ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Αικατερίνης Αλεξανδροπούλου (Α.Μ.: 2102)

DARK PATTERNS, ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ, ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΑΤΑΝΑΛΩΤΗ ΣΤΟΝ ΨΗΦΙΑΚΟ ΧΩΡΟ: Η ΕΞΕΛΙΞΗ ΤΗΣ ΕΝΩΣΙΑΚΗΣ ΝΟΜΟΘΕΣΙΑΣ

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Ιούνιος 2023

ΠΕΡΙΛΗΨΗ

Ο όρος «σκοτεινά μοτίβα» δηλώνει επιλογές κυρίως στον σχεδιασμό και το κείμενο ιστοσελίδων και εφαρμογών σκόπιμα παραπλανητικές, χειριστικές και πιεστικές που εκμεταλλεύονται γνωστικούς μηχανισμούς και ανθρώπινες αδυναμίες και οδηγούν τους χρήστες σε ανεπιθύμητες επιλογές ή αποφάσεις που υπό άλλες συνθήκες δεν θα έπαιρναν αναφορικά με τα προσωπικά τους δεδομένα, προς όφελος των παρόχων online υπηρεσιών και ταυτόχρονα εις βάρος των δικών τους αληθινών συμφερόντων. Η ακαδημαϊκή έρευνα έχει παρουσιάσει μια σειρά από ορισμούς, χαρακτηριστικά και ταξινομήσεις των σκοτεινών μοτίβων. Η παρούσα εργασία αναλύει την εν λόγω έννοια και εξετάζει κατά πόσο ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), η Οδηγία ePrivacy και η Οδηγία για τις Αθέμιτες Εμπορικές Πρακτικές (ΟΑΕΠ) δύνανται να αντιμετωπίσουν επαρκώς τα σκοτεινά μοτίβα στον ψηφιακό χώρο. Καταλήγει ότι οι συγκεκριμένοι νόμοι αντιμετωπίζουν εν μέρει το θέμα, αλλά ότι η συνδυαστική τους εφαρμογή μπορεί να είναι αποτελεσματική. Επίσης, παρουσιάζει τη νέα και την επικείμενη νομοθεσία της ευρωπαϊκής έννομης τάξης που θα διέπει το ψηφιακό περιβάλλον και κρίνει ότι θέτει ορισμένες προκλήσεις, όμως η δημιουργική ερμηνεία των διατάξεων μπορεί να τις αντιμετωπίσει. Συμπληρωματικά προς τη νομοθετική ρύθμιση και τα μέτρα επιβολής, η εργασία προτείνει κυρίως την ανθρωποκεντρική προσέγγιση στον σχεδιασμό και την ευαισθητοποίηση των χρηστών.

Περιεχόμενα

1.ΕΙΣΑΓΩΓΗ

1.1 Παρουσίαση του προβλήματος και νομικά θέματα

Δαιδαλώδη μενού, προ-συμπληρωμένα τετραγωνίδια, cookie banners που δεν αφήνουν περιθώρια επιλογής, μακροσκελείς πολιτικές απορρήτου, διαφορετικά χρώματα και γραφικά είναι μερικά από τα μέσα που χρησιμοποιούν οι online[1] πλατφόρμες και άλλοι πάροχοι online υπηρεσιών (όπως οι Match.com και TurboTax) για να επηρεάσουν τις αποφάσεις των χρηστών[2] προς όφελος των πρώτων και εις βάρος των τελευταίων. Γνωστά ήδη στον αναλογικό κόσμο, διαδίδονται με μεγάλη ταχύτητα και χρησιμοποιούνται ευρύτατα και στον ψηφιακό. Πρόκειται για τα σκοτεινά μοτίβα (άλλως παραπλανητικός σχεδιασμός), ένα όρο που επινόησε ο Harry Brignull (2010), σχεδιαστής εμπειρίας χρήστη (UX), για να περιγράψει συγκεκριμένες επιλογές στον σχεδιασμό διεπαφής χρήστη (εφεξής UI)[3] ως «τεχνάσματα που χρησιμοποιούνται σε ιστοσελίδες και εφαρμογές και οδηγούν τους χρήστες σε ενέργειες που δεν σκόπευαν να κάνουν, όπως μια αγορά ή μια συνδρομή», δηλαδή σε *ενέργειες ανεπιθύμητες και απροσχεδίαστες*[4]. Έκτοτε ο νεολογισμός χρησιμοποιείται εκτενώς τα τελευταία χρόνια στην Ευρώπη και στις ΗΠΑ ως όρος-ομπρέλα (ΟΟΣΑ, 2022) για μεγάλο εύρος παραπλανητικών πρακτικών που σκόπιμα εκμεταλλεύονται γνωστικούς μηχανισμούς και ανθρώπινες αδυναμίες και οδηγούν τους χρήστες σε επιλογές που δεν τους συμφέρουν πραγματικά. Έχει απασχολήσει σχεδιαστές (Jaiswal, 2018, Brownlee, 2016, Brignull, 2010), ερευνητές (Jarovsky, 2022, Berbece, 2019), ακαδημαϊκούς (Waldman, 2020, Bösch et al., 2016), νομοθέτες, αρχές προστασίας προσωπικών δεδομένων (ΕΣΠΔ, 2022, CNIL, 2019), οργανισμούς προστασίας καταναλωτών (Forbrukerrådet, 2022, 2021, 2018, CMA, 2022, 2020) και ΜΚΟ (NOYB, 2021). Ο λόγος είναι ότι στον ψηφιακό κόσμο τα σκοτεινά μοτίβα καταλαμβάνουν όλο και μεγαλύτερη έκταση, γίνονται όλο πιο επιτηδευμένα και σύνθετα, άρα πιο δυσδιάκριτα και απειλητικά (ΟΟΣΑ, 2022, Επιτροπή 2022, US FTC, 2022).

Εμφανίζονται σε πολλά διαφορετικά σχήματα και σχέδια, καθώς χρησιμοποιούν ποικίλα στοιχεία σχεδιασμού ή κειμένου (ΕΣΠΔ, 2022, Forbrukerrådet, 2018) για να παρουσιάσουν ή να κρύψουν πληροφορίες. Ενδεικτικά εντοπίζονται σε ιστοσελίδες ηλεκτρονικού εμπορίου (Mathur et al., 2019, Moser et al., 2019), σε πλατφόρμες

[1] Η επιλογή της λέξης online αντί «επιγραμμική» είναι συνειδητή.

[2] Για τους σκοπούς της εργασίας οι όροι χρήστης, καταναλωτής και υποκείμενο των δεδομένων (εφεξής ΥΔ) εναλλάσσονται ελεύθερα ως συνώνυμοι.

[3] Το User Experience (UX) είναι η στρατηγική πίσω από τον σχεδιασμό ενός ψηφιακού προϊόντος και προσδιορίζει την αλληλεπίδραση του χρήστη με αυτό. Το User Interface (UI) είναι η οπτική υλοποίηση αυτής της διαδικασίας. Το User Journey (UJ) αφορά τα βήματα που εκτελούν οι χρήστες για την online περιήγηση, την ανάρτηση περιεχομένου ή τη ρύθμιση των προτιμήσεων τους.

[4] Η πλάγια γραφή κατά μήκος της εργασίας αποτελεί επιλογή της γράφουσας για έμφαση.

κοινωνικής δικτύωσης (ΕΣΠΔ, 03/2022, Forbrukerrådet, 2018), σε online παιχνίδια (Forbrukerrådet, 2022, Zagal, Björk and Lewis, 2013), σε μηχανές αναζήτησης (Forbrukerrådet, 2018), σε cookie banners (Matte, Bielova and Santos, 2020, Nouwens et al., 2020, Soe et al., 2020, Utz et al., 2019), σε πολιτικές απορρήτου (Gunawan et al., 2021, Bösch, 2016), κατά το opt-out από υπηρεσίες/e-mails (Liu, Iqbal and Saxena, 2023, Dev, Rader, and Patil, 2020, Habib et al., 2020, Habib et al., 2019) και σε εφαρμογές κινητών (Επιτροπή, 2022, Gunawan et al., 2021, Di Geronimo et al., 2020). Μάλιστα, ορισμένα σκοτεινά μοτίβα εντοπίζονται συχνότερα σε εφαρμογές κινητών παρά σε ιστοσελίδες (Gunawan et al., 2021), ενώ όσο δημοφιλέστερη είναι η υπηρεσία, τόσο πιθανότερη είναι η χρήση τους (Mathur et al., 2019) και δη η συνδυαστική (Επιτροπή, 2022, Forbrukerrådet, 2022, US FTC, 2022, CMA, 2022, Luguri and Strahilevitz, 2021). Το 2020 το 95% των 240 δημοφιλέστερων android εφαρμογών κινητού τηλεφώνου περιείχε τουλάχιστον ένα σκοτεινό μοτίβο και το 49% χρησιμοποιούσε πάνω από 7 σκοτεινά μοτίβα στις UI (Di Geronimo et al., 2020). Το 2021 οι 105 δημοφιλέστερες online υπηρεσίες της Google Play Store, διαθέσιμες σε ιστοσελίδες και σε εφαρμογές, περιείχαν ένα σκοτεινό μοτίβο και η πλειοψηφία χρησιμοποιούσε πάνω από 7 σκοτεινά μοτίβα (Gunawan et al., 2021). Το 2022 το 80% δημοφιλών παιδικών εφαρμογών περιελάμβανε ένα τουλάχιστον χειριστικό design feature (Radesky et al., 2022) και το 97% των 75 δημοφιλέστερων ευρωπαϊκών ιστοσελίδων και εφαρμογών κινητού περιείχε τουλάχιστον ένα σκοτεινό μοτίβο (Επιτροπή, 2022).

Οι πάροχοι online υπηρεσιών χρησιμοποιούν τα σκοτεινά μοτίβα για διάφορους σκοπούς. Κατά βάση επιδιώκουν να αποσπάσουν χρήμα, χρόνο, προσοχή, ενέργεια και δεδομένα προσωπικού χαρακτήρα (εφεξής προσωπικά δεδομένα) από τους χρήστες με απώτερο στόχο την αύξηση της κερδοφορίας τους (ΟΟΣΑ, 2022, Narayanan et al., 2020, CNIL, 2019, Harris, 2016, Zagal, Björk and Lewis, 2013). Αντίστοιχα, προκαλούν βλάβες στους χρήστες με πολλούς τρόπους (ΟΟΣΑ, 2022, Citron and Solove, 2022, Gunawan, Santos and Kamara, 2022, Mathur, Kshirsagar and Mayer, 2021, Zagal et al., 2013), η βαρύτητα των οποίων αυξάνεται, όταν αφορούν παιδιά (ΟΟΣΑ, 2022, ΕΣΠΔ, 03/2022). Σε συλλογικό επίπεδο επηρεάζουν τη συμπεριφορά, αφενός των καταναλωτών υπονομεύοντας τον ανταγωνισμό (Day and Stemler, 2020) και κλονίζοντας την εμπιστοσύνη στις ψηφιακές επιχειρήσεις (ΟΟΣΑ, 2022) αφετέρου των ψηφοφόρων υποσκάπτοντας ακόμα και τη δημοκρατία μέσω ψευδών ειδήσεων (Harris, 2016, Campbell-Dollaghan, 2016). Παράλληλα, η μεγάλη αποτελεσματικότητα των σκοτεινών μοτίβων που εντοπίζονται στα κινητά τηλέφωνα δημιουργεί ανησυχία για την όξυνση των κοινωνικών ανισοτήτων και την εκμετάλλευση ευάλωτων ομάδων, ιδίως εκείνων που χρησιμοποιούν αποκλειστικά ή κυρίως το κινητό τηλέφωνο για τη σύνδεση στο διαδίκτυο (Gunawan et al., 2021).

Σε ατομικό επίπεδο η οικονομική ζημία βέβαια είναι η πιο εύκολα αντιληπτή. Οι υπόλοιπες βλάβες είναι μη υλικές και πιο δυσδιάκριτες. Πρακτικές, όπως η συνεχής

κύλιση στις αρχικές σελίδες και η προεπιλεγμένη λειτουργία αυτόματης αναπαραγωγής πολλών υπηρεσιών, όπως το YouTube, απορροφούν τον χρόνο των χρηστών και καλλιεργούν τον εθισμό (Mathur, Kshirsagar and Mayer, 2021, Bongard-Blanchy et al., 2021). Επιπλέον, προκαλούν άνιση μεταχείριση μεταξύ των χρηστών, που μπορεί να φτάσει και σε αλγοριθμικές διακρίσεις με την εξέλιξη της τεχνολογίας (Leiser and Caruana, 2021), και γενικά αρνητικά συναισθήματα. Μελέτες έχουν δείξει ότι οι χρήστες νιώθουν θυμό εξαιτίας της υπερέκθεσης στα σκοτεινά μοτίβα και ενδέχεται να απομακρυνθούν από την online υπηρεσία (Luguri and Strahilevitz, 2021), ανησυχούν για τη σωματική και ψυχική υγεία τους λόγω εσφαλμένων αποφάσεων (Bongard-Blanchy et al., 2021), μετανιώνουν για τις επιλογές που έκαναν αναφορικά με την ιδιωτικότητα τους, αφότου κατάλαβαν ότι είχαν καλύτερες επιλογές (Machuletz and Böhme, 2020), δηλώνουν ενόχληση, αλλά ταυτόχρονα θεωρούν αδύνατο να αποφύγουν την online χειραγώγηση και ότι το αντάλλαγμα της (δωρεάν) υπηρεσίας υπερτερεί των αρνητικών συνεπειών (Maier and Harr, 2020), νιώθουν αγανάκτηση, όταν συναντούν ένα σκοτεινό μοτίβο (Bhoot, Shinde and Mishra, 2020) και θεωρούν ως πιθανές συνέπειες την κοινωνική πίεση και την αντικοινωνική συμπεριφορά (Zagal et al., 2013).

Επιπλέον, τα περισσότερα σκοτεινά μοτίβα, αν όχι όλα, επηρεάζουν ουσιωδώς την αυτονομία και στρεβλώνουν την ικανότητα λήψης απόφασης των χρηστών (Mathur, Kshirsagar and Mayer, 2021). Μελέτη το 2021 παρατήρησε ότι το ποσοστό των καταναλωτών που πείστηκε με τη χρήση σκοτεινών μοτίβων να πραγματοποιήσει συνδρομή σε μια αμφίβολη υπηρεσία ήταν το διπλάσιο έως και τετραπλάσιο σε σχέση με το ποσοστό των καταναλωτών που δεν εκτέθηκαν σε αυτά (Luguri and Strahilevitz, 2021).

Παράλληλα, ο παραπλανητικός σχεδιασμός γεννά προβληματισμούς για την ιδιωτικότητα (privacy) και την ασφάλεια των προσωπικών δεδομένων των χρηστών. Αυτοί συχνά έχουν την ψευδαίσθηση του ελέγχου, αλλά στην πραγματικότητα το μενού των προσφερόμενων επιλογών ελέγχεται από τις online πλατφόρμες (Harris, 2016), που τους εκμεταλλεύονται με στόχο την τροφοδότηση ενός επιχειρηματικού μοντέλου «που διψά για πληροφορίες» (Waldman, 2020). Πράγματι, οι μεγάλες online πλατφόρμες χρησιμοποιούν τακτικές, όπως τις προεπιλεγμένες ρυθμίσεις, την χρήση συναισθηματικά φορτισμένης ή και επιθετικής γλώσσας, τον καταιγισμό ή την απόκρυψη πληροφοριών, τον μεγάλο αριθμό κλικ που απαιτούνται για την επιλογή φιλικών προς την ιδιωτικότητα του χρήστη επιλογών και τα εμπόδια σε μια ακύρωση υπηρεσίας ή σε ένα εύκολο opt-out οδηγώντας τους χρήστες να αποκαλύπτουν περισσότερα προσωπικά δεδομένα από όσα σκοπεύουν και θέτοντας την αυτονομία τους σε μεγαλύτερο κίνδυνο. Αυτές οι τακτικές εντοπίζονται και σε πολλά cookie banners/notices, που ουσιαστικά αποτελούν αιτήματα συγκατάθεσης σε διάφορους σκοπούς επεξεργασίας μέσω των cookies-μικρών αρχείων κειμένου με πληροφορίες-και που εγκαθίστανται στη συσκευή του χρήστη από τον πάροχο (Kampanos and

Shahandashti, 2021, Soe et al., 2020, Di Geronimo et al., 2020, Nouwens et al., 2020, Utz et al., 2019, Machuletz and Böhme, 2019). Ήδη από το 2019 ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων επέστησε την προσοχή των κρατών μελών στο θέμα αναφερόμενος στα σκοτεινά μοτίβα ως ένα μέσο που διαθέτουν οι επιχειρήσεις και τείνει να καθιερωθεί για να «*ωθούν ανελέητα* τους καταναλωτές να αγνοήσουν την ιδιωτική τους ζωή και να παρέχουν περισσότερα προσωπικά δεδομένα από όσα χρειάζεται» (Buttarelli, 2019).

Ωστόσο, προκύπτουν αρκετές δυσκολίες κατά την προσπάθεια αντιμετώπισης του προβλήματος. Η έννοια τους δεν έχει αποκρυσταλλωθεί πλήρως ακόμα, ώστε δεν υπάρχει ούτε ένας ορισμός ούτε μία μοναδική ταξινόμηση. Παρόλο που το Συμβούλιο της Ευρωπαϊκής Ένωσης (εφεξής ΕΕ) διακηρύσσει (2021) πως «ό,τι είναι παράνομο εκτός διαδικτύου είναι παράνομο και στο διαδίκτυο» και οι τεχνικές των σκοτεινών μοτίβων είναι ήδη γνωστές στον αναλογικό κόσμο, τα όρια μεταξύ πειθούς και παραπλάνησης είναι αρκετά ρευστά ιδίως στο online περιβάλλον. Η επιχειρηματική ελευθερία των παρόχων, που κατοχυρώνεται από το άρθρο 16 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ (εφεξής Χάρτης) περιλαμβάνει την ελευθερία του σχεδιασμού και της διαφήμισης (Egberts, 2021), ενώ η νομοθεσία χάριν της τεχνολογικής καινοτομίας ή εξαιτίας συνεχών εξελίξεων στις εμπορικές πρακτικές είναι γενικά διστακτική να ρυθμίσει σχολαστικά τον σχεδιασμό (Jarovsky, 2022). Ενδεχομένως, το κακόβουλο κίνητρο και η χειριστική συμπεριφορά μπορούν να διακρίνουν ένα σκοτεινό μοτίβο από μία πολύ πειστική στρατηγική μάρκετινγκ. Μια πειστική προσέγγιση των χρηστών είναι θεμιτή όταν απλώς τους ενημερώνει ή τους ωθεί προς μία θετική συμπεριφορά, αλλά είναι χειριστική, όταν εκμεταλλεύεται τον σχεδιασμό της UI και την ψυχολογία τους, στοχεύοντας σε τρωτά σημεία που θα επηρεάσουν αρνητικά τη συμπεριφορά τους και την αυτονομία τους (Επιτροπή, 2022). Από την άλλη, μολονότι αυτές οι παραπλανητικές τακτικές έχουν χαρακτηριστεί και ως ανήθικες (Forbrukerrådet, 2018, Narayanan et al., 2020, Soe et al., 2020) και υπάρχει πλήθος μελετών για τη σχέση της ηθικής με τα σκοτεινά μοτίβα (Gray, Chivukula and Lee, 2020, Chivukula et al., 2020, Maier and Harr, 2020, Gray and Chivukula, 2019, Gray et al., 2018, Campbell-Dollaghan, 2016, Zagal et al., 2013), ούτε η ηθική είναι ασφαλές κριτήριο, αφού είναι σχετική μεταξύ χωρών και ανθρώπων (Επιτροπή, 2022, Jarovsky, 2020). Επιπλέον, δεν είναι ακόμα σαφές πόσο επηρεάζεται ο κάθε χρήστης, αφού παίζουν ρόλο οι περιστάσεις, ο βαθμός αντίληψης, η ιεράρχηση των αξιών (Επιτροπή, 2022) και το υπόβαθρο του καθενός, ενώ ειδικά για την ιδιωτικότητα, είναι πολύ δύσκολο να εκτιμηθεί το μέγεθος της βλάβης (Gunawan, Santos and Kamara, 2022, Acquisti et al., 2017). Η σχετική νομολογία ακόμα είναι ελλιπής. Τα δικαστήρια δυσκολεύονται να αναγνωρίσουν τις σχετικές βλάβες της ιδιωτικότητας, διότι συχνά δεν συνδέονται με απτή οικονομική ή σωματική βλάβη (Citron and Solove, 2022).

Έτσι, η κατά περίπτωση αξιολόγηση προβάλλει ως μόνη λύση (ΕΣΠΔ, 2023, ΕΣΠΔ, 03/2022, Επιτροπή 2022, Gunawan, Santos and Kamara, 2022, Forbrukerrådet, 2018), αφού

οι περισσότερες πρακτικές σχεδιασμού αποτελούν *γκρίζα ζώνη* (Egberts, 2021), εξαρτώνται από τον χρόνο, τον τρόπο και τα υπό εξέταση δεδομένα (CNIL, 2019) και δεν μπορούν να θεωρηθούν per se παράνομες ή αθέμιτες με εξαίρεση ορισμένες που υπάγονται με ασφάλεια σε συγκεκριμένες διατάξεις νόμων, όπως του Γενικού Κανονισμού Προστασίας Δεδομένων (εφεξής ΓΚΠΔ) ή της Οδηγίας για τις Αθέμιτες Εμπορικές Πρακτικές (εφεξής ΟΑΕΠ). Από την άλλη, αν τα κριτήρια χαρακτηρισμού μιας πρακτικής ως σκοτεινού μοτίβου είναι χαλαρά, ελλοχεύει ο κίνδυνος να υποβαθμιστεί τελικά το πρόβλημα: «αν όλα είναι σκοτεινά μοτίβα, τότε τίποτα δεν είναι σκοτεινό μοτίβο» (Goanta and Santos, 2023). Το τρέχον νομικό οπλοστάσιο της ΕΕ, ιδίως αυτό που αφορά την προστασία των προσωπικών δεδομένων και του καταναλωτή ρυθμίζει ήδη μερικώς το θέμα με ερμηνεία και επικαιροποίηση των διατάξεων, ενώ μια σειρά από νέα νομοθετήματα, που περιλαμβάνουν συγκεκριμένες αναφορές στα σκοτεινά μοτίβα αναμένονται να ενισχύσουν τον αγώνα κατά αυτών (Επιτροπή, 2022, ΟΟΣΑ, 2022, Brignull, χ.χ.). Παράλληλα, ιδιαίτερα χρήσιμες είναι διάφορες συστάσεις και κατευθυντήριες οδηγίες που εκδίδουν το ΕΣΠΔ και άλλες αρχές (ΕΣΠΔ, 2023, US FTC 2022, ΕΣΠΔ, 03/2022, Επιτροπή, 2022 και 2021, CNIL, 2019), ενώ η αυστηρότητα των προστίμων που επιβάλλονται τελευταία ενισχύουν την υπάρχουσα νομοθεσία και καταδεικνύουν τη σοβαρότητα που αποδίδουν οι αρμόδιες αρχές στο θέμα.

1.2 Τα δικαιώματα που διακυβεύονται

Καθώς βασικός σκοπός της εργασίας είναι η διερεύνηση της σχέσης των σκοτεινών μοτίβων με την ιδιωτικότητα, σκόπιμη είναι η αποσαφήνιση της έννοιας.

Στην ευρωπαϊκή έννομη τάξη η προστασία των δεδομένων είναι θεμελιώδες δικαίωμα, στενά συνδεόμενο αλλά και διακριτό από το εξίσου θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Το πρώτο κατοχυρώνεται από το πρωτογενές δίκαιο της ΕΕ και συγκεκριμένα από το άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (εφεξής ΣΛΕΕ) και το άρθρο 8 του Χάρτη. Σε επίπεδο παραγώγου δικαίου διασφαλίζεται από τον ΓΚΠΔ. Το δεύτερο αναγνωρίζεται από το άρθρο 7 του Χάρτη, το οποίο προστατεύει και το απόρρητο των επικοινωνιών και μετά θεσπίστηκε η Οδηγία σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (εφεξής Οδηγία ePrivacy). Το δικαίωμα του άρθρου 8 είναι ευρύτερο από το δικαίωμα του άρθρου 7, διότι ενεργοποιείται κάθε φορά που πραγματοποιείται επεξεργασία των προσωπικών δεδομένων και ανεξάρτητα από τη σχέση του και τον αντίκτυπο στην ιδιωτική ζωή (FRA και Συμβούλιο της Ευρώπης, 2019). Είναι δικαίωμα ενεργό, καθώς απαιτεί την καθιέρωση ενός συστήματος ελέγχων και ισορροπιών για την προστασία των προσώπων κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Από την άλλη, το άρθρο 7 έχει χαρακτήρα κατ'αρχήν γενικής απαγόρευσης των επεμβάσεων. Παράλληλα, η έννοια της ιδιωτικής ζωής έχει ερμηνευθεί με ευρύτητα από τη νομολογία, ώστε να καλύπτει «προσωπικές καταστάσεις, ευαίσθητες ή εμπιστευτικές

πληροφορίες, οι οποίες θα μπορούσαν να επηρεάσουν αρνητικά την αντίληψη του κοινού για ένα πρόσωπο, αλλά ακόμη και πτυχές της επαγγελματικής ζωής και της δημόσιας συμπεριφοράς προσώπου» (FRA και Συμβούλιο της Ευρώπης, 2019). Αμφότερα τα άρθρα, πάντως, προστατεύουν την αυτονομία και την ανθρώπινη αξιοπρέπεια.

Η αλματώδης ανάπτυξη του διαδικτύου, των τηλεπικοινωνιών και της Κοινωνίας της Πληροφορίας οδήγησαν σε μια νέα αντίληψη περί ιδιωτικής ζωής, γνωστή ως *πληροφοριακή ιδιωτικότητα* ή *δικαίωμα στην πληροφοριακή αυτοδιάθεση*, προκειμένου να διασφαλιστούν τα προσωπικά δεδομένα από τους νέους κινδύνους. Η ιδιωτικότητα είναι άμεσα συνυφασμένη με την *αυτονομία*, την ικανότητα του ανθρώπου να διαμορφώνει και να ζει τη ζωή του σύμφωνα με τις αποφάσεις και τις επιλογές του (Day and Stemler, 2020). Ταυτόχρονα σηματοδοτεί την αξίωση του ατόμου στην απόσυρση– «*the right to be left alone*» (Brandeis and Warren, 1890)– και στο σεβασμό του απορρήτου του. Το δε δικαίωμα του πληροφοριακού αυτοκαθορισμού συνεπάγεται ότι κάθε άτομο είναι ελεύθερο να προσδιορίζει ποιες πληροφορίες από αυτές που το αφορούν θα κοινοποιηθούν στο περιβάλλον του. Ωστόσο, η ιδιωτικότητα δε νοείται αποκομμένη από την κοινωνία (Solove, 2006). Χωρίς την συνύπαρξη και τις τριβές που σημειώνονται εντός της κοινωνίας δεν θα υπήρχε ανάγκη για ιδιωτικότητα (Solove, 2006). Υπάρχουν πολλές απόψεις που την περιγράφουν ως «δημόσιο αγαθό, ανθρώπινο δικαίωμα ή πτυχή της ιδιωτικής αυτονομίας» (Mathur, Kshirsagar and Mayer, 2021). Συνεπώς, η διαφύλαξή της είναι κρίσιμη τόσο σε ατομικό όσο και σε συλλογικό επίπεδο. Στην ελληνική έννομη τάξη καθιερώνεται στο άρθρο 9Α του Ελληνικού Συντάγματος, στο οποίο αναγνωρίζεται ως ιδιαίτερη πτυχή του δικαιώματος της προσωπικότητας (άρθρο 5 παρ.1) και συνδέεται άμεσα με τον σεβασμό και την προστασία της αξίας του ανθρώπου (άρθρο 2 παρ.1). Για χάρη της ευχερούς ανάγνωσης οι όροι της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων εναλλάσσονται ως συνώνυμοι, παρόλο που δεν ταυτίζονται.

Παράλληλα, το άρθρο 38 του Χάρτη εξασφαλίζει υψηλό επίπεδο προστασίας των καταναλωτών. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (Hunstinx, 2014) έχει υποστηρίξει ότι το ρυθμιστικό πλαίσιο της προστασίας δεδομένων και αυτό του καταναλωτή εξυπηρετούν κοινούς σκοπούς, μεταξύ άλλων της ενίσχυσης της ανάπτυξης, της καινοτομίας και της ευημερίας των καταναλωτών. Πράγματι, η μεταξύ τους σύνδεση είναι φανερή τόσο από το γεγονός ότι η συλλογή και επεξεργασία των προσωπικών δεδομένων των χρηστών είναι το αντίτιμο για τις «δωρεάν» υπηρεσίες της Κοινωνίας της Πληροφορίας (Κατευθυντήριες Επιτροπής, 2021), αλλά και από το ότι μοιράζονται κοινές αρχές, όπως τη διαφάνεια και την αντικειμενικότητα.

1.3 Ο στόχος και η συμβολή της εργασίας

Παρά το αυξανόμενο ενδιαφέρον για τα σκοτεινά μοτίβα η υπάρχουσα βιβλιογραφία προσφέρει κυρίως ορισμούς, παραδείγματα και ταξινομήσεις αυτών των πρακτικών ενώ οι πιο πρόσφατες και σημαντικές δημοσιεύσεις της Επιτροπής (2022) και του ΟΟΣΑ (2022) εστιάζουν κυρίως στη φύση των σκοτεινών μοτίβων ως αθέμιτων εμπορικών πρακτικών και στη βλάβη που προκαλούν στους καταναλωτές. Δεδομένου όμως ότι η σημερινή οικονομία και η online διαφήμιση στηρίζονται στη συλλογή και στην επεξεργασία των προσωπικών δεδομένων των χρηστών η παρούσα διπλωματική αναγνωρίζει την προαναφερθείσα βλάβη, αλλά προχωρεί πιο πέρα και διερευνά εκτενώς την σχέση των σκοτεινών μοτίβων με την προστασία των προσωπικών δεδομένων και το απόρρητο. Επιπλέον, παρουσιάζει τη νέα και επικείμενη νομοθεσία, που επιβάλλει υποχρεώσεις στις online πλατφόρμες και περιέχει συγκεκριμένες διατάξεις κατά των σκοτεινών μοτίβων. Έτσι, η συμβολή της εργασίας είναι τριπλή: προσφέρει μία ενημερωμένη βιβλιογραφική ανασκόπηση επί του θέματος, εξετάζει πώς η τρέχουσα -και δη ο ΓΚΠΔ-, η νέα και η επικείμενη νομοθεσία αντιμετωπίζουν το πρόβλημα και επιδιώκει να ενισχύσει την ευαισθητοποίηση των χρηστών καταδεικνύοντας ότι το θέμα ενδιαφέρει και αφορά όλους τους χρήστες, επιχειρήσεις και ιδιώτες, κυβερνώντες και κυβερνώμενους. Για αυτό και στο τέλος προτείνει διάφορα μέτρα επιπλέον της νομοθεσίας που προϋποθέτουν την ενεργή συμμετοχή όλων των εμπλεκομένων. Με αυτό τον τρόπο το παρόν έργο παρέχει μία ενιαία και διαθέσιμη προς όλους πηγή γνώσης και την αφορμή για περαιτέρω εμβάθυνση.

1.4 Το ερευνητικό ερώτημα

Τα σκοτεινά μοτίβα είναι σύνθετο θέμα. Η προσέγγισή τους προϋποθέτει μια διεπιστημονική ανάλυση μεταξύ των επιστημών του προγραμματισμού, του σχεδιασμού, της επικοινωνίας μεταξύ ανθρώπου και υπολογιστή (HCI), των υπολογιστών, της ψυχολογίας, των συμπεριφορικών οικονομικών, της ηθικής και του δικαίου. Ταυτόχρονα, η βλάβη που προκαλούν σημειώνεται σε πολλαπλά επίπεδα. Αναφορικά ιδίως με τον χώρο του δικαίου, πλήθος διατάξεων προερχόμενων από διάφορους τομείς θα μπορούσαν με κατάλληλη ερμηνεία να αντιμετωπίσουν το θέμα, όπως, το δίκαιο της πνευματικής ιδιοκτησίας, του ανταγωνισμού και των συμβάσεων (Berbece, 2019). Λόγω των περιορισμών που θέτουν η έκταση και το πεδίο εφαρμογής της η εργασία προσανατολίζεται κυρίως στην παρουσία των σκοτεινών μοτίβων στον ψηφιακό χώρο και στις επιπτώσεις τους στην ιδιωτικότητα. Για αυτό διερευνά αρχικά την έννοια τους και στη συνέχεια πώς ο ΓΚΠΔ και η Οδηγία ePrivacy μπορούν να τα αντιμετωπίσουν, καίτοι δεν αναφέρονται ρητά σε αυτά. Η εξέταση του εν λόγω ερωτήματος αναδεικνύει την οικονομική αξία των προσωπικών δεδομένων και τη σύνδεση με το δίκαιο των καταναλωτών. Έτσι, γεννώνται δευτερευόντως τα ερωτήματα αν η ΟΑΕΠ αλληλεπιδρά με τους άλλους δύο νόμους και αν αντιμετωπίζει επαρκώς το πρόβλημα. Παράλληλα, η ψήφιση νέων νόμων που στοχεύουν σε ένα ασφαλέστερο ψηφιακό περιβάλλον εγείρει το ερώτημα αν ενισχύει την προστασία των προσωπικών

δεδομένων από τα σκοτεινά μοτίβα και αν υπάρχουν πρόσθετα μέτρα που μπορούν να ληφθούν.

1.5 Η μέθοδος της εργασίας

Η παρούσα εργασία εκπονήθηκε βάσει της βιβλιογραφικής ανασκόπησης. Για τους σκοπούς της συγγραφής συνελέγη το απαραίτητο υλικό με αναζήτηση στην ξενόγλωσση βιβλιογραφία και αρθρογραφία, στη νομοθεσία και στη νομολογία της ΕΕ, καθώς και στις αποφάσεις εποπτικών αρχών με τη χρήση λέξεων–κλειδιών, όπως dark patterns και deceptive design. Για την κατανόηση της θεματικής αντλήθηκαν παραδείγματα από cookie banners, πολιτικές απορρήτου και μεγάλες online πλατφόρμες, ενώ συγκεντρώθηκαν εικόνες από την υπό εξέταση βιβλιογραφία αλλά και από προσωπική αναζήτηση στο διαδίκτυο. Στη συνέχεια, το εν λόγω υλικό έτυχε μεθοδικής επεξεργασίας, ώστε να υποστηρίξει τη νομική ανάλυση των σκοτεινών μοτίβων, να προσδιορίσει πώς η υπάρχουσα και η επικείμενη νομοθεσία αντιμετωπίζει τις επιπτώσεις αυτών των παραπλανητικών πρακτικών, να προτείνει άλλα μέτρα επιπλέον της νομοθεσίας και να διατυπώσει ορισμένα συμπεράσματα.

1.6 Η δομή της εργασίας

Αρχικά, η εργασία παρακολουθεί την εξέλιξη του ορισμού των σκοτεινών μοτίβων, ανιχνεύει τα κίνητρα που κρύβονται πίσω από τη χρήση τους, εξηγεί την αποτελεσματικότητά τους και πώς εκμεταλλεύονται τα τρωτά σημεία των χρηστών και καταγράφει τη στάση των χρηστών.

Στη συνέχεια, αναφέρεται εν συντομία στο παράδειγμα της αμερικανικής έννομης τάξης και εξετάζει πώς ο ΓΚΠΔ και η Οδηγία ePrivacy αντιμετωπίζουν τα σκοτεινά μοτίβα. Η εργασία παρουσιάζει επίσης την ΟΑΕΠ, προκειμένου να διαμορφωθεί μια σφαιρική εικόνα του προβλήματος και της προσπάθειας επίλυσής του.

Ακολούθως, παρουσιάζει τη νέα και επικείμενη νομοθεσία της ΕΕ, η οποία στοχεύει σε έναν ασφαλέστερο ψηφιακό χώρο και στην προστασία των δικαιωμάτων των χρηστών. Ειδικότερα, παρουσιάζει τις Digital Services Act, Digital Market Act και τις Προτάσεις των AI Act και Data Act και αναφέρεται στην Data Governance Act.

Τέλος, προτείνει διάφορα μέτρα επιπλέον της νομοθεσίας και της επιβολής της που προϋποθέτουν την ενεργή συμμετοχή όλων των εμπλεκομένων και καταλήγει σε ορισμένα συμπεράσματα και προβληματισμούς.

2. ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΩΝ ΣΚΟΤΕΙΝΩΝ ΜΟΤΙΒΩΝ

2.1 Η έννοια του μοτίβου

Η ιδέα του μοτίβου (pattern) ξεκίνησε από τον χώρο της αρχιτεκτονικής και σύντομα εισήχθη στην επιστήμη των υπολογιστών και ανάπτυξης λογισμικού (Bösch et al., 2016). Στόχος ενός μοτίβου είναι να συλλάβει το παράδειγμα ενός προβλήματος και της λύσης του, να το απομονώσει από μία συγκεκριμένη περίπτωση χρήσης και να το γενικεύσει, ώστε να μπορεί να εφαρμοστεί σε παρόμοιες περιστάσεις. Στον αντίποδα βρίσκονται τα

αντι-μοτίβα (anti-patterns) και τα σκοτεινά μοτίβα. Τα πρώτα συνιστούν πρακτικές που πρέπει να αποφεύγονται, επειδή αποδεδειγμένα είναι εσφαλμένες. Τα δε σκοτεινά μοτίβα κατά τον Brignull (2013) δεν προκύπτουν ούτε κατά λάθος ούτε κατά τύχη, αλλά έχουν σχεδιαστεί προσεκτικά βάσει μιας βαθιάς κατανόησης της ανθρώπινης ψυχολογίας και δεν αποβλέπουν στο συμφέρον των χρηστών.

2.2 Η γέννηση και η εξέλιξη του ορισμού

Ο Brignull δημιούργησε την ιστοσελίδα darkpatterns.org (τώρα: https://www.deceptive.design/) για να ενισχύσει την ευαισθητοποίηση γύρω από τα σκοτεινά μοτίβα και τις συνέπειές τους, καθώς και για να στιγματίσει τις εταιρείες που τα χρησιμοποιούν. Για αυτό, ταξινόμησε πρώτος στο hall of shame της ιστοσελίδας δώδεκα παραδείγματα παραπλανητικού σχεδιασμού[5]:

1. Ερωτήσεις–παγίδα (Trick-questions): Κατά τη συμπλήρωση μιας φόρμας οι ερωτήσεις ξεγελούν τον χρήση να δώσει μια ανεπιθύμητη απάντηση. Όμως, η προσεκτική ανάγνωση αποκαλύπτει ότι ζητούν κάτι άλλο από αυτό που φαινόταν στην αρχή. Συνήθως χρησιμοποιούν διφορούμενη γλώσσα και διπλές αρνήσεις για την απόρριψη της συγκατάθεσης ή αλλάζουν τη σειρά των επιλογών, ώστε πρώτο να προσφέρεται το opt-out και δεύτερο το opt-in (Brignull, 2011, Mathur, Kshirsagar and Mayer, 2021, CNIL, 2019). Εναλλακτικά υπάρχει το Trick wording που αναφέρεται στη γενικά συγκεχυμένη ή παραπλανητική γλώσσα του κειμένου.
2. Κρυφή προσθήκη στο καλάθι (Sneak into the basket): Κατά τη διάρκεια μιας αγοράς και μέχρι την ολοκλήρωσή της η ιστοσελίδα εισάγει κρυφά ένα επιπλέον αντικείμενο στο καλάθι του χρήστη ή τον παρασύρει να δαπανήσει περισσότερα από όσα είχε υπολογίσει. Παρόμοια μοτίβα είναι τα Hidden costs και Hidden Subscription, (Mathur, A. et al., 2019) και το Chameleon Strategy (CNIL, 2019).
3. Roach motel: Ο χρήστης εμπλέκεται πολύ εύκολα σε μια κατάσταση, από την οποία είναι πολύ δύσκολο – σχεδόν αδύνατον- να απαλλαγεί. Χαρακτηριστικό παράδειγμα αποτελεί η Amazon της οποίας η πολιτική αποσύνδεσης από την υπηρεσία Prime ήταν πολύ δύσκολη, συμπεριλαμβανομένων περίπλοκων μενού πλοήγησης, αμφίσημης διατύπωσης, μπερδεμένων επιλογών και επαναλαμβανόμενων προτροπών (Forbrukerrådet, 2021). Παρόμοια μοτίβα είναι το Hard to cancel/opt-out (ΟΟΣΑ, 2022), τα Dead End και Longer than necessary, (ΕΣΠΔ, 03/2022), το Ease (Forbrukerrådet, 2018), το Obstruction (Gray et al., 2018) και το Immortal accounts (Bösch et al., 2016). Άλλο παράδειγμα αποτελούν τα πολλά κλικ που απαιτούνται για την επιλογή φιλικών προς την ιδιωτικότητα του χρήστη ρυθμίσεων σε αντίθεση με το ένα κλικ που απαιτεί η αποδοχή όλων των

[5] Επιλέγεται η πλήρης αναφορά στην πρώτη ταξινόμηση των σκοτεινών μοτίβων παρόλο που δεν απειλούν όλα άμεσα την ασφάλεια των προσωπικών δεδομένων χάριν ευχερέστερης και πληρέστερης κατανόησης του θέματος.

cookies και σε συνδυασμό ενδεχομένως με τον τρόπο απεικόνισης των επιλογών (π.χ. αφενός εμφανίζεται ένα μεγάλο φωτεινό και έντονο κουμπί «Αποδοχή όλων», αφετέρου η γραμματοσειρά στο κουμπί «Απόρριψη όλων» είναι μικρή και αχνή).

4. Privacy Zuckering: Ο χρήστης παρασύρεται και κοινοποιεί περισσότερα προσωπικά δεδομένα από όσα αρχικά σκόπευε. Το όνομα προέρχεται από τον CEO της Facebook, Mark Zuckerberg, επειδή παλιότερα η Facebook δυσκόλευε τον έλεγχο των ρυθμίσεων απορρήτου εκ μέρους των χρηστών, αλλά διευκόλυνε την εκτεταμένη κοινοποίηση των δεδομένων (Forbrukerrådet, 2018). Σήμερα η τακτική αυτή εκτυλίσσεται κυρίως παρασκηνιακά, στη μεσιτεία δεδομένων και στο σύστημα υποβολής προσφορών σε πραγματικό χρόνο (Real Time Bidding).
5. Παρεμπόδιση σύγκρισης τιμών (Comparison Prevention): Ο πάροχος υπηρεσίας εμποδίζει τον χρήστη να συγκρίνει τις τιμές των προϊόντων, ώστε να μην μπορεί να πάρει μία τεκμηριωμένη απόφαση. Συνήθως, δημιουργεί διαφορετικά πακέτα, στα οποία δεν είναι εύκολο να υπολογιστεί η τιμή μονάδας. Παρόμοιο μοτίβο είναι το Comparison obfuscation (CNIL, 2019).
6. Ετεροκατεύθυνση (Misdirection): Ο σχεδιασμός της ιστοσελίδας στρέφει σκόπιμα την προσοχή του χρήστη σε ένα συγκεκριμένο στοιχείο για να τον αποσπάσει από ένα άλλο. Αυτό επιτυγχάνεται με παρεμβολές εντός της UI (Interface interference, Gray et al., 2018), όπως είναι ο διαφορετικός χρωματισμός και η θέση των προσφερόμενων επιλογών μέσα στη UI, το μέγεθος της γραμματοσειράς, τα μακροσκελή (νομικά) κείμενα και τα πολλά κλικ. Στο ίδιο αποτέλεσμα οδηγούν η Απόκρυψη των πληροφοριών, οι Προεπιλογές και η χρήση συναισθηματικά φορτισμένου λεξιλογίου (ΟΟΣΑ, 2022, Gray et al., 2018). Παρόμοια μοτίβα είναι τα Look over there (ΕΣΠΔ, 03/2022), Attention diversion (CNIL, 2019), Aesthetic Manipulation (Gray et al., 2018).
7. Κρυφά κόστη (Hidden costs): Ο χρήστης φτάνει στην ολοκλήρωση της αγοράς και ανακαλύπτει ορισμένες αναπάντεχες χρεώσεις, όπως έξοδα αποστολής και φόρους. Όμως, το πιθανότερο είναι ότι ο χρήστης θα προχωρήσει στην αγορά επειδή θα έχει ήδη αφιερώσει χρόνο για αυτή και δεν θα αναζητήσει το προϊόν σε άλλη ιστοσελίδα. Μοιάζει με την Κρυφή προσθήκη στο καλάθι.
8. Δόλωμα και μεταστροφή (Bait and Switch): Ο χρήστης σκοπεύει να κάνει κάτι, αλλά τελικά συμβαίνει κάτι άλλο διαφορετικό και ανεπιθύμητο. Το πιο γνωστό παράδειγμα είναι η αναβάθμιση των Windows 10. Σε αντίθεση με όλες τις προηγούμενες εκδόσεις, όπου το κουμπί «Χ» πάνω δεξιά δήλωνε το «κλείσιμο», στη συγκεκριμένη περίπτωση ισοδυναμούσε με αποδοχή της αναβάθμισης (Brownlee, 2016). Παρόμοια μοτίβα είναι τα Wrong signal και Bait and change (CNIL, 2019).
9. Confirmshaming: Η ιστοσελίδα καλλιεργεί σκόπιμα το αίσθημα της ντροπής, της ενοχής ή του φόβου στον χρήστη για να τον οδηγήσει προς μία επιλογή. Κυρίως τον ενθαρρύνει να κάνει opt-in ή τον αποτρέπει από opt-out. Παρόμοια μοτίβα

είναι τα Emotional steering (ΕΣΠΔ, 03/2022), Blaming the individual (CNIL, 2019), Παιχνίδι με τα συναισθήματα (Gray et al., 2018), Framing (Forbrukerrådet, 2018) και Pressured Selling (Mathur, et al., 2019).

10. Συγκαλυμμένες διαφημίσεις (Disguised ads): Οι διαφημίσεις εμφανίζονται ως μέρος του περιεχομένου ή της πλοήγησης προκειμένου να οδηγήσουν τον χρήστη να κάνει κλικ πάνω τους. Παρόμοιο μοτίβο είναι το Chameleon Advertising (CNIL, 2019).
11. Αναγκαστική συνέχεια (Forced Continuity): Μετά τη λήξη της δωρεάν δοκιμαστικής περιόδου μιας υπηρεσίας αρχίζει η χρέωση της πιστωτικής κάρτας του χρήστη χωρίς προειδοποίηση, ενώ μερικές φορές η ακύρωση της συνδρομής είναι ανέφικτη. Παρόμοια μοτίβα είναι τα Hidden subscription (Mathur et al., 2019), Social Pyramid και Gamification (Gray et al., 2018) και Forced action and timing (Forbrukerrådet, 2018). Όλα αυτά υπάγονται στη γενική κατηγορία Forced action (Gray et al., 2018) και αναγκάζουν τον χρήστη να προβεί σε συγκεκριμένη ενέργεια, την οποία ο ίδιος δεν επιθυμεί.
12. Ανεπιθύμητη αλληλογραφία από φίλους (Friend Spam): Ο πάροχος ζητά πρόσβαση στο email ή στα μέσα κοινωνικής δικτύωσης του χρήστη με το πρόσχημα ότι θα χρησιμοποιηθούν για ένα επιθυμητό αποτέλεσμα (π.χ. εύρεση φίλων), αλλά στη συνέχεια στέλνει spam μηνύματα σε όλες τις επαφές του χρήστη, που φαίνονται ότι αποστέλλεται από εκείνον. Το πιο γνωστό παράδειγμα προέρχεται από το Linkedin, το οποίο είχε ως αποτέλεσμα πρόστιμο αξίας 13 εκατομμυρίων δολαρίων μετά από μια συλλογική αγωγή το 2015. Υπάρχει όμως και στα online παιχνίδια, όπως στα Farmville και Candy Crush Saga, όπου παρουσιάζονται ενέργειες που φέρεται να έχει κάνει ο παίκτης, χωρίς εκείνος να τις γνωρίζει (Zagal, Björk and Lewis, 2013). Παρόμοια μοτίβα είναι τα Continuous prompting (ΕΣΠΔ, 03/2022), Nagging και Social Pyramid (Gray et al., 2018).

Σταδιακά, διάφοροι ερευνητές (Conti and Sobiesk, 2010, Zagal, Björk and Lewis, 2013, Lewis. 2014, Bösch et al., 2016, Gray et al., 2018, Mathur et al., 2019, Cara 2019, Luguri and Strahilevitz, 2021, Mathur, Kshirsagar and Mayer, 2021, Jarovsky, 2022, Leiser and Yang, 2022, Gray, Santos and Bielova, 2023) και αρχές (Forbrukerrådet, 2018, CNIL, 2019, ΕΣΠΔ, 03/2022, Επιτροπή, 2022, ΟΟΣΑ, 2022) πρότειναν τους δικούς τους ορισμούς και τις αντίστοιχες ταξινομήσεις των σκοτεινών μοτίβων κατ' εφαρμογή διάφορων κριτηρίων, που αναδεικνύουν τη διαφορετική οπτική του καθενός, αλλά παρουσιάζουν και αλληλεπικάλυψη ως ένα βαθμό. Το πιθανότερο είναι ότι ο κατάλογος των σκοτεινών μοτίβων θα ανανεώνεται διαρκώς. Πέρα από τις εκάστοτε διαφορετικές προσεγγίσεις, όσο η τεχνολογία εξελίσσεται, θα αναδύονται νέα σκοτεινά μοτίβα, όπως αυτά που θα προκύψουν από τη χρήση των αλγορίθμων μηχανικής μάθησης (ΟΟΣΑ, 2022, King and MacKinnon, 2022), την εξέλιξη των ψηφιακών βοηθών, που χρησιμοποιούν ήχο και ομιλία (Rieger and Sinders, 2020), των chatbots που χρησιμοποιούν Τεχνητή Νοημοσύνη (εφεξής ΤΝ) και συνομιλούν με τους χρήστες, όπως η Replika, και των LLM (Large

Language Models), όπως του GPT4 (Europol, 2023). Αναφορικά μάλιστα με την εξέλιξη της ΤΝ η Jarovsky (2023a) προτείνει δύο σκοτεινά μοτίβα που περιέχουν ΤΝ και δημιουργούν πλασματικές εντυπώσεις: α) όταν ένας συγκεκριμένος ήχος, κείμενο, εικόνα, βίντεο ή άλλο μέσο δημιουργείται από ΤΝ και θεωρείται πραγματικό/αυθεντικό, όπως τα deepfakes, και β) όταν οι χρήστες νομίζουν ότι αλληλεπιδρούν με άλλους ανθρώπους, αλλά στην πραγματικότητα πρόκειται για σύστημα ΤΝ.

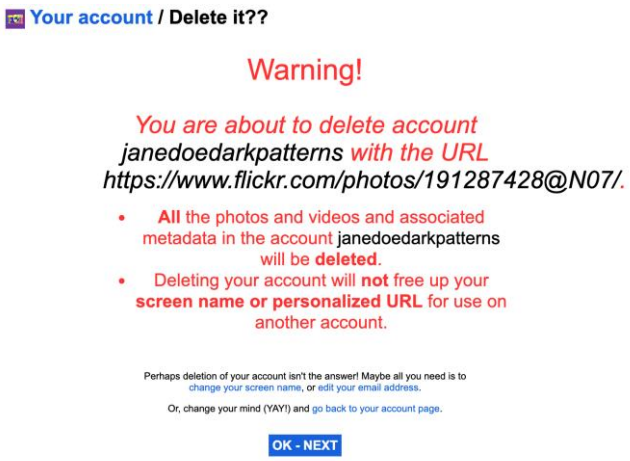
Παρά την απουσία ενός μοναδικού ορισμού τα σκοτεινά μοτίβα έχουν ορισμένα κοινά χαρακτηριστικά. Αρχικά, σχεδιάζονται με πρόθεση να επηρεάζουν τις αποφάσεις των χρηστών. Αυτή είναι η διαφορά τους από τα αντι-μοτίβα. Υποστηρίζεται έντονα από τη βιβλιογραφία ότι ένα σκοτεινό μοτίβο πρέπει να είναι ταυτόχρονα χειριστικό και κακόβουλο (Jarovsky, 2022, Forbrukerrådet, 2018, Fritch, 2017, Bösch et al., 2016, Brignull, 2011, Conti and Sobiesk, 2010). Ωστόσο, διατυπώνεται και η άποψη ότι τα σκοτεινά μοτίβα δεν σχεδιάζονται απαραίτητα με κακόβουλο σκοπό, αλλά μπορεί να προκύπτουν από την κακή χρήση των A/B δοκιμών (Narayanan et al., 2020). Σημειωτέον πάντως ότι ούτε ο ΓΚΠΔ ούτε η ΟΑΕΠ απαιτούν πρόθεση για την εφαρμογή τους.

Για να πετύχουν τον παραπάνω σκοπό, τα σκοτεινά μοτίβα τροποποιούν τις διαθέσιμες επιλογές των χρηστών ή χειραγωγούν τη ροή των πληροφοριών που τους παρέχουν (Mathur, Kshirsagar and Mayer, 2021). Στην πρώτη περίπτωση χαρακτηρίζονται από:

1. Ασυμμετρία: Οι επιλογές που ωφελούν τον πάροχο βρίσκονται σε περίοπτη θέση, ενώ όσες ωφελούν τον χρήστη συνήθως κρύβονται πίσω από πολλά κλικ ή αποκρύπτονται από το οπτικό πεδίο του χρήστη π.χ. λόγω χρωματισμού. Η ασυμμετρία χαρακτηρίζει κυρίως τις UI που ζητούν τη συγκατάθεση του χρήστη, όπως οι Ερωτήσεις-παγίδα (ΟΟΣΑ, 2022, Forbrukerrådet, 2018, Acquisti et al., 2017).
2. Συγκάλυψη: Αποκρύπτεται ο μηχανισμός που εκμεταλλεύονται τα σκοτεινά μοτίβα για να επηρεάσουν τη λήψη απόφασης, όπως είναι οι προκαταλήψεις. Για παράδειγμα, το Disguised data collection (Greenberg et al., 2014) χάριν της στοχευμένης διαφήμισης συγκεντρώνει μεγάλες ποσότητες δεδομένων για τη δημιουργία αναλυτικού προφίλ χρήστη χωρίς τη συγκατάθεση των χρηστών.
3. Περιορισμό επιλογών: Τα σκοτεινά μοτίβα μειώνουν ή αποκλείουν επιλογές που παρουσιάζονται στους χρήστες. Για παράδειγμα, το Forced Action σε μια ιστοσελίδα ενδέχεται να απαιτεί από τους χρήστες να συμφωνούν ταυτόχρονα με τους όρους χρήσης και με τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου μάρκετινγκ προτού δημιουργήσουν έναν λογαριασμό.
4. Άνιση μεταχείριση: Κυρίως χαρακτηρίζει σκοτεινά μοτίβα που εντοπίζονται σε παιχνίδια. Για παράδειγμα, το Pay to Skip επιτρέπει στους χρήστες να πληρώσουν για να αποκτήσουν πλεονέκτημα έναντι των άλλων χρηστών (Zagal et al., 2013).

Στη δεύτερη περίπτωση χαρακτηρίζονται από:

1. Παραπλάνηση: Ο σχεδιασμός της UI, σαν ταχυδακτυλουργός (Harris, 2016) προκαλεί ψευδείς πεποιθήσεις είτε μέσω καταφατικών ανακριβειών, παραπλανητικών δηλώσεων ή παραλείψεων, όπως το Friend Spam. Από την άλλη, το Confirmshaming συνήθως είναι διαφανές και μάλιστα σε ενοχλητικό βαθμό (Mathur, Kshirsagar and Mayer, 2021).
2. Απόκρυψη πληροφοριών: Αποκρύπτονται ή καθυστερούν να εμφανιστούν οι απαραίτητες πληροφορίες στους χρήστες. Για παράδειγμα, το False Continuity (CNIL, 2019) ζητάει από τους χρήστες να δώσουν το mail τους προκειμένου να διαβάσουν ένα άρθρο χωρίς να τους προειδοποιεί σαφώς ότι αυτή η κίνηση ισοδυναμεί με εγγραφή στο newsletter. Το Hidden Legalese Stipulation (Bösch et al., 2016) παραθέτει εκτενώς όρους και προϋποθέσεις και χρησιμοποιεί νομική ορολογία. Ο πάροχος τυπικά συμμορφώνεται με την υποχρέωση ενημέρωσης, αλλά οι περισσότεροι χρήστες δεν θα διαβάσουν την πολιτική.



Εικόνα 1: Παράδειγμα Confirmshaming από την ιστοσελίδα Flickr (Lingareddy, Schaffner and Chetty, 2022)

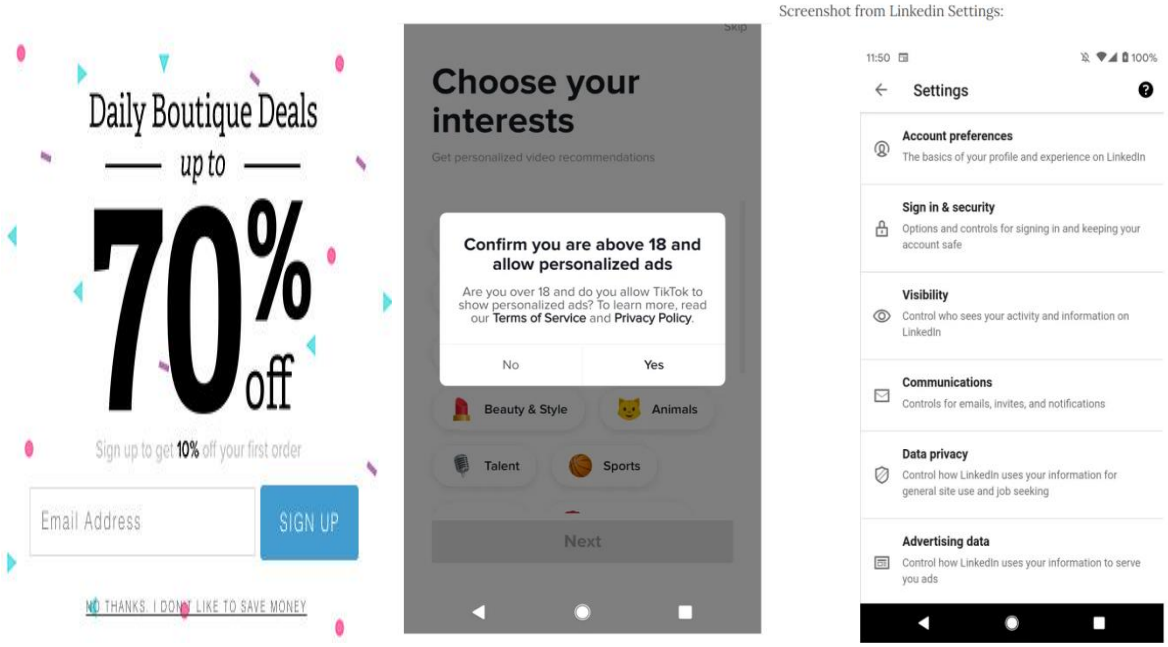
Συναφώς, διαφαίνεται η ανισότητα μεταξύ των μερών, αφού ο πάροχος που κατέχει την απαιτούμενη τεχνογνωσία επιβάλλει τους όρους του, ενώ οι χρήστες ευρισκόμενοι σε ασθενέστερη θέση δεν αποφασίζουν πραγματικά (Jarovsky, 2022, Egberts, 2021, Acquisti et al., 2017, Harris, 2016). Για αυτό ωφελούν τον πάροχο και/ή βλάπτουν τους χρήστες. Επίσης, παρά την τεράστια ποικιλία τους, όλα τα σκοτεινά μοτίβα εκμεταλλεύονται την ανθρώπινη ψυχολογία για να επηρεάσουν τους χρήστες, χωρίς οι τελευταίοι να το αντιλαμβάνονται πάντα. Τα περισσότερα, μάλιστα, εκμεταλλεύονται βασικές προκαταλήψεις, ευρετικές και τις ωθήσεις για να επηρεάζουν τη συμπεριφορά των χρηστών, όπως θα παρουσιαστεί στη συνέχεια. Πάνω σε αυτά τα στοιχεία στηρίχτηκαν αρκετές νομοθετικές πρωτοβουλίες που επιχειρούν να αντιμετωπίσουν τα σκοτεινά μοτίβα στην Ευρώπη και στις ΗΠΑ.

Σημειώνεται ότι για την περιγραφή φαινομένων παρόμοιων με τα σκοτεινά μοτίβα έχει γίνει λόγος για το «sludge» (Thaler, 2018), που αφορά τη σκόπιμη προσθήκη εμποδίων προκειμένου να καταστεί δυσκολότερο για τον χρήστη να κάνει επιλογές που αντιστοιχούν στα συμφέροντά του, καθώς και για τη «χειραγώγηση της ψηφιακής αγοράς». Εντός αυτής η συλλογή και διατήρηση πληροφοριών για τη συμπεριφορά των χρηστών και ο σχεδιασμός της προσέγγισης και αλληλεπίδρασης με εκείνους συνεπάγονται μεταξύ άλλων οικονομική ζημία, απώλεια της ιδιωτικότητας και της ικανότητα λήψης αποφάσεων (Calo, 2014). Επίσης, ορισμένες μελέτες προτιμούν τον ευρύτερο όρο της «online αρχιτεκτονικής της επιλογής», ώστε να καλύπτονται όχι μόνο τα σκοτεινά μοτίβα που εντοπίζονται στις UI, αλλά στην περιήγηση του χρήστη (UJ) (ΟΟΣΑ, 2022). Η αρχιτεκτονική της επιλογής είναι ουσιαστικά το περιβάλλον μέσα στο οποίο παρουσιάζεται η πληροφορία και τα άτομα παίρνουν αποφάσεις (Επιτροπή, 2022, Thaler and Sunstein, 2008). Παρομοίως, ο όρος «αρχιτεκτονική του συστήματος», δηλαδή ο σχεδιασμός της δομής ενός ψηφιακού προϊόντος ή υπηρεσίας, λαμβάνει υπ᾽όψιν παραπλανητικές τεχνικές που βαίνουν πέρα από την UI, δεν προϋποθέτουν αναγκαστικά την αφή ή την όραση, αλλά μια άλλη αίσθηση, όπως είναι οι αλγόριθμοι και οι ψηφιακοί βοηθοί, που χρησιμοποιούν τον ήχο (Leiser and Santos, 2023). Οι παρατηρήσεις αυτές υποδηλώνουν ότι το πρόβλημα δεν περιορίζεται σε επίπεδο UI, αλλά είναι βαθύτερο και διαχέεται σε όλο το σύστημα, για αυτό έχει νόημα η ενεργοποίηση του άρθρου 25 ΓΚΠΔ. Πάντως, η τρέχουσα νομοθεσία φαίνεται να περιορίζεται σε σκοτεινά μοτίβα, τα οποία είναι σχετικά εύκολα ανιχνεύσιμα στον UI/UX σχεδιασμό, και να αγνοεί τις πιο «ύπουλες» τεχνικές που ενσωματώνει γενικά η αρχιτεκτονική ενός συστήματος (Leiser and Santos, 2023).

Τον Νοέμβριο του 2022 ετέθη σε ισχύ η Πράξη για τις Ψηφιακές Υπηρεσίες (Digital Services Act, εφεξής DSA), που αποτελεί *το πρώτο νομοθετικό κείμενο σε ενωσιακό επίπεδο που απαγορεύει ρητά τα σκοτεινά μοτίβα.* Συγκεκριμένα, στην αιτιολογική σκέψη 67, αναφέρει τον «παραπλανητικό σχεδιασμό» στις UI online πλατφορμών και τον ορίζει ως «πρακτικές που στρεβλώνουν ή επηρεάζουν ουσιωδώς, είτε σκόπιμα είτε στην πράξη, την ικανότητα των αποδεκτών της υπηρεσίας να προβαίνουν σε *αυτόνομες και τεκμηριωμένες επιλογές ή αποφάσεις*. Οι πρακτικές αυτές μπορούν να χρησιμοποιηθούν για να πεισθούν οι αποδέκτες της υπηρεσίας να ακολουθήσουν αθέλητες συμπεριφορές ή να λάβουν ανεπιθύμητες αποφάσεις που έχουν αρνητικές συνέπειες για αυτούς». Ο όρος αυτός αντικατέστησε τον νεολογισμό για να αποφευχθεί η σύνδεση με στερεότυπα και ρατσιστικές αντιλήψεις. Παρομοίως, η αιτιολογική σκέψη 34 της Πρότασης της Πράξης για τα Δεδομένα (εφεξής Data Act) αναφέρεται ρητά στις παραπλανητικές τακτικές ως «τεχνικές σχεδιασμού που ωθούν ή εξαπατούν τους καταναλωτές σε αποφάσεις που έχουν αρνητικές συνέπειες για αυτούς. Αυτές οι τεχνικές χειραγώγησης μπορούν να χρησιμοποιηθούν για να πείσουν τους χρήστες, ιδιαίτερα τους ευάλωτους καταναλωτές, να επιδοθούν σε ανεπιθύμητες συμπεριφορές και να παραπλανήσουν τους χρήστες, ωθώντας τους σε αποφάσεις σχετικά με

συναλλαγές κοινολόγησης δεδομένων, ή να μεροληπτήσουν αδικαιολόγητα στη λήψη αποφάσεων των χρηστών της υπηρεσίας, κατά τρόπο που υπονομεύει και θίγει την *αυτονομία*, τη *λήψη αποφάσεων* και την *επιλογή* των χρηστών». Πάντως, οι προαναφερθείσες αιτιολογικές σκέψεις της DSA και της Πρότασης Data Act διευκρινίζουν ότι «θεμιτές πρακτικές […], που είναι σύμφωνες με το δίκαιο της Ένωσης δεν θα πρέπει να θεωρούνται ότι αποτελούν παραπλανητικό σχεδιασμό».

Η παρούσα εργασία προσδιορίζει τα σκοτεινά μοτίβα ως *επιλογές* στον UX/UI/UJ σχεδιασμό, στο κείμενο και γενικά στην αρχιτεκτονική του συστήματος ιστοσελίδων και εφαρμογών που σκόπιμα εκμεταλλεύονται γνωστικούς μηχανισμούς και ανθρώπινες αδυναμίες και που παραπλανούν τους χρήστες, τους θέτουν εμπόδια, τους αποκρύπτουν πληροφορίες, τους χειραγωγούν προωθώντας άνισα ορισμένες επιλογές έναντι άλλων ή τους εξαναγκάζουν προς απροσχεδίαστες και ανεπιθύμητες αποφάσεις αναφορικά με τα προσωπικά τους δεδομένα, προς όφελος των παρόχων online υπηρεσιών και ταυτόχρονα εις βάρος των δικών τους αληθινών συμφερόντων (ΕΣΠΔ, 03/2022, Mathur et al., 2019, Gray et al., 2018, Brignull, 2021, 2013, 2011).



Εικόνα 2: Παραδείγματα πρακτικών που ασκούν πίεση με χειριστικό λεξιλόγιο (α), που παραπλανούν τον χρήστη ώστε να μην μπορεί να απορρίψει τις εξατομικευμένες διαφημίσεις (β), που αποκρύπτουν πληροφορίες ουσιώδεις για την προστασία της ιδιωτικότητας μέσα σε πληθώρα επιλογών (γ) (Jarovsky, 2022d).

2.3 Η φύση των σκοτεινών μοτίβων, τα κίνητρα πίσω από τη χρήση τους και η κρισιμότητα του σχεδιασμού

Η ουσία των σκοτεινών μοτίβων έγκειται στην αξιοποίηση των παραπλανητικών τεχνικών που υπήρχαν ήδη στην αγορά, της τεχνολογίας, του UI/UX σχεδιασμού, των δοκιμών A/B, του τεράστιου αριθμού συλλεγόμενων δεδομένων, των πορισμάτων της ψυχολογίας και των συμπεριφορικών οικονομικών (BEUC, 2022, Brignull, 2021,

Narayanan et al., 2020). Όλα αυτά τα στοιχεία παρουσιάζονται στην τρέχουσα και στην επόμενη ενότητα.

Τακτικές άκρως πειστικές και ενίοτε παραπλανητικές έχουν κάνει την εμφάνισή τους εδώ και πολλά χρόνια ήδη στον αναλογικό κόσμο. Για παράδειγμα, ένα κατάστημα που ισχυρίζεται ψευδώς ότι κλείνει ή τιμές «ευκαιρία» με δεκαδικά ψηφία λήγοντα σε 9, όπως 3,99€ αντί 4€, είναι πια αποδεκτές και θεωρούνται αποτελεσματικές (Narayanan et al., 2020, Harris, 2016). Το διαδίκτυο, όμως, έδωσε άλλη διάσταση σε αυτές τις πρακτικές.

Η σύγχρονη εποχή χαρακτηρίζεται από τον ψηφιακό μετασχηματισμό των υπηρεσιών. Όλο και περισσότεροι καταναλωτές, ιδίως μετά την πανδημία COVID-19, χρησιμοποιούν το Διαδίκτυο για τις αγορές τους, την επικοινωνία, την ενημέρωση, την ψυχαγωγία και άλλους σκοπούς. Μέσα στη δεκαετία 2012-2022 το ποσοστό των χρηστών που πραγματοποιεί online αγορές αυξήθηκε από 55% σε 75% (Eurostat, 2023). Το λεγόμενο Συμμετοχικό Διαδίκτυο (Web 2.0) συνέβαλε στον ψηφιακό μετασχηματισμό των υπηρεσιών και στην ανάπτυξη νέων επιχειρηματικών μοντέλων και εν τέλει στη δημιουργία μιας οικονομίας που τροφοδοτείται από τεράστιες ποσότητες δεδομένων (big data) προερχόμενα από τους χρήστες. Η οικονομία αυτή ωφελεί τόσο τους καταναλωτές, που απολαμβάνουν μεγάλη ποικιλία προσφερόμενων προϊόντων και υπηρεσιών ανεξαρτήτως τόπου και χρόνου, όσο και τις επιχειρήσεις, που συγκεντρώνουν τα δεδομένα με σκοπό να μάθουν όσο το δυνατόν ακριβέστερα τις προτιμήσεις των καταναλωτών και να προσαρμόσουν κατάλληλα τα αγαθά και τις υπηρεσίες τους πάνω σε αυτές τις προτιμήσεις.

Από την άλλη, στο διαδίκτυο τα όρια μεταξύ μιας πειστικής και μιας παραπλανητικής διαφήμισης, που ανέκαθεν ήταν πολύ ρευστά, έγιναν ακόμα πιο δυσδιάκριτα. Σήμερα η online συμπεριφορική διαφήμιση αξιοποιεί τα δεδομένα των χρηστών και τα πορίσματα της συμπεριφορικής οικονομίας και της ψυχολογίας για να βελτιώσει τις στρατηγικές στο μάρκετινγκ (Narayanan et al., 2020). Ταυτόχρονα, οι σχεδιαστές μετατρέπουν όσα μαθαίνουν για τη συμπεριφορά των χρηστών σε αποτελεσματικές UI και κατάλληλες ωθήσεις (Narayanan et al., 2020). Καίριο ρόλο σε αυτά έχει η συστηματική διεξαγωγή σε μεγάλη κλίμακα και σε πραγματικό χρόνο δοκιμών A/B (Narayanan et al., 2020, Brignull, 2021, Calo, 2014), παραλλαγές δηλαδή ιστοσελίδων που προβάλλονται σε δύο ή περισσότερα τυχαία επιλεγμένα υποσύνολα χρηστών και καταγράφονται τυχόν διαφορές στη συμπεριφορά με στόχο τη συνεχή βελτίωση του σχεδιασμού των ιστοσελίδων/εφαρμογών και ακολούθως της αποτελεσματικότητας της εμπορικής τους δραστηριότητας. Ο Douglas Bowman, κορυφαίος σχεδιαστής στη Google παραδέχτηκε ότι κάποτε η *Google δοκίμασε 41 διαφορετικές αποχρώσεις του μπλε για να αποφασίσει ποια αποδίδει καλύτερα* (Narayanan et al., 2020). Συναφώς, ο ΟΟΣΑ (2022) παρατήρησε ότι προβλέπεται η συμβολή της μηχανικής μάθησης και η αντικατάσταση των δοκιμών A/B από το αλγοριθμικό μάρκετινγκ με τον κίνδυνο μεγαλύτερης ζημίας ελλείψει

ανθρώπινης εποπτείας. Τέλος, αν αναλογιστεί κανείς τον μεγάλο αριθμό των χρηστών που μπορεί να προσεγγίσει μία online επιχείρηση, ιδίως αν πρόκειται για μία εκ των GAFAM (Google-Amazon-Facebook-Apple-Microsoft), σε συνδυασμό με το χαμηλό κόστος, αυξάνεται σημαντικά η επιτυχία των σκοτεινών μοτίβων και η πιθανότητα βλάβης των ΥΔ (Επιτροπή 2022). Σταδιακά, αναμένεται ότι τα σκοτεινά μοτίβα θα συνδυάζονται με μεθόδους εξατομίκευσης (Narayanan et al., 2020) ή θα εντοπίζονται σε περιβάλλοντα εικονικής ή επαυξημένης πραγματικότητας, όπως το metaverse, περιπλέκοντας περαιτέρω την κατάσταση και επηρεάζοντας αποφασιστικά τη λήψη αποφάσεων (Επιτροπή 2022).

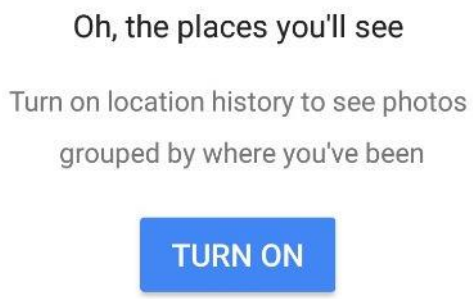
Σύμφωνα με τον Brignull (2021) τα σκοτεινά μοτίβα χρησιμοποιούνται, διότι σε γενικές γραμμές είναι αποτελεσματικά, κερδοφόρα και έχουν μεγάλο αντίκτυπο με μικρή προσπάθεια. Όπως ήδη αναφέρθηκε, απώτερος στόχος είναι η αύξηση των εσόδων των παρόχων online υπηρεσιών, ακόμα και όταν συλλέγουν δεδομένα ή μονοπωλούν το ενδιαφέρον και την προσοχή των χρηστών. Έτσι, οι επιχειρήσεις είναι ανταγωνιστικές είτε με θεμιτά είτε με αθέμιτα μέσα. Ακόμα και αν οι ίδιοι οι σχεδιαστές δεν επιθυμούν να τα χρησιμοποιήσουν, αναγκάζονται να θέσουν το συμφέρον των παρόχων πάνω από το δικαίωμα των χρηστών να επιλέγουν αυτόνομα. Το γεγονός δε ότι είναι συχνά δύσκολο να ανιχνευθούν ενθαρρύνει την περαιτέρω χρήση. Παρά την επιβολή προστίμων και παρόλο που οι χρήστες ενδέχεται να απομακρυνθούν από τον πάροχο μόλις αντιληφθούν ότι χρησιμοποιεί σκοτεινά μοτίβα, τα κέρδη, έστω και βραχυπρόθεσμα, παραμένουν σημαντικά μεγαλύτερα (Brignull, 2021, Egberts, 2021, Brownlee, 2016). Όλα αυτά τις περισσότερες φορές μπορούν να λαμβάνουν χώρα δίχως *οι χρήστες να έχουν πλήρη γνώση των γεγονότων, ενώ* εμπλέκονται πολλοί συμμετέχοντες, όπως είναι οι μεσίτες δεδομένων. Οι παραπάνω παράγοντες και η έλλειψη συγκατάθεσης και διαφάνειας δημιουργούν αρκετή αβεβαιότητα για την τύχη των προσωπικών δεδομένων που ανταλλάσσονται μεταξύ των εμπλεκομένων ως αντίτιμο για τις υπηρεσίες της Κοινωνίας της Πληροφορίας και διακρίνουν τελικά μια πειστική τεχνική από μία που ενέχει το στοιχείο της χειραγώγησης και αθετεί τις διατάξεις του ΓΚΠΔ, της Οδηγίας ePrivacy και της ΟΑΕΠ (Επιτροπή, Κατευθυντήριες 2021).

Στο σημείο αυτό ο *σχεδιασμός αποδεικνύεται κρίσιμος* (Forbrukerrådet, 2018, CNIL, 2019), ενώ, όσο πιο ελκυστικός είναι, θεωρείται πιο αξιόπιστος και παραγνωρίζεται ο παραπλανητικός χαρακτήρας του (Bhoot, Shinde and Mishra, 2020). Πολλές μελέτες πάνω στα cookie banners επιβεβαιώνουν την αποτελεσματικότητα συγκεκριμένων πρακτικών σχεδιασμού, όπως των προεπιλεγμένων ρυθμίσεων, της ετεροκατεύθυνσης/ψευδούς ιεράρχησης/κρυφών πληροφοριών και της προσθήκης εμποδίων/αδυναμίας σαφούς opt-out (Luguri and Strahilevitz, 2021, Graßl et al., 2021, Kampanos and Shahandashti 2021, Soe et al., 2020, Matte, Bielova and Santos, 2020, Nouwens et al., 2020, Utz et al., 2019, Machuletz and Böhme, 2019). Ειδικότερα, ακόμα και

μικρές λεπτομέρειες στον σχεδιασμό μιας UI, όπως η θέση της ειδοποίησης για cookies (αλλαγή από πάνω προς τα κάτω), το χρώμα των επιλογών και οι προεπιλογές μπορούν να επηρεάσουν ουσιωδώς τη συμπεριφορά των χρηστών ώστε να αποδεχτούν ακόμα και τα cookies τρίτων, όπως φάνηκε στο 57.4% των cookie banners των 1.000 δημοφιλέστερων ιστοσελίδων της ΕΕ (Utz et al., 2019). Το 2020 πείραμα σε 40 συμμετέχοντες κατέγραψε αύξηση της συγκατάθεσης κατά 22% όταν δεν δινόταν η επιλογή «Απόρριψη όλων» στην πρώτη σελίδα και απείχε τουλάχιστον δύο κλικ μακριά από αυτή με αποτέλεσμα το click fatigue. Αντίθετα, η παροχή λεπτομερών επιλογών για τα cookies στην πρώτη σελίδα μείωνε τη συγκατάθεση κατά 8-20% (Nouwens et al., 2020).

Σκοτεινά μοτίβα υπάρχουν και στις πολιτικές απορρήτου. Εκεί συμβαίνει να αποκρύπτονται οι υπερσύνδεσμοι που οδηγούν στις πολιτικές, να είναι πολύ θετικό το λεξιλόγιο που συνοδεύει τις επιλογές απορρήτου σε βαθμό μη ρεαλιστικό, να αξιοποιείται το χρονικό κενό μεταξύ της ειδοποίησης και της επιλογής και να μην αποκαλύπτονται πρακτικές με σημαντικό αντίκτυπο στην ιδιωτική ζωή των ανθρώπων. Χαρακτηριστικό παράδειγμα είναι το πυκνό και νομικής φύσεως λεξιλόγιο των πολιτικών, που αποθαρρύνει τους χρήστες να τις διαβάζουν (Gunawan et al., 2021).

Επιπλέον παραδείγματα αντλούνται και από τις μεγάλες πλατφόρμες. Το 2021 μελέτη στις GAFAM εντόπισε ασυμμετρία στον σχεδιασμό, απόκρυψη πληροφοριών και ασαφείς δηλώσεις δείχνοντας ότι αυτοί οι κολοσσοί δεν εξασφαλίζουν πάντα ισχυρή συγκατάθεση (Human and Cech, 2021). Βεβαίως, το Forbrukerrådet είχε ήδη διαπιστώσει από το 2018 ότι ο σχεδιασμός και το κείμενο των αναδυόμενων παραθύρων των Google, Facebook και Microsoft Windows 10 ωθούσαν τους χρήστες προς μη φιλικές προς το απόρρητο επιλογές μέσω π.χ. της Ψευδούς Ιεράρχησης των επιλογών (Ετεροκατεύθυνσης) και του Confirmshaming και ότι τους απέκρυπταν ουσιώδεις πληροφορίες. Επιπλέον, παρατήρησε ότι οι Google και Facebook χρησιμοποιούσαν προεπιλογές παρεμβατικές για το απόρρητο, ενώ οι πιο φιλικές ρυθμίσεις απαιτούσαν μεγάλο αριθμό βημάτων εκ μέρους των χρηστών (Hard to cancel/opt out). Ειδικά για τη Google το Forbrukerrådet (2018a) παρατήρησε ότι προκειμένου να παρακολουθεί την τοποθεσία των χρηστών μέσω των υπηρεσιών της, χρησιμοποιούσε πλήθος σκοτεινών μοτίβων, όπως τα προαναφερθέντα και επιπλέον την επαναλαμβανόμενη προτροπή (Repeated nudging/Όχληση) για την ενεργοποίηση του εντοπισμού τοποθεσίας ή έθετε την τελευταία ως προϋπόθεση για τη χρήση άλλων υπηρεσιών (Bundling of services/Forced disclosure).



Εικόνα 3: Ο χρήστης παρακινείται να ενεργοποιήσει το Location History στις Google Photos (Forbrukerrådet, 2018a).

2.4 Η επίδραση των σκοτεινών μοτίβων στην αυτονομία, στη λήψη απόφασης και στις επιλογές των χρηστών

Η ισχυρή συγκατάθεση που αναγνωρίζει ο ΓΚΠΔ ως νομική βάση επεξεργασίας προσωπικών δεδομένων είναι άμεσα συνυφασμένη με την αυτονομία του χρήστη. Η DSA απαγορεύει στις online πλατφόρμες «να στρεβλώνουν ή να αναιρούν την αυτονομία, τη λήψη αποφάσεων ή την επιλογή» των χρηστών (αιτ.σκ.67). Για αυτό θα γίνει αναφορά στον τρόπο με τον οποίο τα σκοτεινά μοτίβα εκμεταλλεύονται τις ανθρώπινες αδυναμίες ώστε να επηρεάζουν τα παραπάνω στοιχεία.

2.4.1 Προκαταλήψεις, ευρετικές, διάθεση και συναισθήματα

Η παραδοσιακή οικονομική θεωρία υποστήριζε ότι ο άνθρωπος είναι απολύτως ορθολογικό ον, που λαμβάνει αποφάσεις με γνώμονα τη μεγιστοποίηση της ωφέλειας του (Jarovsky 2022, Egberts 2021, CNIL, 2019). Βαθμηδόν, η θεωρία αυτή της λογικής επιλογής και ο homo economicus υποσκελίστηκαν από πειράματα στο πεδίο της γνωστικής ψυχολογίας που έδειξαν ότι ο ορθολογισμός του ανθρώπου είναι περιορισμένος (bounded rationality) (Waldman, 2020) και ότι μη ορθολογικά στοιχεία, όπως προκαταλήψεις και ένστικτα, εμφιλοχωρούν στη διαδικασία λήψης μιας απόφασης. Έτσι, προέκυψε ένας νέος κλάδος, τα συμπεριφορικά οικονομικά. Η κατανόηση της ανθρώπινης ψυχολογίας επιτρέπει την πρόβλεψη της συμπεριφοράς ως ένα βαθμό και ο UI/UX σχεδιασμός μπορεί να την επηρεάσει για την εξυπηρέτηση διάφορων σκοπών, αγαθών και μη (π.χ. δημόσια υγεία ή Cambridge Analytica αντίστοιχα). Ειδικά, στην online συμπεριφορική διαφήμιση τα σκοτεινά μοτίβα γίνονται συχνά εργαλεία εκμετάλλευσης της άγνοιας, των αδυναμιών ή της ψυχολογίας των χρηστών στην προσπάθεια των online υπηρεσιών να συνδέσουν τις αισθήσεις και τις επιθυμίες των χρηστών με συγκεκριμένα προϊόντα. Η τεχνική αυτή του μάρκετινγκ καθιερώθηκε και ενσωματώθηκε περαιτέρω και στον σχεδιασμό των προϊόντων.

Είναι πια ευρέως αποδεκτό ότι υφίστανται δύο συστήματα σκέψης (Bösch et al., 2016, Lewis C, 2014). Κατά το πρώτο (Σύστημα 1) οι χρήστες σκέφτονται και αποφασίζουν γρήγορα χωρίς πολλή προσπάθεια, σχεδόν μηχανικά και αυτόματα, ενώ στο δεύτερο

(Σύστημα 2) αφιερώνουν χρόνο και κόπο για να σκεφτούν και καταλήγουν σε μια απόφαση πιο αργά αλλά και πιο συνειδητά. Με άλλα λόγια, το Σύστημα 1 στηρίζεται στη διαίσθηση, ενώ το Σύστημα 2 στην ορθολογική στάθμιση. Οι Thaler και Sunstein (2009) τα ονομάζουν «αυτόματη» και «στοχαστική» σκέψη αντίστοιχα, ενώ τα χαρακτηριστικά του Συστήματος 1 *απηχούν τον ορισμό της χειραγώγησης* που προτείνει η Sunstein (2016) σχετικά με μια δήλωση ή ενέργεια που «δεν εμπλέκεται επαρκώς ή δεν απευθύνεται στην ικανότητα των ανθρώπων για επιλογή με στοχασμό και διαβούλευση». Οι άνθρωποι χρησιμοποιούν το Σύστημα 1 επειδή στερούνται της απαιτούμενης γνώσης, ικανότητας, χρόνου ή κινήτρων να σκεφτούν πιο διεξοδικά (Bösch et al., 2016). Αυτό το σύστημα συνδέεται στενά με τις ευρετικές/ευριστικές (heuristics) και τις προκαταλήψεις (biases). Οι heuristics ή εμπειρικοί κανόνες (rules of thumb) είναι *συντομεύσεις που χρησιμοποιούνται στη διαδικασία λήψης απόφασης*. Με αυτές τα άτομα απλοποιούν τις επιλογές τους και στη συνέχεια εφαρμόζουν τη λογική για να κάνουν την καλύτερη επιλογή μεταξύ των υπολοίπων (Acquisti et al., 2017). Οι heuristics δεν είναι απαραιτήτως αρνητικές, αφού εξοικονομούν χρόνο και μπορούν να αποδειχθούν αρκετά αποτελεσματικά τις περισσότερες φορές. Υπάρχουν διάφορα είδη heuristics, όπως της διαθεσιμότητας (οι χρήστες θέλοντας να εκτιμήσουν την πιθανότητα μιας ακούσιας αποκάλυψης προσωπικών δεδομένων αξιολογούν πόσο πιθανό είναι να αποκαλύψουν οι άλλοι προσωπικές πληροφορίες στο ίδιο ή σε παρόμοιο περιβάλλον) και της αντιπροσωπευτικότητας (οι χρήστες μπορεί να υποτιμήσουν τον κίνδυνο παραβίασης της ιδιωτικότητας, επειδή συχνά δεν είναι άμεσα αντιληπτός) (Acquisti et al., 2017).

Από την άλλη, οι (γνωστικές και συμπεριφορικές) προκαταλήψεις επηρεάζουν γενικά το σχηματισμό μιας απόφασης, όσο σύνθετη και αν είναι (Acquisti et al., 2017). Αποτελούν συστηματικά (υπό την έννοια ότι είναι προβλέψιμα) σφάλματα κρίσης και συμπεριφοράς (ΟΟΣΑ, 2022, Rieger and Sinders, 2020, CNIL, 2019, Acquisti et al., 2017) και μελετώνται από συμπεριφορικούς οικονομολόγους και ψυχολόγους, που εκτιμούν ότι «αν οι προκαταλήψεις «χρησιμοποιηθούν» σωστά, τότε οι αρχιτέκτονες του online σχεδιασμού μπορούν να επηρεάσουν σημαντικά τη λήψη απόφασης» (Egberts, 2021). Όπως οι heuristics, ούτε οι προκαταλήψεις είναι καθαυτές αρνητικές. Αναφορικά με την ιδιωτικότητα οι πιο συνηθισμένες (ΟΟΣΑ, 2022, Jarovsky, 2022, Egberts, 2021, CNIL, 2019, Mathur et al., 2019, Aquisti et al., 2017, Thaler and Sunstein, 2009) είναι η επίδραση:

- της αγκύρωσης: Η άγκυρα είναι η αρχική πληροφορία που χρησιμοποιείται ως αφετηρία για επόμενες αποφάσεις. Σε ένα πείραμα ζητήθηκε στους συμμετέχοντες να γράψουν έναν ουσιαστικά τυχαίο διψήφιο αριθμό (τα δύο τελευταία ψηφία του αριθμού κοινωνικής ασφάλισης τους) και μετά ερωτήθηκαν αν θα πλήρωναν αυτόν τον αριθμό δολαρίων για ένα μπουκάλι κρασί. Μετά τους ζητήθηκε να δηλώσουν το μέγιστο ποσό που θα πλήρωναν για το μπουκάλι. Παρατηρήθηκε ότι η προθυμία πληρωμής τριπλασιάστηκε σε σχέση με τον πρώτο αυθαίρετο αριθμό. Ελλείψει γνώσης της εμπορικής αξίας του

μπουκαλιού, οι εκτιμήσεις των συμμετεχόντων αγκιστρώθηκαν στο αυθαίρετο σημείο αναφοράς (Narayanan et al., 2020). Η άγκυρα μπορεί να λειτουργήσει ως ώθηση π.χ. όταν οι φιλανθρωπικές οργανώσεις ζητούν μια δωρεά και προσφέρουν μια σειρά από συγκεκριμένες χρηματικές επιλογές (Thaler and Sunstein, 2009). Ως προς την ιδιωτικότητα ο σχεδιαστής θέτει πρώτη μία επιλογή που δεν τη διασφαλίζει και στη συνέχεια άλλες επιλογές που την προστατεύουν λίγο. Ο χρήστης επηρεάζεται από την πρώτη επιλογή και πιστεύει ότι οι επόμενες διαφυλάσσουν την ιδιωτικότητα (Jarovsky, 2022).

- του bandwagon: Παραπέμπει στο σύνδρομο της αγέλης. Είναι η τάση των ατόμων να εκτιμούν κάτι περισσότερο ή λιγότερο, επειδή έτσι κάνουν και οι άλλοι. Για παράδειγμα, η τάση των χρηστών να μοιράζονται φωτογραφίες, βίντεο και προσωπικά δεδομένα χωρίς περιορισμό μεταφέρεται και σε άλλους χρήστες του δικτύου (Jarovsky, 2022). Ένα μοτίβο συναφές είναι το Attention Grabber, όταν δηλαδή ένα άτομο περάσει τυχαία από το οπτικό πεδίο ενός στρατηγικά τοποθετημένου συστήματος και αυτό ενεργοποιεί μια σκόπιμη ενέργεια για να προσελκύσει και να κρατήσει την προσοχή του ατόμου (Greenberg et al., 2014).
- της διατύπωσης (framing): Ο τρόπος που παρουσιάζονται οι επιλογές (έντονο μπλε χρώμα για την αποδοχή, αχνό γκρι για την απόρριψη) ή που διατυπώνονται («Συνέχεια ανάγνωσης» ή «Έξοδος από την ιστοσελίδα») επηρεάζει τις αποφάσεις των χρηστών. Για παράδειγμα, το αναδυόμενο παράθυρο της Facebook σχετικά με τον τρόπο που χρησιμοποιούσε την αναγνώριση προσώπου (βιομετρικά δεδομένα) στους χρήστες παρουσίαζε σκοπούς, όπως «*help protect you from strangers using your photo*» και «*tell people with visual impairments who's in a photo or video*». Στη συνέχεια ενημέρωνε τους χρήστες πως «*if you keep face recognition turned off, we won't be able to use this technology if a stranger uses your photo to impersonate you. If someone uses a screen reader, they won't be told when you're in a photo unless you're tagged*» (Forbrukerrådet, 2018).
- της σπανιότητας: Οι άνθρωποι τείνουν να δίνουν μεγαλύτερη αξία σε πράγματα που είναι σπάνια.
- της αντίθεσης: Ο σχεδιαστής χρησιμοποιεί χαμηλή αντίθεση στο συνδυασμό χρωμάτων, όταν δεν θέλει να γίνει αντιληπτό ή να διαβαστεί ορισμένο κείμενο. Έτσι, κατευθύνει τους χρήστες, τους αποσπά την προσοχή και μειώνεται η πιθανότητα να επιλέξουν υπέρ της προστασίας της ιδιωτικότητάς τους (Jarovsky, 2022).
- της προεπιλογής: Οι χρήστες τείνουν λόγω αδράνειας να αποδέχονται τις ρυθμίσεις που έχουν εξ ορισμού επιλεγεί. Είναι σύνηθες σε δωρεές οργάνων (Forbrukerrådet, 2018). Παρά την απαίτηση του ΓΚΠΔ για ρητή συγκατάθεση και προστασία των δεδομένων από τον σχεδιασμό και εξ ορισμού, αφήνεται περιθώριο στις εταιρείες να υπονοήσουν ότι ορισμένα δεδομένα είναι απαραίτητα για την παροχή μιας υπηρεσίας (Jarovsky, 2022).

- της ψευδούς μοναδικότητας: Οι χρήστες νομίζουν ότι οι πεποιθήσεις τους, η συμπεριφορά τους και άλλες ιδιότητες είναι μοναδικές, ότι βρίσκονται στο επίκεντρο του ενδιαφέροντος και ότι η πλειοψηφία ασπάζεται τη γνώμη τους (Jarovsky, 2022).
- η πλάνη του βυθισμένου κόστους: Οι άνθρωποι επιμένουν σε μια δράση, στην οποία έχουν επενδύσει πόρους, ακόμα κι αν αυτή η κίνηση επιδεινώσει την κατάσταση.
- η αποστροφή για την απώλεια (loss aversion): Οι χρήστες τείνουν να εκτιμούν ένα προνόμιο που κατέχουν ήδη περισσότερο από ένα άλλο που θα μπορούσαν να αποκτήσουν. Για παράδειγμα, ένα banner ζητάει log in από τον χρήστη ως προϋπόθεση για να συνεχίσει την ανάγνωση του άρθρου αυξάνοντας την επιθυμία του να το διαβάσει. Αν το log-in είχε ζητηθεί εξαρχής, ο χρήστης ενδεχομένως να μην αποδεχόταν (CNIL, 2019).
- η υπερβολική έκπτωση: Οι χρήστες τείνουν να προτιμούν ένα άμεσο όφελος από ένα άλλο που ενδεχομένως θα προκύψει στο μέλλον. Προτιμούν, δηλαδή, να χρησιμοποιήσουν μια υπηρεσία αμέσως, ακόμα κι αν εμπεριέχει κινδύνους ή πιθανές μακροπρόθεσμες επιπτώσεις στο απόρρητο, αντί να μην χρησιμοποιήσουν την υπηρεσία και να διατηρήσουν το απόρρητό τους μακροπρόθεσμα. Για παράδειγμα, στις πολιτικές απορρήτου συχνά οι χρήστες προτιμούν να κάνουν απλώς κλικ στην «Αποδοχή», ώστε να μπορούν να απολαύσουν αμέσως την υπηρεσία (Jarovsky, 2022).
- η αισιοδοξία: Οι χρήστες τείνουν να υποτιμούν τους κινδύνους για την ιδιωτικότητα και παρουσιάζουν αμελή συμπεριφορά.
- η υπερφόρτωση με επιλογές που «βραχυκυκλώνει» τους χρήστες (Waldman, 2020).
- οι μετα-γνωστικές διαδικασίες: Αυτές βλάπτουν την ικανότητα των ατόμων να κάνουν επιλογές που αντιπροσωπεύουν ακριβώς τις προτιμήσεις τους (Waldman, 2020).
- η κοινωνική αποδοχή (social proof bias): Ορισμένες επιλογές των ανθρώπων υποτάσσονται στην ανάγκη της κοινωνικής αποδοχής (ΟΟΣΑ, 2022, Harris T, 2016, Bösch, 2016) Για παράδειγμα, σκοτεινά μοτίβα συνδεόμενα με αυτή την προκατάληψη είναι τα Activity notifications, που ενημερώνουν τους χρήστες για τις δραστηριότητες των άλλων χρηστών, όπως τα views, και οι Παραπλανητικές μαρτυρίες ως προς την ασαφή προέλευση μιας ιστοσελίδας (Mathur et al., 2019).
- και η ψευδαίσθηση του ελέγχου, τον οποίο υπόσχονται ότι εξασφαλίζουν στους χρήστες οι πάροχοι υπηρεσιών.

Υποστηρίζεται ότι οι γνωστικές προκαταλήψεις εξηγούν το γνωστό privacy paradox σύμφωνα με το οποίο, αν και φαίνεται να ανησυχούμε για την ιδιωτικότητα μας, στην πράξη μοιραζόμαστε τεράστιες ποσότητες προσωπικών δεδομένων στο διαδίκτυο

αγνοώντας ή αδιαφορώντας για τις συνέπειες αυτής της ενέργειας (Waldman, 2020, CNIL, 2019).

Εικόνα 4: Παράδειγμα αναδυόμενου παραθύρου που εκμεταλλεύεται την αποστροφή για την απώλεια (loss aversion) (Προσωπική περιήγηση στο διαδίκτυο στις 30/3/2023).

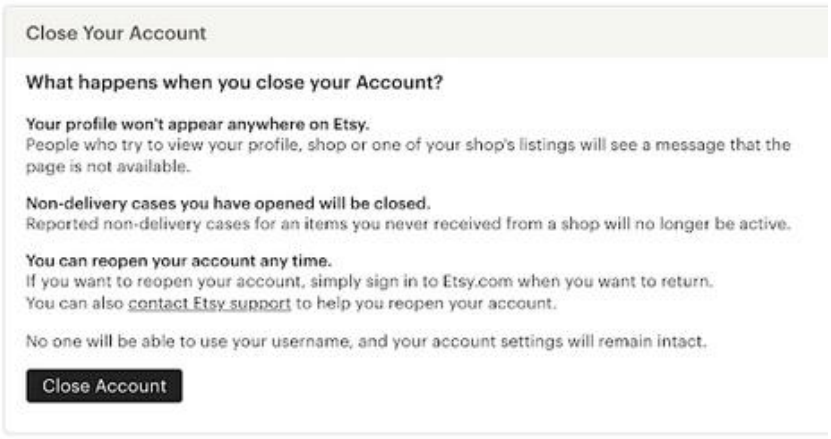
Η διάθεση και τα συναισθήματα του ανθρώπου επηρεάζουν επίσης μιαν απόφαση. Η διάθεση καθορίζει αν η απόφαση θα στηριχτεί στη λογική ή στο ένστικτο. Θετικά συναισθήματα βοηθούν τους ανθρώπους να αποφασίζουν γρηγορότερα, να σκέφτονται ευρύτερα και δημιουργικά για την επίλυση προβλημάτων (Maier and Harr, 2020). Αντίθετα, τα αρνητικά συναισθήματα περιορίζουν τη σκέψη, αλλά και εφιστούν την προσοχή του ανθρώπου ή τον ενεργοποιούν να τα απομακρύνει (CNIL, 2019). Οι online υπηρεσίες εκμεταλλεύονται και τα συναισθήματα, όπως φάνηκε στο παράδειγμα του Confirmshaming. Άλλο χαρακτηριστικό παράδειγμα αποτελεί το Fear Of Missing Out (FOMO). Τα μέσα κοινωνικής δικτύωσης συχνά εκμεταλλεύονται τον φόβο των χρηστών μήπως τους διαφύγει κάτι χρήσιμο, σημαντικό ή διασκεδαστικό (CNIL, 2019, Harris, 2016), ιδίως κατά το στάδιο διαγραφής του λογαριασμού ή της αποσύνδεσης (ΕΣΠΔ, 03/2022, Harris, 2016) με αποτέλεσμα τη συνεχή ανανέωση ή την κύλιση της αρχικής σελίδας, την παρακολούθηση των εικόνων που αναρτώνται και του ηλεκτρονικού γραμματοκιβωτίου. Σε πολλές περιπτώσεις, το αποτέλεσμα είναι ο εθισμός, καθώς έχει παρατηρηθεί ότι η τακτική που χρησιμοποιείται μοιάζει με τις ρουλέτες του καζίνου και ενισχύεται από τις περιοδικές ανταμοιβές (CNIL, 2019, Harris, 2016). Στον εθισμό και τη δέσμευση της προσοχής οδηγούν επίσης τα echo chambers και filter bubbles, που παρουσιάζουν στον χρήστη ειδήσεις με βάση τις προτιμήσεις του αποξενώνοντας τον από την πραγματικότητα και άλλες οπτικές (Leiser and Santos, 2023).

Επομένως, τα σκοτεινά μοτίβα στηρίζονται στο Σύστημα 1, που οδηγεί στη διαισθητική λήψη αποφάσεων σε λίγο χρόνο και με λίγη προσπάθεια. Έτσι, εξηγείται γιατί οι χρήστες αποδέχονται χωρίς ιδιαίτερη περίσκεψη προεπιλεγμένες ρυθμίσεις ή μακροσκελείς πολιτικές απορρήτου με νομική ορολογία χωρίς προηγούμενη ανάγνωση. Οι online πλατφόρμες το γνωρίζουν αυτό, όπως είχε παραδεχτεί ο M. Zuckerberg το 2018 στο Κογκρέσο (npr, 2018). Ομοίως, πολλά cookie banners καθιστούν τους χρήστες επιρρεπείς στη χρήση των προκαταλήψεων και των heuristics λόγω της ασυμμετρίας της πληροφορίας, της διφορούμενης γλώσσας και του σχεδιασμού των επιλογών (Grahl et al., 2021).

2.4.2 Η θεωρία της ώθησης (nudge)

Οι Richard Thaler και Cass Sunstein (2008) ανέπτυξαν την θεωρία της ώθησης (nudge) προκειμένου να αναφερθούν σε «κάθε πτυχή της αρχιτεκτονικής της επιλογής που αλλάζει τη συμπεριφορά των ανθρώπων με προβλέψιμο τρόπο χωρίς να απαγορεύει καμία από τις επιλογές τους ή να μεταβάλλει σημαντικά τα οικονομικά κίνητρά τους. Για να θεωρηθεί μια ώθηση απλή, η παρέμβαση πρέπει να είναι εύκολη και φτηνή για να την αποφύγει κανείς. Οι ωθήσεις δεν είναι εντολές. Η τοποθέτηση φρούτων στο ύψος των ματιών είναι ώθηση. Η απαγόρευση του junk food δεν είναι.» (Thaler and Sunstein, 2009). Η ώθηση με το GPS, που βοηθάει τον οδηγό να φτάσει στον προορισμό που εκείνος θέλει χωρίς να του υπαγορεύει πού θα πάει, απλώς του υποδεικνύει την καλύτερη διαδρομή για να φτάσει εκεί (Thaler, 2018). Το σκεπτικό πίσω από την ώθηση ήταν ότι αφενός δεν ευσταθεί το μοντέλο της αμιγούς ορθολογικής σκέψης, αφετέρου «βελτιώνοντας το περιβάλλον μέσα στο οποίο οι άνθρωποι επιλέγουν μπορούν να κάνουν σοφότερες επιλογές χωρίς να περιορίζουν καμία» (Thaler, 2018). Πρακτικά, πρόκειται για μία τεχνική ενθάρρυνσης ατόμων ή ομάδων να αλλάξουν τη συμπεριφορά τους ή να κάνουν ορισμένες επιλογές χωρίς την άσκηση πίεσης ή την επιβολή υποχρεώσεων ή κυρώσεων (CNIL, 2019). Στόχος ενός συνειδητοποιημένου «αρχιτέκτονα επιλογών» είναι να βοηθήσει τους ανθρώπους να κάνουν καλύτερες επιλογές, όπως οι ίδιοι κρίνουν, και κατ'επέκταση να ωφεληθεί και η κοινωνία, για αυτό η εν λόγω θεωρία σχολιάζεται ως (ήπια) πατερναλιστική (Gunawan et al., 2021, Narayanan et al., 2020, Acquisti et al., 2017). Υπό το πρίσμα του ΓΚΠΔ (άρθρο 4 ορ.7) αυτός είναι ο υπεύθυνος επεξεργασίας (εφεξής ΥΕ) που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας (CNIL, 2019). Ειδικότερα, στον online σχεδιασμό οι καλές ωθήσεις είναι πάντα διαφανείς, εξασφαλίζουν το ευκολότερο δυνατόν opt-out (ιδανικά με ένα κλικ) και ενθαρρύνουν τη συμπεριφορά που θα ενισχύσει την ευημερία αυτών που τις δέχονται. Κατά μία άποψη, οι περισσότερες αποφάσεις σχετικά με τον σχεδιασμό μιας UI μπορούν να θεωρηθούν ως κάποιου είδους ώθηση (Acquisti et al., 20217). Ιδίως τα privacy nudges θα πρέπει να στοχεύουν στην ελαχιστοποίηση της πιθανότητας να μετανιώσουν οι χρήστες για πληροφορίες που μοιράζονται και στην ευθυγράμμιση της συμπεριφοράς τους με τις σαφώς δηλωμένες προτιμήσεις τους (Acquisti et al., 20217).

Ωστόσο, όταν υποβόσκουν κακόβουλα κίνητρα και προστίθενται σκόπιμα εμπόδια που δυσκολεύουν τους χρήστες να κάνουν τις βέλτιστες για το συμφέρον τους επιλογές, τότε το *nudge* (ώθηση) εκφυλίζεται σε *sludge* (λάσπη) που είτε αποθαρρύνει μια συμφέρουσα για αυτούς συμπεριφορά είτε ενθαρρύνει μια βλαπτική συμπεριφορά *στρέφοντας τις προκαταλήψεις και τις heuristics εναντίον τους (*Narayanan et al., 2020, Waldman, 2020, CNIL, 2019). Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2019) προειδοποίησε ότι «υπάρχει μόνο ένα μικρό κενό μεταξύ της ώθησης και της απερίσκεπτης εκμετάλλευσης των φυσικών ανθρώπινων χαρακτηριστικών» και εξέφρασε τους φόβους του για την αυτονομία και την αξιοπρέπεια του ατόμου, καθώς και για το μέλλον των κοινωνικών αξιών και της εμπιστοσύνης στις ψηφιακές υπηρεσίες (Butarelli, 2019). Πράγματι, πολλές online υπηρεσίες χρησιμοποιούν τις ωθήσεις για την τυπική συμμόρφωσή τους με τον ΓΚΠΔ, ενώ ουσιαστικά παραβιάζουν τις απαιτήσεις του (ΕΣΠΔ, 03/2022). Για παράδειγμα, η τοποθέτηση στοιχείων ελέγχου ή πληροφοριών κάτω από το πρώτο επίπεδο ενός cookie banner έχει ως αποτέλεσμα αυτά να περνούν συχνά απαρατήρητα και να αμφισβητείται κατά πόσο μπορεί να γίνεται λόγος για έγκυρη συγκατάθεση. Επιπλέον, κατά το παράδειγμα του Roach Motel πολλές ιστοσελίδες (π.χ. Hard to Cancel, Mathur et al., 2019), εφαρμογές (π.χ. Not possible to logout/delete the account, Di Geronimo et al., 2020) και μεγάλες πλατφόρμες (π.χ. Ease, Forbrukerrådet, 2018) θέτουν εμπόδια (sludges) στο opt-out, στην αποσύνδεση ή στη διαγραφή ενός λογαριασμού παγιδεύοντας και κουράζοντας τους χρήστες (Lingareddy, Schaffner and Chetty, 2022, Habib et al., 2020, Habib et al., 2019, CNIL, 2019). Για παράδειγμα, οι ιστοσελίδες etsy.com και slack.com δεν επιτρέπουν καθόλου τη διαγραφή λογαριασμού (Lingareddy, Schaffner and Chetty, 2022). Η διαγραφή λογαριασμού στην ιστοσελίδα duolingo.com οδηγεί σε μακροσκελές κείμενο που εξηγεί στον χρήστη ότι πρέπει να επιβεβαιώσει μέσω email τη διαγραφή ότι ο λογαριασμός θα απενεργοποιηθεί μετά από μία προθεσμία 7 ημερών προτού ξεκινήσει η διαγραφή των δεδομένων. Η δύναμη της ώθησης αποτυπώνεται και σε δύο πειράματα του 2021, στα οποία οι συμμετέχοντες διατήρησαν τις προεπιλεγμένες ρυθμίσεις είτε αυτές οδηγούσαν προς φιλικές για το απόρρητο επιλογές είτε στην αντίθετη κατεύθυνση (Graßl et al., 2021).



Εικόνα 5: Παράδειγμα Roach Motel/Immortal Account από την ιστοσελίδα etsy.com (Lingareddy, Schaffner and Chetty, 2022).

2.5 Ο αντίκτυπος των σκοτεινών μοτίβων

Βάσει της προηγούμενης ανάλυσης έγινε φανερό ότι ο αντίκτυπος των σκοτεινών μοτίβων σε ένα online περιβάλλον είναι μεγαλύτερος από αυτόν που σημειώνουν οι παραπλανητικές τακτικές στον πραγματικό κόσμο.

2.5.1 Αποτελεσματικότητα

Τα σκοτεινά μοτίβα παρουσιάζονται αρκετά αποτελεσματικά όταν συνδυάζονται (Επιτροπή, 2022, Forbrukerrådet, 2022, US FTC, 2022, CMA, 2022, Luguri and Strahilevitz, 2021), αλλά και όταν χρησιμοποιούνται στα κινητά ή σε μικρές οθόνες, όπου η απόκρυψη πληροφοριών είναι ευκολότερη (Utz et al., 2019, Gunawan et al., 2021) και η διαγραφή του λογαριασμού δυσκολότερη (Lingareddy, Schaffner and Chetty, 2022). Άλλοι παράγοντες που καθορίζουν την επιτυχία τους είναι η διακριτικότητα τους, ο βαθμός διάχυσης τους εντός της UI και η συνακόλουθη δυσκολία ανίχνευσής τους (ΟΟΣΑ, 2022, Gunawan et al., 2021). Φαινομενικά ήπια σκοτεινά μοτίβα, όπως το προεπιλεγμένο κουμπί «Αποδοχή και συνέχεια (συνιστάται)» σε συνδυασμό με το κουμπί «Άλλες επιλογές», μπορούν να αποδειχτούν πιο αποτελεσματικά από επιθετικότερες πρακτικές, όπως είναι τα επαναλαμβανόμενα αιτήματα για μία ενέργεια (Όχληση) και το Παιχνίδι με τα Συναισθήματα/Confirmshaming (Luguri and Strahilevitz, 2021).

2.5.2 Η στάση των χρηστών

Στο σημείο αυτό είναι πολύ σημαντική η στάση των χρηστών. Η Επιτροπή (2022) διαπίστωσε την έλλειψη ευαισθητοποίησης εκ μέρους των καταναλωτών ως προς το θέμα, όμως αντιδρούσαν αρνητικά, αν αντιλαμβάνονταν μιαν αθέμιτη πρακτική. Παρόλα αυτά, η ικανότητα του μέσου καταναλωτή να διακρίνει τη χρήση αυτών των πρακτικών ήταν μάλλον περιορισμένη (Επιτροπή, 2022). Διάφορες ακόμα μελέτες επιβεβαιώνουν την έλλειψη γνώσης σχετικά με το θέμα, την εν τέλει αδιαφορία για την τύχη των δεδομένων ακόμα και αν δηλώνεται ανησυχία (το προαναφερθέν privacy paradox), την αδυναμία αναγνώρισης ή ακόμα και αντίστασης στον παραπλανητικό

σχεδιασμό, ενώ συνεκτιμώνται ενίοτε η ηλικία και το μορφωτικό επίπεδο των χρηστών. Οι συμμετέχοντες σε πειράματα που είτε είχαν χαμηλότερο επίπεδο μόρφωσης είτε πιο προχωρημένη ηλικία είχαν περιορισμένη ικανότητα να αναγνωρίσουν τα σκοτεινά μοτίβα (Επιτροπή, 2022, Luguri and Strahilevitz, 2021, Bongard-Blanchy et al., 2021). Υποστηρίζεται ότι η ικανότητα αναγνώρισης σκοτεινών μοτίβων συνδέεται με προηγούμενη γνώση (Di Geronimo et al., 2020), καθώς και με την αξιοπιστία που εκπέμπουν, τη συχνότητα που τα συναντούν οι χρήστες, το βαθμό απογοήτευσης που βιώνουν, την παραπλανητική συμπεριφορά και την ελκυστικότητα της UI (Bhoot, Shinde and Mishra, 2020). Πολλοί από τους χρήστες είναι «τυφλοί» μπροστά στα σκοτεινά μοτίβα (Di Geronimo et al., 2020, Επιτροπή 2022) ή ακόμα και αν γνωρίζουν σχετικά, παραμένουν άγνωστες πολλές χειριστικές και παραπλανητικές τακτικές και τελικά κατηγορούν τους παρόχους αναγνωρίζοντας στους εαυτούς τους μόνο ένα μικρό μερίδιο ευθύνης (Maier and Harr, 2020). Άλλοι που αναγνωρίζουν σχετικά εύκολα τον χειριστικό σχεδιασμό θεωρούν ότι είναι ελαφρώς μόνο λιγότερο πιθανό να επηρεαστούν σε σχέση με τους υπόλοιπους χρήστες (Bongard-Blanchy et al., 2021). Άλλοι αποδέχονται τα ήπια σκοτεινά μοτίβα ως μέρος της συνήθους ψηφιακής τους εμπειρίας (Επιτροπή, 2022) και δεν αντιδρούν έντονα (Luguri and Strahilevitz, 2021) ή έχουν συνηθίσει να αποδέχονται τις προεπιλογές στα cookie notices, ώστε δεν παρατηρούν την ύπαρξη σκοτεινών μοτίβων (Graßl et al., 2021). Η CNIL (2019) ανησυχεί ότι «η παραδοχή αυτή απειλεί άμεσα την άσκηση των δικαιωμάτων μας». Οι χρήστες σταδιακά βέβαια μαθαίνουν να αναγνωρίζουν τα σκοτεινά μοτίβα και να στιγματίζουν τους παρόχους που τα χρησιμοποιούν σε online περιβάλλοντα, όπως στο hall of shame (Brignull), στο Reddit (r/assholedesign) (Gray, Chivukula and Lee, 2020) ή στο Twitter (#darkpattern) (Mathur, Kshirsagar and Mayer, 2021), αν και ενίοτε το να γνωρίζουν ότι ο σχεδιασμός χρησιμοποιείται εναντίον τους μπορεί να μην είναι αρκετό (ΟΟΣΑ, 2022, CMA, 2022, Bongard-Blanchy et al., 2021). Παράλληλα, υποστηρίζεται ότι η εξατομίκευση των σκοτεινών μοτίβων θα κάμψει την όποια αντίσταση των καταναλωτών (Luguri and Strahilevitz, 2021).

3. Η ΤΡΕΧΟΥΣΑ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΣΚΟΤΕΙΝΩΝ ΜΟΤΙΒΩΝ

3.1 Το παράδειγμα της αμερικανικής έννομης τάξης

Κρίνεται σκόπιμη χάριν της σφαιρικής εξέτασης του θέματος η αναφορά στην προσπάθεια της αμερικανικής έννομης τάξης να αντιμετωπίσει τα σκοτεινά μοτίβα, η οποία μάλιστα προηγείται χρονικά των ενωσιακών ρυθμίσεων. Τόσο σε κρατικό όσο και σε ομοσπονδιακό επίπεδο επικρατεί προβληματισμός για τα δικαιώματα των ατόμων ως φυσικών προσώπων επί των προσωπικών τους δεδομένων και ως καταναλωτών.

Το 2020 ο Επίτροπος της Ομοσπονδιακής Επιτροπής Εμπορίου (εφεξής FTC) εξέδωσε μια δήλωση σχετικά με τη χρήση σκοτεινών μοτίβων, στην οποία σημείωσε ότι τα σκοτεινά

μοτίβα χρησιμοποιούν «οπτικά εσφαλμένη κατεύθυνση, μπερδεμένη γλώσσα, κρυφές εναλλακτικές λύσεις ή ψεύτικη επείγουσα ανάγκη για να κατευθύνουν τους ανθρώπους προς ή μακριά από συγκεκριμένες επιλογές» (Chopra, 2020). Διευκρίνισε δε, ότι πρόκειται για «χαρακτηριστικά σχεδιασμού (design features) που χρησιμοποιούνται για την εξαπάτηση, την καθοδήγηση ή τη χειραγώγηση των χρηστών προς μια συμπεριφορά που είναι κερδοφόρα για μια διαδικτυακή υπηρεσία, αλλά συχνά επιβλαβής για τους χρήστες ή αντίθετη με την πρόθεσή τους» (Chopra, 2020).

Στην Καλιφόρνια, στην πολυπληθέστερη πολιτεία των ΗΠΑ, τα σκοτεινά μοτίβα απαγορεύονται *ρητά* βάσει της California Privacy Rights Act (εφεξής CPRA), η οποία τα ορίζει ως «UI που έχουν σχεδιαστεί ή χειραγωγηθεί έτσι ώστε να υπονομεύουν ή να βλάπτουν ουσιωδώς την αυτονομία, τη λήψη αποφάσεων ή την επιλογή του χρήστη» (CPRA, Cal.Civ.Code §1798.140(l)). Η CPRA ισχύει από τις αρχές του 2023. Είναι γνωστή και ως CCPA 2.0, διότι συμπληρώνει και διορθώνει την California Consumer Privacy Act (CCPA), που τέθηκε σε ισχύ το 2020 και προβλέπει μια σειρά από δικαιώματα καταναλωτών και αντίστοιχες υποχρεώσεις επιχειρήσεων αναφορικά με τη συλλογή και πώληση των προσωπικών δεδομένων των πρώτων. Και στις δύο πράξεις δίνεται έμφαση στη διαφάνεια και την έγκυρη συγκατάθεση. Επιπλέον, προβλέπεται *ρητά* για πρώτη φορά ότι συγκατάθεση χορηγηθείσα υπό την επιρροή ενός σκοτεινού μοτίβου δεν συνιστά αληθινή συγκατάθεση (CPRA, Cal.Civ.Code §1798.140(h)) και καθιερώνεται η υποχρέωση των επιχειρήσεων να σέβονται την ιδιωτικότητα των καταναλωτών, θεσπίζοντας μεταξύ άλλων, αφενός τη δυνατότητα εύκολου opt-out από την πώληση και την κοινή χρήση προσωπικών δεδομένων (καθιερώνεται υποχρέωση για υπερσύνδεσμο με τίτλο «Do Not Sell/Share My Personal Information») (CPRA, Cal.Civ.Code §1798.135(a1) και (c2)), αφετέρου opt-in σε οποιαδήποτε ιστοσελίδα άνευ προηγούμενης χρήσης σκοτεινού μοτίβου (CPRA, Cal.Civ.Code §1798.185(a19) και (a20Ciii)). Η CPRA είναι η *πρώτη νομοθετική ρύθμιση που ορίζει και απαγορεύει ρητά τα σκοτεινά μοτίβα*. Το παράδειγμα της Καλιφόρνια ακολούθησαν και οι πολιτείες του Κολοράντο, του Κονέκτικατ, της Βιρτζίνια, της Γιούτα και μερικών άλλων πολιτειών (IAPP, 2023). Επίσης, ο ενημερωμένος Νόμος της California για την αυτόματη ανανέωση απαιτεί από τις επιχειρήσεις να παρέχουν στους καταναλωτές έναν τρόπο να ακυρώσουν μια συνδρομή που αγόρασαν διαδικτυακά χωρίς να χρειάζεται να περάσουν από επιπλέον βήματα που τους εμποδίζουν να τερματίσουν το πρόγραμμα ανανέωσης (California Legislative Information, χ.χ.).

Σε ομοσπονδιακό επίπεδο η Ενότητα 5 της FTC Act 1914 ρυθμίζει τα σκοτεινά μοτίβα με μία διάταξη που καθιστά παράνομες τις «αθέμιτες ή παραπλανητικές πράξεις ή πρακτικές στο εμπόριο ή αυτές που επηρεάζουν το εμπόριο» (FTC Act, 15 U.S.C. §45). Στη συνέχεια ακολουθεί μία μεθοδολογία τριών βημάτων για να προσδιορίσει αν μια πρακτική είναι αθέμιτη ή παραπλανητική, ενώ δεν απαιτεί πρόθεση. Βάσει αυτής της διάταξης απαγορεύονται η Δυσκολία ακύρωσης της υπηρεσίας, τα Κρυφά κόστη, η

Αναγκαστική συνέχεια, οι Κρυφές πληροφορίες, η Προεπιλογή, οι Ερωτήσεις-παγίδα και η Συγκαλυμμένη διαφήμιση (ΟΟΣΑ, 2022). Υπάρχουν και άλλοι νόμοι που απαγορεύουν παραπλανητικές/χειριστικές πρακτικές, όπως ο CAN-SPAM Act για τη διαφάνεια των email εμπορικού περιεχομένου και ο Νόμος περί Επαναφοράς της Εμπιστοσύνης του Αγοραστή στο Διαδίκτυο (Restore Online Shopper's Confidence Act, ROSCA), που προστατεύει τους καταναλωτές από επαναλαμβανόμενες χρεώσεις και πρακτικές, όπως το Δόλωμα και μεταστροφή, τα Κρυφά κόστη και την Αναγκαστική συνέχεια και επιβάλλει σαφείς και εμφανείς γνωστοποιήσεις των ουσιωδών όρων της συναλλαγής, συγκατάθεση εν επιγνώσει και θετική ενέργεια εκ μέρους του καταναλωτή για συναλλαγές με τρίτα μέρη (Luguri and Strahilevitz, 2021).

Η FTC ασπάστηκε τον όρο «σκοτεινά μοτίβα» και διοργάνωσε μια σειρά από workshops. Το 2022 δημοσίευσε μια σχετική αναλυτική έκθεση και παρουσίασε έξι UI που θέτουν σε κίνδυνο την ιδιωτικότητα των χρηστών (US FTC, 2022). Πρόκειται για αυτές που: α) δεν επιτρέπουν στους καταναλωτές να απορρίψουν οριστικά τη συλλογή ή τη χρήση δεδομένων β) τους προτρέπουν επανειλημμένα να επιλέξουν ρυθμίσεις που επιθυμούν να αποφύγουν γ) παρουσιάζουν μπερδεμένες ρυθμίσεις εναλλαγής που οδηγούν τους καταναλωτές σε ακούσιες επιλογές ως προς την ιδιωτικότητα δ) συσκοτίζουν σκόπιμα τις επιλογές απορρήτου των καταναλωτών και καθιστούν δύσκολη την πρόσβαση σε αυτές ε) επισημαίνουν έντονα μια επιλογή που έχει ως αποτέλεσμα τη συλλογή περισσότερων πληροφοριών, ενώ η επιλογή που επιτρέπει στους καταναλωτές να περιορίζουν τέτοιες πρακτικές έχει πιο θαμπό χρώμα στ) περιλαμβάνουν προεπιλεγμένες ρυθμίσεις που μεγιστοποιούν τη συλλογή και την κοινή χρήση δεδομένων.

Το 2019 δύο γερουσιαστές πρότειναν τη Deceptive Experiences To Online Users Reduction (DETOUR) Act (Fischer, 2019) με στόχο την απαγόρευση των σκοτεινών μοτίβων. Το νομοσχέδιο δεν περιελάμβανε ορισμό, αλλά θα απαγόρευε *στις μεγάλες online πλατφόρμες* να σχεδιάζουν, να τροποποιούν ή να χειραγωγούν μια UI με σκοπό ή ουσιαστικό αποτέλεσμα να συσκοτίζουν, *να υπονομεύουν ή να περιορίζουν την αυτονομία του χρήστη, τη λήψη αποφάσεων ή την εξασφάλιση της συγκατάθεσης ή των δεδομένων του χρήστη*. Επίσης, θα τους απαγόρευε την ομαδοποίηση των καταναλωτών για σκοπούς συμπεριφορικών ή ψυχολογικών πειραμάτων ή μελετών χωρίς την ενημερωμένη συγκατάθεσή τους ή τον σχεδιασμό, την τροποποίηση ή τη διαχείριση μιας UI ή μέρους αυτής, που απευθύνεται σε άτομα κάτω των 13 ετών, με σκοπό ή ουσιαστικό αποτέλεσμα την καλλιέργεια καταναγκαστικής χρήσης, συμπεριλαμβανομένης της αυτόματης αναπαραγωγής βίντεο, που εκκινεί χωρίς τη συγκατάθεση του χρήστη (S.1084 — 116th Congress (2019-2020), Section 3(a)1).

Η DETOUR Act δεν έγινε πλήρως αποδεκτή, αλλά το κείμενό της ενέπνευσε νέους νόμους και στις δύο μεριές του Ατλαντικού, ενώ εισήχθη εκ νέου για συζήτηση το 2021.

Την ίδια χρονιά προτάθηκε ο Αμερικανικός Νόμος για την Προστασία της Ιδιωτικότητας και των Δεδομένων (H.R. 8152, American Data Privacy and Protection Act, ADPPA) που θεωρείται μείζονος σημασίας βήμα προς την απαγόρευση του παραπλανητικού σχεδιασμού και την ανάπτυξη ενός ενιαίου εθνικού πλαισίου προσωπικών δεδομένων. Συγκεκριμένα, το νομοσχέδιο απαιτεί από τις περισσότερες εταιρείες να περιορίζουν τη συλλογή, την επεξεργασία και τη μεταφορά προσωπικών δεδομένων και *απαγορεύει τη μεταφορά προσωπικών δεδομένων ατόμων χωρίς την καταφατική ρητή συγκατάθεσή τους*. Κατοχυρώνει διάφορα δικαιώματα των καταναλωτών, όπως πρόσβασης και διαγραφής και απαιτεί την παροχή δυνατότητας opt-out από τη στοχευμένη διαφήμιση. Ο νόμος θα επιβάλλεται από ομοσπονδιακές και κρατικές ρυθμιστικές αρχές, όπως την FTC και τους Γενικούς Εισαγγελείς των Πολιτειών. Σημειωτέον ότι στις ΗΠΑ οι χρήστες μπορούν να καταγγέλλουν στον αρμόδιο Γενικό Εισαγγελέα ιστοσελίδες που περιέχουν κατά τη γνώμη τους σκοτεινά μοτίβα (https://darkpatternstipline.org/report/). Παράλληλα, τα σκοτεινά μοτίβα συγκεντρώνουν το ενδιαφέρον εταιρειών αυτορρύθμισης της διαφημιστικής τεχνολογίας στις ΗΠΑ, όπως της Network Advertising Industry (εφεξής NAI), η οποία το 2021 είχε ασχοληθεί με το θέμα και το 2022 δημοσίευσε κατευθυντήριες γραμμές για τα μέλη της.

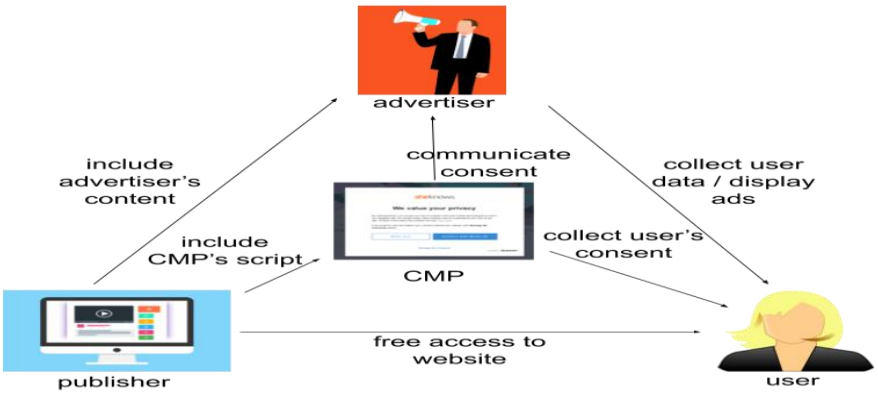
Μερικά πρόσφατα πρόστιμα απεικονίζουν τη σοβαρότητα που αποδίδει η αμερικανική έννομη τάξη στα σκοτεινά μοτίβα. Η Vonage, πάροχος τηλεπικοινωνιών, συμφώνησε τον Νοέμβριο 2022 να πληρώσει 100 εκατομμύρια δολάρια στην FTC προκειμένου να διευθετήσει τις χρεώσεις που δημιουργούσε μέσω μιας εσκεμμένα δύσκολης διαδικασίας που έπρεπε να ακολουθούν οι χρήστες για την ακύρωση της υπηρεσίας και που περιελάμβανε κρυφά τέλη τερματισμού της υπηρεσίας. Τον ίδιο μήνα η Γενική Εισαγγελέας του Όρεγκον ανακοίνωσε ότι η Google προχώρησε σε διακανονισμό 391,5 εκατομμυρίων δολαρίων με 40 γενικούς εισαγγελείς αναφορικά με τις πρακτικές εντοπισμού τοποθεσίας (location tracking) που εφαρμόζει. Πρόκειται για τον μεγαλύτερο διακανονισμό που έχει γίνει ποτέ από γενικούς εισαγγελείς για την ιδιωτικότητα των καταναλωτών στην αμερικανική ιστορία. Συγκεκριμένα, η Google παραπλάνησε τους χρήστες κάνοντας τους να πιστεύουν ότι είχαν απενεργοποιήσει την παρακολούθηση τοποθεσίας, ακόμη και όταν εκείνη συνέχιζε να συλλέγει κρυφά τις πληροφορίες τοποθεσίας τους και να τις χρησιμοποιεί για διαφημίσεις. Στο σχετικό δελτίο τύπου η Γενική Εισαγγελέας του Όρεγκον δήλωσε πως «για χρόνια η Google δίνει προτεραιότητα στο κέρδος έναντι της ιδιωτικότητας των χρηστών της» και πως έχει υπάρξει «πονηρή και παραπλανητική». Τον Δεκέμβριο του 2022 ο Γενικός Εισαγγελέας της Κολούμπια επέβαλε πρόστιμο 9,5 στη εκατομμυρίων δολαρίων στη Google λόγω της χρήσης «σκοτεινών μοτίβων και παραπλανητικών πρακτικών παρακολούθησης τοποθεσίας που παραβίαζαν το απόρρητο των χρηστών». Όμως, το πιο εντυπωσιακό πρόστιμο ύψους 520 εκατομμυρίων δολαρίων επιβλήθηκε τον ίδιο μήνα στην Epic Games, δημιουργό του δημοφιλούς βιντεοπαιχνιδιού Fortnite, για την παραβίαση του νόμου περί του απορρήτου των παιδιών (Children's Online Privacy Protection Act,

COPPA, 1998) και για τη χρήση σκοτεινών μοτίβων για ανεπιθύμητες αγορές και μη εξουσιοδοτημένες χρεώσεις χωρίς έγκριση από τους γονείς. Η εταιρεία δεν εξασφάλιζε ισχυρή συγκατάθεση εκ μέρους των γονέων των ανήλικων παικτών και οι προεπιλεγμένες ρυθμίσεις επέτρεπαν τη ζωντανή επικοινωνία με κείμενου και φωνή, γεγονότα βλαπτικά για την ιδιωτικότητα των παιδιών. Τέλος, τον Μάρτιο του 2023 η FTC απαγόρευσε στην BetterHelp τη γνωστοποίηση ευαίσθητων δεδομένων (υγείας) για διαφημιστικούς σκοπούς παρά τη δέσμευσή της για τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών και της επέβαλε πρόστιμο 7,8 εκατομμυρίων δολαρίων. Η εταιρεία μεταξύ άλλων χρησιμοποιούσε στην πολιτική απορρήτου μικρή γραμματοσειρά και αχνό χρώμα και απέτρεπε ουσιαστικά τους χρήστες να τη διαβάσουν παρά την ύπαρξη σχετικού υπερσυνδέσμου διαβεβαιώνοντας για την ασφάλεια των δεδομένων (Jarovsky, 2023b).

3.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Το 2019, ενώ εφαρμοζόταν για ένα χρόνο ο ΓΚΠΔ, παρατηρήθηκε ότι το 90% 2.000 δημοφιλών ιστοσελίδων από όλο τον κόσμο προσέφερε πλασματικό έλεγχο στους χρήστες. Ενδεικτικά, κατέγραφαν τις δραστηριότητες των χρηστών ακόμα και χωρίς τη συγκατάθεσή τους, η απόρριψη των cookies ήταν συχνά ατελέσφορη και μόνο το 4% έδινε τη δυνατότητα εύκολου opt-out (Sanchez-Rola et al., 2019). Το 2020 μελέτη κατέγραψε 141 ιστοσελίδες που εξέλαβαν εκ των προτέρων ως δεδομένη τη συγκατάθεση των χρηστών, 236 ιστοσελίδες που τους ωθούσαν στην αποδοχή μέσω προεπιλεγμένων ρυθμίσεων και 27 ιστοσελίδες που διατηρούσαν τη συγκατάθεση ακόμα και όταν οι χρήστες είχαν επιλέξει opt-out (Matte, Bielova and Santos, 2020). Την ίδια χρονιά άλλη μελέτη κατέγραψε 22 προϋποθέσεις που πρέπει να πληρούν τα cookie banners βάσει του ΓΚΠΔ και της Οδηγίας ePrivacy και διαπίστωσε ότι οι περισσότερες δεν εφαρμόζονταν λόγω της υφιστάμενης δομής των ιστοσελίδων (Santos, Bielova, and Matte, 2020). Παράλληλα, η γαλλική και βελγική αρχή προστασίας δεδομένων έκριναν ανεπαρκές το πρότυπο Transparency and Consent Framework (TCF) που δημιούργησε ο διαφημιστικός οργανισμός, Interactive Advertising Bureau (IAB Europe), για τους παρόχους διαχείρισης συγκατάθεσης (Consent Management Providers, CMPs). Αυτοί παρέχουν τα cookie banners που ενσωματώνονται στις ιστοσελίδες, είναι υπεύθυνοι για τη λήψη συγκατάθεσης από τον τελικό χρήστη και την αναδιανομή αυτής στους διαφημιστές (Matte, Bielova and Santos, 2020, Gunawan, Santos and Kamara, 2022).

Με αφορμή αυτές τις παρατηρήσεις η εργασία εξετάζει πώς ο σχεδιασμός και η παρουσίαση του περιεχομένου των ιστοσελίδων, εφαρμογών και cookie banners παραβιάζουν τον ΓΚΠΔ και στη συνέχεια την Οδηγία ePrivacy, όπως αναθεωρήθηκε το 2009 και ισχύει ως σήμερα, καθώς και ποια προστασία παρέχεται στα ΥΔ. Με εξαίρεση ορισμένες πρακτικές που απαγορεύει ρητώς ο ΓΚΠΔ (αιτ.σκ.32) οι υπόλοιπες εξετάζονται κατά περίπτωση, καθώς κανένας από τους δύο νόμους δεν αναφέρεται ρητά στα σκοτεινά μοτίβα.



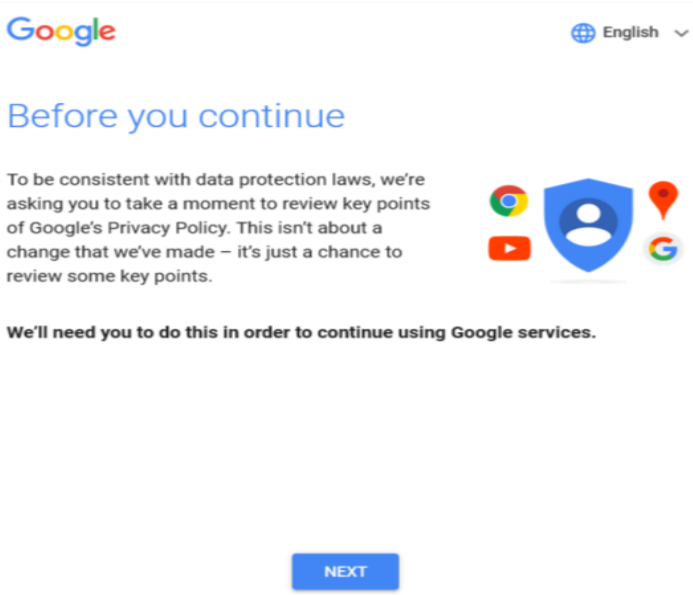
Εικόνα 6: Η λειτουργία των CMPs κατά το πρότυπο TCF του IAB Europe (Matte, Bielova and Santos, 2020).

Ο ΓΚΠΔ θεσπίζει κανόνες για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας (άρθρο 4 ορ.2) των προσωπικών δεδομένων (άρθρο 4 ορ.1). Εφαρμόζεται σε κάθε επεξεργασία που πραγματοποιείται από έναν ΥΕ ή εκτελούντα την επεξεργασία (άρθρο 4 ορ.8) εγκατεστημένο στην ΕΕ, ανεξάρτητα από το πού λαμβάνει αυτή χώρα, ή αφορά προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται στην ΕΕ (άρθρο 3). Η ευθύνη του ΥΕ είναι αντικειμενική, που σημαίνει ότι καλύπτει ακόμη και τα αντι-μοτίβα (Berbece, 2019), ενώ τα πρόστιμα που απειλούνται είναι ιδιαίτερα υψηλά (άρθρο 83). Με οδηγό τις Κατευθυντήριες Γραμμές 03/2022 του ΕΣΠΔ, που παρέχουν συστάσεις και πρακτικές προς τους σχεδιαστές και τους χρήστες σχετικά με την αναγνώριση και αποφυγή σκοτεινών μοτίβων στα μέσα κοινωνικής δικτύωσης, αλλά που μπορούν να τύχουν γενικότερης εφαρμογής σε όλες τις ιστοσελίδες/εφαρμογές, η εργασία ελέγχει τη συμμόρφωση του σχεδιασμού με βάση τις αρχές επεξεργασίας (άρθρο 5 παρ.1), τις προϋποθέσεις της συγκατάθεσης (άρθρα 4, 6, 7), τα δικαιώματα των ΥΔ (άρθρα 15-22) και την προστασία ήδη από το σχεδιασμό και εξ ορισμού (άρθρο 25), ενώ στο τέλος γίνεται αναφορά και στην αυτοματοποιημένη λήψη αποφάσεων (άρθρο 22). Σημειωτέον ότι αν και τα σκοτεινά μοτίβα εμφανίζονται σε προγενέστερο της επεξεργασίας στάδιο, όταν δηλαδή η συλλογή των προσωπικών δεδομένων συνδέεται με το σχεδιασμό της UI, και όχι κατά την επεξεργασία καθαυτή (Jarovsky, 2022, Berbece, 2019, Leiser, 2020), η επίδρασή τους στην τελευταία είναι καθοριστική, όπως θα φανεί στη συνέχεια. Από την άλλη, εξαιτίας αυτού ο ΓΚΠΔ δεν μπορεί να εξασφαλίσει πλήρη προστασία απέναντι στο πρόβλημα.

3.2.1 Αρχή της αντικειμενικότητας της επεξεργασίας

Η αρχή της αντικειμενικότητας της επεξεργασίας (άρθρο 5 παρ.1[α]) μνημονεύεται ήδη από το άρθρο 8 παρ.2 του Χάρτη και συνιστά την αφετηρία στην αξιολόγηση της συμμόρφωσης του σχεδιασμού με τον ΓΚΠΔ. Το ΕΣΠΔ (Κατευθυντήριες γραμμές 04/2019) έχει τονίσει ότι είναι θεμελιώδης αρχή σύμφωνα με την οποία τα προσωπικά δεδομένα δεν πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που είναι *αδικαιολόγητα επιζήμιος, εισάγει αθέμιτα διακρίσεις, είναι απρόβλεπτος ή*

παραπλανητικός για το ΥΔ. Η αρχή συνδέεται στενά με τη διαφάνεια και τη λογοδοσία, λειτουργεί ως «ομπρέλα προστασίας» (ΕΣΠΔ, 03/2022) των προσωπικών δεδομένων από τέτοιες πρακτικές και προσδίδει δεοντολογικό χαρακτήρα στην επεξεργασία (FRA και Συμβούλιο της Ευρώπης, 2019). Διέπει τις σχέσεις του ΥΕ με το ΥΔ και υποδηλώνει μεταξύ άλλων ότι ο πρώτος σέβεται τις επιθυμίες του δεύτερου, ιδίως όταν η συγκατάθεση αποτελεί τη νομική βάση επεξεργασίας (FRA και Συμβούλιο της Ευρώπης, 2019). Στην περίπτωση των online υπηρεσιών πρέπει να διασφαλίζεται η δυνατότητα στους χρήστες να αντιλαμβάνονται τι συμβαίνει με τα δεδομένα τους, ώστε να μη βρεθούν προ εκπλήξεως (FRA και Συμβούλιο της Ευρώπης, 2019). Υποστηρίζεται ότι τα σκοτεινά μοτίβα παραβιάζουν τη συγκεκριμένη αρχή, επειδή δεν ανταποκρίνονται στις εύλογες προσδοκίες των χρηστών, αντιθέτως συνδέουν σκόπιμα τις προσδοκίες τους με εκείνες των ΥΕ λόγω ασυμμετρίας και ανισότητας των μερών (Harris, 2016), επιφέρουν επιπτώσεις στην ικανότητα λήψης απόφασης, χειραγωγούν και εκμεταλλεύονται γνωστικές προκαταλήψεις κατά τη συλλογή των δεδομένων και επηρεάζουν αρνητικά τα σχετικά δικαιώματα των χρηστών (Jarovsky, 2022). Για παράδειγμα, η τακτική των Facebook, Google και Microsoft να πιέζουν τους χρήστες να ολοκληρώσουν την επισκόπηση των ρυθμίσεων εντός του χρόνου που εκείνες όριζαν, χωρίς να παρέχουν σαφή επιλογή αναβολής της διαδικασίας (Forced action and timing) αντιβαίνει στην αρχή της αντικειμενικότητας (Forbrukerrådet, 2018). Το ίδιο ισχύει και για την τακτική των δύο πρώτων παρόχων να εκμεταλλεύονται την τάση των χρηστών να μην αλλάζουν τις προεπιλογές (Forbrukerrådet, 2018). Πάντως, διάφοροι ερευνητές (Jarovsky, 2022, Leiser, 2020) επισημαίνουν ότι η έννοια της αρχής αυτής, παρόλο που διατρέχει τον Κανονισμό, δεν προσδιορίζεται επαρκώς και προσδοκούν ότι η αποσαφήνισή της θα συμβάλει στην αποτελεσματικότερη αντιμετώπιση του προβλήματος.



Εικόνα 7: Το ρορυρ της Google για τον ΓΚΠΔ υποχρεώνει τον χρήστη να ελέγξει τις ρυθμίσεις προτού συνεχίσει τη χρήση της υπηρεσίας. Ακολουθούσε μια σύντομη περίληψη της πολιτικής

απορρήτου της Google και κατά το κείμενο ο έλεγχος του popup ήταν προϋπόθεση για τη συνεχή χρήση των υπηρεσιών της Google (Forbrukerrådet, 2018).

3.2.2 Αρχή της νομιμότητας της επεξεργασίας

Η αρχή της νομιμότητας της επεξεργασίας (άρθρο 5 παρ.1α) επιβάλλει την ύπαρξη και τήρηση μίας τουλάχιστον νομικής βάσης από τις έξι που προβλέπει ο ΓΚΠΔ (άρθρο 6 παρ.1), ενώ προβλέπονται επιπλέον προϋποθέσεις για την νόμιμη επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα στο άρθρο 9. Η συγκατάθεση αποτελεί τη δημοφιλέστερη νομική βάση, αφού την επικαλούνται οι περισσότερες online υπηρεσίες για τη σύννομη επεξεργασία των προσωπικών δεδομένων των χρηστών. Όπως θα φανεί στη συνέχεια, τα σκοτεινά μοτίβα αναιρούν την ισχυρή συγκατάθεση, η οποία συνδέεται με την ικανότητα του χρήστη να παίρνει αποφάσεις. Μάλιστα, πολλοί ΥΕ υπό το βάρος των προϋποθέσεων που πρέπει να πληροί η ισχυρή συγκατάθεση επιλέγουν να αλλάξουν τη νομική βάση της επεξεργασίας από τη συγκατάθεση στην ανάγκη εκτέλεσης μιας σύμβασης (άρθρο 6 παρ.1β). Ως προς την τελευταία το 2023 επιβλήθηκε πρόστιμο 390 εκατομμυρίων ευρώ στη Meta (210 στη Facebook και 180 στο Instagram, ενώ εκκρεμεί η απόφαση για το WhatsApp) μετά από δύο καταγγελίες που είχε υποβάλει η NOYB το 2018, επειδή η Meta θεμελίωνε τις εξατομικευμένες διαφημίσεις στη νομική βάση της σύμβασης που τηρούσε με τους χρήστες αντί της συγκατάθεσης και μάλιστα δεν τους ενημέρωσε επαρκώς για την αλλαγή της νομικής βάσης (NOYB, 2023). Πάντως, η Jarovsky (2022) θεωρεί ότι η απουσία συγκεκριμένου ορισμού, ταξινόμησης και κριτηρίων για τον σαφή προσδιορισμό των σκοτεινών μοτίβων προκαλούν αβεβαιότητα για τις πρακτικές που εμπίπτουν στον ΓΚΠΔ, παρόλο που αυτές αντιβαίνουν στους όρους της συγκατάθεσης. Τέλος, εξυπακούεται ότι βάσει της αρχής η επεξεργασία δεν πρέπει να είναι γενικά παράνομη με την έννοια ότι δεν αντίκειται, για παράδειγμα, στο αστικό ή στο ποινικό δίκαιο (ICO, χ.χ.). Όμως, το στοιχείο της παραπλάνησης που ενυπάρχει στα σκοτεινά μοτίβα μπορεί να ανήκει στην υποκειμενική υπόσταση της απάτης, που τιμωρείται από το ποινικό δίκαιο (Berbece, 2019).

3.2.3 Αρχή της διαφάνειας της επεξεργασίας

Η επεξεργασία των συλλεγόμενων δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται με διαφανή τρόπο σε σχέση με το ΥΔ (άρθρο 5 παρ.1α). Από τη μεριά του ΥΕ η αρχή συμπληρώνεται από το άρθρο 12 παρ.1 (ΕΣΠΔ, 03/2022), κατά το οποίο κάθε πληροφορία σχετική με την επεξεργασία των προσωπικών δεδομένων πρέπει να είναι διατυπωμένη *σε σαφή και απλή γλώσσα, κατανοητή και σε εύκολα προσβάσιμη μορφή* (άρθρο 12 παρ.1 και αιτ.σκ.39). Οι προϋποθέσεις αυτές είναι τόσο σημαντικές όσο το περιεχόμενο της πληροφορίας που παρέχεται στους χρήστες (FRA και Συμβούλιο της Ευρώπης, 2019, CNIL, 2019). Από τη μεριά των ΥΔ ισοδυναμεί με το δικαίωμα ενημέρωσης μεταξύ άλλων σχετικά με τους σκοπούς επεξεργασίας, τους κινδύνους, τις εγγυήσεις και τον τρόπο άσκησης των κατοχυρωμένων δικαιωμάτων των ΥΔ (αιτ.σκ.39).

Η υποχρέωση βαραίνει τον ΥΕ βάσει του άρθρου 26 ακόμα και όταν συλλέγει τα δεδομένα από άλλη πηγή και όχι άμεσα από τους χρήστες, καθώς οι τελευταίοι συχνά δεν γνωρίζουν ότι τρίτοι συλλέγουν και χρησιμοποιούν τα δεδομένα τους θέτοντας σε κίνδυνο τη δυνατότητα άσκησης των δικαιωμάτων τους (VZBV, 2021). Ειδικότερα στα μέσα κοινωνικής δικτύωσης, το ΕΣΠΔ (03/2022) σημειώνει ότι η διαφάνεια είναι σημαντική σε όλο τον κύκλο ζωής ενός λογαριασμού χρήστη, ιδίως κατά τη δημιουργία του. Από την άλλη, ενδεχομένως η άκρα διαφάνεια να παγιδεύει τον χρήστη (ΟΟΣΑ, 2022, Επιτροπή, 2022), ιδίως όταν η ανισότητα των μερών είναι προφανής (Leiser, 2020).

Πλήθος παραπλανητικών τακτικών παραβιάζουν τη συγκεκριμένη αρχή. Η Google και η Facebook επέβαλλαν στους χρήστες να κάνουν πολλά βήματα για να περιορίσουν τη συλλογή δεδομένων (Ease) (Forbrukerrådet, 2018) ή εφάρμοζαν το σύστημα των ανταμοιβών και τιμωρίας «απειλώντας» τους χρήστες με διαγραφή του λογαριασμού τους ή απώλεια λειτουργικότητας στην περίπτωση που απέρριπταν ή προχωρούσαν σε opt-out από την εξατομικευμένη διαφήμιση (Forbrukerrådet, 2018). Σύμφωνα με την Επιτροπή (2022) άλλα σχετικά παραδείγματα είναι η απόκρυψη ή η εσφαλμένη ιεράρχηση πληροφοριών (σημαντικές πληροφορίες δηλαδή αποκρύπτονται από το οπτικό πεδίο του χρήστη ή παρουσιάζονται κατά τρόπο που ωθούν προς συγκεκριμένη επιλογή), οι προεπιλεγμένες προς όφελος του παρόχου ρυθμίσεις, το Παιχνίδι με τα συναισθήματα, οι Ερωτήσεις-παγίδα, η Αναγκαστική εγγραφή και το Friend spam. Ταυτόχρονα, αυτά παραβιάζουν και την αρχή της αντικειμενικότητας. Από τη μεριά του το ΕΣΠΔ (03/2022) εντοπίζει διάφορες πρακτικές που: α) παρεμποδίζουν ή αποκλείουν τους χρήστες από την απόκτηση πληροφοριών ή τη διαχείριση των δεδομένων τους ή β) σχετίζονται με την αστάθεια της UI με αποτέλεσμα να παραβιάζουν την απαίτηση του άρθρου 12 παρ.1. Στην πρώτη περίπτωση ο χρήστης αναζητώντας τις σχετικές πληροφορίες καταλήγει σε υπερσύνδεσμο ανακατεύθυνσης που είτε δεν λειτουργεί είτε δεν είναι καθόλου διαθέσιμος (Dead end) ή αποθαρρύνεται να ενεργοποιήσει επιλογές περισσότερο φιλικές για την ιδιωτικότητα του εξαιτίας των πολλών βημάτων που πρέπει να ακολουθήσει (Longer than necessary) ή εξαιτίας του κενού που μεσολαβεί μεταξύ ενημέρωσης και προσφερόμενων ενεργειών (Παραπλανητική ενημέρωση). Στη δεύτερη περίπτωση ο χρήστης μπερδεύεται από την πληθώρα πληροφοριών και την άτακτη παράθεσή τους (Lacking hierarchy) ή οι πληροφορίες βρίσκονται εκτός πλαισίου και ο χρήστης πιθανόν δεν θα σκεφτεί να τις αναζητήσει εκεί (Decontextualising). Επίσης (ΕΣΠΔ, 03/2022, 2.0), ενδέχεται μια UI να εμφανίζεται διαφορετικά στο κινητό από τον Η/Υ ή να μην ανταποκρίνεται στις προσδοκίες των χρηστών π.χ. με την αλλαγή της θέσης των επιλογών ώστε να μην έχουν τον έλεγχο ή την πληροφορία που αναζητούν (Inconsistent interface).

Τέλος, μια σειρά από πρακτικές συνδεόμενες είτε με τον σχεδιασμό της UI είτε με τις παρεχόμενες πληροφορίες παραβιάζουν και την αρχή της αντικειμενικότητας και την απαίτηση του άρθρου 12 που απορρέει από τη διαφάνεια. Αυτές συνεπάγονται: α) την

υπερφόρτωση (όπως το Privacy maze, εξαιτίας του οποίου ο χρήστης αναγκάζεται να περιηγηθεί σε πολλές σελίδες και το Too many options, κατά το οποίο ο χρήστης καλείται να επιλέξει μεταξύ πολλών δυνατών ρυθμίσεων, αλλά στερείται ενημέρωσης), β) την παράκαμψη (όπως το Look over there, με το οποίο αποσπάται η προσοχή του χρήστη από άλλες επιλογές που μπορεί να μη σχετίζονται με την προστασία δεδομένων), γ) τη συναισθηματική εμπλοκή του χρήστη (όπως το Emotional steering και το Hidden in plain sight, που ωθούν τον χρήστη προς επιλογές πιο παρεμβατικές στο απόρρητο) και δ) την απόκρυψη πληροφοριών (όπως το Conflicting information, το οποίο μπερδεύει τον χρήστη με αντιφατικές πληροφορίες που του δημιουργούν αβεβαιότητα για τις δέουσες ενέργειες και τις συνέπειες τους με αποτέλεσμα να διατηρεί τις προεπιλεγμένες ρυθμίσεις, το Ambiguous wording, κατά το οποίο η ασάφεια των όρων προκαλεί αβεβαιότητα στον χρήστη σχετικά με τον τρόπο επεξεργασίας των δεδομένων του ή της άσκησης των δικαιωμάτων του και το Language discontinuity, κατά το οποίο η ενημέρωση περί της προστασίας δεδομένων δεν παρέχεται στην επίσημη γλώσσα της χώρας του χρήστη σε αντίθεση με την υπηρεσία) (ΕΣΠΔ, 03/2022).

3.2.4 Περιορισμός του σκοπού

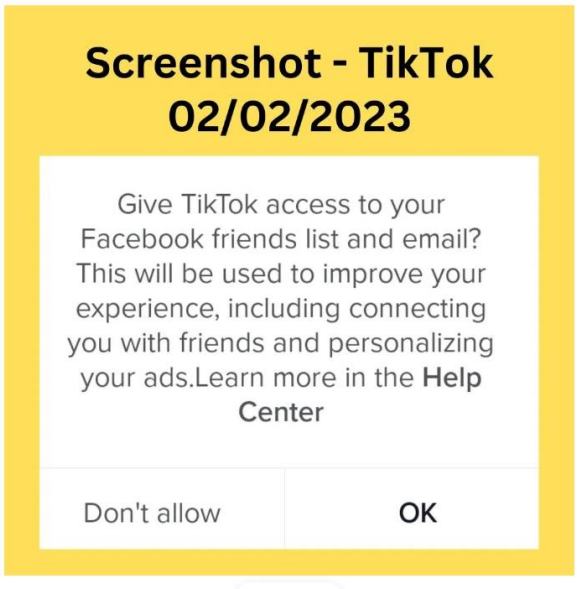
Τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (άρθρο 5 παρ.1β). Κάθε επιπλέον σκοπός που δεν συνδέεται με τον αρχικό πρέπει να έχει τη δική του νομική βάση, οι χρήστες να ενημερώνονται και να τους παρέχονται ξεχωριστά opt-in σε κάθε σκοπό (Machuletz and Böhme, 2019), καθώς περαιτέρω επεξεργασία ενδέχεται να είναι ακατάλληλη ή ανεπιθύμητη για αυτούς.

Έρευνα το 2019 έδειξε ότι το 45,5% περίπου 1.000 cookie notices περιέγραφαν τους σκοπούς με γενικούς όρους (για παράδειγμα, τη βελτίωση της εμπειρίας χρήστη) και το 16,9% δεν δήλωνε κανένα σκοπό (Utz et al., 2019). Παρομοίως, το 2021 το 61% 400 περίπου cookie banners προσδιόριζε εξίσου αόριστα τον σκοπό, το 20% δεν ανέφερε κανέναν και άλλα ενσωμάτωναν σε μία φράση περισσότερους σκοπούς (για παράδειγμα, η φράση «για να αντλήσουμε πληροφορίες σχετικά με το κοινό που βλέπει τις διαφημίσεις και το περιεχόμενο» περικλείει σκοπούς analytics, διαφημιστικούς και profiling) (Santos et al., 2021). Το ΕΣΠΔ (03/2022) παρατήρησε ότι, όταν ο πάροχος στα μέσα κοινωνικής δικτύωσης ζητά τον αριθμό τηλεφώνου των χρηστών για την αυθεντικοποίηση δύο παραγόντων, ο σκοπός επαλήθευσης χρήστη επιτυγχάνεται και με την ηλεκτρονική διεύθυνση.

3.2.5 Ελαχιστοποίηση των δεδομένων

Αναπόσπαστα συνδεδεμένη με τον περιορισμό του σκοπού είναι η αρχή της ελαχιστοποίησης των δεδομένων, σύμφωνα με την οποία αυτά πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους

οποίους υποβάλλονται σε επεξεργασία (άρθρο 5 παρ.1γ). Ωστόσο, σκοτεινά μοτίβα, που υπάγονται στη γενική κατηγορία του Privacy Zuckering προτρέπουν τους χρήστες να παρέχουν υπέρ το δέον προσωπικά τους δεδομένα για την παροχή μιας υπηρεσίας. Για παράδειγμα, το Sweet Seduction (Fritsch, 2017)/Just between you and us (CNIL (2019) διαβεβαιώνει τους χρήστες ότι τα πρόσθετα δεδομένα που θα παράσχουν δεν θα κοινοποιούνται ούτε θα χρησιμοποιούνται ή ότι θα μπορούν να απενεργοποιήσουν την (κοινή) χρήση αυτών των δεδομένων, όπως στην περίπτωση της Facebook που ενθαρρύνει τους χρήστες να δηλώσουν το σχολείο, όπου φοίτησαν, δίνοντας την επιλογή να μην εμφανίζεται η πληροφορία αυτή στο προφίλ τους. Η CNIL (2019) παρουσίασε και άλλα παραδείγματα τακτικών που παραβιάζουν τη συγκεκριμένη αρχή, όπως, όταν ζητείται από τον χρήστη να δώσει τη διεύθυνσή του για να διαβάσει το άρθρο χωρίς να λαμβάνει σαφή προειδοποίηση ότι αυτό ισοδυναμεί με εγγραφή σε ένα newsletter (False continuity) ή όταν η εξατομίκευση και η βελτιωμένη εμπειρία χρήστη τον ενθαρρύνουν να μοιράζεται περισσότερα δεδομένα (Improving the experience). Το ΕΣΠΔ (03/2022) με τη σειρά του αναγνώρισε ως σχετικές πρακτικές τα Longer than necessary και το Emotional steering. Και οι δύο αρχές παρατήρησαν ότι η διατήρηση προεπιλεγμένων παρεμβατικών ρυθμίσεων (Default sharing/Deceptive snugness) καθώς και τα επαναλαμβανόμενα αιτήματα που πιέζουν τον χρήστη να δώσει τον αριθμό τηλεφώνου του για υποτιθέμενους σκοπούς ασφάλειας (Safety Blackmail/Continuous prompting) αντιβαίνουν στην ελαχιστοποίηση των δεδομένων. Στο ίδιο μήκος κύματος βρίσκονται οι Ερωτήσεις-παγίδα (Berbece, 2019) και το παράδειγμα του Linkedin με το Friend Spam (Berbece, 2019). Τέλος, η Google και η Facebook παραβιάζουν την αρχή ποικιλοτρόπως, όταν υπονομεύουν την ανωνυμία και την ψευδωνυμοποίηση χάριν της ασφάλειας (Fogging identification with security) (Fritsch, 2017), όταν χρησιμοποιούν λεξιλόγιο που τονίζει τα πλεονεκτήματα της επεξεργασίας και αποσιωπά τα μειονεκτήματα προκειμένου να εξασφαλίσουν τη συγκατάθεση του χρήστη (Framing) (Berbece, 2019, Forbrukerrådet, 2018) και όταν διευκολύνουν την κοινοποίηση περισσότερων προσωπικών δεδομένων, αλλά δυσκολεύουν σκόπιμα την ελαχιστοποίησή τους (Ease) (Berbece, 2019, Forbrukerrådet, 2018). Η δε πλατφόρμα Tik Tok ζητεί από τον χρήστη πρόσβαση στο email του και στη λίστα των φίλων του στη Facebook, ενέργειες που δεν είναι απαραίτητες για την παροχή της υπηρεσίας, ενώ ο σκοπός της βελτίωσης της εμπειρίας χρήστη είναι αόριστος.



Εικόνα 8: Σύμφωνα με το pop-up κείμενο της Tik Tok η επιλογή «OK» δίνει ταυτόχρονα πρόσβαση στη λίστα των φίλων στη Facebook και στο email του χρήστη (αβέβαιο αν αναφέρεται στις επαφές ή στο περιεχόμενο των mail) για τον σκοπό της βελτίωσης της εμπειρίας χρήστη, της σύνδεσης με φίλους και της εξατομικευμένης διαφήμισης ταυτόχρονα, χωρίς αυτά να είναι απαραίτητα για την παροχή της υπηρεσίας (Jarovsky, 2023c).

3.2.6 Περιορισμός της περιόδου αποθήκευσης και εμπιστευτικότητα

Τα προσωπικά δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των ΥΔ μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των προσωπικών δεδομένων (άρθρο 5 παρ.1^{ε}). Παράλληλα, θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία (άρθρο 5 παρ.1^{στ}). Για παράδειγμα, το σκοτεινό μοτίβο We never forget παραβιάζει αμφότερες τις αρχές, καθώς στην περίπτωση αυτή ένα σύστημα που αποθηκεύει ιστορικό συνδέσεων διατηρεί επ'αόριστον τα διαπιστευτήρια μιας σύνδεσης με κίνδυνο μια one-off σύνδεση να μετατραπεί σε ανεπιθύμητη σύζευξη συσκευών (Berbece, 2019). Το ΕΣΠΔ (03/2022) επίσης παρατηρεί ότι το Deceptive snugness κατά τη δημιουργία λογαριασμού χρήστη, πρακτική που ενεργοποιεί εξ ορισμού τις πιο παρεμβατικές επιλογές, επιμηκύνει την περίοδο αποθήκευσης των δεδομένων.

3.2.7 Λογοδοσία

Ο ΥΕ φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις προηγούμενες αρχές εφαρμόζοντας κατάλληλα τεχνικά και οργανωτικά μέτρα (άρθρα 5 παρ.2 και 24). Για το ΕΣΠΔ (03/2022) η UI και ο UJ μιας πλατφόρμας μπορούν να αποτελέσουν τεκμήριο συμμόρφωσης (ή μη) με τις απαιτήσεις του ΓΚΠΔ. Προδήλως, τα σκοτεινά μοτίβα δεν αποτελούν κατάλληλα τεχνικά και οργανωτικά μέτρα.

3.2.8 Συγκατάθεση

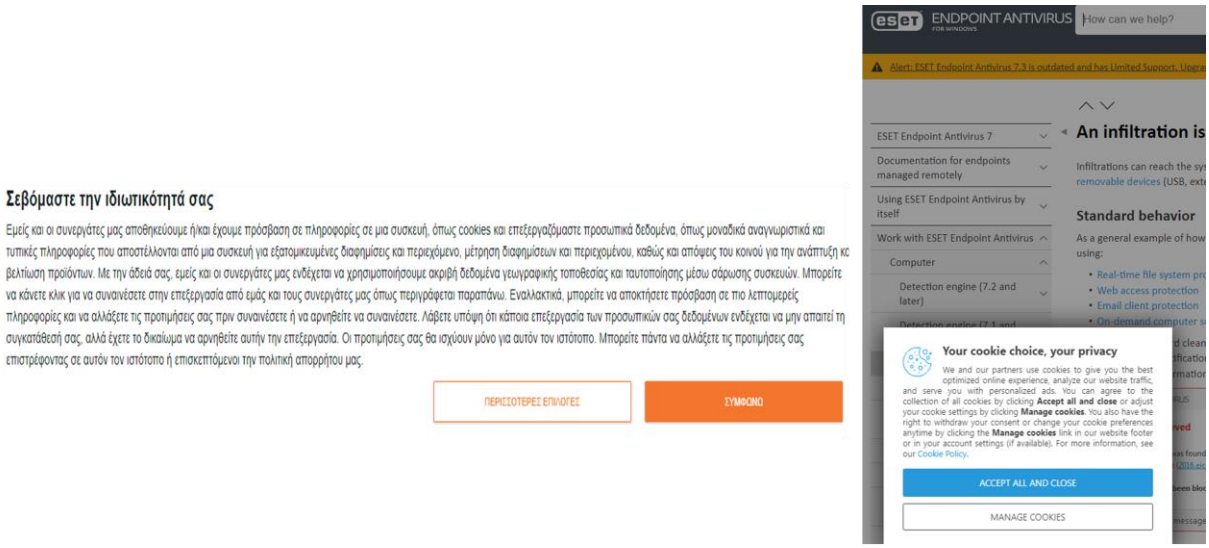
Πρόκειται για κάθε εκ των προτέρων δοθείσα «ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το ΥΔ εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν» (άρθρο 4 ορ.11) και που παρέχεται σε κατανοητή και εύκολα προσβάσιμη μορφή. Οι προϋποθέσεις της έγκυρης συγκατάθεσης είναι αλληλένδετες και αρκεί να μην πληρούται η μία για να θεωρηθεί ανίσχυρη. Επιπλέον, η παρεχόμενη συγκατάθεση δεν απαλλάσσει τον ΥΕ από την υποχρέωση συμμόρφωσης με τις λοιπές αρχές επεξεργασίας (ΕΣΠΔ, Κατευθυντήριες γραμμές 5/2020, CNIL, 2019).

Όσον αφορά τα σκοτεινά μοτίβα και τη σχέση τους με τη συγκατάθεση, το πρόβλημα εντοπίζεται κυρίως στα cookie banners/notices. Το ΕΣΠΔ (2023) έχοντας συγκροτήσει μια ειδική ομάδα δημοσίευσε μία έκθεση σχετικά με τις πολυάριθμες καταγγελίες που είχε υποβάλει η NOYB από το 2021 με στόχο τον τερματισμό της «τρομοκρατίας των cookie banners» και την εξασφάλιση σαφών επιλογών στους χρήστες. Η έκθεση περιλαμβάνει τις ελάχιστες απαιτήσεις που πρέπει να πληροί ένα cookie banner για να συμμορφώνεται με την ενωσιακή νομοθεσία. Βάσει των πορισμάτων μπορούν να χαρακτηριστούν ως σκοτεινά μοτίβα τα cookie banners που: α) δεν περιλαμβάνουν κουμπί για την απόρριψη των cookies στο πρώτο επίπεδο, β) περιλαμβάνουν προσυμπληρωμένα τετραγωνίδια στο δεύτερο επίπεδο, γ) αντί για το κουμπί της απόρριψης των cookies υπάρχει υπερσύνδεσμος που δίνει στο δεύτερο επίπεδο αυτή τη δυνατότητα, αλλά δεν είναι σαφώς ορατός και αντιληπτός, δ) τα χρώματα ή η αντίθεση των κουμπιών μεταξύ τους δίνουν έμφαση στο κουμπί «Αποδοχή όλων», ε) επικαλούνται το έννομο συμφέρον του ΥΕ ως νομική βάση για διάφορες πράξεις επεξεργασίας, όπως για τις εξατομικευμένες διαφημίσεις, στ) χαρακτηρίζουν ως απαραίτητα ή απολύτως απαραίτητα ορισμένα cookies που δεν πληρούν τους όρους του άρθρου 5 παρ.3 της Οδηγίας ePrivacy, η) δεν παρέχουν δυνατότητα –εύκολης– ανάκλησης της συγκατάθεσης.

- Ελεύθερη

Η ελεύθερη συγκατάθεση σημαίνει ότι τα ΥΔ έχουν πραγματική επιλογή και έλεγχο (ΕΣΠΔ, Κατευθυντήριες γραμμές 5/2020). Αν δεν έχουν αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθούν ή να αποσύρουν τη συγκατάθεσή τους χωρίς να ζημιωθούν, τότε η συγκατάθεση δεν είναι ελεύθερη (αιτ.σκ.42). Επίσης, λαμβάνεται υπ᾽όψιν, μεταξύ άλλων κατά πόσο προϋποτίθεται η συγκατάθεση στην επεξεργασία προσωπικών δεδομένων που δεν είναι αναγκαία για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας (άρθρο 7 παρ.4), όπως είναι η εγγραφή σε ένα newsletter. Γενικά, κάθε στοιχείο ανάρμοστης *πίεσης, καταναγκασμού ή επιρροής* στα ΥΔ που δεν τους επιτρέπει να ασκήσουν ελεύθερα τη βούλησή τους καθιστά τη συγκατάθεση ανίσχυρη (ΕΣΠΔ, Κατευθυντήριες γραμμές 5/2020,

Forbrukerrådet, 2018). Το ίδιο ισχύει, όταν υπάρχει κίνδυνος εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων, που υποδηλώνουν σαφή ανισότητα μεταξύ των ΥΔ και του ΥΕ (αιτ.σκ.43). Η ανάκληση της συγκατάθεσης πρέπει να είναι εξίσου ελεύθερη (άρθρο 7 παρ.3 και αιτ.σκ.42). Το ΕΣΠΔ (03/2022) σε αυτό το θέμα ακολουθεί τη λογική του «ίδιου αριθμού κλικ», ενώ ερμηνεύει το αίτημα χρήστη για διαγραφή του λογαριασμού του ως σιωπηρή ανάκληση της συγκατάθεσης.

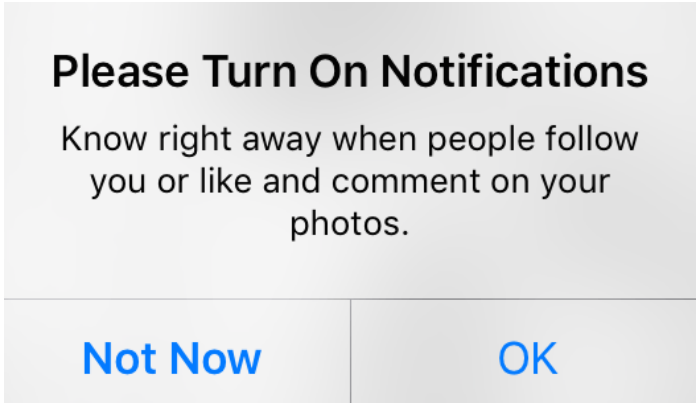


(α) (β)

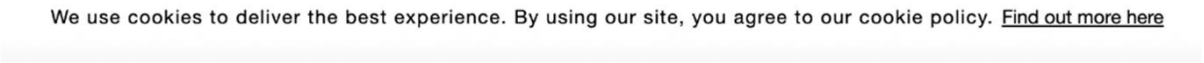
Εικόνα 9: Η απόρριψη στο cookie notice της ιστοσελίδας mixanitouxronou.gr (α) και της endpoint antivirus δεν είναι δυνατή με ένα μόνο κλικ (προσθήκη εμποδίων) και προβάλλεται εντονότερα η επιλογή της αποδοχής (Προσωπική περιήγηση στο διαδίκτυο στις 27/3/2023).

Πολλά σκοτεινά μοτίβα προσκρούουν στην επιταγή της ελεύθερης συγκατάθεσης. Μια μακροσκελής πολιτική απορρήτου που υποχρεώνει τους χρήστες να επιβεβαιώσουν ότι έχουν διαβάσει όλο το κείμενο και αποδέχονται τους όρους και προϋποθέσεις, ειδάλλως δεν μπορούν να κάνουν χρήση της υπηρεσίας, αντιβαίνει στην ελεύθερη συγκατάθεση. Ανάλογες τακτικές εντοπίζονται και στα cookie banners. Ο αχνός χρωματισμός ή/και η απομακρυσμένη τοποθέτηση της απόρριψης της συγκατάθεσης (CNIL, 2019), η πλήρης απουσία αυτής της επιλογής, οι επιλογές στη διατύπωση με αρνητικό λεξιλόγιο (Framing) που συνοδεύουν την απόρριψη των cookies (Santos et al., 2021), φράσεις χαριτωμένες, όπως «Can I have a cookie?» ή άλλες, όπως «We care about your privacy» που αποτρέπουν τον χρήστη να ελέγξει τις επιλογές του (Gunawan, Santos and Kamara, 2022), το δίλημμα του χρήστη που καλείται να επιλέξει μεταξύ των «Αποδοχή Όλων» ή «Περισσότερες Επιλογές» αποτελούν ενδεικτικά παραδείγματα. Το ίδιο ισχύει και για τα consent walls που μπλοκάρουν την πρόσβαση στην ιστοσελίδα μέχρι να εκφράσει ο χρήστης τις προτιμήσεις του για τη συγκατάθεση, καθώς και για τα cookie walls που μπλοκάρουν την παροχή μιας υπηρεσίας, αν δεν συγκατατεθεί στην εγκατάσταση των cookies (Gray et al., 2021, CNIL, 2019) και κατά των οποίων έχει τοποθετηθεί σαφώς το

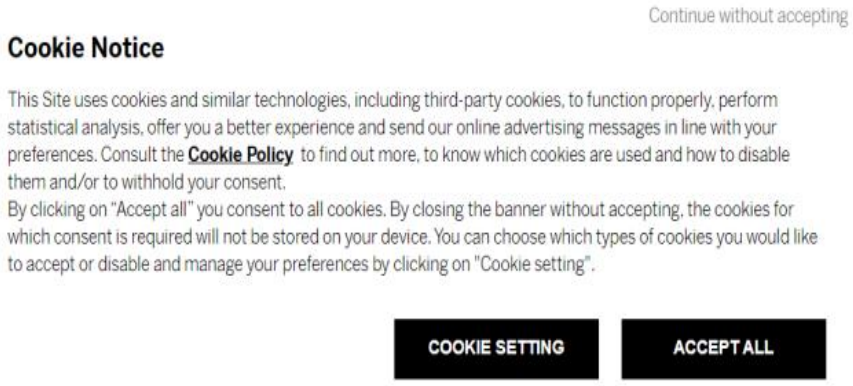
ΕΣΠΔ (05/2020). Ομοίως, η ανακατεύθυνση του χρήστη σε περιβάλλον περιορισμένης λειτουργικότητας λόγω του ότι δεν παρέχει πλήρη ή μερική συγκατάθεση λειτουργεί σαν τιμωρία (Gray et al., 2021). Συναφώς, καταγράφεται και η περίπτωση που οι ιστοσελίδες εκμεταλλευόμενες την ισχύ τους, αρνούνται την πρόσβαση σε όποιον χρησιμοποιεί την τεχνολογία TOR για την ανωνυμία (You can run but you can't hide) (Fritsch, 2017). Για άλλη μία φορά, οι μεγάλες πλατφόρμες προσφέρουν πολλά σχετικά παραδείγματα. Χρησιμοποιούν πρακτικές, που εκμεταλλεύονται τις γνωστικές προκαταλήψεις και την ανισότητα των μερών για να χειραγωγούν τους χρήστες, να τους πιέζουν, να τους παραπλανούν και να τους αποθαρρύνουν από την αποσύνδεση ή το opt-out. Η Facebook *παραπλάνησε* τους χρήστες να αποδεχτούν τη σύνδεση των λογαριασμών τους στο Whatsapp και Facebook (Berbece, 2019), ενώ δεν παρείχε ουσιαστικά επιλογές αναφορικά με τη συλλογή δεδομένων από τρίτα μέρη (Απόκρυψη πληροφοριών). Το αναδυόμενο παράθυρο του Instagram για την ενεργοποίηση των ειδοποιήσεων προσέφερε μόνο τις επιλογές «Όχι τώρα» και «OK» ώστε να πιέζει συστηματικά τους χρήστες (Όχληση, Gray et al., 2018) και η Google *εξανάγκασε* τους χρήστες να αποδεχτούν την καταγραφή της τοποθεσίας, συνδέοντας το Ιστορικό Τοποθεσίας με το Google Assistant ή Places services (Forced disclosure) (Forbrukerrådet, 2018a). Τέλος, υπενθυμίζεται η ψευδαίσθηση του ελέγχου ως παράδειγμα *χειραγώγησης* και η περίπτωση της Amazon ως παράδειγμα *εμποδίων* στον τερματισμό μιας υπηρεσίας (βλ. 2.2).



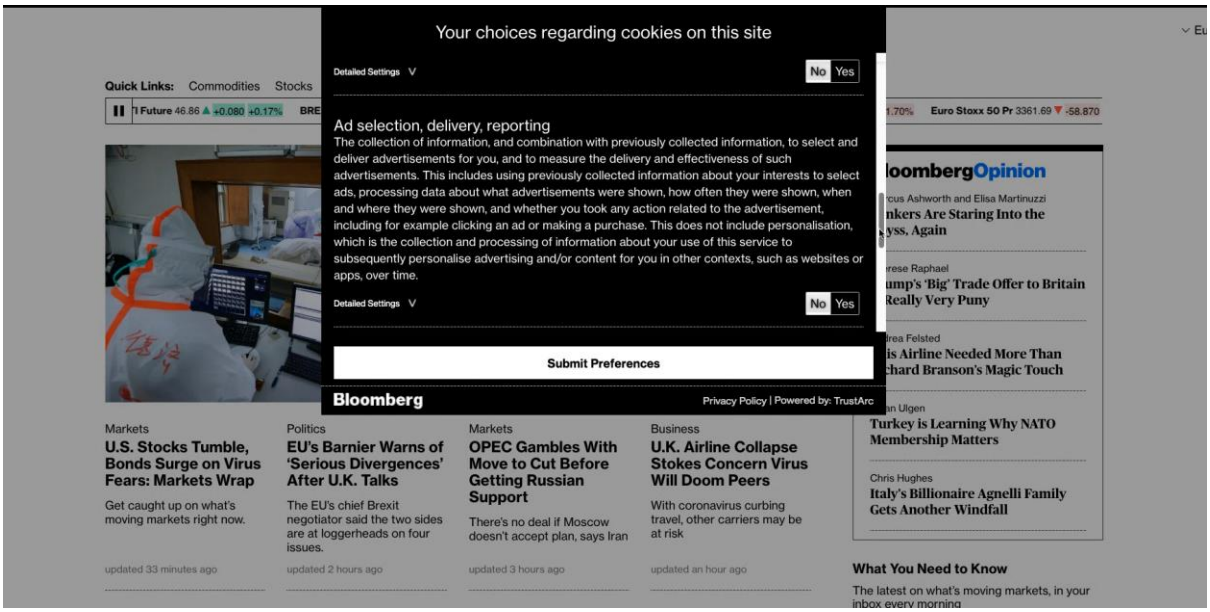
Εικόνα 10: Παράδειγμα Όχλησης (Nagging) στο Instagram. Δεν προσφέρεται η επιλογή οριστικής απόρριψης (Gray et al., 2018).



Εικόνα 11: Το cookie notice περιγράφει εντελώς αόριστα τον σκοπό και δεν προσφέρεται καμία επιλογή. Οι χρήστες ενδέχεται να μην προσέξουν καν το cookie consent και να συνεχίσουν την κύλιση προς τα κάτω του ιστοτόπου (Danyang, 2023).



Εικόνα 12: Η επιλογή της απόρριψης στο cookie notice της ιστοσελίδας prada.com σημειώνεται πάνω δεξιά με αχνό γκρι χρωματισμό και χωριστά από τις άλλες επιλογές (Προσωπική περιήγηση στο διαδίκτυο στις 18/6/2023).



Εικόνα 13: Παράδειγμα Consent Wall από την ιστοσελίδα Yahoo το 2020 (Gray et al., 2021).

- Συγκεκριμένη

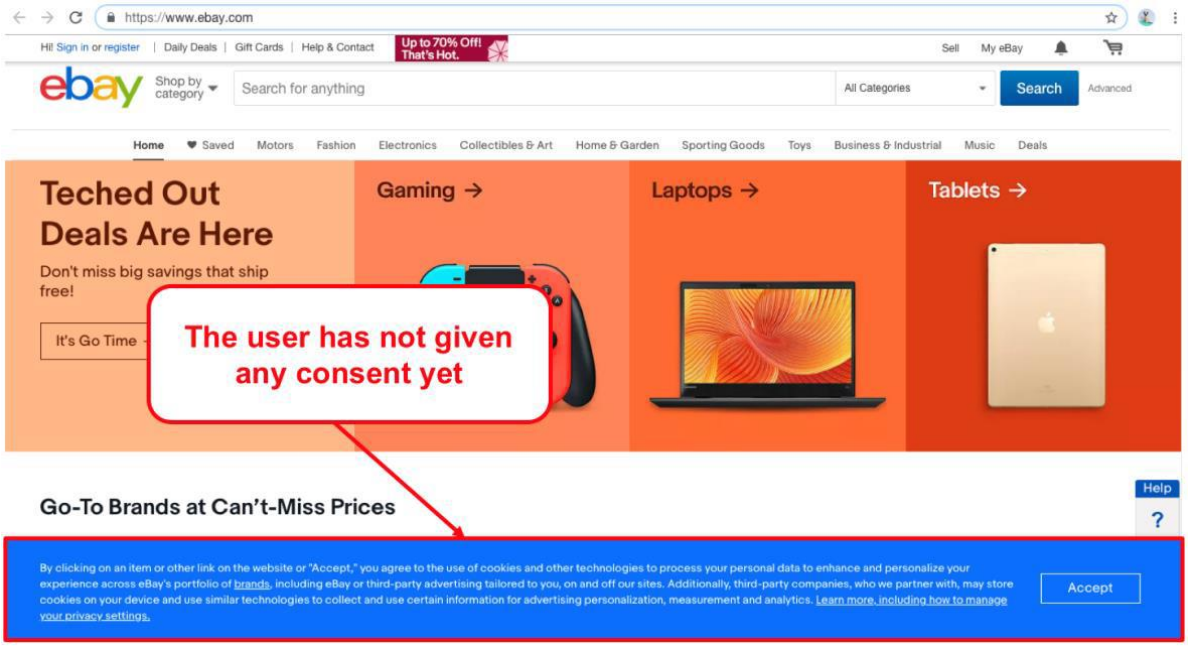
Όταν η συγκατάθεση είναι συγκεκριμένη, διασφαλίζεται «ένας βαθμός ελέγχου για τον χρήστη και διαφάνειας για το ΥΔ» (ΕΣΠΔ, 05/2020). Η συγκατάθεση πρέπει να παρέχεται για «έναν ή περισσότερους συγκεκριμένους» (άρθρο 6 παρ. 1^{α} και αιτ.σκ.32) σκοπούς και το ΥΔ να έχει επιλογή για καθέναν εξ αυτών. Με άλλα λόγια, ο ΥΕ πρέπει να παρέχει για κάθε σκοπό χωριστό αίτημα συγκατάθεσης ως προς τα δεδομένα που υποβάλλονται σε επεξεργασία και τις σχετικές συγκεκριμένες πληροφορίες. Τα σκοτεινά μοτίβα που αποκρύπτουν τις απαραίτητες πληροφορίες παραβιάζουν αυτή την απαίτηση (Berbece, 2019). Συγκεκριμένα, στα cookie banners το προεπιλεγμένο

κουμπί «Αποδοχή όλων» και στη συνέχεια το opt-out που πρέπει να κάνει ο χρήστης σε κάθε προβαλλόμενο σκοπό (Berbece, 2019), ο αχνός χρωματισμός ή η απουσία της δυνατότητας της διαμόρφωσης των επιλογών και η παρουσίαση περισσότερων διαφορετικών σκοπών σαν να πρόκειται για έναν μόνο (Gunawan, Santos and Kamara, 2022) παραβιάζουν την απαίτηση της συγκεκριμένης συγκατάθεσης. Επίσης, τα επαναλαμβανόμενα αιτήματα συγκατάθεσης για την εγκατάσταση cookies αντιβαίνουν τόσο στη συγκεκριμένη όσο και στη ρητή (βλ. κατωτέρω) συγκατάθεση, καθώς η συστηματική πίεση μπορεί να οδηγήσει τους χρήστες να υποχωρήσουν λόγω κόπωσης από τα πολλά κλικ (consent/click fatigue) ή ανυπομονησίας να χρησιμοποιήσουν την υπηρεσία (ΕΣΠΔ, 03/2022) και τελικά να παράσχουν τη συγκατάθεσή τους για πράξεις που υπό άλλες συνθήκες θα απέρριπταν. Τέλος, η χρήση λεξιλογίου με θετικό πρόσημο (Framing) (π.χ. «Χρησιμοποιούμε cookies για να σας προσφέρουμε την καλύτερη δυνατή εμπειρία περιήγησης») παραβιάζει και τη συγκεκριμένη και την ελεύθερη συγκατάθεση, αφού οι σκοποί επεξεργασίας παρατίθενται αόριστα (Santos et al., 2021).

- Ρητή

Η συγκατάθεση θα πρέπει να παρέχεται με δήλωση ή με σαφή θετική ενέργεια. Αντίθετα, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν πρέπει να εκλαμβάνονται ως συγκατάθεση (αιτ.σκ.32), ενώ σε ορισμένες περιπτώσεις ο ΓΚΠΔ απαιτεί συγκεκριμένα τη ρητή συγκατάθεση αποβλέποντας στην υψηλότερη προστασία (άρθρα 9, 22 και 49). Για αυτό οι ΥΕ θα πρέπει να σχεδιάζουν τους μηχανισμούς συγκατάθεσης κατά τρόπο σαφή για τα ΥΔ (ΕΣΠΔ, 05/2020). Ιδίως, ως προς τη σιωπή, η απλή συνέχιση της συνήθους χρήσης ιστοτόπου δεν συνιστά συμπεριφορά από την οποία μπορεί να συναχθεί δήλωση βούλησης του ΥΔ να συμφωνήσει σε προτεινόμενη πράξη επεξεργασίας. Το ίδιο ισχύει και για ενέργειες, όπως η κύλιση προς τα κάτω και η μετατόπιση σε ιστότοπο (ΕΣΠΔ, 05/2020). Παρόλα αυτά, το 2020 στο Ηνωμένο Βασίλειο το 32% 680 ιστοσελίδων χρησιμοποιούσε τη σιωπηρή/εικαζόμενη συγκατάθεση (Nouwens et al., 2020) και το 2021 το 5,7% 950 περίπου γερμανικών ιστοσελίδων ερμήνευε την περιήγηση στην ιστοσελίδα ως σιωπηρή συγκατάθεση στο tracking (Ομοσπονδία Γερμανικών Οργανώσεων Καταναλωτών - VZBV, 2021). Ως προς τα προσυμπληρωμένα τετραγωνίδια, το Δικαστήριο της ΕΕ (εφεξής ΔΕΕ) στην υπόθεση Planet 49 (C-763/17) και στην υπόθεση Orange Romania (C-61/10) διευκρίνισε ότι αυτά δεν αρκούν για την αποθήκευση των cookies, αλλά απαιτείται η παροχή από τους χρήστες του διαδικτύου συγκατάθεσης με θετική ενέργεια. Ανάλογα κινήθηκε και το Περιφερειακό Δικαστήριο του Ρόστοκ της Γερμανίας μετά από καταγγελία που υποβλήθηκε από τη VZBV (2021) κατά μιας online υπηρεσίας που βοηθά τους χρήστες να βρουν δικηγόρο. Το δικαστήριο έκρινε ότι η χρήση προεπιλεγμένων τετραγωνιδίων στα cookie banners παραβίαζαν τον ΓΚΠΔ σημειώνοντας ότι οι επιλογές αποδοχής και απόρριψης πρέπει να προβάλλονται ισότιμα. Υπό αυτό το πρίσμα απαγορεύονται πρακτικές, όπως η προεπιλογή «Αποδοχή

όλων», το αχνό (γκρι συνήθως) χρώμα στο κουμπί «Περισσότερες επιλογές» που δίνει την εντύπωση ότι δεν είναι επιλέξιμο (Aesthetic manipulation/Ετεροκατεύθυνση), το κόκκινο χρώμα στο κουμπί της απόρριψης και το πράσινο στης αποδοχής (Gunawan, Santos and Kamara, 2022) και τα επαναλαμβανόμενα αιτήματα (Berbece, 2019). Συναφώς, μελέτες έχουν δείξει ότι η τοποθέτηση στοιχείων ελέγχου ή πληροφοριών κάτω από το πρώτο επίπεδο του cookie notice, ώστε να διαφύγουν από την προσοχή των χρηστών αντιβαίνει στην ελεύθερη και ρητή συγκατάθεση (Gray et al., 2021, Kampanos and Shahandashti, 2021, Matte, Bielova and Santos, 2020, Nouwens et al., 2020).



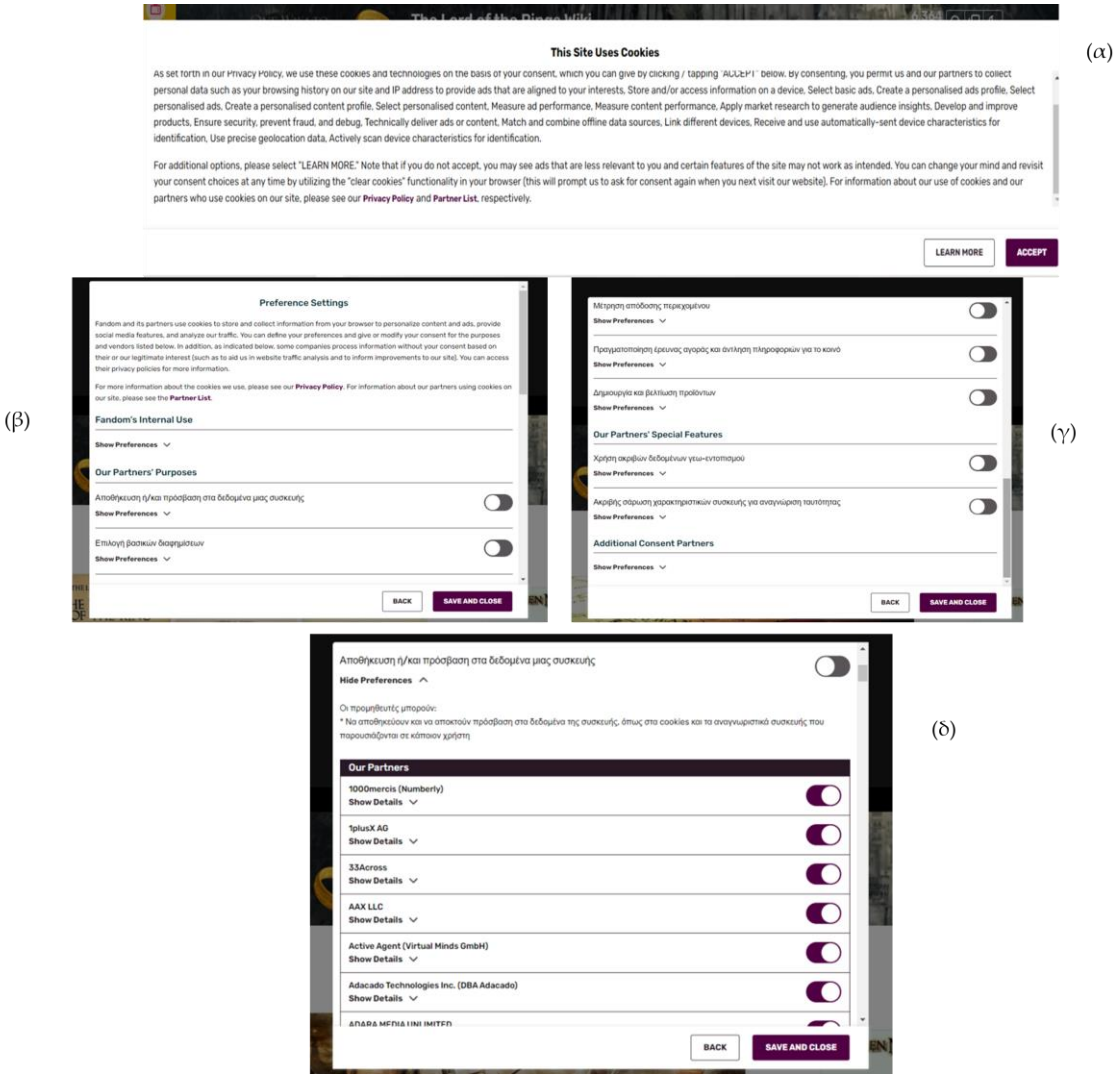
Εικόνα 14: Η ιστοσελίδα Ebay το 2019 περιελάμβανε μόνο την επιλογή της «Αποδοχής» και προειδοποιούσε τον χρήστη ότι ακόμα και το κλικ σε ένα προϊόν ή άλλον υπερσύνδεσμο ισοδυναμούσε με αποδοχή των cookies (Santos, Bielova and Inria, 2020).

- Εν πλήρει επιγνώσει

Η απαίτηση αυτή συνδέεται με την αρχή της διαφάνειας, καθώς το αίτημα για συγκατάθεση πρέπει να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, με σαφή και απλή διατύπωση (άρθρο 7 παρ.2). Όσα σκοτεινά μοτίβα παραβιάζουν την αρχή της διαφάνειας, αντιβαίνουν και στην προϋπόθεση αυτή. Ως προελέχθη, ο καταιγισμός πληροφοριών δεν εξασφαλίζει ότι οι χρήστες θα διαβάσουν ούτε ότι θα αντιληφθούν τις μακροσκελείς δηλώσεις. Ούτε όμως η ελλιπής πληροφόρηση είναι αποδεκτή, για αυτό απαγορεύονται πρακτικές όπως η Προεπιλογή, το Framing και η ψευδαίσθηση του ελέγχου (Berbece, 2019). Το ΕΣΠΔ (03/2022) περιγράφει δύο άλλα παραδείγματα. Το κείμενο ενός cookie banner που εναλλάσσει τις έννοιες του cookie ως ιχνηλάτη και ως γλυκίσματος και περιέχει δύο υπερσυνδέσμους, εκ των οποίων ο πρώτος οδηγεί σε μία συνταγή ζαχαροπλαστικής και ο δεύτερος στην πολιτική απορρήτου προσφέροντας ταυτόχρονα μόνο το κουμπί «ΟΚ» ενδέχεται να μπερδέψει τους χρήστες, οι οποίοι θα πατήσουν το κουμπί χωρίς να έχουν

ενημερωθεί πλήρως. Επίσης, η λίστα συνεργατών σε μια πολιτική απορρήτου που δεν περιέχει υπερσύνδεσμο προς τις δικές τους πολιτικές, αλλά εναπόκειται στον χρήστη να επισκεφτεί τις ιστοσελίδες τους για την ενημέρωσή του τον εμποδίζει να γνωρίζει πλήρως τις συνέπειες της συγκατάθεσής του. Ομοίως, όταν ο χρήστης ανακατευθύνεται προς ιστοσελίδα μειωμένης λειτουργικότητας, επειδή απέρριψε μερικούς ή όλους τους σκοπούς της επεξεργασίας, ενδέχεται να μη γνώριζε εξαρχής ότι η απόφασή του θα επηρέαζε το περιεχόμενο της ιστοσελίδας. Σύμφωνα, όμως, με τον Εισαγγελέα του Δικαστηρίου της ΕΕ η γνώση των συνεπειών της άρνησης στην παροχή συγκατάθεσης είναι κρίσιμη προκειμένου να πληρούται το κριτήριο της πλήρους επίγνωσης (Gray et al., 2021).

Ενδιαφέρουσα ένσταση που διατυπώνει η Jarovsky (2022) αναφορικά με τη συγκατάθεση ως ένδειξη αυτονομίας είναι ότι ο homo economicus φαίνεται να μην αποκλείεται εντελώς από τον ΓΚΠΔ, ο οποίος παραβλέπει την επιρροή των γνωστικών προκαταλήψεων και της online χειραγώγησης. Για αυτό προτείνει να ληφθεί υπ᾽όψιν ο homo manipulable που επηρεάζεται από ποικίλες γνωστικές προκαταλήψεις και που είναι ευάλωτος σε κακόβουλους παράγοντες, ιδίως στο online περιβάλλον.



Εικόνα 15: Το cookie notice της ιστοσελίδας lotr.fandom περιέχει μόνο δύο επιλογές, «Αποδοχή» και «Μάθετε περισσότερα», ενώ ο χρωματισμός προτρέπει τον χρήστη να επιλέξει την «Αποδοχή»(α). Κάνοντας κλικ στο «Μάθετε περισσότερα» εμφανίζεται μια μεγάλη λίστα με τους σκοπούς επεξεργασίας των δεδομένων από την ιστοσελίδα και τους συνεργάτες της, οι οποίοι είναι ανενεργοί και ταυτόχρονα κάθε σκοπός έχει από κάτω μία πτυσσόμενη λίστα επιλογών (β-γ). Πατώντας σε καθεμία από τις λίστες φαίνεται ότι τελικά η σύνδεση με τους συνεργάτες είναι εξ ορισμού επιλεγμένη (δ) (Προσωπική περιήγηση στο διαδίκτυο στις 18/5/2023).

3.2.9 Δικαιώματα υποκειμένων των δεδομένων (ΥΔ)

Ο ΓΚΠΔ αναγνωρίζει μια σειρά από δικαιώματα στα ΥΔ. Από τη μεριά τους, οι ΥΕ υποχρεώνονται να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα που θα διευκολύνει την άσκηση αυτών των δικαιωμάτων (άρθρο 12 παρ. 2). Ευλόγως ο σχεδιασμός είναι καθοριστικός και πάλι, αφού η παρεχόμενη σχετική ενημέρωση πρέπει να είναι απλή, πρακτική και σε εμφανές σημείο. Το ΕΣΠΔ (2022) κατέγραψε στα μέσα κοινωνικής δικτύωσης διάφορες πρακτικές που δυσχεραίνουν την άσκηση των δικαιωμάτων, όπως την ανεπαρκή ενημέρωση και την προσθήκη εμποδίων που δυσκολεύουν τους χρήστες να εντοπίσουν πού και πώς θα ασκήσουν τα δικαιώματα. Για παράδειγμα, η Facebook επιβαρύνει τους χρήστες με πολλά βήματα για τον περιορισμό

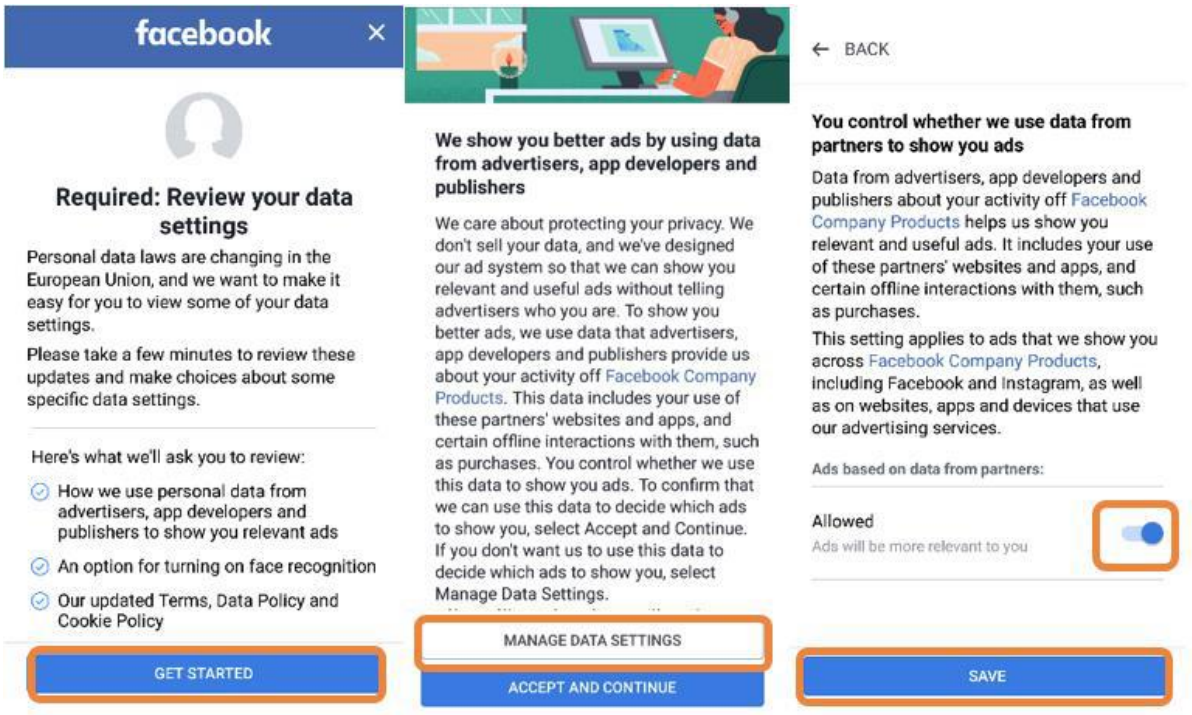
των συλλεγόμενων δεδομένων (Gunawan et al., 2021, Forbrukerrådet, 2018) και τους δημιουργεί εσκεμμένα την ψευδαίσθηση ότι μπορούν να ελέγξουν τη χρήση δεδομένων για σκοπούς διαφήμισης (Forbrukerrådet, 2018). Ομοίως, η Google αναγκάζει τους χρήστες να πατούν περισσότερα κουμπιά και υπερσυνδέσμους για να έχουν πρόσβαση στην ενημέρωση για την επεξεργασία των δεδομένων (Forbrukerrådet, 2018).

3.2.10 Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Η ιδέα της προστασίας των δεδομένων ήδη από το σχεδιασμό προτάθηκε μέσα από επτά βασικές αρχές[6] (Cavoukian, 2009) και ενσωματώθηκε στο άρθρο 25 του ΓΚΠΔ, ενώ πρόσφατα καθιερώθηκε ως πρότυπο ISO 31700 (https://www.iso.org/standard/76772.html). Σύμφωνα με την πρώτη παράγραφο του άρθρου ο ΥΕ εφαρμόζει αποτελεσματικά τόσο *κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας* όσο και κατά τη στιγμή της επεξεργασίας κατάλληλα τεχνικά και οργανωτικά μέτρα, (δηλαδή επιλογές αρχιτεκτονικής, όπως την ελαχιστοποίηση της επεξεργασίας και την ψευδωνυμοποίηση των προσωπικών δεδομένων κατά την αιτ.σκ.78,) σχεδιασμένα για την εφαρμογή των *αρχών προστασίας του άρθρου 5* και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία έτσι ώστε να πληρούνται οι απαιτήσεις του κανονισμού και να προστατεύονται *τα δικαιώματα των ΥΔ*. Το εν λόγω άρθρο λειτουργεί σαν γέφυρα μεταξύ του σχεδιασμού και της νομικής ρύθμισης, καθώς τονίζει την κρισιμότητα διάφορων τεχνικών σχεδιασμού παροχής μιας υπηρεσίας για την προστασία των δεδομένων, ιδίως σε σχέση με τη διαφάνεια, τη συγκατάθεση και τα δικαιώματα των χρηστών (Επιτροπή 2022, CNIL, 2019). Το ΕΣΠΔ (03/2022) αναγνωρίζει την κρισιμότητα του άρθρου, καθώς η εφαρμογή του μπορεί να βοηθήσει τους παρόχους των μέσων κοινωνικής δικτύωσης να αποφύγουν τα σκοτεινά μοτίβα εξαρχής πριν καν προσφέρουν την υπηρεσία τους. Υποστηρίζεται ωστόσο και ο αντίλογος ότι απουσιάζει η σαφής σύνδεση του άρθρου με τα πιθανά μέτρα που πρέπει να λάβουν οι ΥΕ για την αποφυγή των σκοτεινών μοτίβων, καθώς αυτό εστιάζει κυρίως στη φάση της επεξεργασίας και στα μέτρα που θα μπορούσαν να ληφθούν για τη μείωση της βλάβης σε αυτό το στάδιο, ενώ τα σκοτεινά μοτίβα, ως προελέχθη, εντοπίζονται σε προηγούμενο στάδιο. Οι αρχές του άρθρου είναι ευρείες, χρήσιμες ως γενικές κατευθύνσεις, αλλά όχι τεχνολογικά εξειδικευμένες για να αντιμετωπίσουν αποτελεσματικά τα σκοτεινά μοτίβα και μάλιστα τα πιο ήπια (Jarovsky, 2022, Egberts, 2021).

[6] 1) Πρόληψη και όχι αντίδραση ούτε θεραπεία 2) Το απόρρητο ως προεπιλεγμένη ρύθμιση 3) Το απόρρητο ενσωματωμένο στο σχεδιασμό 4) Πλήρης λειτουργικότητα-Θετικό άθροισμα, όχι μηδενικό 5) Ασφάλεια από άκρη σε άκρη-Προστασία σε όλο τον κύκλο ζωής 6) Ορατότητα και διαφάνεια -Διατηρήστε το ανοιχτό 7) Σεβασμός του απορρήτου των χρηστών-Διατηρήστε το με επίκεντρο τον χρήστη.

Σύμφωνα με τη δεύτερη παράγραφο του άρθρου ο ΥΕ εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι εξ ορισμού υφίστανται επεξεργασία μόνο όσα προσωπικά δεδομένα είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Η υποχρέωση αυτή συνδέεται με την *αρχή της ελαχιστοποίησης* των δεδομένων και τον *περιορισμό του σκοπού* (ΕΣΠΔ 4/2019, Forbrukerrådet, 2018) και προτρέπει κάθε ΥΕ να επιλέγει τα λιγότερο παρεμβατικά μέτρα, ώστε οι χρήστες να έχουν τον πραγματικό έλεγχο των δεδομένων τους. Και οι δύο αρχές μαζί εξασφαλίζουν ότι τα προσωπικά δεδομένα προστατεύονται αυτομάτως και δεν απαιτείται καμία ενέργεια εκ μέρους του χρήστη. Στον αντίποδα βρίσκονται οι υπηρεσίες της Facebook σχετικά με την αναγνώριση προσώπου και της Google για τις διαφημίσεις με κρυφές προεπιλεγμένες ρυθμίσεις που υπονόμευαν εξ ορισμού την ιδιωτικότητα (Forbrukerrådet, 2018). Ειδικά η στοχευμένη διαφήμιση δεν αποτελεί απαραίτητο όρο για τη λειτουργικότητα της υπηρεσίας, επομένως η επεξεργασία δεδομένων για έναν τέτοιο σκοπό δεν πρέπει να είναι ούτε υποχρεωτική ούτε προεπιλεγμένη (Forbrukerrådet, 2018). Οι χρήστες που επέλεγαν τα κουμπιά «Συμφωνώ» ή «Αποδέχομαι» δεν θα έβλεπαν ποτέ τις ρυθμίσεις και δεν θα γνώριζαν ποια ήταν η προεπιλογή. Όσοι δεν ήθελαν να είναι ενεργή η αναγνώριση προσώπου ή η εξατομίκευση διαφημίσεων έπρεπε να μπουν στις ρυθμίσεις και να τις από-επιλέξουν.



Εικόνα 16: Το popup της Facebook για τον ΓΚΠΔ απαιτεί από τους χρήστες να επιλέξουν «Manage Data Settings» προκειμένου να απενεργοποιήσουν τη στοχευμένη από τρίτα μέρη διαφήμιση. Αν οι χρήστες επιλέξουν «Αποδοχή και συνέχεια», η στοχευμένη διαφήμιση ενεργοποιείται αυτομάτως. Ο σχεδιασμός αυτός δεν παρέχει προστασία εξ ορισμού (Forbrukerrådet, 2018).

Το ΕΣΠΔ (04/2019) προσδιορίζει ορισμένα βασικά στοιχεία ήδη από τον σχεδιασμό και εξ ορισμού που υλοποιούν τις αρχές επεξεργασίας (κυρίως την αντικειμενικότητα), όπως: α) την αυτονομία των χρηστών, β) τη διευκόλυνση της άσκησης των δικαιωμάτων τους, γ) τις εύλογες προσδοκίες τους, δ) τη μη εισαγωγή αθέμιτων διακρίσεων εις βάρος των ΥΔ, ε) τη μη εκμετάλλευση των αναγκών ή των αδυναμιών τους, στ) την ισορροπία ισχύος μεταξύ του ΥΕ και των ΥΔ, η) την ενημέρωσή τους με αντικειμενικό και ουδέτερο τρόπο, αποφεύγοντας τυχόν λόγο ή σχεδιασμό που κρύβει εξαπάτηση ή χειραγώγηση και ζ) αληθείς πληροφορίες, ώστε ο ΥΕ να μην παραπλανά τα ΥΔ. Όμως, τα σκοτεινά μοτίβα στερούν από τους χρήστες την αυτονομία με αποτέλεσμα να αντιστρατεύονται το άρθρο 25 (Forbrukerrådet, 2018). Επιπλέον, βάσει της προηγούμενης ανάλυσης τα σκοτεινά μοτίβα που υφαρπάζουν τη συγκατάθεση των χρηστών και εμποδίζουν την ενημέρωση ή τον έλεγχο των χρηστών στα δεδομένα τους παραβιάζουν της αρχές της νόμιμης επεξεργασίας και υπονομεύουν τα δικαιώματα των ΥΔ. Ως εκ τούτου, αντίκεινται και στο άρθρο 25.

3.2.11 Αυτοματοποιημένη ατομική λήψη αποφάσεων

Τα σκοτεινά μοτίβα, όταν δεν στηρίζονται σε μια γενικότερη βάση, όπως τις heuristics, μπορούν να εξατομικεύονται βάσει των δεδομένων που τυγχάνουν επεξεργασίας (Κατευθυντήριες Επιτροπής 2021). Σύμφωνα με το άρθρο 22 παρ.1 «το ΥΔ έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο». Η Επιτροπή (2022) υποστηρίζει ότι σε ορισμένες περιπτώσεις η εξατομικευμένη διαφήμιση ενδέχεται να εμπίπτει στη διάταξη αυτή.

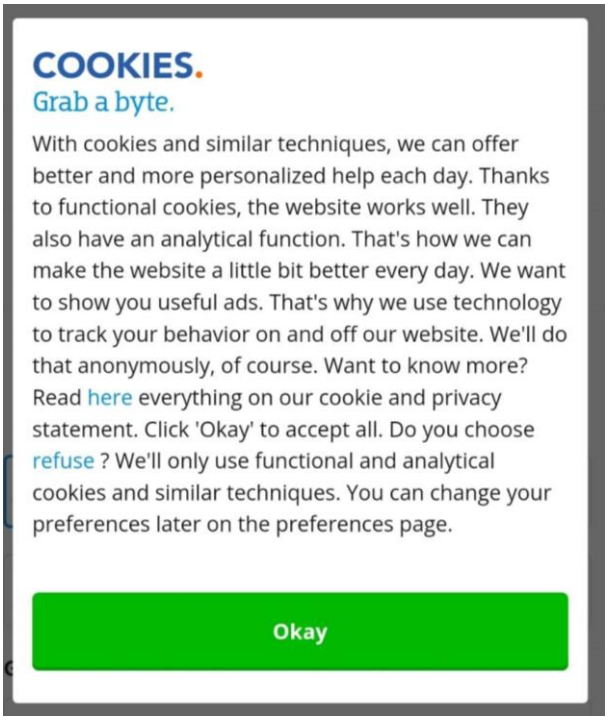
3.3 Η Οδηγία ePrivacy

Η Οδηγία ePrivacy εξειδικεύει και συμπληρώνει τον ΓΚΠΔ ως προς την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Οι πληροφορίες που αποθηκεύονται στον τερματικό εξοπλισμό των χρηστών συνιστούν μέρος της ιδιωτικής ζωής τους και χρήζουν προστασίας (αιτ.σκ.24), ανεξαρτήτως του αν συνιστούν προσωπικά δεδομένα ή όχι (υπόθεση Planet 49, C-763/17). Το άρθρο 5 παρ.3 επιτρέπει την αποθήκευση πληροφοριών ή την πρόσβαση σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό των χρηστών[7] μόνον εφόσον εκείνοι παρέχουν τη συγκατάθεσή τους κατόπιν σαφούς και εκτενούς ενημέρωσης σύμφωνα με τον ΓΚΠΔ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Για τον ορισμό της συγκατάθεσης το άρθρο 2(στ) της Οδηγίας παραπέμπει στον ΓΚΠΔ. Εξαιρείται η αποθήκευση ή η πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διαβίβαση μιας επικοινωνίας ή

[7] Άρα η Οδηγία δεν περιλαμβάνει κανόνες για προγενέστερες ή μεταγενέστερες πράξεις επεξεργασίας που αφορούν τέτοιες πληροφορίες. Αν οι πληροφορίες αυτές συνιστούν προσωπικά δεδομένα, θα πρέπει κατ' αρχήν να αναζητηθεί άλλη νομική βάση για την περαιτέρω επεξεργασία τους.

αυτή που είναι *απολύτως αναγκαία* για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης. Αυτή η παράγραφος αφορά τα cookies που αποθηκεύονται από τον διακομιστή μιας ιστοσελίδας στην τερματική συσκευή ενός χρήστη κατά την πλοήγησή του σε αυτή για διάφορους σκοπούς επεξεργασίας, μεταξύ άλλων για την online παρακολούθηση (tracking), την κατάρτιση προφίλ και τη στοχευμένη διαφήμιση (Machuletz and Böhme, 2020). Βάσει των παραπάνω, η εγκατάσταση cookies για τέτοιους σκοπούς επιτρέπεται μόνο με τη συγκατάθεση του χρήστη και μετά από κατάλληλη ενημέρωσή του, ενώ εξαιρούνται όσα θεωρούνται τεχνικά απαραίτητα για τη σύνδεση στην ιστοσελίδα ή την παροχή της online υπηρεσίας. Οι τρόποι παροχής των πληροφοριών, του δικαιώματος άρνησης ή της αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν πιο προσιτοί στον χρήστη (αιτ.σκ.25).

Παράλληλα, το άρθρο 13 παρ.1 προϋποθέτει την εκ των προτέρων χορήγηση συγκατάθεσης των χρηστών στη χρήση ηλεκτρονικού ταχυδρομείου για σκοπούς εμπορικής προώθησης. Η δεύτερη παράγραφος επιβάλλει την υποχρέωση σαφούς, εύκολου και δωρεάν opt-out με κάθε μήνυμα, αν ο χρήστης δεν είχε αρχικά διαφωνήσει με αυτή τη χρήση. Τέλος, η τέταρτη παράγραφος απαγορεύει συλλήβδην τα spam mails, αυτά δηλαδή που αποστέλλονται με σκοπό την άμεση εμπορική προώθηση και που συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα. Εύλογα οι διατάξεις αυτές απαγορεύουν τακτικές, όπως το Friend Spam, το Roach Motel και τη Συγκαλυμμένη Διαφήμιση (Επιτροπή, 2022).



Εικόνα 17: Τα functional και analytical cookies του cookie notice της ιστοσελίδας coolblue.nl δεν είναι απολύτως απαραίτητα (Προσωπική περιήγηση στο διαδίκτυο στις 11/3/2023).

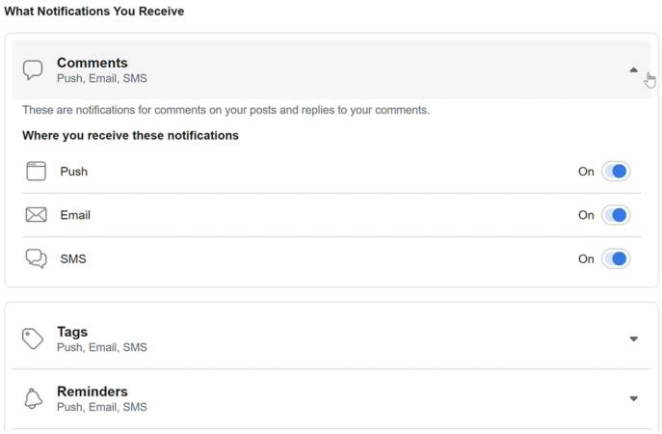
Πολύ σημαντική θα είναι η συμβολή του Κανονισμού ePrivacy που θα αντικαταστήσει την ομώνυμη οδηγία στο θέμα των cookies. Η Πρόταση πυροδότησε έντονες συζητήσεις γύρω από τα σύνθετα ζητήματα που επιχειρεί να ρυθμίσει, αλλά το 2021 εγκρίθηκε το κείμενό της. Αν τελικά ψηφιστεί, ο Κανονισμός θα συνιστά lex specialis έναντι του ΓΚΠΔ, θα ορίζει τις προϋποθέσεις λήψης της συγκατάθεσης των χρηστών πριν την εγκατάσταση cookies και θα αντιμετωπίζει θέματα, όπως τα cookie walls και το consent fatigue. Θεσπίζονται απλούστεροι κανόνες για τα cookies, πιο φιλικοί προς τους χρήστες, καθώς οι ρυθμίσεις του προγράμματος περιήγησης θα παρέχουν έναν εύκολο τρόπο αποδοχής ή άρνησης των cookies παρακολούθησης και άλλων αναγνωριστικών. Συγκεκριμένα, ο τελικός χρήστης θα πρέπει να έχει *πραγματική επιλογή* για την αποδοχή των cookies ή άλλων παρόμοιων αναγνωριστικών κωδικών. Η χρήση των cookie walls ως εναλλακτική λύση αντί της επί πληρωμή πρόσβασης θα επιτρέπεται, εάν ο χρήστης είναι σε θέση να επιλέξει μεταξύ της εν λόγω προσφοράς και ισοδύναμης προσφοράς του ίδιου παρόχου που δεν συνεπάγεται συγκατάθεση για τα cookies (Συμβούλιο της ΕΕ, 2021). Ως προς την αποφυγή του consent fatigue ο τελικός χρήστης θα μπορεί να παρέχει τη συγκατάθεσή του για τη χρήση ορισμένων cookies, καταχωρώντας έναν ή περισσότερους παρόχους σε κατάλογο εγκεκριμένων παρόχων στις ρυθμίσεις του φυλλομετρητή (browser). Οι πάροχοι λογισμικού θα ενθαρρύνονται[8] να διευκολύνουν τους χρήστες στην εγκατάσταση και τροποποίηση καταλόγων εγκεκριμένων παρόχων στους φυλλομετρητές τους και στην ανάκληση της συγκατάθεσής τους ανά πάσα στιγμή (Συμβούλιο της ΕΕ, 2021).Έτσι, οι χρήστες θα μπορούν να καταρτίζουν και να τροποποιούν λίστες με τους εγκεκριμένους παρόχους (whitelisting) και τα cookies που επιθυμούν να εγκαθίστανται, διατηρώντας τον πλήρη έλεγχο στη διαχείριση της συγκατάθεσής τους.

3.4 Επανορθωτικοί μηχανισμοί

3.4.1 Δικαίωμα αποζημίωσης

Η αιτ.σκ.75 του ΓΚΠΔ αναγνωρίζει ότι η επεξεργασία προσωπικών δεδομένων μπορεί να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των χρηστών και να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη. Το μέγεθος της μη υλικής ζημίας είναι πολύ δύσκολο να εκτιμηθεί, γιατί δεν μπορεί να μετρηθεί (ΟΟΣΑ, 2022, Επιτροπή, 2022, Gunawan, Santos and Kamara, 2022). Ενδέχεται μάλιστα οι χρήστες να μην την αντιλαμβάνονται ή ακόμα και να αδιαφορήσουν (Bongard-Blanchy et al., 2021). Κατά μία άποψη ο βαθμός της προσπάθειας που καταβάλλεται για να αποφευχθεί ένα σκοτεινό μοτίβο που παρεμβαίνει στην ιδιωτικότητα αποτελεί ένδειξη του μεγέθους της βλάβης (Gunawan, Choffnes and Wilson, 2021), όπως όταν ο χρήστης αναγκάζεται να απενεργοποιήσει μία προς μία ειδοποιήσεις εξ ορισμού ενεργές με αποτέλεσμα να κουράζεται και να υποχωρεί (Gunawan et al., 2021).

[8] Αιτιολ.σκ.20a 6087/21 Πρότασης του Κανονισμού ePrivacy, 2021 (Συμβούλιο της ΕΕ).



Εικόνα 18: Η Facebook δεν προσφέρει στον χρήστη τη δυνατότητα να αποεπιλέξει όλες τις ενεργοποιημένες επιλογές με μία κίνηση (Gunawan et al., 2021).

Το άρθρο 82 παρ.1 του ΓΚΠΔ δίνει στα ΥΔ το δικαίωμα αποζημίωσης από τον ΥΕ ή τον εκτελούντα την επεξεργασία για τη ζημία που υπέστη λόγω παραβίασης του ΓΚΠΔ. Σύμφωνα με την αιτ.σκ.146 του νόμου η έννοια της ζημίας θα πρέπει να ερμηνεύεται διασταλτικά βάσει της νομολογίας του ΔΕΕ (Gunawan, Santos and Kamara, 2022), ενώ η ευθύνη του ΥΕ είναι αντικειμενική. Δυστυχώς, δεν αξιοποιείται πλήρως ο επανορθωτικός μηχανισμός του ΓΚΠΔ, αφού δεν παρέχει σαφέστερα κριτήρια για τον προσδιορισμό της βλάβης και της έντασής της και αυτή η αοριστία διατηρείται και στις κατευθυντήριες του ΕΣΠΔ (03/2022) και στην DSA (Gunawan, Santos and Kamara, 2022). Ως εκ τούτου, η νομολογία δεν τηρεί ενιαία στάση, ώστε άλλες αποφάσεις εθνικών δικαστηρίων δέχονται τη διασταλτική ερμηνεία της ζημίας ένεκα της αντικειμενικής ευθύνης του ΥΕ, ενώ άλλες απαιτούν επιπλέον της παραβίασης του ΓΚΠΔ την απόδειξη της συγκεκριμένης ζημίας και την ύπαρξη μίας ακόμη σημαντικής ή υλικής βλάβης (Gunawan, Santos and Kamara, 2022).

Πρόσφατα το ΔΕΕ (2023) στην υπόθεση Austrian Post (C-300/21) απεφάνθη ότι για τη θεμελίωση δικαιώματος αποζημίωσης του άρθρου 82 παρ.1 *δεν αρκεί απλώς και μόνον η παράβαση των διατάξεων του ΓΚΠΔ*, αλλά και ζημία (υλική ή μη) ως αποτέλεσμα της παραβίασης και αιτιώδης σύνδεσμος μεταξύ αυτών των δύο. Επίσης, έκρινε ότι η αποκατάσταση της μη υλικής ζημίας *δεν εξαρτάται από ένα ορισμένο όριο ως προς τη βαρύτητά της*. Ο καθορισμός του ύψους της αποζημίωσης εναπόκειται στα εθνικά δικαστήρια υπό τον όρο ότι τηρούνται οι αρχές της ισοδυναμίας και της αποτελεσματικότητας του ενωσιακού δικαίου. Ενδεχομένως, η απόφαση αυτή να κατευθύνει τα εθνικά δικαστήρια προς μία κατεύθυνση και να διευκολύνει τα ΥΔ να διεκδικήσουν αποζημίωση λόγω σκοτεινών μοτίβων.

3.4.2 Τα πρόστιμα από τις εποπτικές αρχές

Οι εποπτικές αρχές δυνάμει των άρθρων 58 παρ.2θ και 83 του ΓΚΠΔ δύνανται να επιβάλλουν διοικητικά πρόστιμα για τυχόν παραβάσεις. Το ΕΣΠΔ (03/2022) τους

αναθέτει την τιμωρία των σκοτεινών μοτίβων, *εφόσον* παραβιάζουν τις απαιτήσεις του ΓΚΠΔ. Η επιβολή κυρώσεων ενισχύει την αποτελεσματικότητα των νόμων. Στο σημείο αυτό αξίζει να αναφερθούν ορισμένα σχετικά πρόστιμα. Η CNIL το 2019 επέβαλε στη Google πρόστιμο 50 εκατομμυρίων ευρώ μεταξύ άλλων για μη συμμόρφωση με την αρχή της διαφάνειας, αφού δεν παρείχε τις πληροφορίες σχετικά με την επεξεργασία σε κατανοητή και εύκολα προσβάσιμη μορφή. Επίσης, η συγκατάθεση των χρηστών δεν ήταν ούτε ρητή, καθώς η αποδοχή των εξατομικευμένων διαφημίσεων ήταν προεπιλεγμένη, ούτε εν πλήρει επιγνώσει, διότι οι πληροφορίες, όπως οι σκοποί της επεξεργασίας, βρίσκονταν διασκορπισμένες σε πολλά έγγραφα, με κουμπιά και συνδέσμους που έπρεπε να επιλέξουν οι χρήστες για να αποκτήσουν πρόσβαση σε συμπληρωματικές πληροφορίες. Οι σχετικές πληροφορίες ήταν προσβάσιμες μόνο μετά από πολλά βήματα, φτάνοντας μερικές φορές έως και τις 6 ενέργειες. Από τη μεριά τους οι χρήστες δεν μπορούσαν να κατανοήσουν πλήρως το εύρος της επεξεργασίας που πραγματοποιούσε η Google ούτε ότι η νόμιμη βάση της εξατομικευμένης διαφήμισης ήταν η συγκατάθεση, ενώ οι σκοποί της επεξεργασίας, οι κατηγορίες δεδομένων που υποβάλλονταν σε αυτή και ο χρόνος διατήρησης τους περιγράφονταν πολύ γενικά και αόριστα (ΟΟΣΑ, 2022).

Το 2021 η ίδια αρχή επέβαλε τα πρόστιμα 35 εκατομμυρίων ευρώ στην Amazon και 100 εκατομμυρίων ευρώ στη Google εξαιτίας της εγκατάστασης cookies για διαφημιστικούς σκοπούς χωρίς την προηγούμενη συγκατάθεση των χρηστών και λόγω ελλιπούς ενημέρωσής τους. Επιπλέον, η Google, αν και παρείχε στους χρήστες τη δυνατότητα απενεργοποίησης της εξατομίκευσης των διαφημίσεων, ένα από τα cookies παρέμενε εγκατεστημένο στον υπολογιστή τους συνεχίζοντας να δίνει πληροφορίες για τη δραστηριότητα του χρήστη που είχε απενεργοποιήσει την επιλογή (πλημμελής ικανοποίηση του δικαιώματος εναντίωσης).

Το 2022 επέβαλε στη Microsoft, τη Google, τη Facebook και την TikTok πρόστιμα 60, 150, 60 και 5 εκατομμυρίων ευρώ αντίστοιχα, καθώς διαπίστωσε ότι οι χρήστες δεν μπορούσαν να απορρίψουν τα cookies όσο εύκολα μπορούσαν να τα αποδεχτούν. Επιπλέον, στην περίπτωση της Microsoft τα cookies για διαφημιστικούς σκοπούς τοποθετούνταν στον τερματικό εξοπλισμό χωρίς τη συγκατάθεσή των χρηστών, ενώ αναφορικά με την TikTok οι χρήστες δεν ενημερώνονταν με επαρκή ακρίβεια για τους σκοπούς των διάφορων cookies. Επίσης, επέβαλε στη Discord πρόστιμο 800 χιλιάδων ευρώ, επειδή μεταξύ άλλων δεν είχε καθορίσει πολιτική περιόδου διατήρησης δεδομένων (άρθρο 5 παρ.1ε), παρείχε ελλιπή ενημέρωση σχετικά με την προαναφερθείσα χρονική περίοδο (άρθρο 13) και εξ ορισμού η εφαρμογή παρέμενε ενεργή, ακόμα και όταν οι χρήστες έκλειναν το βασικό παράθυρο επιλέγοντας το Χ πάνω δεξιά με αποτέλεσμα να διατηρείται η φωνητική επικοινωνία (άρθρο 25 παρ.2). Επίσης, επέβαλε πρόστιμο 8 εκατομμυρίων ευρώ στην Apple για τη μη λήψη της συγκατάθεσης των Γάλλων χρηστών του iPhone (έκδοση iOS 14.6) πριν από την

εγκατάσταση αναγνωριστικών στοιχείων στις συσκευές τους για σκοπούς διαφήμισης. Στον απόηχο αυτής της είδησης η εταιρεία πρόσφατα κυκλοφόρησε το iOS App Tracking Transparency που επιτρέπει στον χρήστη να διαλέξει αν μια εφαρμογή μπορεί να παρακολουθεί τις δραστηριότητές του σε εφαρμογές και ιστοσελίδες άλλων εταιρειών για σκοπούς διαφήμισης ή κοινής χρήσης με μεσίτες δεδομένων (https://support.apple.com/en-us/HT212025). Την ίδια χρονιά η Βελγική αρχή προστασίας δεδομένων (APD) επέβαλε πρόστιμο 50 χιλιάδων ευρώ σε δύο ενημερωτικές ιστοσελίδες του Ομίλου Roularta για τη διαχείριση των cookies.

Τέλος, τον Απρίλιο του 2023 η ιταλική αρχή προστασίας προσωπικών δεδομένων (GARANTE) επέβαλε πρόστιμο 300 χιλιάδων ευρώ στην Ediscom S.p.a. λόγω της παραβίασης πολλαπλών διατάξεων του ΓΚΠΔ κατά τη συλλογή προσωπικών δεδομένων για σκοπούς μάρκετινγκ. Σημειωτέον ότι πρόκειται για την πρώτη απόφαση που μνημονεύει ρητά τα σκοτεινά μοτίβα και επικαλείται τις σχετικές κατευθυντήριες του ΕΣΠΔ (03/2022). Η ρητή αυτή αναφορά είναι σημαντικό βήμα στην ευαισθητοποίηση των χρηστών και στον στιγματισμό των ΥΕ.

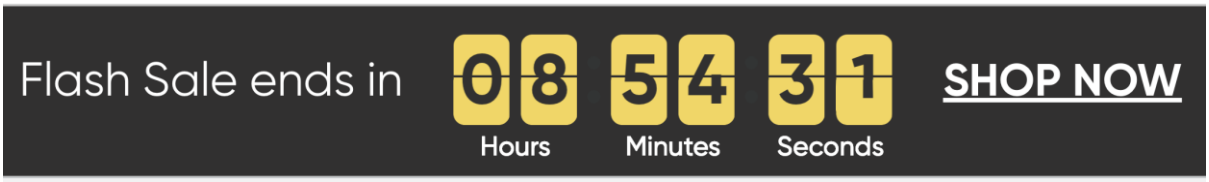
3.4.3 Εκπροσώπηση υποκειμένων των δεδομένων (ΥΔ)

Βάσει του άρθρου 80 ΓΚΠΔ ορισμένες οντότητες που δραστηριοποιούνται στον τομέα της προστασίας των προσωπικών δεδομένων των ΥΔ μπορούν να ασκήσουν αντιπροσωπευτικές αγωγές και το δικαίωμα αποζημίωσης του άρθρου 82 εξ ονόματός των ΥΔ με ή χωρίς προηγούμενη ανάθεση από αυτά. Ο Γενικός Εισαγγελέας στις προτάσεις του στην απόφαση C-300/21 έκρινε ότι το άρθρο διευκολύνει την προστασία γενικών συμφερόντων από πλευράς ιδιωτών. Πράγματι, δεδομένου ότι οι χρήστες συχνά αγνοούν ότι χρησιμοποιούνται σκοτεινά μοτίβα εις βάρος τους, το άρθρο είναι αρκετά χρήσιμο (Gunawan, Santos and Kamara, 2022). Όμως, η NOYB (2022) αντέτεινε ότι είναι η μοναδική ΜΚΟ στην Ευρώπη που δραστηριοποιείται από το συγκεκριμένο άρθρο και εκτιμά ότι ο ετήσιος προϋπολογισμός της είναι προς το παρόν αρκετά περιορισμένος.

3.5 Η Οδηγία για τις Αθέμιτες Εμπορικές Πρακτικές (ΟΑΕΠ)

Το 2019 το 11.1% περίπου 11.000 δημοφιλών ιστοσελίδων ηλεκτρονικού εμπορίου περιείχε σκοτεινά μοτίβα (Mathur et al., 2019). Την ίδια χρονιά 200 δημοφιλείς αμερικανικές εμπορικές και ταξιδιωτικές ιστοσελίδες περιείχαν τουλάχιστον ένα στοιχείο σχεδιασμού που ενθάρρυνε «παρορμητικές αγορές», όρο ευρύτερο από τα σκοτεινά μοτίβα (Moser et al., 2019). Το 2023 η Επιτροπή ανακοίνωσε ότι το 40% ιστοσελίδων ηλεκτρονικού εμπορίου περιέχουν σκοτεινά μοτίβα. Ο ΟΟΣΑ (2022) εκτιμά ότι τα πιο συνηθισμένα σκοτεινά μοτίβα σε ιστοσελίδες ηλεκτρονικού εμπορίου και εφαρμογές είναι η Προεπιλογή, η Ψευδής ιεράρχηση, οι Κρυφές πληροφορίες, η Συγκαλυμμένη διαφήμιση, η Όχληση, τα Εμπόδια κατά την ακύρωση/opt out, η Αναγκαστική εγγραφή ή γνωστοποίηση, καθώς και πρακτικές που συνδέονται με την

αίσθηση του επείγοντος (urgency), όπως χρονόμετρα που μετρούν αντίστροφα μέχρι τη λήξη μιας προσφοράς και με την ανάγκη κοινωνικής αποδοχής (social proof), όπως τα Activity notifications και οι Παραπλανητικές μαρτυρίες άλλων χρηστών. Όταν τα σκοτεινά μοτίβα εφαρμόζονται στις εμπορικές σχέσεις μεταξύ επιχειρήσεων και καταναλωτών (B2C), τότε μπορεί να χρησιμοποιηθεί η ΟΑΕΠ επιπλέον του ΓΚΠΔ για την αμφισβήτηση του θεμιτού χαρακτήρα αυτών των πρακτικών (Κατευθυντήριες Επιτροπής, 2021). Αν και η ΟΑΕΠ δεν αναφέρει ρητά τα σκοτεινά μοτίβα, οι κατευθυντήριες γραμμές της Επιτροπής σχετικά με την ερμηνεία και την εφαρμογή της εν λόγω Οδηγίας περιλαμβάνουν μία ενότητα για τις επίμαχες πρακτικές (Κατευθυντήριες Επιτροπής, 2021).



Εικόνα 19: Χρονόμετρο στην ιστοσελίδα mattressfirm.com που μετρά ψευδώς αντίστροφα μέχρι τη λήξη μιας προσφοράς (Flash Sale), παρόλο που τα περισσότερα προϊόντα παραμένουν και στη συνέχεια σε έκπτωση (Mathur et al., 2019).

Εικόνα 20: Παράδειγμα Activity Notification στην ιστοσελίδα tkmaxx.com, που δηλώνει πόσα άτομα προσέθεσαν στον καλάθι τους το προϊόν τις τελευταίες 72 ώρες (Mathur et al., 2019).

Η ΟΑΕΠ αφορά «εμπορικές πρακτικές που αποβλέπουν άμεσα στον *επηρεασμό* των αποφάσεων των καταναλωτών σε σχέση με προϊόντα» (αιτ.σκ.7) συμπεριλαμβανομένων των υπηρεσιών (όπως τροποποιήθηκε το 2019 το άρθρο 2 ορ.γ). Όπως ο ΓΚΠΔ, έτσι και η ΟΑΕΠ καθιερώνει την αντικειμενική ευθύνη (Κατευθυντήριες Επιτροπής, 2021). Ορίζει με ευρύτητα τις εμπορικές πρακτικές, ώστε να καλύπτουν κάθε πράξη, παράλειψη, τρόπο συμπεριφοράς ή εκπροσώπησης, εμπορική επικοινωνία, συμπεριλαμβανομένης της διαφήμισης και του μάρκετινγκ, η οποία συνδέεται άμεσα με την προώθηση, πώληση ή προμήθεια ενός προϊόντος/υπηρεσίας από επιχειρήσεις προς καταναλωτές (άρθρο 2 ορ.δ). Οι αθέμιτες εμπορικές πρακτικές λαμβάνουν χώρα «πριν, κατά τη διάρκεια και ύστερα από εμπορική συναλλαγή σχετιζόμενη με ένα συγκεκριμένο προϊόν/υπηρεσία» (άρθρο 3 παρ.1). Συνεπώς, δεν απαιτείται η ύπαρξη συμβατικής σχέσης ούτε η αγορά ενός προϊόντος (Επιτροπή, 2022, Leiser, 2020). Έτσι, πολλά σκοτεινά μοτίβα που σχετίζονται άμεσα με την προώθηση των προϊόντων στους καταναλωτές εμπίπτουν στο πεδίο εφαρμογής της ΟΑΕΠ (Επιτροπή 2022). Με ευρύτητα

ορίζεται και η έννοια της απόφασης συναλλαγής (άρθρο 2 ορ.ια), ώστε να θεωρείται αθέμιτη ακόμα και η πρακτική που θα επηρεάσει τον καταναλωτή σε αποφάσεις που *προηγούνται* ή έπονται της αγοράς, όπως το να αφιερώσει περισσότερο χρόνο σε μια διαδικασία κράτησης, να μεταβεί σε σύνδεσμο ή αγγελία ή να συνεχίσει να χρησιμοποιεί την υπηρεσία μέσω περιήγησης ή κύλισης προς τα κάτω (Κατευθυντήριες Επιτροπής, 2021). Σε αντίθεση με τον ΓΚΠΔ η ΟΑΕΠ δίνει έμφαση στην αρχή της αντικειμενικότητας σε προ-συμβατικό στάδιο και σε περιβάλλοντα που προηγούνται της επεξεργασίας (Leiser, 2020).

Σε αντίθεση με την ασάφεια του ΓΚΠΔ, η ΟΑΕΠ προσδιορίζει τον αθέμιτο χαρακτήρα εμπορικών πρακτικών. Συγκεκριμένα, η γενική ρήτρα του άρθρου 5 απαγορεύει ως αθέμιτες εκείνες τις εμπορικές πρακτικές που παραβιάζουν την επαγγελματική ευσυνειδησία (άρθρο 2 ορ.η) και στρεβλώνουν ουσιωδώς ή ενδέχεται να στρεβλώσουν ουσιωδώς την οικονομική συμπεριφορά του μέσου (άρθρο 5 παρ.2) ή ευάλωτου (άρθρο 5 παρ.3) καταναλωτή. Η έννοια του ευάλωτου χαρακτήρα είναι δυναμική και εξετάζεται κατά περίπτωση (Κατευθυντήριες Επιτροπής, 2021). Περιπτωσιολογική είναι και η προσέγγιση της επαγγελματικής ευσυνειδησίας και της ουσιώδους στρέβλωσης (Leiser, 2020). Πάντως και εδώ διατυπώνεται μία ένσταση παρόμοια με την περίπτωση του ΓΚΠΔ, ότι δηλαδή δείχνει να μην λησμονείται ο homo economicus (Egberts, 2021, Leiser, 2020). Η δε ουσιώδης στρέβλωση συνεπάγεται ότι μια εμπορική πρακτική χρησιμοποιείται με σκοπό τη σημαντική μείωση της ικανότητας του καταναλωτή να λάβει τεκμηριωμένη απόφαση, με αποτέλεσμα εκείνος *να λάβει μια απόφαση συναλλαγής που διαφορετικά δεν θα ελάμβανε* (άρθρο 2 ορ.ε). Οι εμπορευόμενοι, λοιπόν, θα πρέπει να λαμβάνουν κατάλληλα μέτρα για να διασφαλίζουν ότι ο *σχεδιασμός της* UI *τους* δεν οδηγεί σε αυτό το αποτέλεσμα (Κατευθυντήριες Επιτροπής, 2021). Διαφορετικά, ανοίγει ο δρόμος για την «ψηφιακή ασυμμετρία», που επιφέρει την ανισορροπία των μερών και καθιστά τον καταναλωτή ευάλωτο *ανά πάσα* στιγμή (BEUC, 2022).

Επιπλέον του άρθρου 5, τα άρθρα 6-7 απαγορεύουν τις παραπλανητικές εμπορικές πρακτικές και τα άρθρα 8-9 τις επιθετικές, που οδηγούν ή ενδέχεται να οδηγήσουν τον μέσο καταναλωτή να «λάβει απόφαση συναλλαγής που διαφορετικά δεν θα ελάμβανε» (άρθρα 6 παρ.1, 7 παρ.1 και 8 παρ.1). Τέλος, το Παράρτημα Ι της Οδηγίας περιλαμβάνει πλήρη κατάλογο εμπορικών πρακτικών που κρίνονται αθέμιτες υπό *οποιεσδήποτε* περιστάσεις.

Έτσι, για να χαρακτηριστεί μια πρακτική αθέμιτη ελέγχεται πρώτα από το δικαστήριο ή από αρμόδιο διοικητικό όργανο αν περιλαμβάνεται στο Παράρτημα Ι, διαφορετικά επιστρατεύονται για μία *κατά περίπτωση* αξιολόγηση τα άρθρα 6-9 και τελευταίο το άρθρο 5. Πολλά σκοτεινά μοτίβα που εντοπίζονται σε online περιβάλλον μπορούν να χαρακτηριστούν αθέμιτες εμπορικές πρακτικές κατά το Παράρτημα Ι, όπως το Δόλωμα

και Μεταστροφή (πρακτικές υπ'αριθμ.5 και 6), η Όχληση (πρακτική υπ'αριθμ.26), η Συγκαλυμμένη διαφήμιση (πρακτική υπ'αριθμ.11) και η Αναγκαστική εγγραφή (πρακτική υπ'αριθμ.24). Άλλες πρακτικές μπορούν να θεωρηθούν παραπλανητικές, όπως οι Ερωτήσεις-παγίδα, η Απόκρυψη πληροφοριών/ψευδής ιεράρχηση, το Friend Spam και η Προεπιλογή, ενώ επιθετικές πρακτικές συνιστούν ενδεικτικά το Παιχνίδι με τα συναισθήματα, το Confirmshaming, η Αναγκαστική εγγραφή και το Roach motel.

Το 2018 η Ιταλική Αρχή Ανταγωνισμού (AGCM) επέβαλε στη Facebook πρόστιμο 10 εκατομμυρίων ευρώ για παραβίαση του Ιταλικού Κώδικα Καταναλωτή, ο οποίος εφαρμόζει την ΟΑΕΠ. Έκρινε μεταξύ άλλων, ότι η Facebook προχώρησε σε κατάχρηση επιρροής (άρθρο 9) στους εγγεγραμμένους καταναλωτές με την προεπιλογή της ευρύτερης δυνατής συγκατάθεσης στην κοινή χρήση δεδομένων και με τη θέση περιορισμών στη χρήση του ιστοτόπου, που αποθάρρυναν τους καταναλωτές να περιορίσουν τη συγκατάθεσή τους.

Ο ΓΚΠΔ και η Οδηγία ePrivacy αλληλεπιδρούν με την ΟΑΕΠ. Από τη μία, τα προσωπικά δεδομένα των καταναλωτών έχουν οικονομική αξία και μαζί με τη διαφήμιση αποτελούν συχνά τη βασική πηγή εσόδων των online επιχειρήσεων. Η παραβίαση των απαιτήσεων της Οδηγίας ePrivacy και του ΓΚΠΔ μπορεί να συνυπολογιστεί στην αξιολόγηση του συνολικού αθέμιτου χαρακτήρα των εμπορικών πρακτικών βάσει της ΟΑΕΠ, ιδίως όταν ο εμπορευόμενος επεξεργάζεται δεδομένα καταναλωτών για σκοπούς άμεσης εμπορικής προώθησης ή άλλους, όπως της κατάρτισης προφίλ. Από την άλλη, κοινός τόπος είναι η διαφάνεια. Η ΟΑΕΠ αφενός απαγορεύει τις παραπλανητικές πράξεις και παραλείψεις που ενδέχεται να επηρεάσουν τις αποφάσεις συναλλαγής των καταναλωτών (άρθρα 6-7 και πρακτική υπ.αριθμ.22 του Παραρτήματος Ι), αφετέρου οι απαιτήσεις πληροφόρησης του ΓΚΠΔ και της Οδηγίας ePrivacy μπορούν να θεωρηθούν ουσιώδεις πληροφορίες κατά το άρθρο 7 παρ.5. Αν ο εμπορευόμενος δεν ενημερώσει τον καταναλωτή ότι τα παρεχόμενα δεδομένα θα χρησιμοποιηθούν για εμπορικούς σκοπούς, αυτό μπορεί να θεωρηθεί *παραπλανητική παράλειψη ουσιωδών πληροφοριών*, καθώς και παραβίαση της διαφάνειας και άλλων απαιτήσεων βάσει των άρθρων 12-14 του ΓΚΠΔ (Κατευθυντήριες Επιτροπής, 2021).

Συνολικά, η ΟΑΕΠ κρίνεται αρκετά ευέλικτη και καλύπτει τις περισσότερες αθέμιτες εμπορικές πρακτικές χάρη στην περιπτωσιολογική προσέγγιση και την ευρύτητα των κριτηρίων (Επιτροπή, 2022, Leiser, 2020, Berbece, 2019). Από την άλλη, υποστηρίζεται ότι η ΟΑΕΠ χρήζει ορισμένων προσαρμογών, ώστε οι παραπλανητικές UI και οι τεχνικές εξατομίκευσης δεδομένων να μπορούν να θεωρηθούν αθέμιτες λόγω της εκμετάλλευσης των ευάλωτων σημείων των καταναλωτών (Επιτροπή, 2022, BEUC, 2022). Για αυτό η BEUC (2022) θεωρεί ότι η εισαγωγή νέων εννοιών, όπως της ψηφιακής ασυμμετρίας, θα υλοποιήσει την αντικειμενικότητα εκ του σχεδιασμού (fairness by design) στην ΟΑΕΠ και θα συμπληρώνει το άρθρο 25 ΓΚΠΔ. Η θέση των καταναλωτών

θα ενισχυθεί και με την Οδηγία 2020/1828, που θα εφαρμοστεί τον Ιούνιο του 2023 σε αντιπροσωπευτικές αγωγές που ασκούνται κατά εμπόρων, οι οποίοι παραβιάζουν τις διατάξεις του ενωσιακού δικαίου, συμπεριλαμβανομένων των ΓΚΠΔ και ΟΑΕΠ, με αποτέλεσμα τη ζημία (έστω και ενδεχόμενη) των συλλογικών συμφερόντων των καταναλωτών (Επιτροπή, 2022).

Τέλος, σημειώνεται ότι η Επιτροπή (2022), η BEUC (2022) και διάφοροι ερευνητές (Leiser, 2022 και 2020, Berbece, 2019) έχουν υποστηρίξει ότι σχετικές είναι και η Οδηγία για τα δικαιώματα του καταναλωτή που προβλέπει υποχρεώσεις προσυμβατικής ενημέρωσης (Οδηγία 2011/83/ΕΕ), η Οδηγία για τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές και *δεν τους δεσμεύουν εφόσον* δεν έχουν αποτελέσει εκ των προτέρων αντικείμενο ατομικής διαπραγμάτευσης (Οδηγία 91/13/ΕΟΚ), η Οδηγία για το ηλεκτρονικό εμπόριο (Οδηγία 2000/31ΕΚ), η Οδηγία για τις υπηρεσίες οπτικοακουστικών μέσων (Οδηγία 2010/13/ΕΕ) και ο Κανονισμός P2B (Κανονισμός 2019/1150/ΕΕ για την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης) και η Οδηγία 2006/114/ΕΚ για την παραπλανητική και τη συγκριτική διαφήμιση.

4. Η ΝΕΑ ΚΑΙ Η ΕΠΙΚΕΙΜΕΝΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΑ ΣΚΟΤΕΙΝΑ ΜΟΤΙΒΑ

Στα προηγούμενα κεφάλαια παρουσιάστηκαν διατάξεις της υφιστάμενης νομοθεσίας που μπορούν με κατάλληλη ερμηνεία να αντιμετωπίσουν τα σκοτεινά μοτίβα. Στο παρόν κεφάλαιο παρουσιάζονται οι νέες προσπάθειες των νομοθετών να τα αντιμετωπίσουν στοχευμένα βάσει συγκεκριμένων διατάξεων ακόμα και σε επίπεδο αρχιτεκτονικής συστήματος. Το πλήθος των νέων κειμένων και η ταχύτητα με την οποία δημοσιεύονται αναδεικνύει κατά τη γνώμη μας την έντονη επιθυμία της ευρωπαϊκής έννομης τάξης να ρυθμίσει τις ραγδαίες εξελίξεις στον ψηφιακό χώρο και μάλιστα χωρίς γεωγραφικούς περιορισμούς.

4.1 Digital Market Act (DMA)

Η DMA ετέθη σε ισχύ τον Νοέμβριο του 2022 και θα εφαρμοστεί τον Μάιο του 2023. Επιδιώκει να διασφαλίσει τη θεμιτή συμπεριφορά των πυλωρών που παρέχουν βασικές υπηρεσίες πλατφόρμας, όπως μηχανές αναζήτησης, κοινωνική δικτύωση και online διαφήμιση (άρθρο 2 παρ.2). Για να οριστεί μια επιχείρηση ως πυλωρός εξετάζεται ο αντίκτυπος που έχει στην εσωτερική αγορά, αν παρέχει βασική υπηρεσία πλατφόρμας, που αποτελεί σημαντική πύλη για τη σύνδεση επαγγελματιών χρηστών με τελικούς χρήστες και αν κατέχει παγιωμένη και σταθερή θέση (άρθρο 3). Ο αντίλογος που αναπτύσσεται εδώ είναι ότι υποτιμάται η επιρροή μικρότερων επιχειρήσεων που δεν φτάνουν το βεληνεκές της GAFAM, αλλά μπορούν να βλάψουν άμεσα τους χρήστες μέσω παραπλανητικών πρακτικών (King and MacKinnon, 2022). Η DMA, αν και δεν απαγορεύει ρητά τα σκοτεινά μοτίβα, μπορεί να τα αντιμετωπίσει μέσω του άρθρου 13.

Αυτό αφορά την καταστρατήγηση των διατάξεων της DMA και συγκεκριμένα απαγορεύει στον πυλωρό να επιδίδεται σε συμπεριφορές που υπονομεύουν την αποτελεσματική συμμόρφωση με τις υποχρεώσεις που επιβάλλει ο κανονισμός, ανεξαρτήτως από το αν η συμπεριφορά αυτή είναι συμβατικής, εμπορικής, τεχνικής ή άλλης φύσης ή συνίσταται στη χρήση *συμπεριφορικών τεχνικών ή σχεδιασμού διεπαφών* (παρ.4). Η Επιτροπή (2022) κρίνει ότι το άρθρο μπορεί να αντιμετωπίσει την Όχληση, το Roach Motel, τις Κρυφές πληροφορίες, την Προεπιλογή και τις Ερωτήσεις-παγίδα. Επίσης, η έκτη παράγραφος του άρθρου με μια διατύπωση που απηχεί την DETOUR Act και τη CPRA (Leiser and Santos, 2023) απαγορεύει στους πυλωρούς να προσφέρουν «επιλογές στον τελικό χρήστη με μη ουδέτερο τρόπο» ή να υπονομεύουν «την *αυτονομία*, τη *λήψη αποφάσεων* ή την *ελεύθερη επιλογή* των τελικών χρηστών ή των επαγγελματιών χρηστών μέσω της δομής, του σχεδιασμού, της χρησιμότητας ή του τρόπου λειτουργίας μιας UI ή μέρους αυτής».

Συναφώς, σημειώνονται ενδεικτικά ορισμένες υποχρεώσεις των πυλωρών. Συγκεκριμένα, ο πυλωρός δεν επεξεργάζεται προσωπικά δεδομένα των τελικών χρηστών, τα οποία απέκτησε ως διαμεσολαβητής για τον σκοπό της online διαφήμισης, δεν συνδυάζει ούτε διασταυρώνει προσωπικά δεδομένα τα οποία συλλέγει μέσα από τις υπηρεσίες που προσφέρει με αυτά που προκύπτουν από άλλες υπηρεσίες ούτε συνδέει τους τελικούς χρήστες σε άλλες υπηρεσίες του πυλωρού προκειμένου να συνδυάσει τα δεδομένα, εκτός εάν τους έχει δοθεί η συγκεκριμένη επιλογή και υπάρχει ισχυρή συγκατάθεση (άρθρο 5 παρ.2). Επιπλέον, ο πυλωρός δεν απαιτεί από τους χρήστες να γίνουν συνδρομητές ή να εγγραφούν σε οποιαδήποτε περαιτέρω βασική υπηρεσία πλατφόρμας ως προϋπόθεση για να μπορούν να χρησιμοποιούν, να έχουν πρόσβαση, να συνδέονται ή να εγγράφονται σε οποιαδήποτε από τις βασικές υπηρεσίες πλατφόρμας του πυλωρού, τακτική που παραπέμπει στο Forced action (άρθρο 5 παρ.8). Τέλος, επιτρέπει και παρέχει την τεχνική δυνατότητα στους τελικούς χρήστες να *απεγκαθιστούν εύκολα* τυχόν εφαρμογές λογισμικού στο λειτουργικό σύστημα του πυλωρού, με την επιφύλαξη αυτών που είναι απαραίτητες για τη λειτουργία του λειτουργικού συστήματος ή της συσκευής καθώς και να αλλάζουν εύκολα τις *προεπιλεγμένες* ρυθμίσεις που κατευθύνουν ή οδηγούν τους τελικούς χρήστες σε προϊόντα ή υπηρεσίες που παρέχει ο πυλωρός (άρθρο 6 παρ.3).

4.2 Digital Service Act (DSA)

Η DSA, «το ευρωπαϊκό σύνταγμα για το διαδίκτυο» (Jarovsky, 2022a), θεσπίζει κανόνες σχετικά με την παροχή ενδιάμεσων υπηρεσιών[9] για ένα ασφαλές, προβλέψιμο και αξιόπιστο online περιβάλλον. Ετέθη σε ισχύ τον Νοέμβριο του 2022 και θα εφαρμοστεί πλήρως τον Φεβρουάριο του 2024. Βασίζεται στην αρχή πως «ό,τι είναι παράνομο εκτός

[9] Άρθρο 3 ορ.ζ: Πρόκειται για υπηρεσίες απλής μετάδοσης, προσωρινής αποθήκευσης και φιλοξενίας πληροφοριών που παρέχει ο αποδέκτης των υπηρεσιών.

διαδικτύου θα πρέπει να είναι παράνομο και στο διαδίκτυο», τα πρόστιμα είναι υψηλότερα από του ΓΚΠΔ (άρθρο 52) και διατηρείται η αντικειμενική ευθύνη (αιτ.σκ.67 «είτε σκόπιμα είτε στην πράξη»). Πρόκειται για *την πρώτη ρητή απαγόρευση* των σκοτεινών μοτίβων. Συγκεκριμένα, το άρθρο 25 παρ.1, που περιέχεται στο Κεφάλαιο ΙΙΙ σχετικά με τις υποχρεώσεις διαφάνειας, προβλέπει ότι «*οι πάροχοι online πλατφορμών*[10] δεν σχεδιάζουν, δεν οργανώνουν και δεν διαχειρίζονται τις online διεπαφές[11] τους κατά τρόπο που παραπλανά ή χειραγωγεί τους αποδέκτες της υπηρεσίας τους, ή κατά τρόπο που οδηγεί σε άλλου είδους ουσιώδη στρέβλωση ή περιορισμό της ικανότητας των αποδεκτών της υπηρεσίας τους να λαμβάνουν ελεύθερες αποφάσεις μετά λόγου γνώσεως». Το άρθρο λοιπόν *δεν συνιστά γενική απαγόρευση* προς όλες τις ενδιάμεσες υπηρεσίες ούτε καλύπτει ιστοσελίδες που εμπεριέχουν διαφημίσεις, παιχνίδια σε πλατφόρμες και εφαρμογές κινητών (Leiser and Santos, 2023). Επίσης, δεν διευκρινίζει τις διαφορές ανάμεσα στις διαφορετικές μορφές επιρροής που ασκούν οι πάροχοι. Ενδεχομένως, η γενικόλογη αυτή διατύπωση του άρθρου να αποσκοπεί να καλύψει μελλοντικές τεχνολογικές εξελίξεις και να μην αναστείλει την καινοτομία στον σχεδιασμό. Ωστόσο, εκφράζεται προβληματισμός ότι η διατύπωση της πρώτης παραγράφου περιορίζεται στα σκοτεινά μοτίβα που εντοπίζονται σε επίπεδο UI και δεν καλύπτει αυτά της «επόμενης γενιάς» και του metaverse (Leiser and Santos, 2023).

Η DSA εφαρμόζεται σε όσες πρακτικές δεν καλύπτονται από τον ΓΚΠΔ και την ΟΑΕΠ (άρθρο 25 παρ.2). Υπό αυτό το πρίσμα ενδέχεται να μπορεί να καλύψει πρακτικές, όπως την άπειρη κύλιση και την αυτόματη αναπαραγωγή, καθώς και πρακτικές που σημειώνονται στις εμπορικές σχέσεις μεταξύ επιχειρήσεων (B2B) (Leiser and Santos, 2023). Από την άλλη, υποστηρίζεται ότι η παράγραφος αυτή περιορίζει την αποτελεσματική ρύθμιση των cookie notices σε επίπεδο ΓΚΠΔ (EDRi, 2022) και αναστέλλει την ενίσχυση δύο νόμων, που αν και μάχονται τα σκοτεινά μοτίβα, δεν τα αντιμετωπίζουν πλήρως (King and MacKinnon, 2022). Σε κάθε περίπτωση, η Επιτροπή θα μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με την απαγόρευση συγκεκριμένων πρακτικών, όπως αυτών που: α) δίνουν μεγαλύτερη προβολή σε ορισμένες επιλογές, όταν ζητείται από τον αποδέκτη της υπηρεσίας να λάβει μια απόφαση (Interface interference/Ετεροκατεύθυνση/Ψευδής Ιεράρχηση) β) ζητούν επανειλημμένα από τον αποδέκτη της υπηρεσίας να πραγματοποιήσει μια επιλογή, ενώ η επιλογή αυτή έχει ήδη γίνει, ιδίως με αναδυόμενα παράθυρα που παρεμβαίνουν στην εμπειρία του χρήστη (Όχληση) γ) καθιστούν τη διαδικασία τερματισμού μιας υπηρεσίας δυσκολότερη από την εγγραφή σε αυτή (Προσθήκη εμποδίων) (άρθρο 25 παρ.3). Η αιτ.σκ.67 προσφέρει επιπλέον παραδείγματα σκοτεινών μοτίβων

[10] Άρθρο 3 ορ.θ: Πρόκειται για υπηρεσίες φιλοξενίας περιεχομένου που κατ'αρχήν αποθηκεύουν και διαδίδουν στο κοινό πληροφορίες, κατόπιν αιτήματος αποδέκτη της υπηρεσίας.

[11] Άρθρο 3 ορ.ιγ: κάθε λογισμικό, συμπεριλαμβανομένου ενός ιστοτόπου ή μέρους αυτού, και εφαρμογές, συμπεριλαμβανομένων των εφαρμογών για φορητές συσκευές.

αναφερόμενη στην εξαπάτηση των χρηστών μέσω της ώθησης σε αποφάσεις για συναλλαγές ή μέσω προεπιλεγμένων ρυθμίσεων που είναι πολύ δύσκολο να αλλάξουν με αποτέλεσμα να προκαταλαμβάνουν αδικαιολόγητα τη διαδικασία λήψης αποφάσεων του αποδέκτη της υπηρεσίας.

Παράλληλα, η DSA επιβάλλει νέες υποχρεώσεις στις online πλατφόρμες με στόχο τη διαφάνεια και τη λογοδοσία. Για παράδειγμα, τα άρθρα 26 και 27 επιβάλλουν τη διαφάνεια της διαφήμισης σε online πλατφόρμες και του συστήματος συστάσεων (άρθρο 3 ορ.ιθ) και απαγορεύουν τη διαφήμιση βάσει κατάρτισης προφίλ (άρθρο 26 παρ.3), που σημαίνει ότι μπορούν να αντιμετωπίσουν τη Συγκαλυμμένη διαφήμιση (Επιτροπή, 2022) και γενικά να θέσουν αυστηρά όρια στη συμπεριφορική διαφήμιση (Jarosvksy, 2023d). Από την άλλη, ενόψει των απρόβλεπτων ενδεχόμενων κινδύνων το άρθρο 35 παρ.1 επιβάλλει βάσει της αρχής της προφύλαξης στις πολύ μεγάλες online πλατφόρμες (VLOPs), όπως η Facebook, και στις πολύ μεγάλες μηχανές αναζήτησης (VLOSEs), όπως η Google, να προσαρμόζουν τον σχεδιασμό, τα χαρακτηριστικά ή τη λειτουργία των υπηρεσιών τους, συμπεριλαμβανομένων των online UI τους και να λαμβάνουν μέτρα ευαισθητοποίησης και να προσαρμόζουν την online UI τους, ώστε να παρέχουν στους αποδέκτες της υπηρεσίας περισσότερες πληροφορίες (Leiser and Santos, 2023). Τέλος, το άρθρο 34 παρ.1 επιβάλλει στις VLOPs και VLOSEs να «εντοπίζουν, να αναλύουν και να αξιολογούν επιμελώς οποιουσδήποτε συστημικούς κινδύνους στην ΕΕ που απορρέουν από τον σχεδιασμό ή τη λειτουργία των υπηρεσιών τους και των σχετικών συστημάτων του, συμπεριλαμβανομένων των αλγοριθμικών συστημάτων, ή από τη χρήση των υπηρεσιών τους στην ΕΕ». Για την εκτίμηση αυτών των κινδύνων λαμβάνονται υπ'όψιν μεταξύ άλλων τυχόν πραγματικές ή προβλέψιμες αρνητικές επιπτώσεις ως προς την άσκηση θεμελιωδών δικαιωμάτων, ιδίως της ιδιωτικότητας και της οικογενειακής ζωής, της προστασίας των προσωπικών δεδομένων και της υψηλού επιπέδου προστασίας των καταναλωτών (άρθρο 34 παρ.1^{α}). Η DSA δεν προβλέπει συγκεκριμένες τεχνικές σχεδιασμού, αλλά υποδεικνύει ποιες είναι οι επιπτώσεις στα δικαιώματα και στις ελευθερίες των χρηστών, τις οποίες πρέπει να αποφύγουν οι σχεδιαστές. Υποστηρίζεται ότι μια ευρύτερη ερμηνεία του άρθρου μπορεί να αντιμετωπίσει σκοτεινά μοτίβα που συνδέονται με αλγορίθμους, καθώς και τον σχεδιασμό αλγοριθμικών συστημάτων που προκαλούν συμπεριφορικές βλάβες, όπως εθισμό (King and MacKinnon, 2022).

Φαίνεται, λοιπόν, εκ πρώτης όψεως ότι η DSA περιορίζεται στην απαγόρευση των πιο συνηθισμένων σκοτεινών μοτίβων και δεν προχωράει σε πιο δυσδιάκριτες πρακτικές που ενσωματώνονται στο σύστημα της ή σε επίπεδο κώδικα (Leiser and Santos, 2023). Όμως, η δημιουργική ερμηνεία γενικών διατυπώσεων, όπως του άρθρου 34 ή των «λειτουργιών μιας online διεπαφής ή μέρους της» (αιτ.σκ.67) από τη νομολογία ίσως να μπορεί να άρει αυτόν τον προβληματισμό (Leiser and Santos, 2023) και να καλύψει ακόμη και παραπλανητικούς αλγορίθμους (King and MacKinnon, 2022).

4.3 Η Πρόταση της Πράξης για την Τεχνητή Νοημοσύνη (AI Act), η Πρόταση της Πράξης για τα Δεδομένα (Data Act) και η Πράξη για τη Διακυβέρνηση Δεδομένων (DGA)

Άλλες διατάξεις που αναμένεται να συμβάλουν στην αντιμετώπιση των σκοτεινών μοτίβων, εφόσον οριστικοποιηθούν και εφαρμοστούν, είναι η Πρόταση της Επιτροπής για την Πράξη για την ΤΝ (AI Act) και η Πρόταση της Data Act σχετικά με την κοινοχρησία δεδομένων με τρίτους (Επιτροπή, 2022).

Η Πράξη για την ΤΝ απαγορεύει τη διάθεση στην αγορά, τη θέση σε λειτουργία ή τη χρήση συστήματος ΤΝ[12] που χρησιμοποιεί τεχνικές, οι οποίες απευθύνονται στο *υποσυνείδητο ενός προσώπου υπερκεράζοντας το συνειδητό του* ή που εκμεταλλεύεται οποιοδήποτε από τα *τρωτά σημεία* μίας ομάδας προσώπων λόγω ηλικίας ή αναπηρίας (σωματικής ή διανοητικής), προκειμένου να *στρεβλωθεί ουσιωδώς η συμπεριφορά* ενός προσώπου κατά τρόπο που προκαλεί ή ενδέχεται να προκαλέσει σε αυτό ή άλλο πρόσωπο σωματική ή ψυχολογική βλάβη (άρθρο 5 παρ.1α και β). Δυστυχώς, η διάταξη δεν αναφέρεται σε άλλες επιπτώσεις, όπως την απώλεια αυτονομίας και τον εθισμό, ενώ η αναφορά σε συγκεκριμένες ομάδες προσώπων παραβλέπει το γεγονός ότι όλα τα πρόσωπα είναι ευάλωτα, όταν τυγχάνουν εκμετάλλευσης οι αδυναμίες τους (Leiser and Santos, 2023). Ήδη εκφράζονται ανησυχίες ότι η ΤΝ και οι αλγόριθμοι μηχανικής μάθησης θα οδηγήσουν σύντομα σε εξατομικευμένα σκοτεινά μοτίβα που θα τροφοδοτούνται από προσωπικά δεδομένα, θα στοχεύουν στα ευάλωτα σημεία των χρηστών και θα είναι ακόμα πιο δυσδιάκριτα (Leiser and Santos, 2023, ΟΟΣΑ, 2022, Επιτροπή, 2022).

Από την άλλη, η Data Act θεσπίζει εναρμονισμένους κανόνες για τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους. Βάσει της αιτιολογικής έκθεσης η Data Act συμπληρώνει τα δικαιώματα που απορρέουν από τον ΓΚΠΔ και την Οδηγία ePrivacy και διασφαλίζει υψηλότερο επίπεδο προστασίας των καταναλωτών. Σε αυτό το πλαίσιο το άρθρο 6 παρ.2α ορίζει ότι «ο τρίτος δεν εξαναγκάζει, εξαπατά ή χειραγωγεί τον χρήστη με οποιονδήποτε τρόπο, υπονομεύοντας ή μειώνοντας την αυτονομία, τη λήψη αποφάσεων ή τις επιλογές του χρήστη, μεταξύ άλλων μέσω ψηφιακής διεπαφής με τον χρήστη». Η διατύπωση είναι αρκετά ευρεία, ώστε να καλύπτει πολλά σκοτεινά μοτίβα που δυσχεραίνουν την άσκηση δικαιωμάτων των χρηστών. Για παράδειγμα, θα πρέπει να είναι εξίσου εύκολο για τον χρήστη να αρνείται ή να διακόπτει την πρόσβαση τρίτων στα δεδομένα, όπως και να επιτρέπει την πρόσβαση (αιτ.σκ.34). Επιπλέον, σύμφωνα με

[12] Άρθρο 3 ορ.1: λογισμικό που αναπτύσσεται με μία ή περισσότερες από τις τεχνικές και προσεγγίσεις που παρατίθενται στο παράρτημα Ι και μπορεί, για ένα δεδομένο σύνολο στόχων που έχουν καθοριστεί από τον άνθρωπο, να παράγει στοιχεία εξόδου όπως περιεχόμενο, προβλέψεις, συστάσεις ή αποφάσεις που επηρεάζουν τα περιβάλλοντα με τα οποία αλληλεπιδρά.

την αρχή της ελαχιστοποίησης των δεδομένων, ο τρίτος θα πρέπει να έχει πρόσβαση μόνο σε όσες πρόσθετες πληροφορίες είναι απαραίτητες για την παροχή της υπηρεσίας που έχει ζητήσει ο χρήστης, ενώ κατόπιν της πρόσβασης στα δεδομένα, θα πρέπει να τα επεξεργάζεται αποκλειστικά για τους σκοπούς που έχουν συμφωνηθεί με τον χρήστη, χωρίς την παρέμβαση του κατόχου των δεδομένων (αιτ.σκ.34). Πάντως, ενδέχεται μια πρακτική που δυσχεραίνει την άσκηση των δικαιωμάτων των χρηστών ή τις επιλογές τους σχετικά με την κοινοχρησία ή τη φορητότητα των δεδομένων να θεωρείται σκοτεινό μοτίβο κατά την Data Act, ακόμα και αν συμμορφώνεται με τον ΓΚΠΔ, όπως μια ιστοσελίδα που δυσχεραίνει το δικαίωμα πρόσβασης ή φορητότητας, αλλά στηρίζει την επεξεργασία δεδομένων σε μία από τις νομικές βάσεις του ΓΚΠΔ (Leiser and Santos, 2023).

Η Data Act αναμένεται να λειτουργεί συμπληρωματικά προς την Πράξη για τη Διακυβέρνηση Δεδομένων (Data Governance Act, DGA). Η τελευταία θα εφαρμοστεί τον Σεπτέμβριο του 2023 και στοχεύει στη ενίσχυση της διαθεσιμότητας των προς χρήση δεδομένων μέσω της αύξησης της εμπιστοσύνης στους διαμεσολαβητές δεδομένων (Jarovsky, 2022a). Συγκεκριμένα προβλέπει ότι ο αλτρουισμός δεδομένων, η οικειοθελής δηλαδή κοινοχρησία δεδομένων βάσει συγκατάθεσης των ΥΔ για την επεξεργασία των προσωπικών τους δεδομένων για σκοπούς γενικού συμφέροντος, δεν επιτρέπεται να χρησιμοποιεί παραπλανητικές πρακτικές εμπορικής προώθησης για την απόκτηση των δεδομένων (άρθρο 21 παρ.2).

5. ΠΡΟΤΑΣΕΙΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Προτάσεις

Η εργασία προτείνει ορισμένα μέτρα αυτορρύθμισης και συρρύθμισης συμπληρωματικά προς τη νομοθεσία και τα μέτρα επιβολής της (Επιτροπή 2022, NAI, 2022, Narayanan et al., 2020), που θα συμβάλλουν στην ανθρωποκεντρική προσέγγιση στον σχεδιασμό των online υπηρεσιών με στόχο τη διασφάλιση της ιδιωτικότητας.

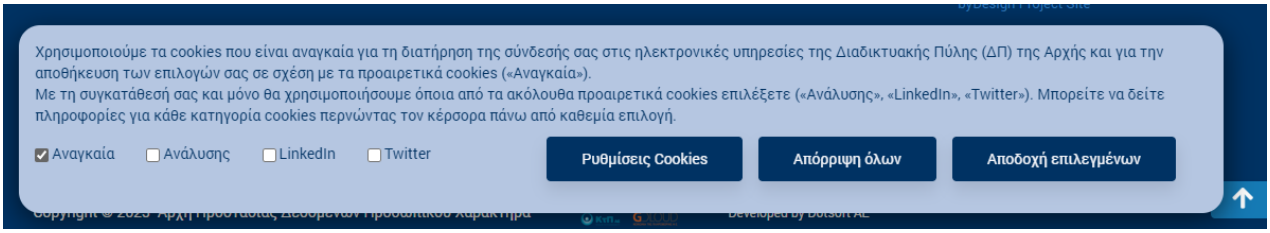
5.1.1 Ο επανασχεδιασμός των ιστοσελίδων/εφαρμογών/cookie banners

Προκρίνεται ο επανασχεδιασμός των ιστοσελίδων/εφαρμογών, ώστε να ενσωματώνουν στην αρχιτεκτονική των επιλογών την αντικειμενικότητα και τη διαφάνεια και να παρέχουν ουδέτερες ή φιλικές προς τους χρήστες επιλογές (ΟΟΣΑ, 2022, Επιτροπή, 2022). Σημαντικό επίσης είναι να λαμβάνονται υπ'όψιν στον σχεδιασμό οι γνωστικές προκαταλήψεις, ώστε να ενισχυθεί η αυτονομία των χρηστών (Jarovsky, 2022b-c). Αρχές προστασίας καταναλωτών έχουν προτείνει την καθιέρωση της απαίτησης fairness by design στις online πλατφόρμες συμπληρωματικά προς το άρθρο 25 του ΓΚΠΔ, προκειμένου αυτές να σχεδιάζουν την αρχιτεκτονική των επιλογών κατά τρόπο που ενθαρρύνει την ελεύθερη και εν επιγνώσει επιλογή των καταναλωτών σχετικά με τη χρήση των προσωπικών τους δεδομένων (BEUC, 2022, CMA, 2020). Στο ίδιο μήκος

κύματος βρίσκονται και τα φωτεινά μοτίβα, δηλαδή ωθήσεις που παρακινούν και διευκολύνουν τους χρήστες να επιλέξουν μεταξύ των διάφορων επιλογών εκείνες που διασφαλίζουν το αληθινό τους συμφέρον (Grahl et al., 2021). Τέτοιες, για παράδειγμα, είναι η παροχή αναλυτικών πληροφοριών για τη χορήγηση συγκατάθεσης (Nouwens et al., 2020), η εύκολη ακύρωση/αποσύνδεση από μια υπηρεσία, η απόρριψη με ένα κλικ, προεπιλεγμένες ρυθμίσεις ή η κατάλληλη διατύπωση/παρουσίαση του περιεχομένου (Graßl et al., 2021). Ωστόσο, τα φωτεινά μοτίβα δεν προϋποθέτουν την ενεργή συμμετοχή των χρηστών, για αυτό και διατυπώνονται επιφυλάξεις κατά πόσο οι ΥΕ θα τα χρησιμοποιούν και προτείνονται εναλλακτικά τα στοχαστικά μοτίβα, που ενθαρρύνουν τους χρήστες να προσέχουν ή να επιλυθεί το θέμα των cookie notices σε νομικό επίπεδο (Επιτροπή 2022). Επίσης, προτείνεται η εξασφάλιση της ισοτιμίας των χαρακτηριστικών μεταξύ των εκδόσεων μιας υπηρεσίας (από Η/Υ σε κινητό) (Gunawan et al., 2021).

Το ΕΣΠΔ (03/2022) απηύθυνε διάφορες βέλτιστες πρακτικές προς τους σχεδιαστές αναφορικά με την εύκολη πρόσβαση στις σχετικές πληροφορίες, τη διαφάνεια, την ορολογία που χρησιμοποιείται και τις ειδοποιήσεις που λαμβάνουν οι χρήστες. Ενδεικτικά, προτείνει υπερσυνδέσμους που οδηγούν σε πληροφορίες, ρυθμίσεις ή ενέργειες που βοηθούν τους χρήστες να διαχειριστούν τα δεδομένα τους, ευδιάκριτες εντός της UI πληροφορίες για τα προσωπικά δεδομένα, τη σαφή επισήμανση τυχόν αλλαγών που σημειώνονται σε ένα cookie notice, την παροχή εξηγήσεων και παραδειγμάτων, τη χρήση απλής γλώσσας και ειδοποιήσεων για τυχόν παραβιάσεις. Η CNIL (χ.χ.) επίσης έχει δημοσιεύσει παραδείγματα UI που βοηθούν τους σχεδιαστές να συμμορφώνονται με τον ΓΚΠΔ, ενώ το γερμανικό ινστιτούτο ConPolicy (2023) εξέδωσε κατευθυντήριες για τον σχεδιασμό των cookie banners.

Ειδικά για τα cookie banners, αισίως παρατηρείται τελευταία η προσθήκη του κουμπιού της απόρριψης, ώστε να εμφανίζονται συνολικά τρεις διαθέσιμες επιλογές στον χρήστη («Συμφωνώ», «Διαφωνώ», «Περισσότερες επιλογές»). Ενδεικτικά αναφέρεται ότι πρόσφατα το Γραφείο Επιτρόπου Προστασίας προσωπικών δεδομένων της Κύπρου (2023) κατόπιν ελέγχου που διενεργήθηκε σε ιστοσελίδες για τη χρήση cookies διαπίστωσε ότι σημειώθηκε πρόοδος στη συμμόρφωση με τη νομοθεσία. Οι περισσότερες στην αρχή δεν ενημέρωναν σχετικά με τους σκοπούς χρήσης των cookies, ή παρά την ενημέρωση η συγκατάθεση δεν ήταν ισχυρή λόγω του τρόπου λήψης της, ενώ ορισμένα cookies, όπως αυτά που μετρούν την επισκεψιμότητα της ιστοσελίδας χαρακτηρίζονταν εσφαλμένα ως απολύτως αναγκαία.



Εικόνα 21: Cookie banner με τριπλή επιλογή (Προσωπική περιήγηση στο διαδίκτυο, 5/4/2023).

5.1.2 Η ενσωμάτωση της ηθικής στον σχεδιασμό

Υποστηρίζεται η ανάγκη κατάρτισης ενός κώδικα δεοντολογίας για τους σχεδιαστές και γενικά της ενσωμάτωσης ηθικών αρχών στον σχεδιασμό (Επιτροπή 2022, ΟΟΣΑ, 2022, Gunawan et al., 2021, Chivukula et al., 2020, Narayanan et al., 2020, Di Geronimo et al., 2020, Gray et al., 2018, Acquisti et al., 2017, Harris, 2016). Μάλιστα, άνθρωποι προερχόμενοι από τον χώρο του UI/UX σχεδιασμού προτείνουν να συμπεριληφθούν θέματα ηθικής μεταξύ των μαθημάτων που διδάσκονται οι υποψήφιοι σχεδιαστές (Επιτροπή, 2022, Gray, Chivukula and Lee, 2020). Είναι αλήθεια ότι οι σχεδιαστές βρίσκονται στη μέση, καθώς αναλαμβάνουν να εξισορροπήσουν τα συμφέροντα των επιχειρήσεων με των χρηστών, ενώ έχουν διατυπωθεί διάφορες γνώμες για το αν μπορούν να θεωρηθούν συνένοχοι (Gunawan et al., 2021, Cara 2019, Jaiswal, 2018, Brownlee, 2016). Όμως, σε κάθε περίπτωση οφείλουν να αποφύγουν τη χρήση των σκοτεινών μοτίβων. Εξάλλου, η ίδια η νομοθεσία ενθαρρύνει την κατάρτιση κωδίκων συμπεριφοράς ως ήπιο δίκαιο (π.χ. άρθρο 40 ΓΚΠΔ, άρθρο 10 ΟΑΕΠ, άρθρο 45 DSA).

5.1.3 Η χρήση εργαλείων

Προτείνεται η χρήση διάφορων εργαλείων που παρουσιάζονται κατά καιρούς από ερευνητές προκειμένου να εντοπίζουν τα σκοτεινά μοτίβα, να αξιολογούν την επίδρασή τους, την υπεροχή τους, καθώς και κατά πόσο η νομοθεσία μπορεί να τα αντιμετωπίζει αποτελεσματικά. Ενδεικτικά τέτοια εργαλεία είναι το mystery shopping (Επιτροπή, 2022) η έρευνα-σκούπα (sweep) (BEUC, 2022), επιλεκτικοί έλεγχοι UI μέσω A/B δοκιμών (Luguri and Strahilevitz, 2021, Narayanan et al., 2020), διάφορες επεκτάσεις στα προγράμματα περιήγησης, όπως τα Cookie Glasses που επιτρέπουν στους χρήστες να μάθουν αν η συγκατάθεση αποθηκεύεται από τις CMPs (Matte, Bielova and Santos, 2020), το CookieViz της CNIL (2023) για τα cookies τρίτων μερών, το λογισμικό της NOYB (2021) για παράνομα cookie banners, αλλά και άλλες εφαρμογές που εντοπίζουν ιστοσελίδες που χρησιμοποιούν σκοτεινά μοτίβα (Mathur et al., 2019) ή ελέγχουν τη διαφάνεια (Bongard-Blanchy et al. 2021). Ο αντίκτυπος επίσης μπορεί να ελέγχεται με συμπεριφορικά πειράματα και έρευνες καταναλωτών (Επιτροπή, 2022, Luguri and Strahilevitz, 2021, Graßl et al., 2021, Di Geronimo et al., 2020). Η αποτελεσματικότητα της υπάρχουσας νομοθεσίας μπορεί να αξιολογείται βάσει A/B δοκιμών, της νομολογίας και της σύγκρισης διάφορων δικαιοδοσιών (Επιτροπή, 2022, Luguri and Strahilevitz, 2021). Ειδικά για την αξιολόγηση των δοκιμών A/B υποστηρίζεται ότι πρέπει να περιλαμβάνει τουλάχιστον μία μέτρηση των μακροπρόθεσμων επιπτώσεων, διότι η

αντιμετώπιση των σκοτεινών μοτίβων απαιτεί δομικές αλλαγές στη διαδικασία σχεδιασμού (Επιτροπή, 2022). Η CNIL (2019) μάλιστα υποστηρίζει ότι η δημόσια συζήτηση για τις καταχρηστικές ή παραπλανητικές πρακτικές σχεδιασμού θα μπορούσε να οδηγήσει σε φαινόμενα «τιμωρίας της αγοράς». Έτσι, οι ΥΕ θα ενθαρρύνονται να αλλάξουν τις μεθόδους τους και οι χρήστες θα ενημερώνονται για αυτές τις πρακτικές.

5.1.4 Η ενημέρωση και η ευαισθητοποίηση των χρηστών

Η Επιτροπή (2022) υποστήριξε ότι θα πρέπει να δοθούν στις επιχειρήσεις κίνητρα να συμμορφωθούν μέσω κυρώσεων και αρνητικής δημοσιότητας, καθώς σύντομα η εξατομίκευση των παραπλανητικών μεθόδων δεν θα μπορεί να αντιμετωπιστεί επαρκώς από το νόμο. Πράγματι, ενδεικτικά αναφέρεται ότι η Google Chrome το 2021 ανακοίνωσε ότι σχεδιάζει να απομακρύνει τα cookies τρίτων μερών και ότι δεν θα χρησιμοποιήσει εναλλακτικούς ιχνηλάτες στη θέση τους (Temkin, 2021). Η Επιτροπή (2022) επίσης αναγνώρισε ότι πολλές online πλατφόρμες, όπως η Facebook, έχουν υιοθετήσει κατά καιρούς μέτρα αυτορρύθμισης, όπως είναι η παροχή σύντομων εξηγήσεων στους χρήστες, προκειμένου να μετριαστεί η έλλειψη διαφάνειας στη στοχευμένη διαφήμιση και να αυξηθεί η αποδοχή της συμπεριφορικής διαφήμισης.

Όμως, ως γνωστόν, τα σκοτεινά μοτίβα θέτουν ως προτεραιότητα το συμφέρον των παρόχων και υπονομεύουν τα αληθινά συμφέροντα των χρηστών. Δε μοιάζει λοιπόν πολύ ρεαλιστική η ελπίδα ότι οι επιχειρήσεις θα απαρνηθούν τα σκοτεινά μοτίβα (ΟΟΣΑ, 2022, Bongard-Blanchy et al., 2021, Acquisti et al., 2017) παρά τα μεγάλα πρόστιμα και τον ανήθικο χαρακτήρα των πρακτικών. Για αυτό είναι πολύ σημαντική η ενημέρωση των χρηστών και η παροχή κινήτρων, ώστε να ενεργοποιήσουν το Σύστημα 2 (Bösch et al., 2016), να συνειδητοποιήσουν τους πιθανούς κινδύνους και να αναμιχθούν ενεργά στην αντιμετώπιση του παραπλανητικού σχεδιασμού (ΕΣΠΔ, 03/2022, Επιτροπή, 2022, Bongard-Blanchy et al., 2021, Maier and Harr, 2020, CNIL, 2019, Forbrukerrådet, 2018, Gray et al., 2018, Bösch et al., 2016, Brignull, 2011). Για το στόχο αυτό χρήσιμες είναι εκστρατείες ενημέρωσης από τις αρμόδιες αρχές καταναλωτών και προστασίας δεδομένων, στοχευμένες παρεμβάσεις και η διάθεση εργαλείων για καταγγελία και στιγματισμό των ΥΕ που χρησιμοποιούν σκοτεινά μοτίβα (Επιτροπή, 2022, ΟΟΣΑ, 2022). Επίσης, πολύτιμη είναι η ακαδημαϊκή έρευνα και η χρηματοδότηση ερευνών –και δη εμπειρικών. (CNIL, 2019). Όμως, δεν αρκεί η γνώση και η ευαισθητοποίηση, γιατί ενδέχεται ακόμα και αν οι χρήστες αναγνωρίζουν τον παραπλανητικό σχεδιασμό, να μην μπορέσουν να αντισταθούν. Επομένως, είναι σημαντική και η ενίσχυση της ικανότητας αντίστασης (Bongard-Blanchy et al.). Πρόσφατα η CNIL (2023) παρατήρησε ότι οι περισσότεροι χρήστες δηλώνουν ενήμεροι για την έννοια και τα είδη των cookies, ότι απορρίπτουν την παροχή συγκατάθεσης, αλλά και ότι παρατηρούν έλλειμμα διαφάνειας στην ενημέρωση που τους παρέχουν οι ιστοσελίδες.

5.2 Συμπεράσματα

Στον ψηφιακό κόσμο τα σκοτεινά μοτίβα εξαπλώνονται ταχέως. Πληθαίνουν, εντοπίζονται σε διάφορα online περιβάλλοντα μεμονωμένα ή συνδυαστικά, εκμεταλλεύονται αδυναμίες των χρηστών και υφαρπάζουν τον χρόνο, την προσοχή τους και τα δεδομένα τους. Διεισδύουν στις σκέψεις και τις ζωές τους και σταδιακά μεταβάλλουν τις προτιμήσεις τους, τη συμπεριφορά τους και εν τέλει την *αυτονομία* τους. Μπορούν να υπονομεύσουν την ιδιωτικότητα έως και τη δημοκρατία. Από την άποψη αυτή είναι ανήθικα και άκρως επικίνδυνα.

Η ραγδαία ανάπτυξη της ΤΝ αναμένεται να αυξήσει την αποτελεσματικότητα και τον κίνδυνο των σκοτεινών μοτίβων. Αλγόριθμοι μηχανικής μάθησης με χαμηλό βαθμό επεξηγησιμότητας (black box) χρησιμοποιούνται ήδη για την εξατομίκευση των υπηρεσιών επί τη βάση προσωπικών δεδομένων και δη ευαίσθητων με αποτέλεσμα να είναι πολύ δύσκολο για τους χρήστες να συνειδητοποιήσουν ότι χειραγωγούνται. Αναπόφευκτα, θα προκύψουν νέα είδη σκοτεινών μοτίβων, που θα είναι πολύ πειστικά, αλλά και πιο δυσδιάκριτα από τα υπόλοιπα, άρα και πιο απειλητικά για την αυτονομία και τα δικαιώματα των χρηστών. Η απαγόρευση αυτών των πρακτικών από το άρθρο 5 της Πρότασης για την ΤΝ θα καλλιεργήσει την υπεύθυνη και ηθική χρήση της ΤΝ.

Ευτυχώς, αυξάνεται ολοένα το ενδιαφέρον για την αντιμετώπισή τους. Η CNIL (2019) προέβλεψε ότι η αρχιτεκτονική της επιλογής θα είναι από τα πιο σημαντικά θέματα προς ρύθμιση την επόμενη δεκαετία στον ψηφιακό κόσμο και θα βαίνει πέρα από τα θέματα ιδιωτικότητας. Ο Ευρωπαίος Επίτροπος για τη δικαιοσύνη και την προστασία των καταναλωτών διευκρίνισε ότι τα σκοτεινά μοτίβα και η online διαφήμιση θα είναι οι στόχοι της επόμενης Επιτροπής (Euractiv, 2022). Προς το παρόν η αντιμετώπισή τους εμπίπτει στο ρυθμιστικό πεδίο πολλών νομικών κειμένων κατόπιν ερμηνείας και επικαιροποίησης, αλλά προκαλεί και την παραγωγή νέων. Η νομοθεσία που παρουσιάστηκε, από την Οδηγία ePrivacy έως την πρόταση της Data Act, επιδιώκει να καθιερώσει την αντικειμενικότητα, τη διαφάνεια και τη λογοδοσία. Το νέο νομοθετικό κύμα και η ανάληψη δράσης από τις αρμόδιες αρχές είτε προληπτικά με την έκδοση κατευθυντηρίων γραμμών είτε κατασταλτικά με την επιβολή κυρώσεων εμπνέουν αποφασιστικότητα για την αντιμετώπιση των σκοτεινών μοτίβων.

Η εργασία εξέτασε τις βασικές νομικές οδούς που μπορούν να επιλέξουν οι χρήστες για να αντιμετωπίσουν τα σκοτεινά μοτίβα, δηλαδή το δίκαιο προστασίας των προσωπικών δεδομένων και του καταναλωτή. Αναμφισβήτητα, τα σκοτεινά μοτίβα αντιβαίνουν σε πολλά άρθρα του ΓΚΠΔ, όπως στις αρχές νομιμότητας της επεξεργασίας και στους όρους της συγκατάθεσης παρά την απουσία ρητής αναφοράς σε αυτά. Το γεγονός ότι εκτυλίσσονται σε προγενέστερο της επεξεργασίας στάδιο, η αοριστία της έννοιας της αντικειμενικότητας, η απουσία κριτηρίων προσδιορισμού της βλάβης, η αποσιώπηση των γνωστικών προκαταλήψεων και η απουσία εξειδικευμένων μέτρων για την

πραγμάτωση του άρθρου 25 αναχαιτίζουν ως ένα βαθμό τη δυναμική του νόμου και χρήζουν περαιτέρω αποσαφήνισης. Ωστόσο, ο ΓΚΠΔ συμπλήρωσε πρόσφατα μόλις πέντε χρονιά εφαρμογής. Η κατάλληλη ερμηνεία των σχετικών διατάξεων και η επιβολή τους μέσα από τις κατευθυντήριες οδηγίες και τις αποφάσεις των εποπτικών αρχών μπορεί να δώσει νέα ώθηση στην πάταξη των σκοτεινών μοτίβων στο ψηφιακό περιβάλλον. Ως θετικά μηνύματα εκλαμβάνονται το πρώτο πρόστιμο με ρητή αναφορά στα σκοτεινά μοτίβα, τα αρκετά υψηλά πρόστιμα που επιβάλλονται τελευταία στην προσπάθεια επιβολής της υφιστάμενης νομοθεσίας και το ότι το ΔΕΕ δεν εξαρτά την αποκατάσταση της μη υλικής ζημίας που προκαλείται από παραβίαση του ΓΚΠΔ από ένα ορισμένο όριο ως προς τη βαρύτητά της. Ο ΓΚΠΔ είναι lex generalis ως προς την Οδηγία ePrivacy, οπότε η προηγούμενη προβληματική που αναπτύχθηκε εφαρμόζεται και εδώ.

Επιπλέον, η ΟΑΕΠ, αν και αντιμετωπίζει το θέμα επίσης εν μέρει και περιπτωσιολογικά, κρίνεται ακόμα πιο ευέλικτη, ιδίως μετά την προσαρμογή της στους κινδύνους του διαδικτύου. Ήδη η Επιτροπή (2022α) ανακοίνωσε ότι στο Νέο Θεματολόγιο για τους Καταναλωτές (New Consumer Agenda) θα εξετάσει την καταλληλότητα της ευρωπαϊκής νομοθεσίας (fitness check) για την προστασία των καταναλωτών ως προς την ψηφιακή δικαιοσύνη (digital fairness). Ενδέχεται η ΟΑΕΠ να αποδειχτεί ακόμα πιο αποτελεσματική στη συνέχεια.

Βάσει των παραπάνω, μπορεί να ειπωθεί ότι ο ΓΚΠΔ, η Οδηγία ePrivacy και η ΟΑΕΠ παρέχουν συνολικά ένα ισχυρό ρυθμιστικό πλαίσιο για την αντιμετώπιση των σκοτεινών μοτίβων που εντοπίζονται στις UI/UX των online πλατφορμών, ιστοσελίδων, εφαρμογών, cookie banners και σε πολιτικές απορρήτου. Υποστηρίζεται, μάλιστα, ότι η «πλουραλιστική» προσέγγιση του ΓΚΠΔ και της ΟΑΕΠ μπορεί να αξιοποιεί τα δυνατά τους σημεία και να αντισταθμίζει τυχόν ελλείψεις (Leiser, 2020). Ωστόσο, οι αποφάσεις που έχουν δημοσιευθεί ως τώρα συνδέονται με συγκεκριμένα σκοτεινά μοτίβα, που αναγνωρίζονται σχετικά εύκολα. Σε συνδυασμό με τις γενικές απαγορεύσεις των νόμων ενδέχεται ορισμένα σκοτεινά μοτίβα που δεν είναι ξεκάθαρα παραπλανητικά να μην αντιμετωπιστούν.

Κρίσιμο παράγοντα στην αντιμετώπιση των σκοτεινών μοτίβων αποτελεί λοιπόν και η αποτελεσματική επιβολή της υπάρχουσας νομοθεσίας, αφού εξασφαλίζει τη συμμόρφωση των παρόχων online υπηρεσιών και των επιχειρήσεων με τις επιταγές του νόμου για θεμιτό και διαφανή σχεδιασμό. Καθίσταται εφικτή με προσαρμογές κατάλληλες για τον ψηφιακό κόσμο, τις κατευθυντήριες οδηγίες που δημοσιεύουν οι αρμόδιες αρχές, τη μεταξύ τους συνεργασία (ΕΣΠΔ, 2023), τα πρόστιμα που επιβάλλουν και την εξειδίκευση που αποκτούν επί των παραπλανητικών UI (Επιτροπή, 2022, Riegers and Sinders, 2020, CNIL, 2019).

Η νέα και η επικείμενη νομοθεσία επιχειρεί να θέσει όρια στην ασυδοσία των Big Tech και να διαμορφώσει ένα ασφαλές ψηφιακό περιβάλλον. Ιδίως οι DSA και DMA θέτουν στο στόχαστρό τους τις VLOPs, τις VLOSEs και τους πυλωρούς και υπερβαίνουν με αυτόν τον τρόπο την περιπτωσιολογική αντιμετώπιση των σκοτεινών μοτίβων, στην οποία τείνει η προγενέστερη νομοθεσία και εξετάζουν τις συνέπειες σε συλλογικό επίπεδο. Υπάρχει επιτέλους ρητή απαγόρευση των σκοτεινών μοτίβων και στις δύο πλευρές του Ατλαντικού. Η ενωσιακή νομοθεσία εμπνέεται από την DETOUR Act και προχωρεί στην επίσημη ρητή απαγόρευση του παραπλανητικού σχεδιασμού σε όλη την ΕΕ. Η DSA απειλεί με ακόμα μεγαλύτερα από τον ΓΚΠΔ πρόστιμα και φαίνεται να απαγορεύει και σκοτεινά μοτίβα που κρύβονται εντός της αρχιτεκτονικής του συστήματος, αλλά θα εφαρμοστεί το 2024 και δεν επεκτείνει την προστασία των προσωπικών δεδομένων. Το άρθρο 25 παρ.2 της DSA εγείρει προβληματισμό για τυχόν αλληλοσυγκρουόμενες διατάξεις με κίνδυνο τη νομική αβεβαιότητα και τη δυσκολία απόδοσης ευθυνών. Για να τελεσφορήσουν οι προσπάθειες, θα είναι κρίσιμη η ερμηνεία των διατάξεων, από την Επιτροπή, τις εποπτικές αρχές και το ΔΕΕ, ώστε να μην καταλήξουν κενό γράμμα του νόμου. Ακόμα και ως προς τον σχεδιασμό των cookie banners, υπάρχει αβεβαιότητα για τις πρακτικές που επηρεάζουν την ιδιωτικότητα. Το disclaimer του ΕΣΠΔ (2023) στην έκθεση σχετικά με τα cookie banners διευκρινίζει ότι παρουσιάζει απλώς τις ελάχιστες απαιτούμενες νόμιμες προϋποθέσεις και ουσιαστικά επιβεβαιώνει άτυπα ότι υπάρχει ακόμα δρόμος για την εξομάλυνση της κατάστασης.

Η δυναμική της νομοθεσίας μπορεί να υπονομευθεί, αν οι συμμετέχοντες στο σύστημα και κυρίως οι χρήστες εφησυχάζουν. Δεδομένου ότι είναι αμφίβολη η πραγματική μεταστροφή των επιχειρήσεων, αυξάνεται το μερίδιο ευθύνης των χρηστών να αντιδράσουν και να διεκδικήσουν την αυτονομία τους. Η αντιμετώπισή των σκοτεινών μοτίβων σίγουρα δεν είναι εύκολη, καθώς από πίσω τους κρύβεται η οργανωμένη δουλειά εξειδικευμένων σχεδιαστών, προγραμματιστών και άλλων επαγγελματιών, που παρακολουθούν τη συμπεριφορά των χρηστών. Για αυτό απαιτείται η κατανομή ρόλων και ευθυνών μεταξύ όλων των εμπλεκομένων παραγόντων. Πρακτικά αυτό συνεπάγεται αφενός τη διεπιστημονική προσέγγιση και συνεργασία μεταξύ σχεδιαστών, προγραμματιστών και νομοθετών (Gray et al., 2021, CNIL, 2019), ιδίως τώρα που εξελίσσεται η TN (Leiser and Santos, 2023), αφετέρου την ευαισθητοποίηση των χρηστών.

Η παρούσα διπλωματική ανέδειξε το πρόβλημα των σκοτεινών μοτίβων και διαπιστώνοντας την έλλειψη γνώσης και ευαισθητοποίησης των χρηστών επιδίωξε να συμβάλει στην μεγαλύτερη ευαισθητοποίηση και στην αντίστασή τους απέναντι σε αυτές τις παραπλανητικές πρακτικές, που υφαρπάζουν τα προσωπικά τους δεδομένα με ή χωρίς ταυτόχρονη πρόκληση οικονομικής ζημίας. Φιλοδοξία της είναι να συμμετάσχει στη χάραξη πολιτικής και στον διάλογο που αφορά τη ρύθμιση του παραπλανητικού σχεδιασμού και να δώσει το έναυσμα για περαιτέρω εμβάθυνση στο

πρόβλημα και για σχετικές διεπιστημονικές μελέτες, ιδίως ενόψει της εφαρμογής των DSA και DMA και της ψήφισης της Πρότασης για την ΤΝ.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλιογραφία - αρθρογραφία

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., Wilson, S. (2017), "Nudges for Privacy and Security", *ACM Computing Surveys (CSUR)*, Vol. 50/3, https://dl.acm.org/doi/10.1145/3054926

Berbece, S. (2019), "'Let There Be Light!' Dark Patterns Under the Lens of the EU Legal Framework", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3472316

BEUC (2022), *"DARK PATTERNS" AND THE EU CONSUMER LAW ACQUIS. Recommendations for better enforcement and reform*.

Bhoot, A., Shinde M. and Mishra W. (2020), "Towards the identification of dark patterns: An analysis based on end-user reactions", *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, pp. 24-33, https://doi.org/10.1145/3429290.3429293

Bongard-Blanchy, K., Rossi A., Rivas S., Doublet S., Koening V. and Lenzini G. (2021), "I am Definitely Manipulated, even When I am Aware of it. It's Ridiculous! - Dark Patterns from the End-User Perspective", *Designing Interactive Systems Conference 2021*, pp. 763-776, https://doi.org/10.1145/3461778.3462086

Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S. (2016), "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns", *Proceedings on Privacy Enhancing Technologies*, Vol. 2016/4, pp. 237-254, https://doi.org/10.1515/popets-2016-0038

Brignull, H. (2021), *Comments at US FTC workshop "Bringing Dark Patterns to Light"*, . Διαθέσιμο στο: https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf

Brignull, H. (2013), Dark Patterns: inside the interfaces designed to trick you. Διαθέσιμο στο: https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you [Πρόσβαση 10 Φεβρουαρίου 2023]

Brignull, H. (2011), Dark Patterns: Deception vs. Honesty in UI Design. Διαθέσιμο στο: https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design [Πρόσβαση 10 Φεβρουαρίου 2023]

Brignull, H. (χ.χ.), *Cases*. Διαθέσιμο στο: https://www.deceptive.design/cases [Πρόσβαση 10 Φεβρουαρίου 2023]

Brignull, H. (χ.χ.), *Laws*. Διαθέσιμο στο: https://www.deceptive.design/laws [Πρόσβαση 10 Φεβρουαρίου 2023]

Brignull, H. (χ.χ.), *Types of Deceptive Pattern*. Διαθέσιμο στο: https://www.deceptive.design/types [Πρόσβαση 10 Φεβρουαρίου 2023]

Brownlee, J. (2016), *Why Dark Patterns Won't Go Away*. Διαθέσιμο στο: https://www.fastcompany.com/3060553/why-dark-patterns-wont-go-away [Πρόσβαση 10 Φεβρουαρίου 2023]

Butarelli, G. (2019), Speech on Dark Patterns, Legal Design Roundtable. Διαθέσιμο στο: https://edps.europa.eu/sites/edp/files/publication/19-04-27_dark_patterns_en.pdf

Calo, R. (2014), "Digital market manipulation", *George Washington Law Review*, Vol. 82/4, pp. 995-1051. https://doi.org/10.2139/ssrn.2309703

Campbell-Dollaghan, K. (2016), *The Year Dark Patterns Won.* Διαθέσιμο στο: https://www.fastcompany.com/3066586/the-year-dark-patterns-won [Πρόσβαση 10 Φεβρουαρίου 2023]

Cara, C. (2019), "Dark Patterns in the Media: a Systematic Review", *Network Intelligence Studies*, Vol. VII/14, pp. 105-113, https://www.researchgate.net/publication/341105338

Cavoukian A. (2011), *Privacy By design. The 7 Foundational Principles*, Διαθέσιμο στο: https://privacybydesign.ca/

Chivukula, S. et al. (2020), "Dimensions of UX Practice that Shape Ethical Awareness", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3313831.3376459

Chopra R. (2020), Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc, https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-rohit-chopra-regarding-dark-patterns-matter-age-learning-inc

Citron, D. and Solove, D. (2022), "Privacy Harms", *Boston University Law Review*, Vol. 102/793, pp. 793-863, http://dx.doi.org/10.2139/ssrn.3782222

CMA (2022), *Evidence review of Online Choice Architecture and consumer and competition harm*.

CMA (2022), *Online Choice Architecture. How digital design can harm competition and consumers*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf

CMA (2020), *Online platforms and digital advertising - Market study final report*.

CNIL (2023), *Évolution des pratiques du web en matière de cookies: la CNIL évalue l'impact de son plan d'action*, https://www.cnil.fr/fr/evolution-des-pratiques-du-web-en-matiere-de-cookies-la-cnil-evalue-limpact-de-son-plan-daction

CNIL (2019), "Shaping Choices in the Digital World - From dark patterns to data protection: the influence of ux/ui design on user empowerment", *IP Reports*, Vol. 6.

CNIL (χ.χ.), *Données & Design. Co-building user journeys compliant with the GDPR and respectful of privacy*, https://design.cnil.fr [Πρόσβαση 20 Απριλίου 2023]

ConPolicy (2023), *Good Practice Initiative for Cookie Banner Consent Management.* Διαθέσιμο στο: https://www.bmuv.de/fileadmin/Daten_BMU/Download_PDF/Verbraucherschutz/cookie_guidelines_bf.pdf [Πρόσβαση 20 Απριλίου 2023]

Conti, G. and Sobiesk, E. (2010), "Malicious Interface Design: Exploiting the User", *Proceedings of the 19th international conference on World wide web - WWW '10*, https://doi.org/10.1145/1772690.1772719

Danyang Li. (2023), The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices, https://businesslawreview.uchicago.edu/print-archive/ftc-and-cpras-regulation-dark-patterns-cookie-consent-notices

Day, G. and Stemler, A. (2020), "Are Dark Patterns Anticompetitive?", *Alabama Law Review*, Vol. 72/1, https://doi.org/10.2139/ssrn.3468321

Dev, J., Rader, E. and Patil S. (2020), Why Johnny Can't Unsubscribe: Barriers to Stopping Unwanted Email. *In Proc. of CHI.*

Di Geronimo, L. Braz, L., Fregnan, E., Palomba F. and Bachelli, A. (2020), "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-14, https://doi.org/10.1145/3313831.3376600

EDRi (2022), *The DSA fails to reign in the most harmful digital platform businesses – but it is still useful*, Διαθέσιμο στο: https://edri.org/our-work/the-dsa-fails-to-reign-in-the-most-harmful-digital-platform-businesses-but-it-is-still-useful/

Egberts, A. (2021), *Manipulation through Design: A Law and Economics Analysis of EU Dark Patterns Regulation*.

Euractiv (2022), *Dark patterns, online ads will be potential targets for the next Commission, Reynders says*. Διαθέσιμο στο: https://www.euractiv.com/section/digital/interview/dark-patterns-online-ads-will-be-potential-targets-for-the-next-commission-reynders-says/ [Πρόσβαση 5 Ιανουαρίου 2023]

Europol (2023), *ChatGPT. The impact of Large Language Models on Law Enforcement*, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

Eurostat, 2023, E-commerce statistics for individuals. Διαθέσιμο στο: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals#Main_points [Πρόσβαση 22 Μαρτίου 2023]

Fischer, D. (2019), Senators introduce bipartisan legislation to ban manipulative dark patterns. Διαθέσιμο στο: https://www.fischer.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns [Πρόσβαση 22 Μαρτίου 2023]

Forbrukerrådet (2022), *Enough deception*.

Forbrukerrådet (2021), *You can log out, but you can never leave. How Amazon manipulates consumers to keep them subscribed to Amazon Prime.*

Forbrukerrådet (2018), *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy.*

Forbrukerrådet (2018a), *Every step you take. How deceptive design lets Google track users 24/7.*

Fritsch L. (2017), Privacy dark patterns in identity management. *Lecture Notes in Informatics (LNI),* Gesellschaft für Informatik, Bonn.

Goanta C. and Santos, C. (2023), *Dark Patterns Everything: An Update on a Regulatory Global Movement*, Network Law Review. Διαθέσιμο στο: https://www.networklawreview.org/digiconsumers-two/ [Πρόσβαση 19 Ιανουαρίου 2023]

Graßl, P. et al. (2021), "Dark and Bright Patterns in Cookie Consent Requests", *Journal of Digital Social Research*, Vol. 3/1, pp. 1-38, https://doi.org/10.33621/jdsr.v3i1.54

Gray, C.M., Santos, C. and Bielova, N. (2023), "Towards a Preliminary Ontology of Dark Patterns Knowledge". *In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023*, Hamburg, Germany. ACM, NewYork, NY, USA, 9 pages. https://doi.org/10.1145/3544549.3585676

Gray, C.M., Santos, C., Bielova, N., Toth, M. and Clifford, D. (2021), Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. *In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21).* ACM Press. https://doi.org/10.1145/3411764.3445779

Gray, C.M., Chivukula, S. and Lee A. (2020), "What Kind of Work Do ``Asshole Designers'' Create? Describing Properties of Ethical Concern on Reddit", https://doi.org/10.1145/3357236.3395486

Gray, C.M. and Chivukula, S. (2019), Ethical Mediation in UX Practice. *In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019)*, May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3290605.3300408

Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A. L. (2018), "The dark (patterns) side of UX design", *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3173574.3174108

Greenberg S., Boring, S., Vermeulen, J. and Dostal J. (2014), Dark Patterns in Proxemic Interactions: A Critical Perspective. *In Proceedings of the 2014 Conference on Designing Interactive Systems (DIS '14).* ACM, New York,NY, USA, 523–532. https://doi.org/10.1145/2598510.2598541

Gunawan, J., Santos, C. and Kamara, I. (2022), Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. *In Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22)*, November 1–2, 2022, Washington, DC, USA. ACM, New York, NY, USA, 14pages. https://doi.org/10.1145/3511265.3550448

Gunawan, J., Choffnes, D., Hartzog W. and Wilson C. (2021), "Towards an Understanding of Dark Pattern Privacy Harms", *CHI'21, May 8–13, 2021, Online Virtual Conference*.

Gunawan, J. Pradeep A., Choffnes D., Hartzog W. and Wilson C. (2021), "A Comparative Study of Dark Patterns across Web and Mobile Modalities", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5/CSCW2, pp. 1-29, https://doi.org/10.1145/3479521

Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L.F., Sadeh, N. and Schaub, F. (2020), "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. *In Proc. Of CHI*.

Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., , L.F., Sadeh, N. and Schaub, F. (2019). An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. *In Proc. of the Workshop on Usable Security*.

Harris T., 2016. How Technology is Hijacking Your Mind — from a Magician and Google Design Ethicist. Διαθέσιμο στο: https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3

Human S. and Cech, F. (2021), A Human-Centric Perspective on Digital Consenting: The Case of GAFAM: *Proceedings of KES-HCIS 2020 Conference.* In Human Centred Intelligent Systems, Alfred Zimmermann, Robert J Howlett, and Lakhmi C Jain (Eds.). Smart Innovation, Systems and Technologies, Vol. 189. Springer Singapore, 139–159. https://doi.org/10.1007/978-981-15-5784-2_12

Hunstinx, P. (2014), *Preliminary Opinion of the European Data Protection Supervisor*. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

IAPP (2023), US State Privacy Legislation Tracker**.** Διαθέσιμο στο: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

ICO (χ.χ.), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ [Πρόσβαση 17 Ιουνίου 2023]

Jaiswal A. 2018, *'Dark patterns in UX: how designers should be responsible for their actions'.* Διαθέσιμο στο: https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c [Πρόσβαση 17 Ιουνίου 2023]

Jarovsky, L. (2023a), *'Dark Patterns in AI: Privacy Implications'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/dark-patterns-in-ai-privacy-implications [Πρόσβαση 22 Μαρτίου 2023]

Jarovsky, L. (2023b), *'FTC vs. Dark Patterns in Privacy'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/ftc-vs-dark-patterns-in-privacy [Πρόσβαση 8 Μαρτίου 2023]

Jarovsky, L. (2023c), *'Dark Patterns in Privacy: An Autonomy Problem'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/dark-patterns-in-privacy-an-autonomy [Πρόσβαση 1 Μαρτίου 2023]

Jarovsky, L. (2023d), *'Is Behavioral Advertising Dying?'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/is-behavioral-advertising-dying [Πρόσβαση 5 Ιανουαρίου 2023]

Jarovsky, L. (2022), "Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.4048582

Jarovsky, L. (2022a), *'Ready For The Upcoming Legislation Tsunami From Europe?'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/ready-for-the-upcoming-legislation [Πρόσβαση 5 Ιανουαρίου 2023]

Jarovsky, L. (2022b), *'Understand Privacy-Enhancing Design and How it Can Be a Game Changer for Data Protection'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/understand-privacy-enhancing-design [Πρόσβαση 5 Ιανουαρίου 2023]

Jarovsky, L. (2022c), *'Designing Meaningful Choices to Protect User Privacy'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/designing-meaningful-choices-to-protect [Πρόσβαση 5 Ιανουαρίου 2023]

Jarovsky, L. (2022d), *'Dark Patterns (Deceptive Design) in Data Protection'*. Διαθέσιμο στο: https://www.theprivacywhisperer.com/p/dark-patterns-deceptive-design-in [Πρόσβαση 5 Ιανουαρίου 2023]

King, J. and MacKinnon, E. (2022), '*Do the DSA and DMA Have What It Takes to Take on Dark Patterns?'*. Διαθέσιμο στο: https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/ [Πρόσβαση 17 Ιουνίου 2023]

Leiser, M. and Santos, C. (2023), Dark Patterns, Enforcement, and the emerging Digital Design Acquis -Manipulation beneath the Interface, *SSRN Electronic Journal,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4431048

Leiser, M. and Yang, W. (2022), Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive, *SSRN Electronic Journal*, https://ssrn.com/abstract=4418586

Leiser, M. and Caruana, M. (2021), Dark Patterns: Light to be found in Europe's Consumer Protection Regime. *Journal Of European Consumer AndMarket Law*, *10* (6), 237-251, https://hdl.handle.net/1887/3278362

Leiser, M. (2020), "'Dark Patterns': the case for regulatory pluralism", *SSRN Electronic Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625637

Lewis, C. (2014), Irresistible Apps: Motivational Design Patterns for Apps, Games, and Web-based Communities (1st ed.). Apress, Berkely, CA, USA.

Lingareddy, N., Schaffner, B. and Chetty, M. (2022). Can I Delete My Account?: Dark Patterns In Account Deletion on Social Media. 1, 1 (April 2022), 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Liu Z., Iqbal, U. and Saxena N. (2023), Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?

Luguri, J. and Strahilevitz, L. (2021), "Shining a Light on Dark Patterns", *Journal of Legal Analysis*, Vol. 13/1, pp. 43-109, https://doi.org/10.1093/jla/laaa006

Kampanos, G. and Shahandashti, S.F. (2021), Accept All: The Landscape of Cookie Banners in Greece and the UK. *In ICT Systems Security and Privacy Protection*, http://arxiv.org/abs/2104.05750

Machuletz, D. and Böhme, R. (2019), "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR", *Proceedings on Privacy Enhancing Technologies*, Vol. 2020/2, pp. 481-498, https://doi.org/10.2478/popets-2020-0037

Maier, M. and Harr, R. (2020), "Dark design patterns: An end-user perspective", *Human Technology*, Vol. 16/2, pp. 170-199, https://doi.org/10.17011/ht/urn.202008245641

Mathur, A., Kshirsagar, M. and Mayer, J. (2021), "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods", *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3411764.3445610

Mathur, A. Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A. (2019), "Dark patterns at scale: Findings from a crawl of 11K shopping websites", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3/CSCW, https://doi.org/10.1145/3359183

Matte, C., Bielova, N. and Santos, C. (2020), "Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB europe's transparency and consent framework", *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 791-809, https://doi.org/10.1109/SP40000.2020.00076

Moser, C., Resnick, P., Schoenebeck, S. (2019), "Impulse buying: Design practices and consumer needs", *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, https://doi.org/10.1145/3290605.3300472

NAI (2022), *Best Practices for User Choice and Transparency*. https://thenai.org/best-practices-for-user-choice-and-transparency/

NAI (2021), "Dark" and "Light" Patterns: When is Nudge a Problem?. Διαθέσιμο στο: https://thenai.org/dark-and-light-patterns-when-is-a-nudge-a-problem/

Narayanan, A., Mathur A., Chetty M. and Kshirsagar, M. (2020), "Dark patterns: Past, Present, and Future. The Evolution of Tricky User Interfaces", *Acmqueue*, March-April 2020, 1-25, https://queue.acm.org/detail.cfm?id=3400901

Nouwens, M., Liccardi I., Veale, M., Karger, D., and Kagal L. (2020), "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-13, https://doi.org/10.1145/3313831.3376321

NOYB (2023), *'Breaking news: Meta prohibited from use of personal data of advertising'*. Διαθέσιμο στο: https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising Πρόσβαση 5 Ιανουαρίου 2023]

NOYB (2022), '*Legal Analysis: No non-material damages for GDPR violations (C-300/21)?*'. Διαθέσιμο στο: https://noyb.eu/en/analysis-no-non-material-damages-gdpr [Πρόσβαση 17 Ιουνίου 2023]

NOYB (2021), *noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints*, Διαθέσιμο στο: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints [Πρόσβαση 6 Απριλίου 2023]

npr, 2018, *Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race'*. Διαθέσιμο στο: https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate [Πρόσβαση 6 Απριλίου 2023]

Radesky, J., Hiniker, A., McLaren C., Akgun E., Schaller A., Weeks H.M., Campbell S. and Gearhardt A. (2022), "Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children", *JAMA Network Open*, Vol. 5/6, p. e2217641, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2793493

Rieger, S. and Sinders, C. (2020), *Dark Patterns: Regulating Digital Design. How digital design practices un-dermine public policy efforts & how governments and regulators can respond*, https://www.stiftung-nv.de/sites/default/files/dark.patterns.english.pdf

Sanchez-Rola, I., Dell'Amico M., Kotzias P., Balzarotti D., Bilge L., Vervier P. and Santos I. 2019, Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. *In ACM Asia Conference on Computer and Communications Security (AsiaCCS '19)*, July 9–12, 2019, Auckland, New Zealand. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3321705.3329806

Santos, C., Rossi, A., Sanchez Chamorro, L., Bongard-Blanchy, K. and Abu-Salma, R. (2021), Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. *In Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES '21)*, November 15, 2021, Virtual Event, Republic of Korea. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3463676.3485611

Santos, C., Bielova, N. and Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation (2020)*, 91–135. https://doi.org/10.26116/techreg.2020.009

Soe, T. et al. (2020), "Circumvention by design -- dark patterns in cookie consents for online news outlets", *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, https://doi.org/10.1145/3419249.3420132

Solove, D. (2006), *A Taxonomy of Privacy*. University of Pennsylvania Law Review. 154 (2006). Issue 3. https://ssrn.com/abstract=667622

Sunstein, C. (2016), "Fifty Shades of Manipulation", *J. Behavioral Marketing*, Vol. 213, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2565892

Temkin, D. (2021) 'Charting a course towards a more privacy-first web', *Google Ads & Commerce Blog*. Διαθέσιμο στο: https://blog.google/products/ads-commerce/a-more-privacy-first-web/ [Πρόσβαση 17 Ιουνίου 2023]

Thaler, R.H. (2018), "Nudge, not sludge", *Science*, Vol. 361/6401, p. 431, https://doi.org/10.1126/science.aau9241

Thaler, R.H. and Sunstein, C. (2008), *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Yale University Press.

US FTC (2022), *Bringing Dark Patterns to Light - Staff Report*, https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop

Utz, C. Degeling, M., Fahl, S., Schaub, F. and Holz, T. (2019), "(Un)informed Consent: Studying GDPR consent notices in the field", *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, pp. 973-990, https://doi.org/10.1145/3319535.3354212

Waldman, A. (2020), "Cognitive biases, dark patterns, and the 'privacy paradox'", *Current Opinion in Psychology*, Vol. 31, pp. 105-109, https://doi.org/10.1016/j.copsyc.2019.08.025.

Zagal, J., Björk, S. and Lewis, C. (2013), "Dark Patterns in the Design of Games", *Foundations of Digital Games Conference*, http://www.fdg2013.org/program/papers/paper06_zagal_etal.pdf

Επιτροπή (2022α), *Digital fairness – fitness check on EU consumer law*. Διαθέσιμο στο: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

Επιτροπή (2022), Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F.et al. (2022) *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation : final report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2838/859030

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Κύπρου (2023), *Ανακοίνωση Επιτρόπου σε σχέση με τα αποτελέσματα των ελέγχων για τη χρήση Cookies από ιστοσελίδες*. Διαθέσιμο στο: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/99981BE9F8E399EFC22589A9002E6742?OpenDocument&highlight=cookies

ΟΟΣΑ (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης (2019), *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*, Έκδοση 2018.

Νόμοι – Πράξεις Ευρωπαϊκών οργάνων – Κατευθυντήριες γραμμές-Δελτία Τύπου

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/2065 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 19ης Οκτωβρίου 2022 σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/ΕΚ (πράξη για τις ψηφιακές υπηρεσίες).

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/1925 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 14ης Σεπτεμβρίου 2022 σχετικά με διεκδικήσιμες και δίκαιες αγορές στον ψηφιακό τομέα και για την τροποποίηση των οδηγιών (ΕΕ) 2019/1937 και (ΕΕ) 2020/1828 (Πράξη για τις Ψηφιακές Αγορές).

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/868 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 30ής Μαΐου 2022 σχετικά με την ευρωπαϊκή διακυβέρνηση δεδομένων και την τροποποίηση του κανονισμού (ΕΕ) 2018/1724 (πράξη για τη διακυβέρνηση δεδομένων).

Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους (Πράξη για τα δεδομένα).

Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης.

Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ 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).

Πρόταση του Κανονισμού ePrivacy, 2021, κείμενο από το Συμβούλιο της ΕΕ, διαθέσιμη στο: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

Επιτροπή (2023), Δελτίο Τύπου για πρακτικές χειραγώγησης μέσω του Διαδικτύου. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418

Επιτροπή (2021), Κατευθυντήριες γραμμές για την ερμηνεία και την εφαρμογή της οδηγίας 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά.

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

ΟΔΗΓΙΑ 2005/29/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 11ης Μαΐου 2005 για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά και για την τροποποίηση της οδηγίας 84/450/ΕΟΚ του Συμβουλίου, των οδηγιών 97/7/ΕΚ, 98/27/ΕΚ, 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («Οδηγία για τις αθέμιτες εμπορικές πρακτικές»)

ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 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).

ΕΣΠΔ (2023), *Report of the work undertaken by the Cookie Banner Taskforce.*

ΕΣΠΔ (2023), *Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: How to recognize and avoid them. Version 2.0.*

ΕΣΠΔ (2022), *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them. Version 1.0.*

ΕΣΠΔ (2020), *Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, Έκδοση 1.1.*

ΕΣΠΔ (2020), *Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Έκδοση 2.0.*

Συμβούλιο της ΕΕ, Δελτίο Τύπου 25/11/2021, διαθέσιμο στο: https://www.consilium.europa.eu/el/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/

Συμβούλιο της ΕΕ, Δελτίο Τύπου 10/2/2021, διαθέσιμο στο: https://www.consilium.europa.eu/el/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

Νομολογία
Απόφαση στην υπόθεση C-300/21, Oberster Gerichtshof UI κατά Österreichische Post AG

Απόφαση στην υπόθεση C-673/17, BVV-VBVκατά Planet49 GmbH

Απόφαση στην υπόθεση C-61/10, Orange Romania SA κατά Autoritatea Naţională de

Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)

Απόφαση στην υπόθεση VZBV κατά Advocado, 2021 (VZBV, 2021),
https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/
[Πρόσβαση 6 Απριλίου 2023]

Ιστοσελίδες

Α) Αναφορικά με τα πρόστιμα
GARANTE κατά Ediscom S.p.a. (2023),
https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9870014 [Πρόσβαση 17 Ιουνίου 2023]

APD κατά Roularta (2022), https://www.autoriteprotectiondonnees.be/citoyen/enquete-cookies-sur-les-sites-de-presse-roularta-mis-a-lamende [Πρόσβαση 17 Ιουνίου 2023]

Όρεγκον κατά Google (2022), https://www.doj.state.or.us/media-home/news-media-releases/largest-ag-consumer-privacy-settlement-in-u-s-history/ [Πρόσβαση 6 Απριλίου 2023]

Κολούμπια κατά Google (2022), https://oag.dc.gov/release/ag-racine-announces-google-must-pay-95-million [Πρόσβαση 6 Απριλίου 2023]

FTC κατά Epic Games (2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Microsoft Ireland Operations Limited (2022), https://www.cnil.fr/en/cookies-microsoft-ireland-operations-limited-fined-60-million-euros [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Tik Tok (2022),https://gdprhub.eu/index.php?title=CNIL_(France)_-_D%C3%A9lib%C3%A9ration_SAN-2022-027_du_29_d%C3%A9cembre_2022&mtc=today&mtc=hubasm [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Discord (2022), https://www.cnil.fr/en/discord-inc-fined-800-000-euros [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Apple (2022), https://www.cnil.fr/en/advertising-id-apple-distribution-international-fined-8-million-euros [Πρόσβαση 6 Απριλίου 2023]

FTC κατά Vonage (2022), https://www.theverge.com/2022/11/3/23439368/vonage-ericsson-dark-patterns-junk-fees-ticketmaster-ftc [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Google και Facebook (2022), https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Amazon (2021), https://www.lawspot.gr/nomika-nea/cookies-prostimo-100-ekatommyrion-eyro-sti-google-kai-35-ekatommyrion-eyro-stin-amazon?lspt_destination=upgrade [Πρόσβαση 6 Απριλίου 2023]

CNIL κατά Google (2019), https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en [Πρόσβαση 6 Απριλίου 2023]

AGCM κατά Facebook (2018), https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes [Πρόσβαση 6 Απριλίου 2023]

Β) Αναφορικά με την αμερικανική έννομη τάξη

California Legislative Information (χ.χ.), https://leginfo.legislature.ca.gov/faces/home.xhtml

CPRA https://www.caprivacy.org/cpra-text/

CAN-SPAM Act (χ.χ.), https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business [Πρόσβαση 17 Ιουνίου 2023]

ROSCA (χ.χ.), https://www.ftc.gov/legal-library/browse/statutes/restore-online-shoppers-confidence-act [Πρόσβαση 17 Ιουνίου 2023]

DETOUR Act (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1084/text. https://iapp.org/news/a/ongoing-dark-pattern-regulation/ [Πρόσβαση 17 Ιουνίου 2023]

ADPPA (2021), https://www.congress.gov/bill/117th-congress/house-bill/8152/text [Πρόσβαση 17 Ιουνίου 2023]

Για καταγγελίες ιστοσελίδων στον αρμόδιο Γενικό Εισαγγελέα (χ.χ.), https://darkpatternstipline.org/report/ [Πρόσβαση 17 Ιουνίου 2023]

Γ) Άλλες ιστοσελίδες

Για τους Brandeis and Warren, 1890, https://www.brandeis.edu/now/2013/july/privacy.html [Πρόσβαση 3 Φεβρουαρίου 2023]

Για την προστασία δεδομένων ήδη από τον σχεδιασμό ως πρότυπο ISO: https://www.iso.org/standard/76772.html [Πρόσβαση 17 Ιουνίου 2023]

Για τη Replika: https://www.reuters.com/technology/italy-bans-us-based-ai-chatbot-replika-using-personal-data-2023-02-03/ [Πρόσβαση 3 Φεβρουαρίου 2023]

Για τη Match.com: https://www.ftc.gov/news-events/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love [Πρόσβαση 3 Μαρτίου 2023]

Για την TurboTax: https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes [Πρόσβαση 17 Ιουνίου 2023]