής του κανονισμού. Επιπλέον, τονίστηκε ότι ο Κανονισμός, ως ειδικός νόμος σε σχέση με τον ΓΚΠΔ, θα έπρεπε

να ρυθμίζει πλήρως την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Συνεπώς, κατά την άποψη των κρατών μελών, το σχέδιο έπρεπε να συμπληρωθεί με μια επίσημη βάση για την επεξεργασία των διατηρούμενων δεδομένων, αντίστοιχη με τους νομικούς λόγους επεξεργασίας προσωπικών δεδομένων που προβλέπονται στο άρθρο 6 του ΓΚΠΔ. Επισημάνθηκε, επίσης, ότι η γενικότητα των προτεινόμενων κανόνων διατήρησης δεδομένων θα μπορούσε να οδηγήσει σε πιο περιοριστικούς κανονισμούς σε σύγκριση με τους ισχύοντες, ενώ η πλειοψηφία των κρατών μελών ήλπιζε σε μεγαλύτερη ευελιξία στη ρύθμιση αυτού του θέματος στο εσωτερικό δίκαιο.

Η συζήτηση αυτή οδήγησε στην πρώτη σειρά τροποποιήσεων του σχεδίου κανονισμού, οι οποίες διευκρίνιζαν ότι οι πάροχοι υπηρεσιών μπορούν να επεξεργάζονται τα απαραίτητα μεταδεδομένα για να συμμορφώνονται με τους εθνικούς κανονισμούς διατήρησης. Επιπλέον, επεξηγήθηκε ότι το δίκαιο της ΕΕ ή των κρατών μελών μπορεί να προβλέπει μεγαλύτερη περίοδο διατήρησης μεταδεδομένων από αυτή που προβλέπεται από τους γενικούς κανόνες. Το Συμβούλιο αποφάσισε, επίσης, να τροποποιήσει τη ρήτρα παρέκκλισης του άρθρου 11, αφαιρώντας την αναφορά στην εθνική ασφάλεια και άμυνα από τους λόγους που δικαιολογούν τη θέσπιση μέτρων διατήρησης δεδομένων. Στόχος ήταν να διασφαλιστεί ότι τα κριτήρια νομιμότητας του άρθρου 11 δεν θα χρησιμοποιούνται ως βάση για την αξιολόγηση των εθνικών νόμων διατήρησης δεδομένων στον τομέα της κρατικής ασφάλειας. Παρόλο που κάποιες από τις αλλαγές αυτές θα μπορούσαν να αμφισβητηθούν ως προς τη συμβατότητά τους με τη νομολογία του ΔΕΕ εκείνη την περίοδο, αναμενόταν ότι το Δικαστήριο θα αποσαφήνιζε τις προϋποθέσεις για τη στοχευμένη διατήρηση σε μελλοντικές αποφάσεις, επιτρέποντας έτσι στους κανόνες που εγκρίθηκαν με τον κανονισμό να αποτελέσουν τη βάση για πιο εκτεταμένες διατάξεις διατήρησης.

Οι αποφάσεις του ΔΕΕ στις υποθέσεις Privacy International και LQN οι οποίες οδήγησαν στη μείωση και όχι στη χαλάρωση (όπως αναμενόταν) των εθνικών κανόνων διατήρησης δεδομένων και ο φόβος ότι το προτεινόμενο κείμενο θα έρθει σε αντίφαση με απαιτήσεις που απορρέουν από τον Χάρτη των Θεμελιωδών Δικαιωμάτων οδήγησαν τη γερμανική Προεδρία στην απόφαση να παραπέμψει το κείμενο του κανονισμού για περαιτέρω διαβούλευση, διαγράφοντας τις αλλαγές που είχαν εισαχθεί προηγουμένως (ιδίως το άρθρο 6 παράγραφος 1 στοιχείο δ) και το άρθρο 7 παράγραφος 4) και εμμένοντας στο γενικό περιεχόμενο του άρθρου 11 - όπως είχε αρχικά προτείνει η Επιτροπή.

Οι αντιδράσεις από τα κράτη μέλη και δη της Γαλλίας η οποία απείλησε ακόμη και με απόρριψη του σχεδίου Κανονισμού εάν δε γινόταν δεκτό το αίτημά της για πλήρη αποκλεισμό της εφαρμογής του κανονισμού για ζητήματα εθνικής ασφάλειας, οδήγησαν σε νέο γύρο συζητήσεων. Εν τέλει, το κείμενο που συμφωνήθηκε από το Συμβούλιο όχι μόνο επανέφερε αναλυτικές διατάξεις για τους κανόνες διατήρησης δεδομένων, όπως το άρθρο 6, παράγραφος 1, στοιχείο δ) και το άρθρο 7, παράγραφος 4, αλλά έκανε και μια σημαντική αλλαγή. Στο πεδίο εφαρμογής του κανονισμού (άρθρο 2 παρ.2), διευρύνθηκε η εξαίρεση για δραστηριότητες που δεν καλύπτονται από το δίκαιο της ΕΕ.

Η νέα διατύπωση δηλώνει ότι ο Κανονισμός δεν εφαρμόζεται σε μέτρα, δραστηριότητες επεξεργασίας και πράξεις που αφορούν την εθνική ασφάλεια και άμυνα. Αυτή η αλλαγή στοχεύει να εξαιρέσει τις διατάξεις για τη διατήρηση δεδομένων στον τομέα της εθνικής ασφάλειας από το πεδίο εφαρμογής του κανονισμού και είναι προφανές ότι με αυτήν την τροποποίηση γίνεται προσπάθεια επιρροής της νομολογίας του Δικαστηρίου. Η εξαίρεση του τομέα της εθνικής ασφάλειας από τις διατάξεις για τη διατήρηση δεδομένων καθιστά άνευ αντικειμένου την ερμηνεία του ΔΕΕ στις υποθέσεις Privacy International και La Quadrature du Net, μια απόφαση- ορόσημο που εξετάζει τη συμβατότητα των κανονιστικών πλαισίων με τον Χάρτη των Θεμελιωδών Δικαιωμάτων - ο οποίος, μετά τη μεταρρύθμιση της Λισαβόνας, έχει καταστεί μέρος του πρωτογενούς δικαίου της ΕΕ.

Κάτι που θα πρέπει να ληφθεί υπόψη, ωστόσο, στο σημείο αυτό είναι ότι ο ePR ως lex specialis θα εφαρμοστεί στον τομέα της προστασίας της ιδιωτικής ζωής των χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών. Συνεπώς, η αξιολόγηση των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων στον τομέα της εθνικής ασφάλειας θα εξακολουθήσει να γίνεται σύμφωνα με τις διατάξεις του γενικού νομικού πλαισίου, δηλαδή του ΓΚΠΔ. Αυτό συμβαίνει επειδή η διατήρηση τηλεπικοινωνιακών δεδομένων θεωρείται επεξεργασία δεδομένων και οι τηλεπικοινωνιακοί πάροχοι που την πραγματοποιούν καλύπτονται από τον ΓΚΠΔ. Έτσι, αν ο Κανονισμός ePR εγκριθεί όπως έχει προταθεί από το Συμβούλιο, το Δικαστήριο θα κρίνει την συμβατότητα των κανόνων διατήρησης δεδομένων με το άρθρο 23 του ΓΚΠΔ αντί για το άρθρο 11 του ePR.

Ένα άλλο σημείο που θα πρέπει να σχολιασθεί είναι ότι το σχέδιο του Συμβουλίου αναφέρει ότι η εξαίρεση θα πρέπει να καλύπτει όλα τα «μέτρα, τις δραστηριότητες επεξεργασίας και τις πράξεις που αφορούν την εθνική ασφάλεια και άμυνα, ανεξάρτητα

από το ποιος εκτελεί αυτές τις δραστηριότητες». Ωστόσο, το Δικαστήριο στην υπόθεση Privacy International υπογράμμισε ότι οι δραστηριότητες διατήρησης δεδομένων από ιδιωτικούς φορείς, όπως είναι οι τηλεπικοινωνιακοί πάροχοι, δεν εξυπηρετούν λόγους εθνικής ασφάλειας.

Ακόμη και εάν δεχθούμε την προσέγγιση ότι η διατήρηση δεδομένων από τους ιδιωτικούς φορείς αποτελεί μέρος των δραστηριοτήτων εθνικής ασφάλειας ενός κράτους που εξαιρούνται από το δίκαιο της ΕΕ, το Δικαστήριο έχει διατυπώσει παγίως τη θέση ότι η επίκληση της ρήτρας δημόσιας ασφάλειας δεν αποκλείει τη δικαστική αναθεώρηση της εγκυρότητας αυτής της εξαίρεσης και ότι «αν και εναπόκειται στα κράτη μέλη να λάβουν τα κατάλληλα μέτρα για να εξασφαλίσουν την εσωτερική και εξωτερική τους ασφάλεια, το γεγονός και μόνο ότι μια απόφαση αφορά την κρατική ασφάλεια δεν μπορεί να οδηγήσει στην ανυπαρξία εφαρμογής του δικαίου της Ευρωπαϊκής Ένωσης» (ΔΕΕ Υπόθεση C-300/11,παρ. 38).

Η έναρξη ισχύος του ePR, όπως έχει προταθεί από το Συμβούλιο, θα μπορούσε να θεωρηθεί ότι αναστέλλει την άσκηση των αρμοδιοτήτων της ΕΕ και, ως εκ τούτου, σύμφωνα με το άρθρο 2 παράγραφος 2 της ΣΛΕΕ, να επιτρέψει στα κράτη μέλη να ρυθμίζουν ανεξάρτητα τους κανόνες διατήρησης δεδομένων στον τομέα της εθνικής ασφάλειας. Ωστόσο, ακόμη και αν αυτή η άποψη γίνει αποδεκτή, η δυνατότητα των κρατών μελών να θεσπίζουν κανονισμούς σε εθνικό επίπεδο δεν συνεπάγεται πλήρη ελευθερία στον καθορισμό τους καθώς τόσο τα θεμελιώδη δικαιώματα που περιορίζονται λόγω της θέσπισης της υποχρέωσης διατήρησης δεδομένων (όπως το δικαίωμα στην ιδιωτική ζωή και το δικαίωμα στην προστασία προσωπικών δεδομένων) όσο και οι προϋποθέσεις για νόμιμη παρέμβαση σε αυτά τα δικαιώματα (οι αρχές της αναλογικότητας και της αναγκαιότητας) πηγάζουν άμεσα από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

7. Ο ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ Η ΕΠΙΠΤΩΣΗ ΤΟΥ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΨΗΦΙΑΚΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

7.1. Περιεχόμενο και ορισμοί

Ο Κανονισμός για την ΤΝ [41] παρουσιάζεται από την Επιτροπή ως «μια ισορροπημένη και αναλογική οριζόντια ρυθμιστική προσέγγιση για την ΤΝ που περιορίζεται στις ελάχιστες αναγκαίες απαιτήσεις για την αντιμετώπιση των κινδύνων και προβλημάτων που συνδέονται με την ΤΝ, χωρίς να περιορίζεται ή να παρεμποδίζεται αδικαιολόγητα η τεχνολογική ανάπτυξη ή να αυξάνεται δυσανάλογα το κόστος διάθεσης λύσεων ΤΝ στην αγορά» (Ευρωπαϊκή Επιτροπή 2021, σελ.3).

Η αιτιολογική έκθεση του σχεδίου νόμου επικεντρώνεται σε ένα ρυθμιστικό πλαίσιο που βασίζεται στην εκτίμηση κινδύνου, διαχωρίζοντας τα συστήματα ΤΝ σε τρεις κατηγορίες κινδύνου: απαράδεκτο, υψηλό και χαμηλό ή ελάχιστο κίνδυνο[42]. Σύμφωνα με την τελική έκδοση του νόμου για την τεχνητή νοημοσύνη (ΤΝ), τα συστήματα ΤΝ που ενέχουν απαράδεκτους κινδύνους απαγορεύονται εντελώς, χωρίς καμία εξαίρεση. Αυτή η κατηγορία περιλαμβάνει συστήματα που θεωρούνται επικίνδυνα για την ανθρώπινη ασφάλεια, τα δικαιώματα ή τις αξίες και επομένως αποκλείονται πλήρως από την αγορά και τη χρήση.

Για τα συστήματα ΤΝ που χαρακτηρίζονται ως υψηλού κινδύνου, ο νόμος απαιτεί την τήρηση μιας σειράς αυστηρών προϋποθέσεων. Πρώτον, πρέπει να εφαρμόζεται ένα σύστημα διαχείρισης κινδύνων που καλύπτει ολόκληρο τον κύκλο ζωής τους, όπως ορίζεται στο Άρθρο 9. Αυτό το σύστημα είναι κρίσιμο για την ανίχνευση, την εκτίμηση και τον

[41] Ο Κανονισμός Τεχνητής Νοημοσύνης (AI Act) της ΕΕ τέθηκε σε ισχύ τον Αύγουστο 2024. Θα τεθεί σε πλήρη εφαρμογή τον Αύγουστο 2026, εκτός από τις ακόλουθες ειδικές διατάξεις:
-Οι απαγορεύσεις, οι ορισμοί και οι διατάξεις σχετικά με την αλφαβητική γνώση της ΤΝ θα εφαρμοστούν 6 μήνες μετά την έναρξη ισχύος στις 2 Φεβρουαρίου 2025,
-Οι κανόνες για τη διακυβέρνηση και οι υποχρεώσεις για την ΤΝ γενικού σκοπού θα εφαρμοστούν 12 μήνες μετά την έναρξη ισχύος στις 2 Αυγούστου 2025,
-Οι υποχρεώσεις για τα συστήματα ΤΝ υψηλού κινδύνου που κατατάσσονται ως υψηλού κινδύνου επειδή είναι ενσωματωμένα σε ρυθμιζόμενα προϊόντα, τα οποία απαριθμούνται στο παράρτημα ΙΙ (κατάλογος της ενωσιακής νομοθεσίας εναρμόνισης), εφαρμόζονται 36 μήνες μετά την έναρξη ισχύος στις 2 Αυγούστου 2027.

[42] Στο τελικό κείμενο, προστέθηκε μία επιπλέον κατηγορία κινδύνου, αυτή του Ειδικού κίνδυνου διαφάνειας: συστήματα όπως τα διαλογικά ρομπότ πρέπει να ενημερώνουν σαφώς τους χρήστες ότι αλληλεπιδρούν με μηχανή, ενώ ορισμένα περιεχόμενα που παράγονται από τεχνητή νοημοσύνη πρέπει να επισημαίνονται ως τέτοια.

μετριασμό των κινδύνων που μπορεί να παρουσιαστούν κατά τη χρήση τους. Επιπλέον, τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση και τη δοκιμή αυτών των συστημάτων πρέπει να είναι κατάλληλα για τον σκοπό τους, διασφαλίζοντας ότι τα συστήματα λειτουργούν με ακρίβεια και αξιοπιστία, όπως αναφέρεται στο Άρθρο 10.

Η τεχνική τεκμηρίωση που συνοδεύει τα συστήματα αυτά πρέπει να περιγράφει λεπτομερώς τη λειτουργία και τους κινδύνους του συστήματος, όπως προβλέπεται στο Άρθρο 11. Παράλληλα, οι φορείς ανάπτυξης και οι χρήστες πρέπει να ενημερώνονται για τους πιθανούς κινδύνους που σχετίζονται με τη χρήση αυτών των συστημάτων, σύμφωνα με το Άρθρο 13. Ένα άλλο σημαντικό στοιχείο είναι η αυτόματη καταγραφή των συμβάντων του συστήματος (Άρθρο 12), που επιτρέπει την παρακολούθηση και την ανάλυση της λειτουργίας του συστήματος σε πραγματικό χρόνο ή μετά τη χρήση.

Τα συστήματα ΤΝ υψηλού κινδύνου πρέπει επίσης να υπόκεινται σε ανθρώπινη επίβλεψη κατά τη χρήση τους (Άρθρο 14), για να διασφαλίζεται ότι η τελική απόφαση ή δράση μπορεί να ελεγχθεί και να διορθωθεί από έναν άνθρωπο, αν χρειαστεί. Τέλος, πριν από τη διάθεση αυτών των συστημάτων στην αγορά ή την έναρξη της λειτουργίας τους, πρέπει να περάσουν από μια διαδικασία αξιολόγησης της συμμόρφωσης (Άρθρο 16), για να επιβεβαιωθεί ότι πληρούν όλες τις απαραίτητες κανονιστικές απαιτήσεις.

Επιπλέον, τα μοντέλα ΤΝ γενικού σκοπού [43] ταξινομούνται σε δύο κατηγορίες, ανάλογα με το αν ενέχουν συστημικούς κινδύνους ή όχι, όπως αναφέρεται στο Άρθρο 52α. Κάθε κατηγορία συνοδεύεται από διαφορετικές υποχρεώσεις, που διασφαλίζουν ότι η χρήση αυτών των μοντέλων είναι ασφαλής και συμβατή με τους κανονισμούς, ανάλογα με την εφαρμογή τους.

[43] Πρόσφατα, η Επιτροπή δρομολόγησε διαβούλευση σχετικά με κώδικα ορθής πρακτικής για τους παρόχους GPAI. Ο κώδικας αυτός, που προβλέπεται από την πράξη για την τεχνητή νοημοσύνη, θα καλύπτει κρίσιμους τομείς, όπως η διαφάνεια, οι κανόνες που σχετίζονται με τα δικαιώματα πνευματικής ιδιοκτησίας και η διαχείριση κινδύνων. Οι πάροχοι GPAI με δραστηριότητες στην ΕΕ, οι επιχειρήσεις, οι εκπρόσωποι της κοινωνίας των πολιτών, οι κάτοχοι δικαιωμάτων και οι ακαδημαϊκοί εμπειρογνώμονες καλούνται να υποβάλουν τις απόψεις και τα πορίσματά τους, τα οποία θα τροφοδοτήσουν το επικείμενο σχέδιο κώδικα δεοντολογίας για τα μοντέλα GPAI από την Επιτροπή.Οι διατάξεις σχετικά με τη GPAI θα τεθούν σε εφαρμογή σε 12 μήνες. Η Επιτροπή αναμένει να οριστικοποιήσει τον κώδικα ορθής πρακτικής έως τον Απρίλιο του 2025. Επιπλέον, οι παρατηρήσεις από τη διαβούλευση θα τροφοδοτήσουν επίσης το έργο της υπηρεσίας τεχνητής νοημοσύνης, η οποία θα εποπτεύει την εφαρμογή και την επιβολή των κανόνων της πράξης για την τεχνητή νοημοσύνη στη GPAI.

Παρόλο που ο Κανονισμός είναι φιλόδοξος, υπάρχει σκεπτικισμός με τον τρόπο που προωθεί την προστασία των θεμελιωδών δικαιωμάτων του ανθρώπου. Όπως θα δούμε στη συνέχεια, παρά την έμφαση στις «ευρωπαϊκές αξίες» που αναφέρει το άρθρο 2 της ΣΕΕ και το σημαντικό βήμα που κάνει με την εισαγωγή της εκτίμησης αντικτύπου για τα θεμελιώδη δικαιώματα, η προσέγγιση του Κανονισμού δεν είναι τόσο ανθρωποκεντρική όσο άλλες νομοθεσίες, όπως ο Κανονισμός για τις ψηφιακές υπηρεσίες ή ο ΓΚΠΔ. Αυτό γίνεται ιδιαίτερα εμφανές από την έλλειψη ένδικων μέσων για παραβάσεις του Κανονισμού[44].

7.2. Αδυναμίες και Προβλήματα

Προφανώς, η ψήφιση του Κανονισμού προκάλεσε αντιδράσεις από μη κυβερνητικούς οργανισμούς. Είναι ενδιαφέρον να αναφερθούμε στην ανάλυση του Κανονισμού που κάνουν τρεις σημαντικές οργανώσεις (European Center for Not-for-Profit Law (ECNL), Liberties (Civil Liberties Union for Europe), European Civic Forum (ECF) οι οποίες διαδραματίζουν κρίσιμο ρόλο στην υπεράσπιση της κοινωνίας των πολιτών, των ανθρωπίνων δικαιωμάτων και των δημοκρατικών αρχών στην Ευρώπη.

Η ανάλυσή τους (European Civic Forum, 2024) εντοπίζει πέντε βασικές αδυναμίες του Κανονισμού από την οπτική του πολιτικού χώρου και του κράτους δικαίου.

Κενά και «παραθυράκια» στις απαγορεύσεις

Ο Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act) θεσπίζει απαγορεύσεις για ορισμένες εφαρμογές ΤΝ που θεωρούνται απαράδεκτες υπό το πρίσμα των θεμελιωδών δικαιωμάτων. Οι κυριότερες απαγορεύσεις περιλαμβάνουν την αναγνώριση προσώπων σε πραγματικό χρόνο σε δημόσιους χώρους για σκοπούς επιβολής του νόμου (με πολλές εξαιρέσεις), την κατηγοριοποίηση βιομετρικών δεδομένων για την εξαγωγή ευαίσθητων πληροφοριών, τη δημιουργία ή επέκταση βάσεων δεδομένων αναγνώρισης προσώπων, την αναγνώριση συναισθημάτων στην εκπαίδευση ή την εργασία, και την προληπτική αστυνόμευση βάσει προφίλ ατόμων.

[44] Ο νομοθέτης αντισταθμίζει την έλλειψη άμεσων ένδικων μέσων στο κείμενό του, επιβεβαιώνοντας τη διαθεσιμότητα των υφιστάμενων διοικητικών και δικαστικών ένδικων μέσων βάσει του ενωσιακού και του εθνικού δικαίου και σε καταστάσεις όταν τα φυσικά πρόσωπα θεωρούν ότι τα δικαιώματα και οι ελευθερίες τους θίγονται από τη χρήση συστημάτων ΤΝ (De Gregorio and Demková, 2024).

Ωστόσο, αυτές οι απαγορεύσεις τείνουν να καταστούν αναποτελεσματικές λόγω των εκτεταμένων εξαιρέσεων. Για παράδειγμα, η χρήση αναγνώρισης προσώπων σε πραγματικό χρόνο από την αστυνομία επιτρέπεται για την αναζήτηση αγνοουμένων, την πρόληψη τρομοκρατικών επιθέσεων ή την ταυτοποίηση υπόπτων σοβαρών εγκλημάτων. Αυτές οι εξαιρέσεις ενδέχεται να οδηγήσουν σε παραβιάσεις της ελευθερίας της ειρηνικής συνάθροισης και να επιτρέψουν την ταυτοποίηση, παρενόχληση ή σύλληψη διαδηλωτών.

Αυτοαξιολόγηση κινδύνων από εταιρείες ΤΝ

Οι περισσότερες απαιτήσεις του Κανονισμού για την Τεχνητή Νοημοσύνη εφαρμόζονται σε συστήματα ΤΝ υψηλού κινδύνου, τα οποία απαιτούν στενή επίβλεψη για την αποτροπή κοινωνικής και ατομικής βλάβης. Οι πάροχοι συστημάτων ΤΝ υψηλού κινδύνου πρέπει να αξιολογούν και να παρακολουθούν τους κινδύνους για την υγεία, την ασφάλεια και τα θεμελιώδη δικαιώματα, να χρησιμοποιούν υψηλής ποιότητας δεδομένα για την εκπαίδευση των αλγορίθμων και να αποτρέπουν την προκατάληψη. Ωστόσο, η τελική έκδοση του Κανονισμού επιτρέπει στους παρόχους να αποφασίζουν μονομερώς ότι το σύστημά τους δεν ενέχει σημαντικούς κινδύνους, απαλλάσσοντάς τους από τις υποχρεώσεις. Η ανάλυση καταλήγει ότι η ευθύνη για την έρευνα αυτών των αυτοεξαιρούμενων συστημάτων θα μετατοπιστεί στις νέες εθνικές και ευρωπαϊκές αρχές, οι οποίες μπορεί να μην διαθέτουν τους απαραίτητους πόρους για την αποτελεσματική επίβλεψη.

Αδύναμα πρότυπα για τις μελέτες εκτίμησης αντικτύπου στα θεμελιώδη δικαιώματα

Η αποτελεσματική προστασία του πολιτικού χώρου και του κράτους δικαίου απαιτεί από τις δημόσιες αρχές και τις εταιρείες να μην χρησιμοποιούν ΤΝ χωρίς να επαληθεύουν ότι η τεχνολογία δεν παραβιάζει τα θεμελιώδη δικαιώματα ή δεν έχει αρνητικές επιπτώσεις στη δημοκρατία. Πράγματι, ο Κανονισμός απαιτεί από τους φορείς που αναπτύσσουν συστήματα ΤΝ υψηλού κινδύνου να καταγράφουν τις πιθανές επιπτώσεις στα θεμελιώδη δικαιώματα, διενεργώντας την αναφερόμενη στο κείμενο «ως εκτίμηση επιπτώσεων στα θεμελιώδη δικαιώματα» (FRIA). Ωστόσο, δεν υπάρχει σαφής υποχρέωση να αξιολογήσουν αν αυτές οι επιπτώσεις είναι αποδεκτές ή να τις αποτρέψουν. Επίσης, η υποχρέωση γνωστοποίησης των FRIA δεν ισχύει για τις αρχές επιβολής του νόμου και τις

μεταναστευτικές αρχές, γεγονός που περιορίζει τον δημόσιο έλεγχο. Τέλος, η υποχρέωση διαβούλευσης με εξωτερικούς φορείς, όπως οι οργανώσεις της κοινωνίας των πολιτών, αφαιρέθηκε από το τελικό κείμενο.

Χρήση ΤΝ για λόγους εθνικής ασφάλειας χωρίς προστασία δικαιωμάτων

Το θέμα της εξαίρεσης για λόγους εθνικής ασφάλειας στον Κανονισμό Τεχνητής Νοημοσύνης (AI Act) έχει προκαλέσει έντονες αντιδράσεις, ιδιαίτερα σε σχέση με τις επιπτώσεις που μπορεί να έχει στο κράτος δικαίου και τη δημοκρατία στην Ευρωπαϊκή Ένωση. Η εξαίρεση αυτή, η οποία εισήχθη κατά τα τελικά στάδια των τριμερών διαπραγματεύσεων, επιτρέπει στα συστήματα ΤΝ που χρησιμοποιούνται για σκοπούς εθνικής ασφάλειας να εξαιρούνται από τον έλεγχο και τις απαιτήσεις συμμόρφωσης του Κανονισμού. Αυτό δημιουργεί σοβαρές ανησυχίες για την πιθανή κατάχρηση αυτής της εξαίρεσης από κυβερνήσεις για την εισαγωγή συστημάτων βιομετρικής μαζικής επιτήρησης και άλλων τεχνολογιών που μπορούν να υπονομεύσουν τα θεμελιώδη δικαιώματα των πολιτών.

Οι ανησυχίες αυτές εντείνονται από το γεγονός ότι η εξαίρεση αυτή αντιβαίνει στην πάγια νομολογία του Ευρωπαϊκού Δικαστηρίου και παραβλέπει τις αρχές του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Ειδικότερα, η ευρεία εφαρμογή της εξαίρεσης για την εθνική ασφάλεια χωρίς σαφή και αυστηρά κριτήρια αξιολόγησης κατά περίπτωση μπορεί να οδηγήσει σε κατάχρηση εξουσίας, ειδικά σε χώρες όπου το κράτος δικαίου και οι δημοκρατικοί θεσμοί έχουν ήδη υπονομευθεί. Σημειώνεται ότι αυτό το ρυθμιστικό κενό δημιουργεί επίσης ένα ανησυχητικό προηγούμενο σε διεθνές επίπεδο, καθώς μπορεί να επηρεάσει άλλες διεθνείς συμφωνίες, όπως η πρόσφατα οριστικοποιημένη Σύμβαση του Συμβουλίου της Ευρώπης για την Τεχνητή Νοημοσύνη, όπου ενσωματώθηκε μια παρόμοια εξαίρεση.

Έλλειψη συμμετοχής της κοινωνίας των πολιτών

Ο Κανονισμός δεν εξασφαλίζει επαρκή συμμετοχή της κοινωνίας των πολιτών στην αξιολόγηση των επιπτώσεων στα θεμελιώδη δικαιώματα. Τα άτομα μπορούν να υποβάλλουν καταγγελίες, αλλά οι οργανώσεις της κοινωνίας των πολιτών μπορούν να τους εκπροσωπούν μόνο σε υποθέσεις καταναλωτικών δικαιωμάτων και όχι για παραβιάσεις

πολιτικών ελευθεριών που παραβιάζονται από τη χρήση συστημάτων ΤΝ, όπως η βιομετρική παρακολούθηση. Στην πραγματικότητα, η μόνη επίσημη συμμετοχή της κοινωνίας των πολιτών στην εφαρμογή και την παρακολούθηση του νόμου προβλέπεται μέσω του συμβουλευτικού φόρουμ που θα ιδρυθεί στο πλαίσιο του Γραφείου ΤΝ και του Συμβουλίου ΤΝ της ΕΕ. Αυτό το φόρουμ, στο οποίο θα πρέπει να εκπροσωπούνται εξίσου εμπορικά και μη εμπορικά συμφέροντα, θα παρέχει συστάσεις στους αρμόδιους φορείς.

Συμπερασματικά, οι βασικές διαφορές του Κανονισμού από τα λοιπά «κλασικά» κείμενα του ευρωπαϊκού ψηφιακού συνταγματισμού, ως προς τα θεμελιώδη ανθρώπινα δικαιώματα, όπως αναλύθηκαν προηγουμένως εστιάζονται στα εξής σημεία (Kusche, 2024):

1) Η γενική λειτουργία ενός νόμου που στοχεύει στην προστασία των ανθρωπίνων δικαιωμάτων είναι η μείωση της αβεβαιότητας όσον αφορά τις προσδοκίες, διασφαλίζοντας τη χρονική σταθερότητα ορισμένων κανόνων, ακόμη και σε περιπτώσεις παραβίασής τους. Στην περίπτωση της ΤΝ, η έννοια της νομικής βεβαιότητας έχει δύο διαστάσεις, γεγονός που συνδέεται με το ότι ο Κανονισμός δίνει έμφαση στη χρονική διάσταση[45]. Από τη μία πλευρά, ο Κανονισμός στοχεύει να διασφαλίσει ότι τα συστήματα ΤΝ που κυκλοφορούν στην αγορά της ΕΕ είναι ασφαλή και συμμορφώνονται με το υφιστάμενο δίκαιο που προστατεύει τα θεμελιώδη δικαιώματα και τις αξίες της Ένωσης. Αυτά τα θεμελιώδη δικαιώματα λειτουργούν ως ένα σταθερό σημείο αναφοράς για την προστασία των πολιτών.

Από την άλλη πλευρά, αυτά τα ίδια δικαιώματα είναι και το σημείο όπου η ΤΝ μπορεί να προκαλέσει προβλήματα. Η αβεβαιότητα για το πώς ακριβώς θα μπορούσε η ΤΝ να παραβιάσει ή να επηρεάσει αρνητικά αυτά τα δικαιώματα στο μέλλον είναι η κύρια αιτία που χρειάζεται να εισαχθούν νέοι κανονισμοί. Συνεπώς, η μεγάλη διαφορά σε σχέση με τα προηγούμενα κείμενα ψηφιακού συνταγματισμού είναι ότι ο Κανονισμός αναγνωρίζει ότι κάποιες θεμελιώδεις νομικές προσδοκίες μπορεί να γίνουν μη βιώσιμες εξαιτίας της ΤΝ. Εν προκειμένω, εισάγει μια νέα θεώρηση για τα θεμελιώδη δικαιώματα, όχι ως αυστηρούς κανόνες που λένε τι πρέπει να γίνει σε κάθε περίπτωση, αλλά ως αρχές που θέτουν στόχους για την προστασία των δικαιωμάτων. Ο Κανονισμός αναγνωρίζει ότι η ικανότητά τους να παρέχουν σταθερότητα στο μέλλον είναι σχετικά περιορισμένη όταν πρόκειται για

[45] Ο Κανονισμός αναγνωρίζει τη διαφορά μεταξύ παρόντος και μέλλοντος και την αβεβαιότητα που απορρέει από αυτή τη διαφορά, ακόμα και σε σχέση με το αντικείμενο της ρύθμισης.

συγκεκριμένες πράξεις. Και αυτό οφείλεται στο γεγονός ότι στο πλαίσιο της ρύθμισης βάσει κινδύνου, το αν και πότε παραβιάζεται ένα θεμελιώδες δικαίωμα εξαρτάται από την αξιολόγηση του κινδύνου, η οποία μπορεί να είναι μέρος μιας νομικής διαδικασίας, αλλά δεν ταυτίζεται με την απλή εξισορρόπηση ανταγωνιστικών συμφερόντων και αρχών[46].

2) Η επιλογή του Κανονισμού να στηρίζεται κυρίως σε μια ρύθμιση βασισμένη στον κίνδυνο, αντί για απόλυτες απαγορεύσεις ή "δοκιμαστικά ρυθμιστικά περιβάλλοντα" (regulatory sandboxing), σημαίνει ότι ο Κανονισμός επιλέγει να αξιολογεί και να αντιμετωπίζει τους κινδύνους που συνδέονται με την ΤΝ ανάλογα με το επίπεδο κινδύνου που ενέχουν, αντί να απαγορεύει συνολικά ορισμένες τεχνολογίες ή να επιτρέπει την ανάπτυξή τους σε ελεγχόμενο και περιορισμένο περιβάλλον.

Το regulatory sandboxing θα μπορούσε να χρησιμοποιηθεί για την ανάπτυξη και δοκιμή συστημάτων ΤΝ που αφορούν την επεξεργασία προσωπικών δεδομένων σε ελεγχόμενο περιβάλλον πριν από την πλήρη εφαρμογή τους στην αγορά. Αυτός ο τρόπος θα επέτρεπε την αναγνώριση και διαχείριση των κινδύνων προτού οι τεχνολογίες αυτές επηρεάσουν το ευρύ κοινό ή την αγορά. Ωστόσο, αυτή η προσέγγιση δεν είναι η κύρια στρατηγική, αλλά παίζει δευτερεύοντα ρόλο με αποτέλεσμα να αυξάνονται οι κίνδυνοι για

[46] Ένα απλό παράδειγμα μπορεί να μας βοηθήσει να αντιληφθούμε καλύτερα τη διαφορετική θεώρηση που θέτει ο Κανονισμός. Π.χ. ένα σύστημα Τεχνητής Νοημοσύνης χρησιμοποιείται από την αστυνομία για την παρακολούθηση δημόσιων χώρων μέσω καμερών που αναγνωρίζουν πρόσωπα (βιομετρική παρακολούθηση). Ένα από τα θεμελιώδη δικαιώματα που μπορεί να επηρεαστεί από αυτή τη χρήση είναι το δικαίωμα στην ιδιωτικότητα. Αν αυτό το ζήτημα εξεταζόταν απλά με βάση την εξισορρόπηση συμφερόντων, θα έπρεπε να εξετάσουμε τα οφέλη της δημόσιας ασφάλειας σε σχέση με την προστασία της ιδιωτικότητας. Η αστυνομία μπορεί να υποστηρίξει ότι η χρήση της τεχνητής νοημοσύνης βελτιώνει την ασφάλεια, αποτρέποντας εγκλήματα. Από την άλλη, οι πολίτες μπορεί να υποστηρίξουν ότι αυτή η τεχνολογία παραβιάζει το δικαίωμα στην ιδιωτική ζωή.Η αξιολόγηση του κινδύνου, όμως, προσθέτει μια επιπλέον διάσταση σε αυτήν τη συζήτηση. Αντί να σταθμίζεται απλά το ένα συμφέρον απέναντι στο άλλο, η διαδικασία της αξιολόγησης κινδύνου εξετάζει συγκεκριμένα πώς και πόσο πιθανό είναι αυτό το σύστημα να παραβιάσει τα δικαιώματα των πολιτών. Για παράδειγμα, η αξιολόγηση κινδύνου θα μπορούσε να εξετάσει αν το σύστημα αναγνώρισης προσώπων είναι ακριβές ή αν υπάρχει πιθανότητα να γίνει κατάχρηση των δεδομένων από την αστυνομία.
Αν η αξιολόγηση κινδύνου δείξει ότι το σύστημα έχει μεγάλο περιθώριο σφάλματος ή ότι μπορεί να χρησιμοποιηθεί καταχρηστικά, τότε αυτό θα θεωρηθεί μεγαλύτερος κίνδυνος για την ιδιωτικότητα των πολιτών. Σε αυτήν την περίπτωση, η χρήση του συστήματος μπορεί να απαγορευτεί ή να απαιτήσει αυστηρότερα μέτρα προστασίας, ανεξάρτητα από τα οφέλη που μπορεί να προσφέρει για τη δημόσια ασφάλεια. Έτσι, η αξιολόγηση κινδύνου δεν είναι απλά μια εξισορρόπηση συμφερόντων, αλλά μια λεπτομερής ανάλυση των συγκεκριμένων κινδύνων που ενέχει η τεχνολογία για τα θεμελιώδη δικαιώματα, και αυτή η ανάλυση μπορεί να καθορίσει αν και πότε θεωρείται παραβίαση ενός δικαιώματος.

την προστασία των θεμελιωδών δικαιωμάτων καθώς επίσης να προκαλείται μεγαλύτερη αβεβαιότητα και έλλειψη εμπιστοσύνης από τους χρήστες. Αντίστοιχα, το γεγονός ότι ο Κανονισμός δε θέτει απόλυτες απαγορεύσεις μπορεί να οδηγήσει σε αβεβαιότητα και ασάφεια στην εφαρμογή των κανονισμών, καθώς οι κανόνες ερμηνεύονται και να εφαρμόζονται διαφορετικά ανάλογα με τις εκάστοτε περιστάσεις. Αυτό μπορεί να δημιουργήσει προκλήσεις για την αποτελεσματική επιβολή του νόμου και την προστασία των δικαιωμάτων των πολιτών, ιδίως σε περιπτώσεις όπου οι τεχνολογίες εξελίσσονται ταχύτερα από τη νομοθετική διαδικασία ή σε τεχνολογίες που είναι νέες και λιγότερο κατανοητές.

7.3. Κανονισμός, ιδιωτικότητα και επιτήρηση

7.3.1. Βιομετρική ταυτοποίηση, δημιουργία προφίλ και εξαιρέσεις

Ο Κανονισμός αναγνωρίζει ότι το δικαίωμα προστασίας της ιδιωτικής ζωής μπορεί να καταστεί ευάλωτο από τη χρήση ορισμένων συστημάτων ΤΝ. Μάλιστα, όχι μόνο υπογραμμίζει ρητά τη δυνατότητα εφαρμογής του ισχύοντος δικαίου της ΕΕ για την προστασία της ιδιωτικής ζωής και των δεδομένων (άρθρο 2, παρ. 7), αλλά ζητεί να διασφαλίζεται το δικαίωμα στην ιδιωτική ζωή και την προστασία των δεδομένων προσωπικού χαρακτήρα καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος ΤΝ (αιτιολογική σκέψη 69).

Όπως ήδη έχουμε αναφέρει, σύμφωνα με το άρθρο 2 παρ. 3 του Κανονισμού, «η Πράξη ΤΝ δεν επηρεάζει τις αρμοδιότητες των κρατών μελών όσον αφορά την εθνική ασφάλεια», ανεξαρτήτως της οντότητας που τα κράτη μέλη αναθέτουν να ασκεί αυτές τις αρμοδιότητες[47]. Επιπρόσθετα, ο ορισμός των εννοιών «επιβολή του νόμου» και «αρχές επιβολής του νόμου» με τρόπο που επιτρέπει την ευρεία ερμηνεία τους μπορεί να οδηγήσει στη δυνητική προστασία των δραστηριοτήτων επιβολής του νόμου ως δραστηριοτήτων εθνικής ασφαλείας. Συγκεκριμένα, η χρήση βιομετρικών τεχνολογιών σε δημόσιους χώρους για την ταυτοποίηση ατόμων μπορεί να δικαιολογηθεί ως δραστηριότητα σχετική με την εθνική ασφάλεια, παρακάμπτοντας έτσι τους περιορισμούς που θα επιβάλλονταν υπό

[47] Όπως ήδη έχουμε αναφέρει σε προηγούμενο σημείο, το ΔΕΕ στην υπόθεση Privacy Int έχει αποφανθεί ότι «το απλό γεγονός ότι ένα εθνικό μέτρο έχει ληφθεί με σκοπό την προστασία της εθνικής ασφάλειας δεν μπορεί να καταστήσει την ευρωπαϊκή νομοθεσία ανεφάρμοστη και να απαλλάξει τα κράτη μέλη από την υποχρέωσή τους να συμμορφώνονται με αυτήν».

άλλες συνθήκες. Αυτό μπορεί να οδηγήσει σε μαζική παρακολούθηση και συγκέντρωση προσωπικών δεδομένων, με τον κίνδυνο η νομιμότητα τέτοιων ενεργειών να βασίζεται σε ένα νομικό πλαίσιο που επιτρέπει την υπερβολική ερμηνεία του σκοπού της «εθνικής ασφάλειας».

Η πιθανότητα κατάχρησης αυτού του νομοθετικού κενού δημιουργεί ανησυχίες για την προστασία της ιδιωτικής ζωής και την ανάγκη ύπαρξης ισχυρών δικλίδων ασφαλείας για την αποφυγή της υπερβολικής παρακολούθησης και της ανεξέλεγκτης χρήσης τεχνολογιών επιτήρησης από τις αρχές επιβολής του νόμου.

Δύο από τις οκτώ πρακτικές που απαγορεύονται βάσει του Κανονισμού για την Τεχνητή Νοημοσύνη συνδέονται άμεσα με τις δραστηριότητες των αρχών επιβολής του νόμου: η χρήση βιομετρικών τεχνολογιών για αναγνώριση προσώπων σε πραγματικό χρόνο σε δημόσιους χώρους και η εφαρμογή συστημάτων τεχνητής νοημοσύνης για την πρόβλεψη της πιθανότητας εγκληματικής συμπεριφοράς. Παρ' όλα αυτά, οι απαγορεύσεις αυτές δεν είναι απόλυτες, καθώς υπάρχουν αρκετές εξαιρέσεις που ενδέχεται να αποδυναμώσουν την εφαρμογή των κανόνων (Gabrera, 2024).

Στο σημείο αυτό, είναι αξιοσημείωτο ότι ο ορισμός για τη βιομετρική ταυτοποίηση εμφανίζεται σε αιτιολογική σκέψη του Κανονισμού, αντί να περιλαμβάνεται στο τμήμα που είναι αφιερωμένο στους ορισμούς. Σε αντίθεση με αυτό, ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) προσδιορίζει τα "βιομετρικά δεδομένα" απευθείας στο τμήμα των ορισμών του. Αυτό εγείρει ερωτήματα σχετικά με το αν οι αιτιολογικές σκέψεις είναι το κατάλληλο μέρος για την εισαγωγή βασικών όρων που μπορεί να έχουν σοβαρές επιπτώσεις στα θεμελιώδη δικαιώματα καθώς οι αιτιολογικές σκέψεις συνήθως εξηγούν το πλαίσιο και την πρόθεση του νομοθέτη, αλλά δεν έχουν την ίδια νομική ισχύ ή σαφήνεια με τις κύριες διατάξεις του νόμου.

Ο Κανονισμός περιλαμβάνει πολλές εξαιρέσεις στην απαγόρευση της αναγνώρισης βιομετρικών δεδομένων σε πραγματικό χρόνο, οι οποίες μπορεί να υπονομεύσουν τον κανόνα. Επιτρέπει τη χρήση της αναγνώρισης σε τρεις περιπτώσεις: α) για την αναζήτηση αγνοουμένων ή θυμάτων εμπορίας ανθρώπων, β) για την πρόληψη άμεσων απειλών ή τρομοκρατικών επιθέσεων και γ) για την ταυτοποίηση υπόπτων σοβαρών εγκλημάτων όπως αυτά ορίζονται στο Παράρτημα ΙΙ του Κανονισμού. Καθώς αυτές οι εξαιρέσεις μπορεί

να ερμηνευτούν ευρέως [48], η απαγόρευση μπορεί να αρθεί και η αναγνώριση βιομετρικών δεδομένων σε πραγματικό χρόνο, αντί να εμπίπτει στην απαγορευμένη κατηγορία, κατατάσσεται στην κατηγορία υψηλού κινδύνου και υπόκειται σε ασφαλιστικές δικλίδες με τη μορφή: i) ανεξάρτητης έγκρισης, ii) εκπόνησης εκτίμησης επιπτώσεων στα θεμελιώδη δικαιώματα και iii) τήρησης αρχείων[49].

Ωστόσο και στη διαδικασία αυτή, υπάρχουν σημαντικοί περιορισμοί που παρεμποδίζουν τη δημόσια εποπτεία και τη διαφάνεια. Πρώτον, η βάση δεδομένων στην οποία οι αρχές επιβολής του νόμου πρέπει να καταχωρίζουν το σύστημα τεχνητής νοημοσύνης που χρησιμοποιούν, δεν είναι δημόσια και είναι προσβάσιμη μόνο από την Ευρωπαϊκή Επιτροπή. Επιπλέον, υπάρχουν πρακτικές δυσκολίες στο να αναγνωριστεί από το κοινό ένα εργαλείο τεχνητής νοημοσύνης που χρησιμοποιείται από τις αρχές επιβολής του νόμου καθώς ο Κανονισμός απαιτεί μόνο περιορισμένες υποχρεώσεις διαφάνειας για τους παρόχους και τους χρήστες τέτοιων συστημάτων[50]. Άλλωστε, δεδομένου ότι οι αρχές επιβολής του νόμου συχνά χρησιμοποιούν τεχνολογίες που παρέχονται από τρίτους, θεωρούνται «χρήστες» σύμφωνα με τον Κανονισμό.

---

[48] Για παράδειγμα, η εξαίρεση για σοβαρά εγκλήματα δεν απαιτεί συγκεκριμένη σύνδεση με μια εν εξελίξει έρευνα, αλλά μπορεί να θεωρηθεί ότι η ταυτοποίηση είναι απαραίτητη για μια ενδεχόμενη έρευνα.

[49] Οι αρχές επιβολής του νόμου πρέπει να εξασφαλίσουν δικαστική ή ανεξάρτητη διοικητική έγκριση πριν την εφαρμογή της βιομετρικής ταυτοποίησης σε πραγματικό χρόνο, ή σε «κατεπείγουσες περιστάσεις», εντός 24 ωρών από την ανάπτυξη της τεχνολογίας (Άρθρο 5, παρ.2. Ο Κανονισμός αναφέρει ότι η τεχνολογία Τεχνητής Νοημοσύνης πρέπει να περιορίζεται στην ταυτοποίηση του συγκεκριμένου ατόμου που αποτελεί στόχο, αγνοώντας όμως ότι, κατά τη διαδικασία σάρωσης βιομετρικών δεδομένων σε πραγματικό χρόνο, σαρώνεται το πρόσωπο κάθε ατόμου για να βρεθεί μια αντιστοιχία.
Για να εξασφαλιστεί η έγκριση, οι αρχές επιβολής του νόμου πρέπει να υποβάλουν μια αξιολόγηση των επιπτώσεων στα θεμελιώδη δικαιώματα και να επιβεβαιώσουν ότι το αντίστοιχο σύστημα Τεχνητής Νοημοσύνης έχει καταχωριστεί στο μη δημόσιο τμήμα της βάσης δεδομένων της ΕΕ για συστήματα υψηλού κινδύνου (Άρθρο 49). Η αρχή που χορηγεί την έγκριση πρέπει να αξιολογήσει αν η χρήση της τεχνολογίας για τη βιομετρική ταυτοποίηση είναι: i) απαραίτητη και ανάλογη προς τους επιδιωκόμενους στόχους, και ii) αν είναι αυστηρά περιορισμένη σε χρονική διάρκεια, γεωγραφική και προσωπική εμβέλεια. Αν η έγκριση απορριφθεί, τότε η διαδικασία πρέπει να σταματήσει αμέσως και όλα τα σχετικά δεδομένα και αποτελέσματα να διαγραφούν.
Εκτός από τη διαδικασία έγκρισης, κάθε χρήση τέτοιου είδους τεχνολογίας πρέπει να κοινοποιείται στην αρμόδια αρχή εποπτείας της αγοράς και στην εθνική αρχή προστασίας δεδομένων (Άρθρο 5 παρ.4).

[50] Για παράδειγμα, όσοι χρησιμοποιούν συστήματα τεχνητής νοημοσύνης για τη δημιουργία deepfakes δεν υποχρεούνται να αποκαλύπτουν ότι το περιεχόμενο είναι τεχνητά δημιουργημένο, εφόσον η χρήση αυτών των συστημάτων είναι εξουσιοδοτημένη από το νόμο για την ανίχνευση, πρόληψη ή διερεύνηση εγκλημάτων.

Συνεπώς, επιτρέπεται στους χρήστες της τεχνητής νοημοσύνης να μην αποκαλύπτουν ότι χρησιμοποιούν τεχνητή νοημοσύνη για βιομετρική κατηγοριοποίηση και αναγνώριση συναισθημάτων, εφόσον τους το επιτρέπει ο νόμος για την ανίχνευση, πρόληψη ή διερεύνηση εγκλημάτων, υπό την προϋπόθεση ότι τηρούνται οι κατάλληλες ασφαλιστικές δικλίδες (Άρθρο 50, παρ.3). Ωστόσο, ο Κανονισμός δεν παρέχει περαιτέρω λεπτομέρειες για αυτές τις ασφαλιστικές δικλίδες. Ομοίως, οι χρήστες συστημάτων τεχνητής νοημοσύνης που δημιουργούν deepfakes δεν είναι υποχρεωμένοι να αποκαλύπτουν ότι το περιεχόμενο είναι τεχνητά δημιουργημένο, εάν η χρήση αυτών των συστημάτων είναι νόμιμη για την ανίχνευση, πρόληψη, διερεύνηση ή δίωξη εγκλημάτων (Άρθρο 50, παρ. 4).

Για την εκ των υστέρων βιομετρική παρακολούθηση, οι εγγυήσεις του Κανονισμού είναι ακόμη λιγότερο ισχυρές. Συγκεκριμένα, ο Κανονισμός δεν θέτει περιορισμούς σχετικά με τους τύπους εγκλημάτων που μπορούν να δικαιολογήσουν τη χρήση της μεταγενέστερης αναγνώρισης. Ενώ η αναγνώριση σε πραγματικό χρόνο επιτρέπεται μόνο για συγκεκριμένα σοβαρά αδικήματα, όπως ορίζονται στο Παράρτημα ΙΙ και μόνο αν οι ποινές περιλαμβάνουν φυλάκιση ή κράτηση τουλάχιστον 4 ετών, η μεταγενέστερη αναγνώριση δεν έχει τέτοιου είδους περιορισμούς καθώς δεν απαιτείται το ερευνώμενο αδίκημα να είναι συγκεκριμένου τύπου ή βαθμού σοβαρότητας.

Για παράδειγμα, παρόμοια με τους κανόνες που αφορούν την αναγνώριση βιομετρικών δεδομένων σε πραγματικό χρόνο, εάν απορριφθεί η αίτηση έγκρισης, οι αρχές επιβολής του νόμου πρέπει να σταματήσουν αμέσως τη χρήση του συστήματος τεχνητής νοημοσύνης και να διαγράψουν όλα τα σχετικά δεδομένα. Ωστόσο, οι απαιτήσεις αναφοράς διαφέρουν καθώς ο Κανονισμός απαιτεί μόνο την καταγραφή αυτών των χρήσεων, ώστε να είναι διαθέσιμες στις αρχές αν ζητηθούν (Άρθρο 26, παρ.10), δηλ. δεν υπάρχει υποχρέωση των αρμόδιων αρχών για κάθε περίπτωση χρήσης της μεταγενέστερης αναγνώρισης βιομετρικών δεδομένων.

Επιπρόσθετα, ο Κανονισμός προσπαθεί να απαγορεύσει τη χρήση συστημάτων τεχνητής νοημοσύνης (ΑΙ) που προβλέπουν αν ένα άτομο είναι πιθανό να διαπράξει ένα έγκλημα, βασιζόμενα αποκλειστικά στα χαρακτηριστικά ή το προφίλ αυτού του ατόμου. Ωστόσο, υπάρχει μια εξαίρεση: αν το σύστημα χρησιμοποιείται για να βοηθήσει έναν άνθρωπο να κρίνει αν κάποιος έχει εμπλακεί σε εγκληματική δραστηριότητα και αυτή η

κρίση βασίζεται σε πραγματικά και επαληθεύσιμα στοιχεία, τότε το σύστημα τεχνητής νοημοσύνης μπορεί να χρησιμοποιηθεί.

Αυτό σημαίνει ότι η απαγόρευση ισχύει μόνο όταν οι εκτιμήσεις γίνονται ανεξάρτητα από ένα σύστημα τεχνητής νοημοσύνης, χωρίς την ανθρώπινη παρέμβαση. Αν όμως το σύστημα χρησιμοποιείται για να υποστηρίξει την ανθρώπινη κρίση, η απαγόρευση δεν ισχύει και το σύστημα μπορεί να χρησιμοποιηθεί υπό την προϋπόθεση ότι ακολουθούνται οι ασφαλιστικές δικλίδες για τις χρήσεις υψηλού κινδύνου όπως αναφέρονται στο Παράρτημα ΙΙΙ. Υπάρχει ανησυχία ότι αυτή η εξαίρεση μπορεί να αξιοποιηθεί από την αστυνομία για να χρησιμοποιήσει αυτά τα συστήματα σε προγνωστική αστυνόμευση. Επίσης, υπάρχει φόβος ότι τα συστήματα αυτά μπορεί να χρησιμοποιηθούν και στη δικαιοσύνη για να προβλέψουν αν κάποιος θα ξανακάνει έγκλημα (υποτροπή).

Ένα άλλο πρόβλημα με τον Κανονισμό είναι ότι επιτρέπει στους παρόχους τεχνητής νοημοσύνης να αποφασίζουν αν το σύστημά τους είναι «υψηλού κινδύνου» ή όχι. Ωστόσο, όταν πρόκειται για συστήματα που βασίζονται στη δημιουργία προφίλ ατόμων, δεν μπορούν παρά να χαρακτηριστούν ότι ανήκουν στην κατηγορία «υψηλού κινδύνου».

7.3.2. Πολιτική βιασύνη και θεμελιώδη δικαιώματα

Η πολιτική βιασύνη [51] για την επέκταση του πεδίου εφαρμογής της προστασίας των θεμελιωδών δικαιωμάτων στον Κανονισμό έχει εγείρει ερωτήματα σχετικά με τη διαδικασία συμμόρφωσης (De Gregorio et al., 2024). Η εκτίμηση επιπτώσεων στα θεμελιώδη δικαιώματα είναι μόνο ένα παράδειγμα αυτής της διαδικασίας που απαιτεί από τους φορείς ανάπτυξης συστημάτων ΤΝ να προσεγγίσουν με διαφορετικό τρόπο την εξισορρόπηση των κινδύνων στην ψηφιακή εποχή.

Η εισαγωγή της FRIA στον Κανονισμό αναδύεται ως απαραίτητη απάντηση στην ανάγκη εξισορρόπησης μεταξύ της καινοτομίας και των κινδύνων που αυτή εγκυμονεί για τα θεμελιώδη δικαιώματα. Ωστόσο, η ταχύτητα με την οποία ενσωματώθηκε αυτή η διάταξη, η συνοχή της με τον υπόλοιπο κανονισμό -ο οποίος βασίζεται κυρίως σε πρότυπα ασφάλειας

[51] Κανόνες ειδικά για τα συστήματα GPAI εισήχθησαν από το Ευρωπαϊκό Κοινοβούλιο στην έκδοσή του που δημοσιεύθηκε λίγο πριν από την έναρξη των τριμερών διαπραγματεύσεων τον Ιούνιο του 2023.

προϊόντων- καθώς και η πρακτική εφαρμογή της από δημόσιους και ιδιωτικούς φορείς αποτελούν ζητήματα που θα απαιτήσουν απαντήσεις κατά τον πρώτο χρόνο εφαρμογής του Κανονισμού.

Αρχικά, ο Κανονισμός δεν διασαφηνίζει επαρκώς το ευρύτερο πλαίσιο των θεμελιωδών δικαιωμάτων που πρέπει να λαμβάνουν υπόψη τα κράτη μέλη, τα οποία έχουν υπογράψει την Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα (ΕΣΔΑ). Αυτή η αδυναμία αναδεικνύει την αναγκαιότητα για ισορροπία μεταξύ των θεμελιωδών δικαιωμάτων, όπως αυτή υπαγορεύεται όχι μόνο από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ αλλά και από την ίδια την ΕΣΔΑ και τη Σύμβαση-πλαίσιο για την ΤΝ. Η έλλειψη σαφούς αναφοράς σε κριτήρια εξισορρόπησης των δικαιωμάτων αυτών ενδέχεται να δημιουργήσει περαιτέρω προβληματισμούς.

Ένα άλλο σημαντικό ζήτημα αφορά τον προσδιορισμό του υπεύθυνου για την αξιολόγηση. Σύμφωνα με τον Κανονισμό περί ΤΝ, η αξιολόγηση πρέπει να διεξάγεται από τον φορέα ανάπτυξης πριν από την ενεργοποίηση του συστήματος. Ειδικότερα, αυτή η εκ των προτέρων αξιολόγηση αφορά τα συστήματα υψηλού κινδύνου, όπως περιγράφονται στο άρθρο 27. Ωστόσο, η σύγκλιση της μελέτης εκτίμησης αντικτύπου (DPIA) με την FRIA, ιδίως σε περιπτώσεις που απαιτείται και η μία και η άλλη, μπορεί να οδηγήσει σε προβλήματα συμμόρφωσης. Η διεξαγωγή αυτών των αξιολογήσεων συχνά βαρύνει τον φορέα ανάπτυξης, ο οποίος μπορεί να θεωρηθεί υπεύθυνος επεξεργασίας δεδομένων σύμφωνα με τον ΓΚΠΔ, ενδεχομένως συγχέοντας τους ρόλους του παρόχου και του χρήστη.

Σχετικά με τις επιπτώσεις για τα μοντέλα τεχνητής νοημοσύνης γενικού σκοπού, τα μοντέλα αυτά μπορεί να θεωρηθούν «υψηλού κινδύνου» όταν χρησιμοποιούνται σε συγκεκριμένους τομείς, όπως ορίζει ο Κανονισμός, στο άρθρο 6 και το Παράρτημα ΙΙΙ ή ενέχουν συστημικό κίνδυνο (άρθρο 3). Σε αυτές τις περιπτώσεις, απαιτείται μια ειδική αξιολόγηση για να διασφαλιστεί ότι δεν προκαλούν σοβαρούς κινδύνους, όπως προβλήματα στη «δημόσια υγεία, την ασφάλεια, τα θεμελιώδη δικαιώματα ή την κοινωνία στο σύνολό της, η οποία μπορεί να εξαπλωθεί σε μεγάλη κλίμακα κατά μήκος της αλυσίδας αξίας» (άρθρο 55). Αυτή η αξιολόγηση που επίσης εξετάζει τον αντίκτυπο στα θεμελιώδη δικαιώματα, διενεργείται από τον πάροχο του μοντέλου και επικεντρώνεται στο ίδιο το μοντέλο και όχι στη συγκεκριμένη του χρήση, δημιουργώντας δύο διαφορετικές διαδικασίες ελέγχου.

Έτσι, ενώ ο πάροχος ενός τέτοιου μοντέλου με υψηλό ή συστημικό κίνδυνο υποχρεούται να διενεργήσει μια «αξιολόγηση συμμόρφωσης» σύμφωνα με το άρθρο 55, ο χρήστης του μοντέλου ή αλλιώς ο φορέας εφαρμογής συστημάτων ΤΝ θα πρέπει επίσης να εκτελέσει μια FRIA εάν το μοντέλο χρησιμοποιείται για σκοπό που κατατάσσεται ως υψηλού κινδύνου σύμφωνα με το Παράρτημα ΙΙΙ. Ενώ αυτές οι διαδικασίες μπορεί να φαίνονται παρόμοιες, η κάθε μία έχει τον δικό της στόχο. Προφανώς, η FRIA, όταν συνδυάζεται με την αξιολόγηση συμμόρφωσης από τον πάροχο, προωθεί έναν διάλογο μεταξύ παρόχου και χρήστη, που είναι κρίσιμος για την ολοκληρωμένη και αποτελεσματική διαχείριση των κινδύνων. Χωρίς αυτή τη συνεργασία, η αξιολόγηση των κινδύνων θα ήταν αποσπασματική και ανεπαρκής, ειδικά δεδομένης της πολυπλοκότητας των μοντέλων τεχνητής νοημοσύνης γενικού σκοπού.

ΕΠΙΛΟΓΟΣ

Η κριτική προς τον ψηφιακό συνταγματισμό έχει ήδη αρχίσει να διερευνά τα κενά και τις παρανοήσεις του. Όπως υποστηρίζει ο Terzis (2024), το έργο του ψηφιακού συνταγματισμού αφηγείται μια συγκεκριμένη ιστορία, προσπαθώντας να αντιμετωπίσει τα προβλήματα που εντοπίζει με τρόπους που εξυπηρετούν τις επιδιωκόμενες παρεμβάσεις του. Όπως και άλλοι συνταγματισμοί, στηρίζεται σε θεσμικές ελπίδες για επίτευξη ισορροπίας ισχύος μεταξύ ανταγωνιστικών δυνάμεων σε πολιτικές και οικονομικές συγκρούσεις, αλλά αγνοεί ή απλοποιεί κρίσιμα ζητήματα τα οποία ο Terzis (ibid) κατηγοριοποιεί σε τρεις βασικούς άξονες:

1. Ο ψηφιακός συνταγματισμός αναδύεται από την αυξανόμενη επιρροή των ιδιωτικών εταιρειών στον έλεγχο των ανθρωπίνων δικαιωμάτων μέσω των ψηφιακών τεχνολογιών, με τις κοινωνικές σχέσεις να διαμορφώνονται από δημόσιους και ιδιωτικούς φορείς. Παραδείγματα όπως το Συμβούλιο Εποπτείας του Facebook και ο ΓΚΠΔ θεωρούνται προσπάθειες συνταγματοποίησης του ψηφιακού χώρου. Ωστόσο, η πολιτική εκπροσώπηση των πολιτών στον ψηφιακό κόσμο συχνά παραμελείται, καθώς υποτίθεται λανθασμένα ότι οι χρήστες των ψηφιακών πλατφορμών απολαμβάνουν τα ίδια δικαιώματα με τους πολίτες σε μια συνταγματική τάξη. Η εκμετάλλευση των χρηστών ως πηγή δεδομένων δεν συμβαδίζει με την εικόνα του αυτόνομου πολίτη και οι υποστηρικτές του ψηφιακού συνταγματισμού αποτυγχάνουν να αναγνωρίσουν πλήρως αυτή τη διάσταση. Η χρήση της θεωρίας του κοινωνικού συμβολαίου στον ψηφιακό χώρο επικρίνεται για την υπεραπλούστευση των σχέσεων εξουσίας και την αδυναμία αντιμετώπισης των θεμελιωδών προβλημάτων εξάρτησης που χαρακτηρίζουν τις σύγχρονες ψηφιακές πλατφόρμες.

2. Οι ψηφιακοί συνταγματολόγοι υποστηρίζουν ότι οι ψηφιακές εταιρείες ασκούν μια μοναδική μορφή εξουσίας, που διαφέρει από τις παραδοσιακές πολυεθνικές, καθώς οι ψηφιακές τεχνολογίες έχουν μειώσει την ισχύ των κρατών. Θεωρούν ότι η ανάπτυξη του Διαδικτύου και των κοινωνικών μέσων δημιούργησε συνταγματική ανισορροπία, η οποία απαιτεί άμεσες και ριζικές νομικές παρεμβάσεις. Ωστόσο, η άποψη αυτή βασίζεται σε έναν παραδοσιακό διαχωρισμό μεταξύ δημόσιου και ιδιωτικού τομέα, ο οποίος μπορεί να μην ανταποκρίνεται στην πραγματικότητα, δεδομένης της συνεργασίας των ψηφιακών εταιρειών με τις κυβερνήσεις. Η κριτική προς τον ψηφιακό συνταγματισμό τονίζει ότι προτού αναπτυχθεί μια θεωρία διακυβέρνησης, είναι αναγκαία η διαμόρφωση μιας πιο

ολοκληρωμένης κοινωνικής θεωρίας που θα λαμβάνει υπόψη τις ιστορικές εξελίξεις και τη συνεχή αλλαγή.

3. Ένα βασικό πρόβλημα στον ψηφιακό συνταγματισμό είναι η πεποίθηση ότι οι ψηφιακές εταιρείες έχουν αποκτήσει υπερβολική εξουσία λόγω της έλλειψης επαρκούς νομικής ρύθμισης. Ο De Gregorio υποστηρίζει ότι η απουσία ενός ενιαίου νομικού πλαισίου έχει επιτρέψει σε αυτές τις εταιρείες να εκμεταλλεύονται τα προσωπικά δεδομένα για να αυξήσουν την επιρροή τους. Στην πραγματικότητα, όμως, ο νόμος δεν ήταν απών σε αυτή τη διαδικασία, αλλά αντίθετα, έχει συμβάλει στην ενίσχυση της εξουσίας των ψηφιακών εταιρειών, επιτρέποντας τους να παρακάμπτουν τα ατομικά δικαιώματα. Συχνά, οι ψηφιακές εταιρείες κατορθώνουν να παραβιάζουν ή να προσαρμόζουν τους νόμους προς όφελός τους, με ελάχιστες συνέπειες.

Αυτό φανερώνει ότι το πρόβλημα δεν είναι μόνο νομικό αλλά και πολιτικό, καθώς η παραδοσιακή νομική προσέγγιση που προσπαθεί να ισορροπήσει το δημόσιο και ιδιωτικό συμφέρον δεν φαίνεται επαρκής για να αντιμετωπίσει τις σύγχρονες προκλήσεις. Οι τεχνολογικές εταιρείες επηρεάζουν τις πολιτικές συνθήκες και αναδιαμορφώνουν την κοινωνική πραγματικότητα σύμφωνα με τα δικά τους συμφέροντα. Για να προστατευτούν τα δικαιώματα των πολιτών στον ψηφιακό κόσμο, απαιτείται μια ριζική αναθεώρηση των νομικών πλαισίων και η ανάπτυξη νέων μορφών ρύθμισης που θα ανταποκρίνονται στις προκλήσεις της ψηφιακής εποχής. Η κατανόηση της αλληλεπίδρασης μεταξύ τεχνολογίας και εξουσίας είναι απαραίτητη για την ανάπτυξη αποτελεσματικών και δίκαιων νομικών και πολιτικών απαντήσεων.

Συνοψίζοντας, ο ψηφιακός συνταγματισμός δεν πρέπει να εξετάζεται αποκλειστικά ως νομικό ζήτημα, αλλά ως ένα πολύπλευρο κοινωνικό φαινόμενο που απαιτεί συλλογικές και διεπιστημονικές λύσεις. Προσφέρει, συνεπώς, μια ποικιλία προοπτικών για την κατανόηση της προστασίας των δικαιωμάτων, καθώς ακολουθεί εξ ορισμού μια συνεχή εξελικτική πορεία, η οποία ανταποκρίνεται στους αέναους κοινωνικούς και εξουσιαστικούς μετασχηματισμούς.

Ως πολιτικο-ιστορικό φαινόμενο και διεκδικητικό κίνημα παραμένει πιστό σε ένα κεντρικό θεωρητικό και ανθρωπολογικό πρότυπο: αυτό της οριοθέτησης της εξουσίας και της αισιόδοξης προσδοκίας για έναν «καλύτερο κόσμο» όπου η τεχνολογία εξυπηρετεί το

κοινό καλό και σέβεται τα θεμελιώδη ανθρώπινα δικαιώματα Το κατά πόσον όλοι οι συμμετέχοντες στον συνταγματικό διάλογο ενστερνίζονται με ειλικρίνεια αυτές τις παραδοχές μπορεί βέβαια να αμφισβητηθεί καθώς κάθε θεωρία δικαίου προϋποθέτει ένα πλέγμα κοινωνικών συνθηκών εντός του οποίου αξιώνει την κανονιστική της επέμβαση.

Παρά ταύτα, η στροφή που συντελείται με τον ψηφιακό συνταγματισμό, στρέφει τη θεωρητική σκέψη προς τρόπους πραγμάτωσης των συνταγματικών, δημοκρατικών αρχών τόσο σε τοπικό όσο και σε υπερεθνικό, σε κρατικό όσο και σε ιδιωτικό επίπεδο. Στο πλαίσιο αυτό, οι δικαιοδοτικοί και διοικητικοί μηχανισμοί καλούνται, αφενός, να αναλάβουν καίριο ρόλο στην προσαρμογή του δικαίου και των διοικητικών πρακτικών, ερμηνεύοντας τους ισχύοντες κανόνες υπό το φως των ψηφιακών εξελίξεων και των νέων κοινωνικών δεδομένων και αφετέρου να είναι ευέλικτοι και προορατικοί, προκειμένου να διασφαλίσουν ότι οι θεμελιώδεις αρχές της δημοκρατίας και του κράτους δικαίου δεν υπονομεύονται, αλλά αντίθετα ενισχύονται από τις τεχνολογικές εξελίξεις. Ο συνταγματικός διάλογος στον ψηφιακό κόσμο είναι, επομένως, μια συνεχιζόμενη πρόκληση που θα καθορίσει το μέλλον της δημοκρατίας και των ατομικών δικαιωμάτων σε παγκόσμιο επίπεδο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία Ξενόγλωσσα

Celeste, E. (2022) *Digital Constitutionalism: The Role of Internet Bills of Rights* (1st ed.), London: Routledge. Available at: https://doi.org/10.4324/9781003256908

De Gregorio G. (2022) *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge University Press.

DeCew, J.W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY: Cornell University Press, pp. 4-5.

Karavas, V. (2010) "Governance of Virtual Worlds and the Quest for a Digital Constitution", in Christoph B. Graber and Mira Burri-Nenova (eds) *Governance of Digital Game Environments and Cultural Diversity: Transdisciplinary Enquiries.* Cheltenham-Northampton: Edward Elgar Publishing.

Krause, G. (2023) *Die praxis des digitalen humanismus. (The practice of digital humanism).* Wiesbaden: Springer Vieweg.

Lindorfer, M. (2024) "The Threat of Surveillance and the Need for Privacy Protections", in Werthner, H. et al. (eds) *Introduction to Digital Humanism*. Cham: Springer. Available at: https://doi.org/10.1007/978-3-031-45304-5_37

Longman (2014) *Longman Dictionary of Contemporary English,* 6th ed. Harlow: Pearson Education.

Nida-Rümelin, J. and Weidenfeld, N. (2022) *Digital Humanism: For a Humane Transformation of Democracy, Economy, and Culture in the Digital Age*. Cham: Springer International Publishing.

Nowotny, H. (2021) *AI we trust: Power, illusion and control of predictive algorithms.* Cambridge: Polity Press.

Redmiles, E. (2022) The Need for Respectful Technologies: Going Beyond Privacy *Perspectives on digital humanism.* Bern: Springer. Available at: https://library.oapen.org/handle/20.500.12657/51945 (Accessed May 4th, 2024).

Roessler, B. (2006) "New Ways of Thinking about Privacy", in Anne Philips Bonnie Honig & John Dryzek (eds.), *Oxford Handbook of Political Theory.* Oxford University Press, pp. 694-713.

Rössler, B. (2005) *The Value of Privacy*. Cambridge: Polity Press.
Suzor, N. (2019) *Lawless: The Secret Rules That Govern Our Digital Lives.* Cambridge University Press 2019.
Turner, J. (2019) *Robot Rules: Regulating Artificial Intelligence*. UK: Palgrave Macmillan
Werthner, H. (2020) The Vienna Manifesto on Digital Humanism. In M. Hengstschläger (Ed.), *Digital Transformation and Ethics,* Ecowin, pp. 338–357.
Werthner, H., Prem, E., Lee, E. A. and Ghezzi, C. (2022) *Perspectives on digital humanism.* Bern: Springer. Available at: https://library.oapen.org/handle/20.500.12657/51945 (Accessed May 4th, 2024).
Zuboff, S. (2019) *The age of surveillance capitalism*. N.Y: Profile Books Ltd.

Βιβλία Ελληνόγλωσσα

Μήτρου, Λ. (2010) «Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες: Η νομική διάσταση», σε: Λαμπρινουδάκης, Κ., Μήτρου, Λ., Γκρίτζαλης, Σ. και Κάτσικας, Σ. (επιμ.) *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα*. Αθήνα: Παπασωτηρίου, σσ. 505-545.
Παναγοπούλου - Κουτναζή, Φ. (2023) *Τεχνητή Νοημοσύνη: Ο δρόμος προς έναν ψηφιακό συνταγματισμό : μια ηθικο-συνταγματική θεώρηση.* Αθήνα: Παπαζήση.
Σμιτ, Ε., Κίσινγκερ, Χ. και Χούτενλοχερ, Ν. (2022) *Η εποχή της τεχνητής νοημοσύνης και το ανθρώπινο μέλλον μας*. Αθήνα: Liberal Books.
Τάσης, Θ. (2019) *Ψηφιακός Ανθρωπισμός: Εικονιστικό Υποκείμενο και Τεχνητή Νοημοσύνη.* Αθήνα: Αρμός.
Häberle, P. (1982) *Έννοια και περιεχόμενο της ανθρώπινης αξιοπρέπειας κατά το γερμανικό και ελληνικό Σύνταγμα*, μτφ.. Δημητρόπουλος, Α. και Παπαϊωάννου, Ζ. ΤοΣ.
Kant, I. (1984) *Τα θεμέλια της μεταφυσικής των ηθών,* μτφ. Τζαβάρας, Γ. Αθήνα: Δωδώνη

Άρθρα

Adhikari, A., Das, S. and Dewri, R. (2023) "Evolution of composition, readability, and structure of privacy policies over two decades", *Proceedings on Privacy Enhancing Technologies (PETS)*. Available at: https://doi.org/10.56553/popets-2023-0074
Berman, P. (2000) "Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation", *University of Colorado Law Review* 71, pp. 1263–1310.
Calacci, D. & Stein, J. (2023) "From access to understanding: Collective data governance for workers", *European Labour Law Journal*, 14(2). Available at: https://doi.org/10.1177/20319525231167981
Celeste, E. (2019) "Digital constitutionalism: a new systematic theorization", *International Review of Law, Computers & Technology*, 33(1), pp. 76–99. Available at: https://doi.org/10.1080/13600869.2019.1562604
Celeste, E. and De Gregorio, G. (2021) "Digital Humanism: The Constitutional Message of the GDPR", *Global Privacy Law Review* 4. Available at: https://ssrn.com/abstract=4045029 (Accessed May 4th, 2024).
Celeste, E. and Formici, G. (2024) "Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia", *German Law Journal*, pp.1-20. Available at: https://dx.doi.org/10.1017/glj.2023.105
Coeckelbergh, M. (2024) "What is digital humanism? A conceptual analysis and an argument for a more critical and political digital (post)humanism", *Journal of Responsible Technology*, Vol.17. Available at: https://doi.org/10.1016/j.jrt.2023.100073
De Gregorio, G. (2021a) "The rise of digital constitutionalism in the European Union", *International Journal of Constitutional Law*, Vol.19, Issue 1, pp. 41–70.Available at: https://doi.org/10.1093/icon/moab001
De Gregorio, G. (2021b) "The digital services act: a paradigmatic example of European digital constitutionalism", *Diritti Comparati*, March 17. Available at: https://www.dirittocomparati.it/the-digital-services-act-a-paradigmatic-example-of-european-digital-constitutionalism/ (Accessed June 1st, 2024).

De Gregorio, G. and Demková, S. (2024) "The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe", *Cgsl working papers*,no. 3/2024. Available at: https://ciencia.ucp.pt/ws/portalfiles/portal/99623527/99623114.pdf (Accessed August 1st 2024).

De Gregorio, G., Fasciglione, M., Paolucci, F. and Pollicino, O. (2024) "Compliance through Assessing Fundamental Rights: Insights at the Intersections of the European AI Act and the Corporate Sustainability Due Diligence Directive, *Media Laws,* July 30th. Available at : https://www.medialaws.eu/compliance-through-assessing-fundamental-rights-insights-at-the-intersections-of-the-european-ai-act-and-the-corporate-sustainability-due-diligence-directive/ (Accessed August 21st, 2024).

Dreyer, S. and Schulz, W. (2019) "The General Data Protection Regulation and Automated Decision-Making: Will It Deliver? Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole", *BertelsmannStiftung*. Available at: https://doi.org/10.11586/2018018

Edwards, L. and Veale, M. (2017) "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", *Duke Law & Technology Review,* pp.18-84

Emami-Naeini, P., Agarwal, Y., Cranor, L. F. and Hibshi, H. (2020) "Ask the experts: What should be on an IoT privacy and security label?", *Proceedings of the IEEE symposium on security and privacy (S&P)*. Available at: https://doi.org/10.1109/SP40000.2020.00043

European Civic Forum (2024*) Packed with loopholes: Why the AI Act fails to protect civic space and the rule of law*, April 4. Available at: https://civic-forum.eu/advocacy/artificial-intelligence/packed-with-loopholes-why-the-ai-act-fails-to-protect-civic-space-and-the-rule-of-law (Accessed June 3rd, 2024).

Fitzgerald, B. F. (1999) "Software as discourse? A constitutionalism for informa tion society", *Alternative Law Journal*, 24(3), 144–149. Available at: https://search.informit.org/doi/10.3316/ielapa.200000096 (Accessed June 3rd, 2024).

Gabrera, L. (2024) *EU AI Act Brief – Pt. 2, Privacy & Surveillance*", April 30th. Available at: https://cdt.org/insights/eu-ai-act-brief-pt-2-privacy-surveillance/ (Accessed August 21st, 2024)

Gellman, B. and Lindeman, T. (2013) "Inner workings of a top-secret spy program, *Washington Post,* June 29. Available at: https://goodtimesweb.org/surveillance/2013/wp-prism-jun-29-2013.html (Accessed July 23rd, 2024)

Gellman, B. and Poitras, L. (2013) "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", *Washington Post*, June 7. Available at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (Accessed June 3rd, 2024).

Gerber, N., Gerber, P. and Volkamer, M. (2018) "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior", *Computers and Security*, 77. Available at: https://doi.org/10.1016/j.cose.2018.04.002

Gill, L., Redeker, D. and Gasser, U. (2015) "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights", *Berkman Klein Center Research Publication*, 2015-15. Available at: https://www.dennisredeker.com/papers.html [Accessed August 1st, 2024].

Green, W. and Lancaster, B. (2006) Over The Top Services. *Pipeline*, 4(7). Available at: http://www.pipelinepub.com/1207/pdf/Article_3.pdf [Accessed April 1st, 2024].

Greenwald, G. and MacAskill, E. (2013) "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, June 7. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Accessed July 22nd, 2024).

Hintz, E. and Winterberg, M. (2001) 'Die modernen Superstars als "Reforner" der Verfassung', *Zeitschrift fur Rechtpolitik*, 7, pp. 295.

Hoofnagle, C. J. (2003) "Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcemet", *North Carolina Journal of International Law*, Vol. 29 (4),pp.595-638.

Jones, M. (2017) "Right to a Human in the Loop: Political Constructions of Computer Automation & Personhood from Data Banks to Algorithms", *Social Studies of Science*, Vol 47 (2), pp. 216 – 239. Available at: http://dx.doi.org/10.2139/ssrn.2758160

Kantor, J. and Sundaram, A. (2022) "The rise of the worker productivity score", *The New York Times*, August 14. Available at: https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html (Accessed June 3rd, 2024).

Keegan, J. and Eastwood, J. (2023) "From 'heavy purchasers' of pregnancy tests to the depression-prone: We found 650,000 ways advertisers label you", *The Markup*, June 8. Available at: https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you (Accessed July 23rd, 2024).

Kelley, P. G., Bresee, J., Cranor, L. F. and Reeder, R. W. (2009) "A 'nutrition label' for privacy", *Proceedings of the USENIX symposium on usable privacy and security (SOUPS)*. Available at: https://doi.org/10.1145/1572532.1572538

Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J. and Deibert, R. (2020) "We chat, they watch how international users unwittingly build up wechat's Chinese censorship apparatus", Technical Report, *CitizenLab*. Available at: https://citizenlab.ca/2020/05/we-chat-they-watch/ (Accessed July 23rd, 2024)

Kokolakis, S. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security*, 64, pp.122-134

Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. *Journal of Risk Research*, pp. 1–14. Available at: https://doi.org/10.1080/13669877.2024.2350720

Leino-Kilpi, H., M. Välimäki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott, M. Arndt,Privacy: a review of the literature, *International Journal of Nursing Studies,* Volume 38, Issue 6, 2001, pp. 663-671. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404815001017?via%3Dihub (Accessed July 23rd, 2024).

Lex, G., Redeker, D. and Gasser, U. (2015) "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights", *Berkman Center Research Publication,* No. 2015-15. Available at: https://papers.ssrn.com/abstract=2687120 (Accessed June 4th, 2024)

Litman-Navarro, K. (2019) "We read 150 privacy policies. They were an incomprehensible disaster", *The New York Times*, June 12. Available at: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (Accessed July 23rd, 2024)

Lovato, J., Mueller, P., Suchdev, P. and Dodds, P. (2023) "More data types more problems: A temporal analysis of complexity, stability, and sensitivity in privacy policies", *Proceedings of the ACM conference on fairness, accountability, and transparency*, pp. 1088 – 1100. Available at: https://doi.org/10.1145/3593013.3594065

Madrigal, A. C. (2012) "Reading the privacy policies you encounter in a year would take 76 workdays." *The Atlantic*, March 1 . Available at: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ (Accessed June 3rd, 2024).

McDonald, A. M. and Cranor, L. F. (2008) "The cost of reading privacy policies", *I/S: A Journal of Law and Policy for the Information Society*, 4(3). Available at: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (Accessed June 3rd, 2024).

Norberg, P.A, Horne, D.R and Horne, D.A. (2007) "The privacy paradox: personal information disclosure intentions versus behaviors», *Journal of Consumer Affairs*, 41 (1), pp.100-126. Available at: https://doi.org/10.1111/j.1745-6606.2006.00070.x

Palen, L. and Dourish, P. (2003) "Unpacking "privacy" for a networked world", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Ft. Lauderdale, FL. pp. 129–136. Available at: https://doi:10.1145/642611.642635

Peck, D. (2013) "They're watching you at work", *The Atlantic,* December 15. Available at: https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/ (Accessed July 23rd, 2024)

Prem, E. (2024) "Principles of digital humanism: A critical post-humanist view", *Journal of Responsible Technology*, 17. Available at: https://www.sciencedirect.com/science/article/pii/S2666659624000015 (Accessed July 25th, 2024)

Reidenberg, J. (1998) "Lex Informatica: The Formulation of Information Policy Rules through Technology", *Texas Law Review*, 76. Available at: https://ir.lawnet.fordham.edu/faculty_scholarship/42/ (Accessed June 3rd, 2024)

Rojszczak, M. (2021) "The uncertain future of data retention laws in the EU: Is a legislative reset possible?" *Computer Law & Security Review*, Vol. 41. Available at: https://doi.org/10.1016/j.clsr.2021.105572

Rosenberg, M., Confessore, N. and Cadwalladr, C. (2018) "How Trump consultants exploited the Facebook data of millions", *The New York Times*, March 17. Available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (Accessed July 23rd, 2024)

Scuotto, V. (2023) "The digital humanism era triggered by individual creativity", *Journal of Business Research*, 158. Available at: https://doi.org/10.1016/j.jbusres.2023.113709

Szymielewicz, K. (2019) "Your digital identity has three layers, and you can only protect one of them", *Quartz*, January 25. Available at: https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them (Accessed July 23rd, 2024).

Tagliaro, C., Hahn, F., Sepe, R., Aceti, A. & Lindorfer, M. (2023) "I still know what you watched last Sunday: Privacy of the HbbTV protocol in the European smart TV landscape", Proceedings *of the annual network and distributed system security symposium* (NDSS) (Accessed July 23rd, 2024).

Terzis, P. (2024) "Against digital constitutionalism", *European Law Open*, pp. 1–17. Available at: https://doi:10.1017/elo.2024.15

Teubner, G. (2004) "Societal constitutionalism: Alternatives to state-centred constitutional theory?", in Joerges, C., Sand, I.-J. and Teubner, G. (eds) *Transnational Governance and Constitutionalism*. Oxford: Hart Publishing, pp. 3-28.

Teubner, G. (2018) Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory*? Journal of Law, 1(1)*. Available at: https://jlaw.tsu.ge/index.php/JLaw/article/view/2573 (Accessed August 21st, 2024).

Teubner, G. and Fischer-Lescano, A. (2024) "Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law", *Michigan Journal of International Law 25,* pp.999–1046. Available at: https://ssrn.com/abstract=873908 (Accessed June 4th, 2024).

Vienna Manifesto on Digital Humanism (2019). Available at: https://caiml.org/dighum/dighum-manifesto/ (Accessed July 25th, 2024).

Warren, S. & Brandeis, L. (1890)"The Right to Privacy", *Harvard Law Review*, 4. Available at: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (Accessed July 23rd, 2024).

Whittaker, Z. (2023) "US intelligence confirms it buys Americans' personal data", *TechCrunch*, June 13th. Available at: https://techcrunch.com/2023/06/13/us-intelligence-report-purchase-americans-personal-data/#:~:text=A%20newly%20declassified%20government%20report,web%20browsing%20data%2C%20and%20smartphones. (Accessed July 22nd, 2024).

Ακριβοπούλου, Χ. (2011) «Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από τον φακό του δικαιώματος στην ιδιωτική ζωή», *Θεωρία και Πράξη Διοικητικού Δικαίου*, 7, σσ. 679-691.

Δημοσιεύσεις Ευρωπαϊκής Ένωσης

Europol (2027) *Proportionate data retention for law enforcement purposes*, WK 9957/2017 INIT, LIMITE, 21 September. Available at: http://www.statewatch.org/news/2018/feb/eu-council-data-retention-europol-presentation-targeted-data-ret-wk-9957-17.pdf (Accessed May 1st, 2024).

Ευρωπαϊκή Επιτροπή (1992) *Τροποποιημένη Πρόταση για Οδηγία του Συμβουλίου σχετικά με την προστασία των ατόμων όσον αφορά την επεξεργασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων αυτών* (COM(92) 422 τελικό). Διαθέσιμο σε: https://op.europa.eu/en/publication-detail/-/publication/fba22cf4-be1a-41ca-b12a-4cb69f4d525f/language-en/format-PDF/source-342400756 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκή Επιτροπή (2021) *Πρόταση Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (πράξη για την τεχνητή νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης*. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52021PC0206 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο (2018) *Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής* (2015/2103(INL)). Διαθέσιμο σε : https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52017IP0051&from=EL
(Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (1995) *Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, L 281, σσ. 31-50. Διαθέσιμο σε: https://www.dpa.gr/sites/default/files/2020-05/CELEX_31995L0046_EL_TXT.pdf (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2000) *Οδηγία (ΕΕ) 2019/790 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για τα δικαιώματα πνευματικής ιδιοκτησίας και τα συγγενικά δικαιώματα στην ψηφιακή ενιαία αγορά και την τροποποίηση των οδηγιών 96/9/ΕΚ και 2001/29/ΕΚ*. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32019L0790 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2000) *Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)*. Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000L0031 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2002) *Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)*. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2006) *Οδηγία 2006/24/ΕΚ για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ*. Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2016), *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και για την κατάργηση της Οδηγίας 95/46/ΕΚ* (Γενικός Κανονισμός για την Προστασία Δεδομένων), L 119, σσ. 1-88. Διαθέσιμο

σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32016R0679 Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2017) *Πρόταση Κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58/ΕΚ (Κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες)* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2022) *Κανονισμός σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της Οδηγίας 2000/31/ΕΚ (πράξη για τις ψηφιακές υπηρεσίες).* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32022R2065 (Πρόσβαση 1η Ιουνίου 2024).

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ (2024) *Κανονισμός 2024/1689 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (Κανονισμός για την τεχνητή νοημοσύνη)* Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L_202401689 (Πρόσβαση 1η Ιουνίου 2024).

Μεταπτυχιακές εργασίες και διδακτορικές διατριβές

Suzor, N.P. (2010) *Digital constitutionalism and the role of the rule of law in the governance of virtual communities,* PhD thesis, Queensland University of Technology

Κίτσος, Π. (2011) *Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών* (διδακτορική διατριβή), Πανεπιστήμιο Μακεδονίας Οικονομικών και Κοινωνικών Επιστημών. Διαθέσιμο σε: https://www.didaktorika.gr/eadd/handle/10442/26521

Κουφάκη, Α. (2019) *Άρση απορρήτου ηλεκτρονικών επικοινωνιών και όρια των αποδεικτικών απαγορεύσεων,* Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Διαθέσιμο σε: https://pergamos.lib.uoa.gr/

Μπακιρτζόγλου,Χ. (2022) *Η νέα Πρόταση Κανονισμού για την Τεχνητή Νοημοσύνη και ζητήματα προσωπικών δεδομένων* (διπλωματική εργασία), Πανεπιστήμιο Πειραιά. Διαθέσιμο σε: https://dione.lib.unipi.gr/

Νικολάου,Ν. (2013) *Θεολογική ανθρωπολογία και βιοηθική* (διπλωματική εργασία), Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα

Τσίτσιρας, Χ., 2018. *Προτεινόμενος Κανονισμός ePrivacy για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες.* Τελική εργασία [online]. Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης. Διαθέσιμο σε: https://repositoryesdda.ekdd.gr/handle/123456789/283 [Πρόσβαση 6 Απριλίου 2023]

Νομολογία

European Court of Human Rights (2021) *Big Brother Watch and Others v. the United Kingdom,* Applications nos. 58170/13, 62322/14, and 24960/15, Judgment of the Court (Grand Chamber) of 25 May 2021. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-12080%22]} (Accessed May 1st,2024).

European Court of Justice (2008) *Productores de Música de España (Promusicae) v Telefónica de España SAU*. Case C-275/06, Judgment of the Court (Grand Chamber) of 29 January 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62006CJ0275 (Accessed May 1st,2024).

European Court of Justice (2010) *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08), Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08),* Joined cases C-236/08 to C-238/08, Judgment of the Court (Grand Chamber) of 23 March 2010. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62008CJ0236 (Accessed May 1st,2024).

European Court of Justice (2011) *L'Oréal SA and Others v eBay International AG and Others,* Case C-324/09, Judgment of the Court (Grand Chamber) of 12 July 2011. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CJ0324 (Accessed May

1st,2024).

European Court of Justice (2011) *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* Case C-70/10, Judgment of the Court (Third Chamber) of 24 November 2011. Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62010CJ0070 (Accessed May 1st,2024).

European Court of Justice (2014) *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* Joined cases C-293/12 and C-594/12, Judgment of the Court (Grand Chamber) of 8 April 2014. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 (Accessed May 1st,2024).

European Court of Justice (2014) *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, Judgment of the Court (Grand Chamber) of 13 May 2014**.** Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (Accessed May 1st,2024).

European Court of Justice (2014) *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH,* Case C-314/12, Judgment of the Court (Fourth Chamber) of 27 March 2014. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0314 (Accessed May 1st,2024).

European Court of Justice (2015) *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 (Accessed May 1st,2024).

European Court of Justice (2016) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* Joined cases C-203/15 and C-698/15, Judgment of the Court (Grand Chamber) of 21 December 2016. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62015CJ0203 (Accessed May 1st,2024).

European Court of Justice (2016) *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH,* Case C-484/14, Judgment of the Court (Third Chamber) of 15 September 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0484

(Accessed May 1st,2024).

European Court of Justice (2018) *Ministerio Fiscal*, Case C-207/16, Judgment of the Court (Grand Chamber) of 2 October 2018. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0207 (Accessed May 1st,2024).

European Court of Justice (2020) *La Quadrature du Net and Others v Premier ministre and Others,* Joined cases C-511/18, C-512/18, and C-520/18, Judgment of the Court (Grand Chamber) of 6 October 2020. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62018CJ0511 (Accessed May 1st,2024).

European Court of Justice (2020) *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* Case C-311/18, Judgment of the Court (Grand Chamber) of 16 July 2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311 (Accessed May 1st,2024).

European Court of Justice (2020), *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others,* Case C-623/1, Judgment of the Court (Grand Chamber) of 6 October 2020. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62017CJ0623 (Accessed May 1st,2024).

European Court of Justice (2021) *H.K. v Prokuratuur*, Case C-746/18, Judgment of the Court (Grand Chamber) of 2 March 2021. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62018CJ0746 (Accessed May 1st,2024).

Μονομελές Πρωτοδικείο Αθηνών (2002) Απόφαση 4701/2002, *ΔιΜΕΕ*, 2004, σ. 213.

Λοιπά Κείμενα

African Declaration on Internet Rights and Freedoms Coalition, n.d. *African Declaration on Internet Rights and Freedoms.* Available at: https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf (Accessed May 1st,2024).

Association for Progressive Communications (APC), n.d. *APC Internet Rights Charter*. Available at: https://www.apc.org/sites/default/files/APC_charter_EN_1.pdf (Accessed May 1st,2024).

British Council, n.d. *Magna Carta: My Digital Rights*. Available at: https://www.britishcouncil.org/sites/default/files/magna_carta_my_digital_rights.pdf (Accessed May 1st,2024).

Charter of Fundamental Digital Rights of the European Union, n.d. *Digital Charter*. Available at: https://digitalcharta.eu/sprachen/ (Accessed May 1st,2024).

Internet Principles and Rights Coalition, n.d. *The Charter of Human Rights and Principles for the Internet.* Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf (Accessed May 1st,2024).

Italian Parliament, n.d. *Declaration of Internet Rights*. Available at: https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf (Accessed May 1st,2024).

The Santa Clara Principles, n.d. *The Santa Clara Principles on Transparency and Accountability in Content Moderation*. Available at: https://santaclaraprinciples.org/ (Accessed May 1st,2024).