ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΚΟΙΝΩΝΙΚΩΝ ΕΡΕΥΝΩΝ

NATIONAL CENTRE FOR SOCIAL RESEARCH

Ιδιωτική ζωή και επιτήρηση στο Διαδίκτυο: η εποχή της μετα-ιδιωτικότητας

Νίκος Δεμερτζής, Κατερίνα Μανδενάκη, Χαράλαμπος Τσέκερης

Κείμενα Εργασίας 2020/32

Working Papers 2020/32

ΚΕΙΜΕΝΑ ΕΡΓΑΣΙΑΣ

WORKING PAPERS

ΑΘΗΝΑ

ATHENS

Η παρούσα ηλεκτρονική έκδοση πραγματοποιήθηκε στο πλαίσιο της Πράξης «Έρευνα, Εκπαίδευση και Υποδομές: ο τριγωνισμός των αξόνων στρατηγικής ανάπτυξης του ΕΚΚΕ (REDI)» (MIS 5002378) που εντάσσεται στη «Δράση Στρατηγικής Ανάπτυξης Ερευνητικών και Τεχνολογικών Φορέων» και χρηματοδοτείται από το Επιχειρησιακό Πρόγραμμα «Ανταγωνιστικότητα, Επιχειρηματικότητα και Καινοτομία» στο πλαίσιο του ΕΣΠΑ 2014-2020, με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης (Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης).

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΤΠΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΚΟΙΝΩΝΙΚΩΝ ΕΡΕΥΝΩΝ

NATIONAL CENTRE FOR SOCIAL RESEARCH

Ιδιωτική ζωή και επιτήρηση στο Διαδίκτυο: η εποχή της μετα-ιδιωτικότητας

Νίκος Δεμερτζής, Κατερίνα Μανδενάκη, Χαράλαμπος Τσέκερης

Κείμενα Εργασίας 2020/32

Working Papers 2020/32

ΚΕΙΜΕΝΑ ΕΡΓΑΣΙΑΣ

WORKING PAPERS

ΑΘΗΝΑ ΙΟΥΝΙΟΣ 2020

ISSN 1108-1732

Υπεύθυνος έκδοσης: ΕΚΚΕ, Τμήμα Εκδόσεων

Ιδιωτική ζωή και επιτήρηση στο Διαδίκτυο: η εποχή της μετα-ιδιωτικότητας

Νίκος Δεμερτζής, Κατερίνα Μανδενάκη, Χαράλαμπος Τσέκερης

Περίληψη

Ο ψηφιακός κόσμος είναι ένα πεδίο διασκέδασης και πληροφόρησης για τους χρήστες και πεδίο εξόρυξης ενός εκ των πολυτιμότερων αγαθών, όπως διαμορφώθηκε τα τελευταία χρόνια, των προσωπικών δεδομένων. Πόσο μεγάλη απειλή για την ιδιωτικότητα είναι η συλλογή και επεξεργασία δεδομένων από τρίτα μέρη; Πόσο μπορεί αυτή η παραβίαση να συμβάλει στη διαμόρφωση προβληματικών κοινωνικών καταστάσεων; Με αφορμή τις εκτεταμένες μεθόδους επιτήρησης και συλλογής δεδομένων των πολιτών στην παγκόσμια κρίση του COVID-19 αυτή η μελέτη παρουσιάζει τα στοιχεία της πρόσφατης διεθνούς έρευνας για τη χρήση του Διαδικτύου από το World Internet Project για τις στάσεις και συμπεριφορές των ατόμων αναφορικά με τη διαδικτυακή ιδιωτικότητα και την επιτήρηση. Σκοπός είναι να ιχνηλατήσουμε το αν και κατά πόσο η καταγεγραμμένη ανησυχία για την παραβίαση της ιδιωτικότητας διασταυρώνεται με μια εκτεινόμενη αποδοχή της έλλειψής της.

Abstract

The digital world is a field of entertainment and information for users and a mining field of one of the most valuable goods as it has been formed in recent years: personal data. How much of a threat to privacy is the collection and processing of data by third parties? How much can this violation contribute to the formation of problematic social situations? On the occasion of the extensive methods of surveillance and data collection of citizens in the global crisis of COVID-19 this study presents the data of the recent international research on the use of the Internet by the World Internet Project on attitudes and behaviors of individuals regarding online privacy and surveillance. The aim is to trace whether and to what extent the recorded concern about the violation of privacy intersects with an expanding acceptance of its absence.

Εισαγωγή

Από ελεύθερο, αποκεντρωμένο εργαλείο έρευνας και επικοινωνίας, το διαδίκτυο έχει μετουσιωθεί τα τελευταία χρόνια σε ένα κεντροποιημένο και εμπορικά προσανατολισμένο πεδίο, χωρίς το οποίο δύσκολα μπορεί κανείς πλέον να φανταστεί τη ζωή του. Διάφορες οντότητες που ονομάζονται πλατφόρμες λειτουργούν με ένα εντελώς νέο επιχειρηματικό μοντέλο, ενώ οι μεγάλοι παίχτες όπως το Google, Facebook, Amazon, Apple and Microsoft (GAFAM) προσφέρουν καινοτόμες και κυρίως «δωρεάν» υπηρεσίες επικοινωνίας, διαμοιρασμού και πρόσβασης σε πληροφορία, βολικά και γρήγορα από την άνεση του σπιτιού μας ή οπουδήποτε κι αν είμαστε (de Bustos and Izquierdo-Castillo 2019). Ωστόσο, είναι γνωστό ότι η Google ή το Facebook γνωρίζουν ποιοι είναι οι χρήστες, πότε έχουν γενέθλια, τι ψάχνουν στο διαδίκτυο, τι δουλειά κάνουν τώρα, πού έχουν πάει· γνωρίζουν τα πρόσωπά τους και αυτά των φίλων και των συγγενών τους, γνωρίζουν ακόμα και τις απόψεις τους για πιο περίπλοκα θέματα και τις πολιτικές τους θέσεις.[1]

Το πρόσφατο ξέσπασμα της παγκόσμιας πανδημίας του COVID-19 αναμόχλευσε εκ νέου τη συζήτηση για τα ζητήματα της ιδιωτικότητας αναδεικνύοντας σημαντικές αντιδημοκρατικές τάσεις στις κοινωνίες (Σπουρδαλάκης, 2020· Δουζίνας, 2020) καθώς, ενώ ο πλανήτης νοσεί, διάφορες κυβερνήσεις επιβάλλουν με συνοπτικές διαδικασίες αυταρχικές πολιτικές.[2] Παράλληλα, διαπιστώθηκε ότι οι κυβερνήσεις σε συνεργασία με ιδιωτικές εταιρίες εφαρμόζουν ακόμα πιο γενικευμένες και αδιάκριτες μεθόδους παρακολούθησης και συγκομιδής δεδομένων για την παρατήρηση της εξάπλωσης του

[1] Πρβ. Curran, D. (2018). «Are you ready? Here is all the data Facebook and Google have on you». *The Guardian*, 30 Μαρτίου 2018, https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy · Smith, D. (2020). «Google keeps a frightening amount of data on you. Here's how to find and delete it». *CNET,* 7 Μαρτίου 2020, https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/· Nield, D. (2019). «All the ways Google tracks you—and how to stop it». *The Wired*, 27 Μαΐου 2019, https://www.wired.com/story/google-tracks-you-privacy/· Norval and Prasopoulou, 2017.

[2] Η Πολωνία επέβαλε σε όσους είναι σε αυτοπεριορισμό να κατεβάσουν μια εφαρμογή που παρακολουθεί τις κινήσεις και τις επαφές τους (Δουζίνας, 2020), ενώ το ίδιο σκεπτόταν και η Βρετανική κυβέρνηση. Στην Ουγγαρία, η κυβέρνηση Όρμπαν ανέστειλε επ' αόριστον την κοινοβουλευτική λειτουργία και μεταβίβασε όλες τις αρμοδιότητες στην εκτελεστική εξουσία αναιρώντας και τυπικά την αστική δημοκρατία. (Τζαρέλας, 2020).

ιού (Tzogopoulos, 2020· Stein, 2020). Άρθρο των *New York Times*[3] παρουσίασε την αμφιλεγόμενη υιοθέτηση πρακτικών ψηφιακής επιτήρησης που εφαρμόστηκαν σε διάφορες χώρες του κόσμου (Singer and Sang-Hun, 2020), ενώ ο Gross (2020) αναφέρει ότι στο Ισραήλ η κυβέρνηση επέτρεψε στις μυστικές υπηρεσίες να προβούν σε μαζική παρακολούθηση κινητών τηλεφώνων χωρίς δικαστική εντολή προκειμένου να ελεγχθεί η καμπύλη αύξησης των κρουσμάτων του ιού.[4] Τα ευαίσθητα δεδομένα που συλλέγονται κατά την περίοδο αυτής της κρίσης, όμως, δεν αφορούν αποκλειστικά οργανισμούς υγείας και κυβερνήσεις, καθώς, όπως σημειώνει η Stein (2020),[5] στις ΗΠΑ οι δημόσιες υπηρεσίες επιστρατεύουν εφαρμογές και εργαλεία και δεδομένα τοποθεσίας από τη Google και το Facebook προσφέροντας σε αυτές τις εταιρίες πρόσβαση σε απόρρητες πληροφορίες των πολιτών, όπως, π.χ., στην ημερομηνία που ένα άτομο ενδεχομένως προσβλήθηκε από το ιό, μαζί με την εθνικότητά του, το φύλο, την ηλικία και τις τοποθεσίες που επισκέφτηκε.

Αναδεικνύοντας το ζήτημα της διαχείρισης του κοινωνικού σώματος μέσω του ελέγχου της βιοπολιτικής ζωής, ο Δουζίνας (2020) σημειώνει ότι η υποχρέωση των Ελλήνων να πάρουν ηλεκτρονική άδεια στο κινητό τους για να βγουν από το σπίτι τους παραχώρησε στο κράτος πρόσβαση σε προσωπικά στοιχεία επιτρέποντάς του να παρακολουθεί τις κινήσεις και τη δραστηριότητα της πλειονότητας του πληθυσμού. Ο Πετρίδης (2020), με την αφορμή της πανδημίας και τον τρόπο αντιμετώπισής της στην Κίνα –την αρχική ποινική στόχευση γιατρών που προειδοποιούσαν για το πρόβλημα και τα μέτρα που επιβλήθηκαν στη χώρα–, σχολιάζει το πώς τα δυτικά μέσα ενημέρωσης, ειδικά στα ρεπορτάζ που αφορούν την Κίνα, τείνουν να παράγουν «αναπαραστάσεις οργουελικών καταστάσεων» μιας κοινωνίας που ζει υπό διαρκή επιτήρηση και

[3] Singer, N. and Sang-Hun, C. (2020). «As Coronavirus surveillance escalates, personal privacy plummets». *The New York Times*, 23 Μαρτίου 2020, https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[4] Gross, J.A. (2020). «Government okays mass surveillance of Israelis' phones to curb coronavirus». *Times of Israel*, 15 Μαρτίου 2020, https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/

[5] Stein, A. (2020). «How to restore data privacy after the coronavirus pandemic». *World Economic Forum*, 31 Μαρτίου 2020, https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic

παραβίαση της ιδιωτικότητας των πολιτών ως κάτι όμως που συμβαίνει «αλλού» και όχι «εδώ». Ο Τζαρέλας (2020) προειδοποιεί ότι η ψηφιοποίηση και ο έλεγχος της κοινωνικής αναπαραγωγής στο όνομα αρχικά της αντιμετώπισης των πανδημιών και της θωράκισης της δημόσιας υγείας μπορεί να είναι ένα προείκασμα για επισταμένη επιτήρηση στο μέλλον και σημειώνει ότι μπορεί μεν η παραγωγή ζωτικών κλάδων για την κοινωνία να παραμένει υλική και άρα να θέτει ένα όριο στον ψηφιακό μετασχηματισμό της, αυτό, όμως, δεν αναστέλλει την ψηφιακή καταγραφή και την απαλλοτρίωση της κοινωνικής ζωής. Θα έλεγε κανείς ότι πολύ εύκολα αλώθηκαν τα προπύργια της ιδιωτικότητας –και άλλων θεμελιωδών δικαιωμάτων– στο όνομα της δημόσιας υγείας.

Με την ψηφιακή ιδιωτικότητα να δέχεται πρωτοφανείς πιέσεις την εποχή του COVID 19, αυτή η μελέτη επιχειρεί να συμβάλει με νέα εμπειρικά δεδομένα στη διερεύνηση των στάσεων και των αντιλήψεων των πολιτών για τα ζητήματα της διαδικτυακής ιδιωτικότητας. Στην πρόσφατη έρευνα που διεξήγαγε το Center of the Digital Future[6] με τη συνεργασία 39 χωρών από όλο τον κόσμο, το World Internet Project (WIP 2018)[7] καταγράφει την ανησυχία των πολιτών για την ιδιωτικότητα και την διαδικτυακή προστασία των ψηφιακών δεδομένων τους, αναδεικνύοντας και μια παραδοξότητα: η ανησυχία αντισταθμίζεται από την αυξανόμενη εμπλοκή των ατόμων σε διαδικτυακές διαδικασίες και τη καταγεγραμμένη αποδοχή τους ότι δεν υπάρχει πλέον ιδιωτικότητα. Οι χρήστες τείνουν να πιστεύουν ότι μη έχοντας «τίποτα να κρύψουν» μπορούν να παραχωρούν τα δεδομένα τους και, εν τέλει, την προσωπική τους ζωή σε εταιρίες ή κυβερνήσεις επιλήσμονες, όμως, της μοίρας αυτών των δεδομένων ή των αποτελεσμάτων της επεξεργασίας τους.

Στην παγκόσμια οικονομία της συνδεσιμότητας

Πολύ πριν το ξέσπασμα της παγκόσμιας κρίσης υγείας, η έλευση των μέσων κοινωνικής δικτύωσης είχε επιτρέψει σε εταιρίες να στοχεύουν συγκεκριμένες ομάδες χρηστών για να εκμεταλλευτούν όχι μόνο τα δικά τους δεδομένα αλλά και τα δεδομένα που

[6] https://www.digitalcenter.org/
[7] http://www.worldinternetproject.com/

παράγουν (μεταδεδομένα) όταν μοιράζονται περιεχόμενο ή επικοινωνούν με άλλους (Fuchs, 2014). Η «*dataveillance*» (παρακολούθηση δεδομένων), όπως χαρακτηριστικά έχει ονομάσει το φαινόμενο ο Roger Clarke (1988), επιτρέπει σε κυβερνήσεις και εταιρίες να παρατηρούν τα άτομα με στόχο μια άνευ προηγουμένου συγκέντρωση προσωπικής πληροφορίας αλλά και μια μορφή ελέγχου (Clarke, 1994) όπως αποκάλυψαν οι φάκελοι Snowden[8] (Lyon, 2014) ή οι συνεντεύξεις με τον πρώην διευθυντή της Εθνικής Υπηρεσίας Πληροφοριών των Ηνωμένων Πολιτειών, Michael Hayden (Hayden, 2014), επιβεβαιώνοντας τον Fuchs (2014: 92) ότι «*οι πραγματικές πρακτικές της εμπορευματοποίησης δεδομένων, του ελέγχου των μέσων ενημέρωσης καθώς και η εταιρική και κρατική επιτήρηση περιορίζουν τη φιλελεύθερη ελευθερία της σκέψης, της γνώμης, της συνάθροισης και της συσχέτισης*».[9]

Το ζήτημα είναι ότι στο ψηφιακό σύμπαν των GAFAM έχει πλέον καθιερωθεί μια «μη-εναλλακτική»: παρέχοντας τα υλισμικά και λογισμικά θεμέλια ολόκληρου του διαδικτύου είναι αδύνατον για τον χρήστη να μην χρησιμοποιήσει τα προϊόντα τους και να μην υποκύψει στο κόστος της δωρεάν παροχής τους τα δεδομένα του. Στον «καπιταλισμό της πλατφόρμας» (Srnicek, 2017) η νέα οικονομία λειτουργεί μέσα από τη συνδεσιμότητα, καθώς βασικός πόρος αυτών των εταιρειών που σηματοδοτεί μια συστηματική στροφή στην διαδικασία της κερδοφορίας τους και γενικά στον παγκόσμιο καπιταλισμό είναι τα δεδομένα των χρηστών τους. Όπως κατέθεσε το 2018 και ο πρόεδρος του Facebook Mark Zuckerberg στην εξεταστική επιτροπή της αμερικανικής Γερουσίας, το επιχειρηματικό μοντέλο του Facebook και της Google είναι η παροχή δωρεάν υπηρεσιών στους χρήστες με αντάλλαγμά τα δεδομένα τους.[10] Τη δεκαετία του 1970 οι Serra και Schoolman, στην ταινία μικρού μήκους *Television delivers people* είχαν

[8] Τα αρχεία Snowden διαθέσιμα στο https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi
[9] Πρβ. Fuchs (2015)· Cammaerts (2008)· Hindman (2009)· Mosco (2009).
[10] Watson, C. (2018). «The key moments from Mark Zuckerberg's testimony to Congress». *The Guardian*, 11 Απριλίου 2018, https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments (πρόσβαση Φεβρουάριος 2020) · Hsu, T. and Celia Kang, C. (2018). «Demands grow for Facebook to explain its privacy policies». *New York Times*, 26 Μαρτίου 2018, https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge-analytica.html, (πρόσβαση Μάρτιος 2020).

πρωτοδιατυπώσει την ιδέα ότι «αν ένα προϊόν είναι δωρεάν τότε το προϊόν είσαι εσύ». Φαίνεται ότι στη συγκεκριμένη περίπτωση το προϊόν είναι τα δεδομένα μας.

Δεδομενοποίηση και μετα-ιδιωτικότητα

Η παρακολούθηση και συγκομιδή δεδομένων έχει αποτελέσει αντικείμενο μελέτης για δεκαετίες (Rule et al., 1983· Clarke, 1994· Derikx et al., 2015). Σύμφωνα με τον Lyon (2001a), η συστηματική προσοχή που δίνεται στις ζωές των ανθρώπων είναι μέρος μιας ευρύτερης διαδικασίας διατήρησης του κοινωνικού ελέγχου και της οικονομικής διαχείρισης, η οποία προκειμένου να επιτευχθεί πρέπει να θολώσει τα όρια ανάμεσα το ιδιωτικό και το δημόσιο. Οι τεχνολογίες της πληροφορίας παίζουν κεντρικό ρόλο σε αυτό ελαχιστοποιώντας το κόστος απόκτησης της προσωπικής πληροφορίας –χωρίς φανερό κοινωνικό κόστος– και αυξάνοντας την «πληροφοριακή ασυμμετρία» (Laudon, 1997· Acquisti et al., 2016). Συνεπώς, το πληροφοριακό μωσαϊκό των ψηφιακών εαυτών αποτελεί τη βάση μιας νέας πληροφοριακής σχέσης που υπερβαίνει την ψηφιοποίηση και οδηγεί στην δεδομενοποίηση (datafication) του εαυτού (van Dijck, 2014· Mai, 2016). Εάν η ψηφιοποίηση έχει δώσει τη δυνατότητα για μεγαλύτερη αποθήκευση και ταχύτερη επεξεργασία της πληροφορίας, η δεδομενοποίηση επιτρέπει στην πληροφορία να μετασχηματιστεί σε μια μορφή στην οποία μπορεί να ποσοτικοποιηθεί, να ταξινομηθεί και να αναλυθεί με πολύ πιο εξελιγμένους και σύνθετους τρόπους (Mayer-Schonberger and Cukier, 2013) μέσα σε μεγάλα σύνολα, εγείροντας μια σειρά προβλημάτων: από την ηθική της πληροφορίας (Lyon, 2001b) και τα νομικά ζητήματα (Schuster et al., 2017), στον προσδιορισμό των προσωπικών δεδομένων (Fuchs, 2012) και την εκμετάλλευση της πληροφορίας με σκοπό το κέρδος (Van Dijck, 2013).

Για να σημειωθούν κέρδη την εποχή της «οικονομίας της προσοχής» (Davenport and Beck, 2013· Boyd and Crawford, 2012) οι πληροφορίες που εξορύσσονται από τα μεγάλα δεδομένα εξατομικεύονται και προσωποποιούνται με αποτέλεσμα να επηρεάζουν την προσοχή, τα συναισθήματα και τη συμπεριφορά των ατόμων (Demertzis and Tsekeris, 2018). Ο συνδυασμός και με άλλες επικοινωνιακές τεχνικές, όπως το νευρομάρκετινγκ (Zurawicki, 2010· Ariely and Berns, 2010· Sampson, 2012), το

νευρομπράντινγκ (Steidl, 2012) ή τα αυτοματοποιημένα μποτ στα μέσα κοινωνικής δικτύωσης (Shorey and Howard, 2016), μπορούν να δημιουργήσουν μια πολύ αποτελεσματική προπαγάνδα, να χειραγωγήσουν ή και να εξαπατήσουν.[11] Η εκτεινόμενη συζήτηση για τα fake news και την κοινωνία των *μετα-γεγονότων* ή της *μετα-αλήθειας* (Keyes, 2004· McIntyre, 2018) και της *μετα-δημοκρατίας* (Crouch, 2001) φανερώνει τον προβληματισμό (Sunstein, 2017). Κι ενώ η Heller (2011) μιλά για την εποχή της «μετα-ιδιωτικότητας», ο Κιουπκιολής (2020: 150-151) σημειώνει ότι η κρίση του Covid 19 και οι άμεσες παραβιάσεις της ιδιωτικότητας που έλαβαν χώρα σε πολλές περιπτώσεις ανέδειξαν τον «*μετα-πολιτικό* μανδύα της κυβερνολογικής της βιοεξουσίας», εφαρμόζοντας «πολιτικές σοκ στο κλονισμένο σώμα της κοινωνίας» ως επιταγές ενός τεχνοκρατικού και επιστημονικού λόγου που υποβιβάζει σε έναν απλό φορμαλισμό τη δημοκρατική μορφή και καλεί τους πολίτες να εσωτερικεύσουν αυτή την κατάσταση «εξαίρεσης» με τις συνακόλουθες λογικές επιτήρησης.

Αν και η συγκομιδή δεδομένων των πολιτών δεν είναι κάτι καινούριο (Flick, 2016), αυτό που είναι καινούργιο είναι η έκταση της έκθεσης αυτών των δεδομένων, η δυνατότητα παραποίησης και ανεξέλεγκτου μετασχηματισμού. Χαρακτηριστικά, στα τέλη του προηγουμένου χρόνου, η Γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων (Commission Nationale de l'Informatique et des Libertés) επέβαλε πρόστιμο ύψους 150 εκατομμυρίων ευρώ στη Google για παραβίαση των κανόνων προστασίας προσωπικών δεδομένων της ΕΕ, με το σκεπτικό ότι υπήρχε έλλειψη διαφάνειας και σαφήνειας ως προς τον τρόπο με τον οποίο η εταιρία ενημερώνει τους χρήστες της για τη διαχείριση των προσωπικών τους δεδομένων χωρίς καμία νομική βάση και χωρίς να έχει λάβει τη συναίνεσή τους.[12] Λίγο νωρίτερα, στην άλλη όχθη του Ατλαντικού, έρευνα του *Observer*

[11] Οι Kramer, Guillory και Hancock (2014) έδειξαν ότι είναι πιθανό να επηρεαστούν οι χρήστες των κοινωνικών μέσων με μια μορφή «συναισθηματικής μεταδοτικότητας», αν οι σελίδες περιορίζουν τη δημοσίευση πληροφοριών με θετικό ή ανάλογα αρνητικό συναισθηματικό περιεχόμενο.

[12] Όπως αναφέρεται στην ανακοίνωση της CNIL: «*το ποσό που αποφασίστηκε, και η δημοσιότητα που έλαβε το πρόστιμο, δικαιολογούνται από τη σοβαρότητα των παραβάσεων που παρατηρήθηκαν ως προς τις βασικές αρχές του GDPR: Διαφάνεια, πληροφόρηση και συναίνεση*». Βλ. «Πρόστιμο 50 εκατ. ευρώ στη Google από τη Γαλλική Αρχή Προστασίας Δεδομένων. *Enikos.gr*, 21 Ιανουαρίου 2019, https://www.enikos.gr/international/621080/prostimo-50-ekat-evro-sti-google-apo-ti-galliki-archi-prostasias- (πρόσβαση Ιανουάριος 2020).

και της *New York Times* αποκάλυπτε ότι 50 εκατομμύρια προφίλ χρηστών του Facebook έγιναν αντικείμενο επεξεργασίας από την εταιρία Cambridge Analytica με αποτέλεσμα τη διαμόρφωση ενός προγράμματος που μπορούσε να προβλέψει και να επηρεάσει την εκλογική συμπεριφορά των ατόμων αποστέλλοντάς τους στοχοποιημένα, εξατομικευμένα μηνύματα βάσει των προσωπικών τους δεδομένων.[13] Η ίδια έρευνα, όμως, αποκαλύπτει ότι πέρα από τις αμερικάνικες εκλογές η συγκεκριμένη μέθοδος αξιοποιήθηκε και για τη χειραγώγηση των αποτελεσμάτων στο βρετανικό δημοψήφισμα του 2016 που οδήγησε τη Μεγάλη Βρετανία στο περιβόητο Brexit.

Το «ιδιωτικό παράδοξο»

Φαίνεται, όμως, ότι αυτές οι πρακτικές δεν αποτρέπουν τους ανθρώπους από τη χρήση του διαδικτύου, την αποδοχή cookies όταν επισκέπτονται μια ιστοσελίδα ή τη συμμετοχή τους στα μέσα κοινωνικής δικτύωσης με τη συνακόλουθη παροχή προσωπικών πληροφοριών (Ngwenyama and Klein, 2018· Van Dijck, 2013). Το 2007 οι Norberg et al. (2007) καθιέρωσαν τον όρο «ιδιωτικό παράδοξο» (*privacy paradox*) για να περιγράψουν αυτή τη διχοτόμηση ανάμεσα στην προθυμία των ατόμων να παραχωρήσουν πρόσβαση στα δεδομένα τους με σχεδόν μηδαμινά ανταλλάγματα και στις εκπεφρασμένες ανησυχίες τους για την παραβίαση της ιδιωτικότητάς τους (Kokolakis, 2017). Σε μια πειραματική έρευνα, οι Carrascal et al. (2013) διαπίστωσαν ότι οι χρήστες του Διαδικτύου τιμολογούν την πληροφορία του ιστορικού αναζήτησής τους στο διαδίκτυο περίπου 7 ευρώ, ενώ οι Egelman et al. (2012) έδειξαν ότι, αν και οι καταναλωτές είναι πρόθυμοι να πληρώσουν κάποιο τίμημα για να αγοράσουν την προστασία της ιδιωτικότητας τους, αυτό είναι πολύ μικρό.[14] Άλλες έρευνες πάνω στις στάσεις των

[13] Σύμφωνα με πληροφορίες που παρείχε εργαζόμενος στην εταιρία, «*εκμεταλλευτήκαμε το Facebook για να συλλέξουμε εκατομμύρια προφίλ χρηστών και να δημιουργήσουμε μοντέλα για να αξιοποιήσουμε αυτά που γνωρίζαμε για αυτούς και να στοχεύσουμε τους εσωτερικούς δαίμονές τους*». Πρβ. Cadwalladr, C. and Graham-Harrison, E. (2018). «Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach», *The Guardian*, 17 Μαρτίου 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (πρόσβαση Φεβρουάριος 2020).

[14] Συγκεκριμένα στο πείραμα οι χρήστες δεν ήταν διατεθειμένοι να πληρώσουν περισσότερο από 1,50 δολάριο για να «αγοράσουν» ασφάλεια της ιδιωτικότητάς του.

χρηστών έδειξαν ότι το ζήτημα της ιδιωτικότητας και της συλλογής των προσωπικών πληροφοριών είναι κάτι που τους απασχολεί ιδιαίτερα (TRUSTe, 2014· Madden, 2014) αλλά τις παραχωρούν άμεσα στο βαθμό που κρίνουν ότι έχουν κάτι να κερδίσουν –τάση που ανιχνεύθηκε ήδη από τις αρχές του 21ου αιώνα– (Brown, 2001· Spiekermann et al., 2001). Η Taddicken (2014) έδειξε ότι οι ανησυχίες για την προστασία των προσωπικών δεδομένων δεν επηρεάζουν την αυτοαποκάλυψη στον βαθμό που το επικοινωνιακό μοτίβο ανάμεσα τους χρήστες εκτελείται σε μια βάση ανταλλαγής, «πες μου για σένα και θα πω κι εγώ για μένα», ή ενέχει το κέρδος του διαμοιρασμού (Lee et al., 2013). Οι Zafeiropoulou et al. (2013) προσέγγισαν τις στάσεις των χρηστών σχετικά με τα δεδομένα τοποθεσίας, δηλαδή την αποκάλυψη τού πού βρίσκονται μια δεδομένη στιγμή ή πού έχουν βρεθεί στο παρελθόν και διαπίστωσαν ότι με κάποιο αντάλλαγμα συμμετοχής σε μια δικτυακή εμπειρία ή υπηρεσία οι χρήστες πάλι πρόθυμα, ακόμα και απερίσκεπτα, αποκαλύπτουν αυτή την πληροφορία.

Οι Ngwenyama και Klein (2018) έδειξαν ότι η συμμόρφωση των ατόμων με αμφιλεγόμενες πρακτικές παραβίασης της ιδιωτικότητάς τους οφείλεται σε μια εκούσια αμνησία και έλλειψη επίγνωσης που σχετίζεται με την μπερδεμένη φύση των πρακτικών της παρακολούθησης δεδομένων στα μέσα κοινωνικής δικτύωσης. Στην παρακολούθηση δεδομένων, στον έλεγχο και την τελική εκμετάλλευσή τους, κατέληξαν οι ερευνητές, εμπλέκονται ποικίλες ηθικές αντιφάσεις, συγκεκαλυμμένοι σκοποί, ατζέντες και εντέλει ιδεολογία (Van Dijck, 2013, 2014· Ngwenyama and Klein, 2018). Οι Oetzel και Gonja (2011) απέδωσαν την ευκολία στην παροχή προσωπικών πληροφοριών στη δυσκολία κατανόησης της παραβίασης διαδικτυακής ιδιωτικότητας λόγω έλλειψης κοινωνικών αναπαραστάσεων. Στερημένοι από σχήματα που θα τους επιτρέψουν να νοηματοδοτήσουν τα προβλήματα που αυτή η παραβίαση μπορεί να επιφέρει, οι χρήστες υπολογίζουν τα ρίσκα και τα οφέλη της αποκάλυψης προσωπικών πληροφοριών επηρεασμένοι, κυρίως, από γνωστικές προκαταλήψεις (Acquisti and Grossklags, 2007) ή από τον ευριστικό κανόνα των συναισθημάτων, σύμφωνα με τον οποίο οι άνθρωποι υποτιμούν τους κινδύνους που σχετίζονται με την απόκτηση κάποιου αρεστού αγαθού,

ενώ τους υπερεκτιμούν όταν συσχετίζονται με κάτι που τους προκαλεί απαρέσκεια (Finucane et al., 2000).

Το κοινωνικό κεφάλαιο στη συναισθηματική δημόσια σφαίρα

Οι Demertzis και Tsekeris (2018) σημειώνουν ότι η απόφαση ενός ατόμου να παραχωρήσει την ιδιωτική του πληροφορία στο Διαδίκτυο σχετίζεται με πολλούς παράγοντες όπως το προσωπικό συμφέρον, ο ψηφιακός εγγραμματισμός και η κοινωνική του επίγνωση. Επιπλέον, η ενεργή συμμετοχή στα κοινωνικά δίκτυα που αφορά την αυτοαποκάλυψη σχετίζεται με τρεις βασικές ανάγκες: την ανάγκη για διασκέδαση, την ανάγκη για κοινωνικές σχέσεις και την ανάγκη για την κατασκευή ταυτότητας (Debatin et al., 2009). Για τους περισσότερους χρήστες, η ικανοποίηση των παραπάνω αναγκών υπερβαίνει τους κινδύνους έκθεσης των προσωπικών δεδομένων, ακόμα κι αν έχουν υποστεί παραβιάσεις, ανταποκρινόμενοι σε μια «τελετουργική» ενσωμάτωση της διαδικτυακής κοινωνικοποίησης. Η κοινωνική δικτύωση είναι πλέον ένας τρόπος απόκτησης κοινωνικού κεφαλαίου (Ellison et al., 2011) που ανταλλάσσεται με την αποκάλυψη προσωπικών πληροφοριών.[15] Οι Demertzis και Tsekeris (2018: 16) σημειώνουν ότι τα εργαλεία και οι μηχανισμοί ελέγχου που συνεπάγεται η «*κυβερνητικότητα της νεοφιλελεύθερης οικονομίας του χρέους*» δημιουργούν νέους συναισθηματικούς κανόνες, από-τυποποιούν τους τρόπους συμπεριφοράς και συνθέτουν μια *συναισθηματική δημόσια σφαίρα* (Richards, 2007) μέσα στην οποία οι άνθρωποι, απελευθερωμένοι από τους περιορισμούς του παρελθόντος, εκφράζονται ελεύθερα στο δρόμο της «*χειραφέτησης των συναισθημάτων*» (Wouters, 2007). Συνεπώς, αν η παραχώρηση ιδιωτικών πληροφοριών αποτελεί το κόστος συμμετοχής δικτυωμένων αλλά αποσυνδεδεμένων ατόμων στη «συναισθηματική δημόσια σφαίρα» όπου η ναρκισσιστική αυτοαποκάλυψη γίνεται στο όνομα της αυθεντικότητας του εαυτού (Sennett, 1993), τότε, ενδεχομένως, το όφελος να είναι μεγάλο. Σχετικά με αυτό, Wilson και Valacich (2012) εντοπίζουν και άλλους δύο παράγοντες που συμβάλλουν στην

[15] Για παράδειγμα, οι Stutzman et al. (2012) παρατηρούν ότι αν κάποιο άτομο αποκαλύψει ένα ιατρικό πρόβλημα του είναι πιο πιθανό να λάβει μηνύματα υποστήριξης από άλλα μέλη του δικτύου του κάτι που άλλωστε επιδιώκει.

εκδήλωση του ιδιωτικού παράδοξου: την αμεσότητα του οφέλους και τη διάχυση του ρίσκου. Όταν τα άτομα αντιλαμβάνονται τα οφέλη της αυτοαποκάλυψης ως κάτι άμεσο τείνουν να αξιολογούν τους κινδύνους ως κάτι απόμακρο. Έτσι ο κίνδυνος διαχέεται όταν, π.χ., το άτομο πιστεύει ότι τα δεδομένα του μπορεί να συλλεχθούν αρκετά αργότερα από τη στιγμή που δίνει τη συναίνεσή του και αξιολογεί τους κινδύνους ως πολύ χαμηλότερους από τα οφέλη.

Τι είναι τα προσωπικά δεδομένα

Το δικαίωμα στην προστασία των προσωπικών δεδομένων είναι ένα κατεξοχήν νέο συνταγματικό δικαίωμα, μια «εξελιγμένη μορφή του δικαιώματος ιδιωτικού βίου» (Ακριβοπούλου, 2011· Ανθόπουλος, 2007). Κατοχυρωμένο με την αναθεώρηση του 2001 στο άρθρο 9Α,[16] ανταποκρίνεται στην ανάγκη για κανονιστικό επαναπροσδιορισμό της προστασίας του υποκειμένου έναντι των απειλών που η σύγχρονη χρήση της τεχνολογίας γεννά για την αυτονομία και την ελευθερία του. Ωστόσο, η προστασία των προσωπικών δεδομένων, αν και συνδέεται, δεν ταυτίζεται με την ιδιωτικότητα. Ο ετεροαναφορικός χαρακτήρας του δικαιώματος στην προστασία των προσωπικών δεδομένων προϋποθέτει την προστασία της ιδιωτικότητας και της προσωπικότητας του υποκειμένου αλλά και την κατάληξη στο αν και κατά πόσο το περιεχόμενο των δεδομένων των χρηστών είναι και περιεχόμενο της πληροφοριακής ελευθερίας και αυτονομίας τους. Σύμφωνα με την τυπολογία που αναπτύσσει στο βιβλίο του *Data and Goliath*, ο Schneier (2015) περιγράφει έξι διαφορετικούς τύπους δεδομένων περιεχομένου ή ψηφιακών αποτυπωμάτων:

- **Δεδομένα υπηρεσιών** (Service Data) αφορούν πληροφορίες που δίνουμε για να λάβουμε μια υπηρεσία, π.χ. όνομα, ηλικία, διεύθυνση. Πρόκειται για πληροφορίες που ελέγχονται σχετικά εύκολα καθώς ο χρήστης μπορεί να παρακρατήσει κάποια πληροφορία ή να δώσει κάποιες ψεύτικες.

[16] Άρθρο 9Α: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

- **Αποκαλυφθέντα δεδομένα** (Disclosed Data): αφορούν περιεχόμενο, όπως φωτογραφίες ή κείμενα που δημοσιεύει ο χρήστης σε μια ιστοσελίδα ή σε blog που κατέχει ο ίδιος. Αυτά τα δεδομένα είναι θεωρητικά εντελώς υπό τον έλεγχο του χρήστη, καθώς εκείνος αποφασίζει τι θα δημοσιεύσει αλλά και ποιος μπορεί να έχει πρόσβαση στην υποδομή και το περιεχόμενό του.
- **Εμπιστευόμενα δεδομένα** (Entrusted Data): είναι τα δεδομένα που οι χρήστες παραχωρούν σε τρίτα μέρη, όπως διάφορες υπηρεσίες ή τράπεζες, αλλά και εταιρίες, όπως το Facebook ή η Google, τα οποία εμπιστεύονται ότι θα τα διαχειριστούν με σύνεση. Αν και ο χρήστης μπορεί να αποφασίσει αν θα δημοσιεύσει περιεχόμενο σε αυτές τις πλατφόρμες, δεν ελέγχει τι είδους επεξεργασία θα υποστεί αυτό το περιεχόμενο.
- **Παρεμπίπτοντα δεδομένα** (Incidental Data): είναι τα δεδομένα που προκύπτουν από τρίτους χωρίς τη συναίνεση του χρήστη μέσα από ετικέτες (tags) ή hashtags, αναφορές σε δημοσιεύματα άλλων, ηλεκτρονικό ταχυδρομείο ακόμα και τηλεφωνικές συνομιλίες που είναι πιο δύσκολο να ελεγχθούν, καθώς ένας χρήστης μπορεί μόνο σε περιορισμένο αριθμό ανθρώπων να ζητήσει να μην δημοσιεύουν πράγματα που τον αφορούν.
- **Συμπεριφορικά δεδομένα** (Behavioral Data): αυτά προκύπτουν από τη χρήση του υπολογιστή ή του κινητού και σκιαγραφούν την εικόνα του χρήστη, όπως για παράδειγμα τα δεδομένα γεωεντοπισμού, τα οποία γνωστοποιούν πού βρίσκεται κάποιο άτομο, πόσο χρόνο έμεινε εκεί ακόμα και με ποιον πήγε.
- **Παράγωγα δεδομένα** (Derived Data): είναι το αποτέλεσμα επεξεργασίας, συνδυασμού και διαχείρισης χαρακτηριστικών που προκύπτουν από τα μέσα κοινωνικής δικτύωσης και τα μοτίβα συμπεριφοράς και αναζητήσεων στις μηχανές αναζήτησης.

Η άλλη μορφή δεδομένων είναι τα *μεταδεδομένα*. Πρόκειται για δεδομένα που αφορούν δεδομένα (π.χ., τα μεταδεδομένα ενός e-mail περιέχουν τα στοιχεία του αποστολέα, του παραλήπτη, την ώρα και μέρα αποστολής, το θέμα και ενίοτε τη φυσική διεύθυνση του υπολογιστή). Καθώς, όμως, αποτελούν βασικά στοιχεία λειτουργίας των

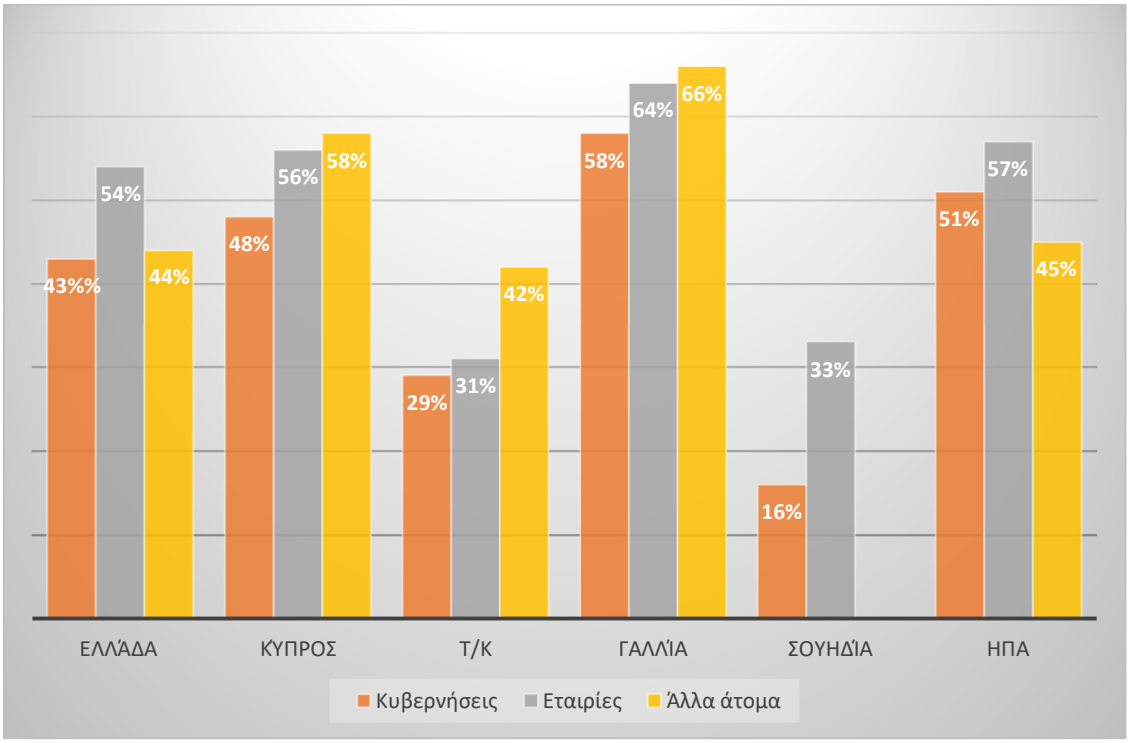
διαδικτυακών υποδομών, τα μεταδεδομένα δεν μπορούν να ελεγχθούν από τον χρήστη, ο οποίος δεν μπορεί καν να τα δει ή να τα διαβάσει (Cooke, 2020). Πρώτον, η πολύ δομημένη μορφή τους είναι ιδανική για να «διαβαστούν» από υπολογιστές, να ποσοτικοποιηθούν και να ταξινομηθούν. Δεύτερον, η τεράστια ποσότητά τους δίνει πολύτιμες πληροφορίες για τον εντοπισμό και την κατανόηση μοτίβων συμπεριφοράς καθώς και για τα δίκτυα επαφών των ατόμων[17] και καταλήγουν να πωλούνται με τη μορφή προφίλ αναζήτησης χρήστη (Jaworski, 2011).

World Internet Project: στάσεις και συμπεριφορές

Ο Manovich (2011) εντοπίζει τρεις τάξεις στις δεδομενοκεντρικές κοινωνίες: «αυτούς που παράγουν δεδομένα, συνειδητά ή αφήνοντας ψηφιακά αποτυπώματα, εκείνους που έχουν τα μέσα να τα συλλέξουν κι εκείνους που έχουν τη γνώση να τα επεξεργαστούν». Σε αυτό το πλαίσιο, οι τύποι των δρώντων που εντάσσονται στη δεύτερη και στην τρίτη κατηγορία είναι οι *εταιρίες*, οι *κυβερνήσεις* και *άλλα άτομα*. Στην έρευνα του WIP, από τις τρεις πιθανές πηγές παραβίασης της διαδικτυακής ιδιωτικότητας (*κυβερνήσεις*, *εταιρίες*, *άτομα*), οι κυβερνήσεις συγκεντρώνουν τη χαμηλότερη ανησυχία (Γράφημα 1), εκτός από τις Ηνωμένες Πολιτείες, όπου εκεί ο λιγότερο ανησυχητικός εισβολέας της διαδικτυακής ιδιωτικότητας είναι τα άλλα άτομα σε ποσοστό 45%.

[17] Οι πληροφορίες μεταδεδομένων, π.χ. ενός ηλεκτρονικού ταχυδρομείου, είναι η συχνότητα επικοινωνίας του χρήστη, η ώρα που συνήθως το κάνει, τα χαρακτηριστικά της συχνότητας αυτής σε σχέση με συγκεκριμένα γεγονότα, καθώς και τα άτομα που συμμετέχουν στα κοινωνικά δίκτυά του. Πρβλ. Share Lab 2016, «Browsing Histories – Metadata Explorations», https://labs.rs/en/browsing-histories (πρόσβαση Ιανουάριος 2020).

Γράφημα 1: Ανησυχίες παραβίασης ιδιωτικότητας στο διαδίκτυο



Η Σουηδία είναι η χώρα που δείχνει τη μεγαλύτερη εμπιστοσύνη στην κυβέρνησή της, καθώς μόνο το 16% των συμμετεχόντων ανησυχεί ότι οι κυβερνήσεις συλλέγουν δεδομένα, ενώ αμέσως μετά την εμπιστοσύνη τους δείχνουν και οι Τουρκοκύπριοι (Τ/Κ), με ένα χαμηλό ποσοστό 29% να εκφράζει την ανησυχία του για κυβερνητικές παραβιάσεις ιδιωτικότητας. Από τα δεδομένα της έρευνας φαίνεται ότι οι πιο καχύποπτοι σε σχέση με την κυβερνητική επιτήρηση είναι οι Γάλλοι συμμετέχοντες σε ποσοστό 58%.

Οι κυβερνήσεις επιτηρούν και συλλέγουν πληροφορίες και στοιχεία επιδιώκοντας να αντιμετωπίσουν διαδικτυακά εγκλήματα, απάτη, τρομοκρατία ή άλλες παραβάσεις (Amoore and De Goede, 2005), να εγκαταστήσουν μια πιο αποτελεσματική γραφειοκρατία, να ελέγξουν την μετανάστευση. Ανάλογα, ωστόσο, με την κοινωνική ή πολιτική κατάσταση μιας χώρας, οι κυβερνήσεις μπορούν με την συλλογή και την επεξεργασία προσωπικών δεδομένων να αποκλείσουν ομάδες από συγκεκριμένες

υπηρεσίες (Ganesh et al., 2016), να ασκήσουν λογοκρισία, να καθορίσουν και να εντοπίσουν μια κοινωνική ή πολιτική απειλή (Hache and Jansen, 2018) αλλά και να ελέγξουν τις ροές επικοινωνίας μιας ολόκληρης χώρας.[18] Όπως παρατηρούν οι Foa και Muounk (2017), με πρόσχημα την ασφάλεια, τα ψηφιακά μέσα δεν συνεισφέρουν στον «εκδημοκρατισμό της δημοκρατίας» αλλά στην αποσταθεροποίησή της.

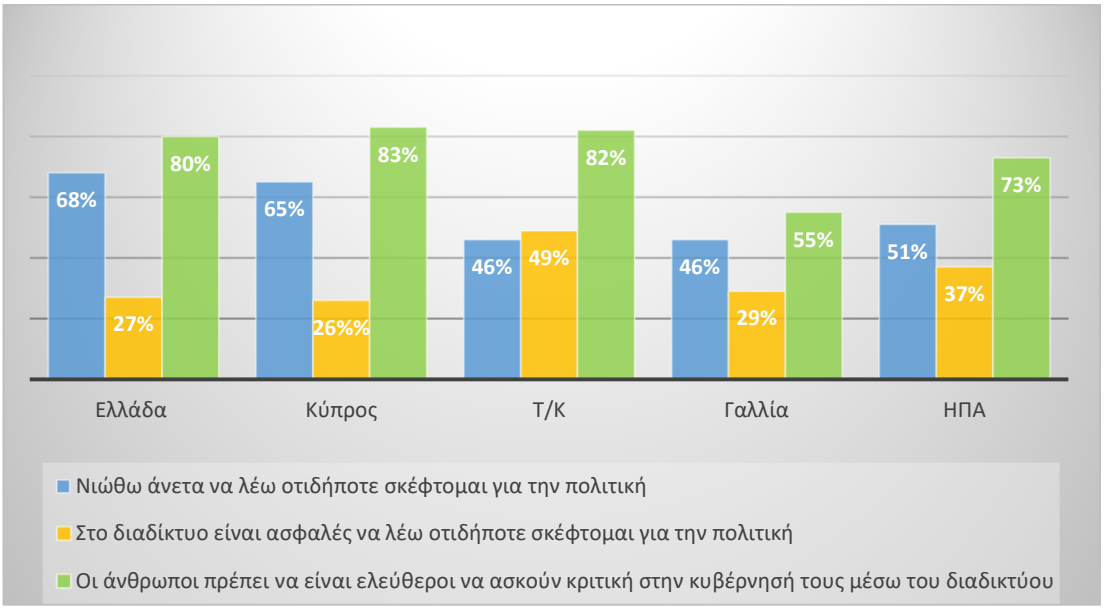
Όπως είχε δείξει, ωστόσο, η έρευνα των Dinev και Hart (2008), η μεγαλύτερη πρόσβαση σε προσωπικά δεδομένα εκ μέρους κυβερνήσεων μπορεί να είναι καλοδεχούμενη από τους χρήστες ως μια αναγκαία πρακτική που θα εξασφαλίζει προστασία, τάξη καθώς και βολικές και άνετες συναλλαγές. Αγνοώντας, ενδεχομένως, τη σημασία και τις βαθύτερες συνέπειες της επιτήρησης στην ψηφιακή εποχή, οι χρήστες παρουσιάζουν σημεία προσχώρησης στην κουλτούρα της επιτήρησης την οποία έχουν ήδη αντιληφθεί. Γιατί αν οι κυβερνήσεις επιτηρούν, πόσο ελεύθεροι είναι οι πολίτες στην άσκηση της ελευθερίας του λόγου στο Διαδίκτυο;

Τα στοιχεία του WIP παρουσιάζουν μια επιφυλακτικότητα και μια υποφώσκουσα επίγνωση. Η πλειονότητα των συμμετεχόντων έδωσε πολύ μεγάλα ποσοστά συμφωνίας στην θέση ότι «*οι άνθρωποι πρέπει να είναι ελεύθεροι να κριτικάρουν τις κυβερνήσεις τους διαδικτυακά*», ξεκινώντας από τους με τους Γάλλους συμμετέχοντες να συμφωνούν σε ποσοστό 55% και τους Κύπριους να το πιστεύουν σε ποσοστό 83%. Ωστόσο, ήταν λιγότεροι οι συμμετέχοντες που δηλώνουν ότι νιώθουν *άνετα* να λένε γενικά στη ζωή οτιδήποτε σκέφτονται για την πολιτική –με τους Έλληνες συμμετέχοντες να είναι οι πιο άνετοι από όλους σε ποσοστό 68%– και ακόμα λιγότεροι εκείνοι που πιστεύουν ότι είναι *ασφαλές* να λένε στο Διαδίκτυο οτιδήποτε σκέφτονται για την πολιτική. Οι Έλληνες και οι Κύπριοι συμμετέχοντες συμφώνησαν με αυτή τη θέση μόνο κατά 27% και 26% αντίστοιχα και οι Γάλλοι κατά 29%, ενώ οι συμμετέχοντες από την Τ/Κ Κοινότητα παρουσιάζονται ως οι περισσότερο ασφαλείς να εκφράζονται πολιτικά στο διαδίκτυο σε ποσοστό 49%. Όσον αφορά τους ερωτηθέντες από τις Ηνωμένες Πολιτείες, αν και

[18] Πρβ. Reportes without Borders (2014). *Enemies of the Internet 2014 Report* https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf (πρόσβαση Μάρτιος 2020).

νιώθουν άνετα να συζητούν για την πολιτική γενικά (51%), ποσοστό μόνο 37% πιστεύει ότι είναι ασφαλές να λέει ότι θέλει για τα πολιτικά στο Διαδίκτυο (Γράφημα 2).

Γράφημα 2: Πολιτική έκφραση στο διαδίκτυο

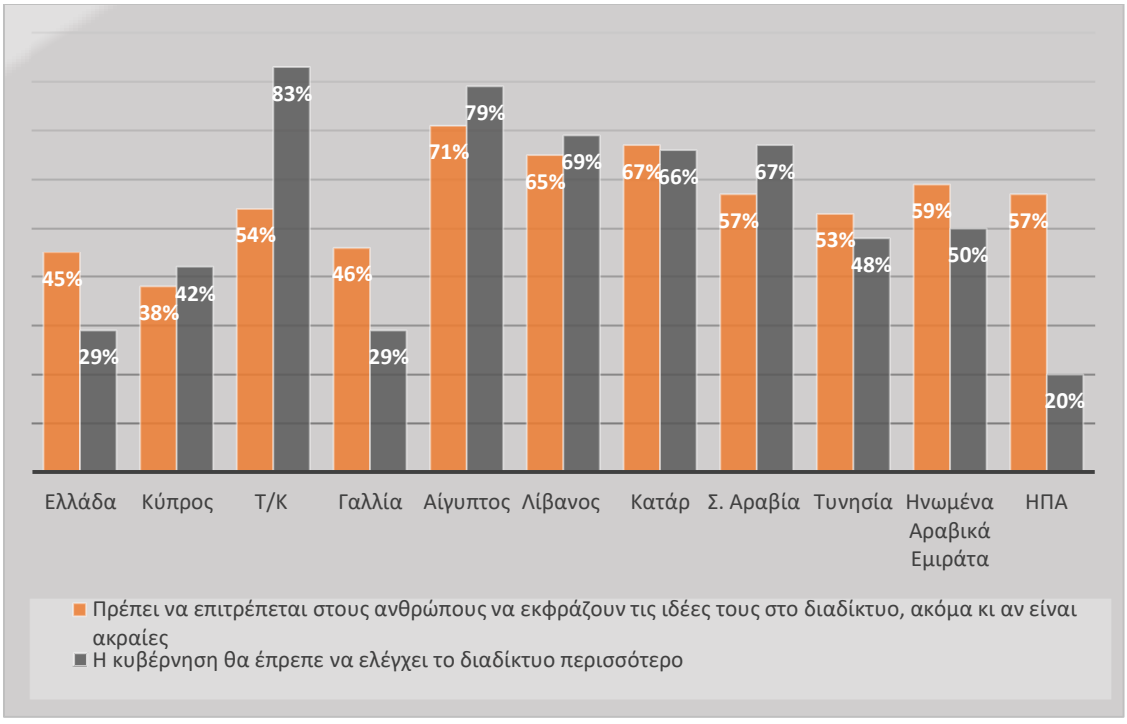


Όπως φαίνεται, οι συμμετέχοντες θεωρούν ότι το διαδίκτυο ενέχει τελικά το ρίσκο της έκθεσης τόσο απέναντι σε κέντρα εξουσίας που μπορεί να τους παρακολουθούν όσο και στις αντίθετες απόψεις άλλων που μπορεί να επιτεθούν. Δεν είναι λίγες οι περιπτώσεις του διαδικτυακού εκφοβισμού (cyberbulling) με αφορμή πολιτικές διαφωνίες, ένα φαινόμενο που κλιμακώθηκε στις αμερικανικές εκλογές του 2016.[19] Σχετικά με αυτό (βλ. Γράφημα 3), μετρώντας τις στάσεις των συμμετεχόντων σχετικά με το αν πιστεύουν ότι το Διαδίκτυο μπορεί να είναι ένα πεδίο ελεύθερης διακίνησης ιδεών «*ακόμα κι αν είναι ακραίες*», οι θετικές απαντήσεις ξεκινούν από το χαμηλό ποσοστό 29% στη Γαλλία, φανερώνοντας την επιφυλακτικότητα των ερωτηθέντων ως προς το αν πρέπει να εκφράζονται διαδικτυακά απόψεις που, ενδεχομένως, είτε γίνονται αντικείμενο παρακολούθησης είτε στρέφονται και ενάντια

[19] Πρβ. https://www.pewresearch.org/internet/2012/03/12/social-networking-sites-and-politics

στη δημοκρατία (π.χ. φασιστικές διακηρύξεις, προπαγάνδα) αλλά και σε αυτόν που τις εκφράζει. Στην Αίγυπτο, ωστόσο, το αίτημα για την απελευθέρωση ακόμα και της ακραίας πολιτικής εκφραστικότητας φτάνει στο 71%. Ωστόσο, στην ερώτηση σχετικά με το αν «*θα έπρεπε η κυβέρνηση να ελέγχει περισσότερο το διαδίκτυο*», συμφωνούν πάνω από τα δύο τρίτα των συμμετεχόντων σε πέντε από εννέα χώρες, με τους Τουρκοκυπρίους να δίνουν το υψηλότερο ποσοστό με 83%. Στο άλλο άκρο, η χώρα που επιθυμεί λιγότερο από τις άλλες τον κυβερνητικό έλεγχο στο διαδίκτυο είναι οι Ηνωμένες Πολιτείες με ποσοστό μόνο 20% των ερωτηθέντων να συμφωνεί. Σχετικά κοντά σε αυτή την απορριπτική για τον κυβερνητικό έλεγχο στάση βρίσκονται οι Έλληνες και οι Γάλλοι συμμετέχοντες σε ποσοστό29%.

Γράφημα 3: Ελευθερία του λόγου και διαδίκτυο



Η ανησυχία παραβίασης που αφορά τις εταιρίες πιθανότατα συνάδει με το ότι οι περισσότεροι χρήστες του διαδικτύου είχαν ήδη εμπειρίες στοχοποιημένων διαφημίσεων και προτάσεων για υπηρεσίες και προϊόντα με δεδομένο το προφίλ των

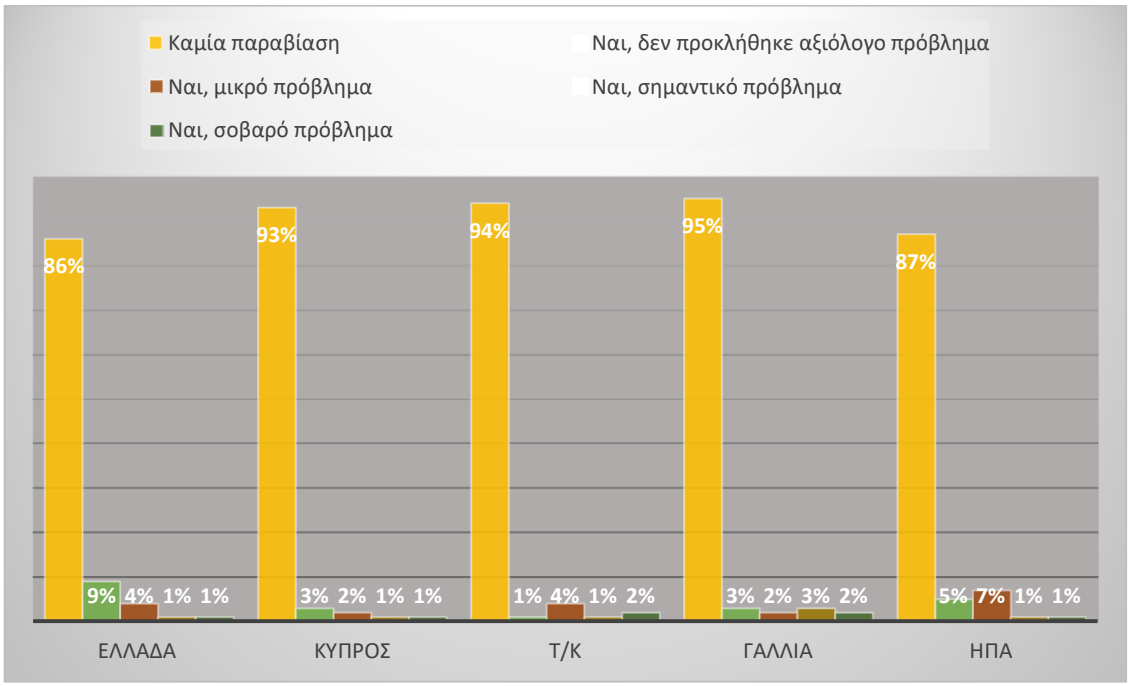
αναζητήσεών τους. Το χαμηλότερο ποσοστό ανησυχίας παραβίασης από εταιρίες δίνει η Τ/Κ Κοινότητα με ποσοστό 31% και το υψηλότερο η Γαλλία με 66% (βλ. Γράφημα 4).

Το πρόβλημα που θέτει η ομολογούμενη πλέον «dataveillance» από εταιρίες είναι ότι οι διαδικασίες λήψης αποφάσεων σχετικά με την ψηφιοποίηση της κοινωνίας εναπόκεινται σε λίγους φορείς το συμφέρον των οποίων αφορά τη μεγιστοποίηση του κέρδους τους (Ngwenyama and Klein, 2018: 14). Γιατί, όπως παρατηρεί ο Smith (2016), δεν αρκεί σε μια εταιρία όπως το Facebook να αποθηκεύει 300 εκατομμύρια φωτογραφίες ή να καταγράφει τα 2,7 δις likes που καταχωρούνται καθημερινά. Μέσα από τη χρήση αλγορίθμων προχωρά στην εξόρυξη αυτών των δεδομένων, την επεξεργασία, τον συνδυασμό τους (Wilken, 2014), μετασχηματίζοντας «καταχρηστικά» την πληροφορία (van der Schyff et al., 2018). Όπως παρατηρεί ο Δουζίνας (2020) «το οπλοστάσιο της βιοπολιτικής του κοινωνικού ελέγχου περιλαμβάνει προβλέψεις, στατιστικούς υπολογισμούς, χρήση αλγορίθμων και άλλα μέτρα που ως μηχανισμοί ελέγχου επιβάλλονται στο στοιχείο της τυχαιότητας που υπάρχει σε κάθε ζώντα πληθυσμό». Χωρίς την εμπλοκή του ανθρώπινου στοιχείου οι αλγοριθμικές προσεγγίσεις εξόρυξης και μετασχηματισμού δεδομένων επιτρέπουν όχι μόνο τον αλγοριθμικό έλεγχο της ζωής (Τζαρέλας, 2020) αλλά και την πρόβλεψή της (Mosco, 2014: 182). Η Cathy o' Neil στο βιβλίο της *Weapons of Math Destruction* (2016: 3), ξεκινώντας την έρευνα της από την οικονομική κρίση του 2008, διαπιστώνει με ποιο τρόπο οι άνθρωποι μπορεί να ωθηθούν στο περιθώριο ή να γίνουν θύματα αλγοριθμικών διακρίσεων (Conrad, 2009· Noble, 2018), καθώς σημαντικές στιγμές στη ζωή τους, όπως το αν θα γίνουν δεκτοί σε ένα πανεπιστήμιο ή αν θα πάρουν δάνειο, κρίνονται μέσα από τα προφίλ που δημιουργούνται από τυχαία διαδικτυακά δεδομένα (Helbing, 2015: 7· O' Neil, 2016: 13· Eubanks, 2018). Οι ανθρώπινες ζωές γίνονται όλο και περισσότερο ορατές, την ίδια στιγμή που, όπως υποστηρίζει ο Lupton (2014), οι ασυμμετρίες εξουσίας γίνονται περισσότερο *αόρατες* και χάρη στην αυξανόμενη παρουσία περίπλοκων συστημάτων δεδομένων, γίνονται *κοινός τόπος*.

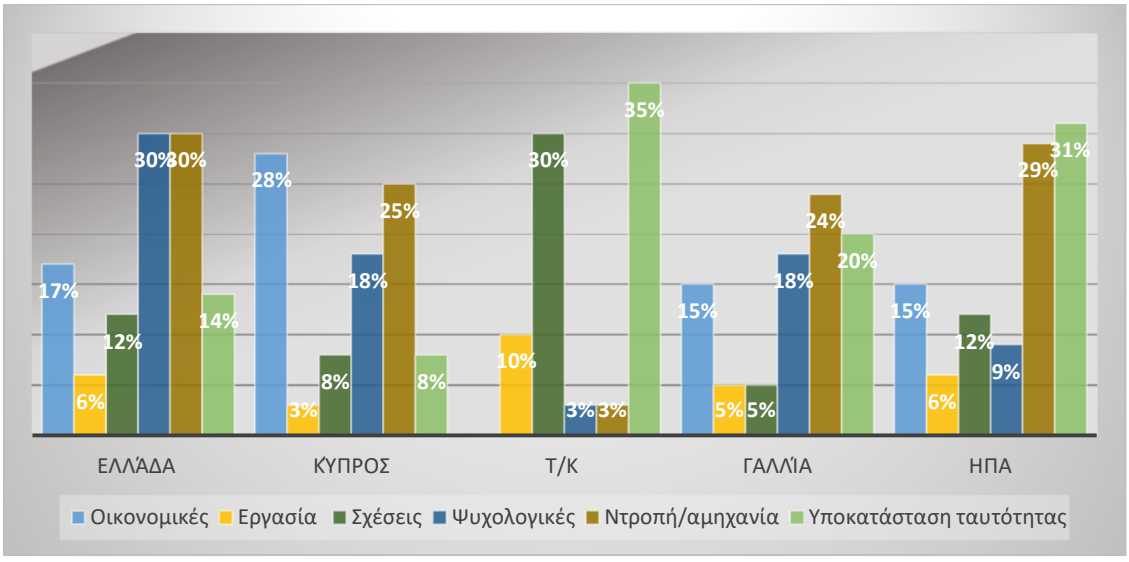
Εκτός από τις εταιρίες και τις κυβερνήσεις, τα δεδομένα των χρηστών εποφθαλμιούν και μεμονωμένα άτομα με αμφιλεγόμενους στόχους κυρίως

παραβατικής φύσης, όπως κλοπή ταυτότητας, υποκλοπή τραπεζικών δεδομένων, εκβιασμό ή παρενόχληση. Και σύμφωνα με τα στοιχεία του WIP από τις τρεις πιθανές πηγές παραβίασης της διαδικτυακής ιδιωτικότητας (κυβερνήσεις, εταιρίες, άτομα), τα *άλλα άτομα* βρίσκονται στην πρώτη θέση σε αρκετές χώρες ως εισβολείς της διαδικτυακής ιδιωτικότητας, με πιο «ανήσυχους» γι' αυτό το θέμα τους Γάλλους σε ποσοστό 66%. Οι Park et al. (2018) παρατήρησαν ότι οι ανησυχίες των χρηστών για την παραβίαση των δεδομένων τους από άλλα άτομα συσχετίζονται με την έλλειψη επίγνωσης ως προς την ίδια τη φύση και την ουσία της ιδιωτικότητας: οι συγκεκριμένες ανησυχίες αφορούν την «κοινωνική ιδιωτικότητα» και το πώς οι ψηφιακές τεχνολογίες την απειλούν σε επίπεδο διαπροσωπικών σχέσεων, έκθεσης και αμηχανίας ενώπιον του κοινωνικού ή επαγγελματικού περίγυρου. Αυτό, ωστόσο, διαφέρει από τη «θεσμική ιδιωτικότητα» και τις παραβιάσεις που μπορεί να γίνουν από εταιρίες ή κυβερνήσεις. Με δυο λόγια, η συλλογή και επεξεργασία δεδομένων από το κοινωνικοοικονομικό υπόβαθρο των χρηστών για κερδοσκοπικούς ή ελεγκτικούς σκοπούς δεν ανησυχεί τόσο τους συμμετέχοντες στην έρευνα του WIP όσο το να δουν, π.χ., ντροπιαστικές φωτογραφίες που μπορεί κάποιος κακόβουλος να αναρτήσει στο Facebook. Ωστόσο, παρά τις εκπεφρασμένες ανησυχίες τους, οι ερωτηθέντες δηλώνουν τουλάχιστον σε ποσοστό 86% ότι δεν υπέστησαν καμία παραβίαση. (Γράφημα 4). Οι αναφορές σοβαρών προβλημάτων από την παραβίαση της ιδιωτικότητας κυμαίνονται από 1% μέχρι 9% στην Ελλάδα, ενώ αφορούν κυρίως ζητήματα κλοπής ταυτότητας (Κύπρος, ποσοστό 35%), ντροπής/αμηχανίας (Ηνωμένες πολιτείες, ποσοστό 29%) και προβλήματα σχέσεων (Τ/Κ κοινότητα, ποσοστό 30%) (Γράφημα 5).

Γράφημα 4: Παραβίαση ιδιωτικότητας στο διαδίκτυο



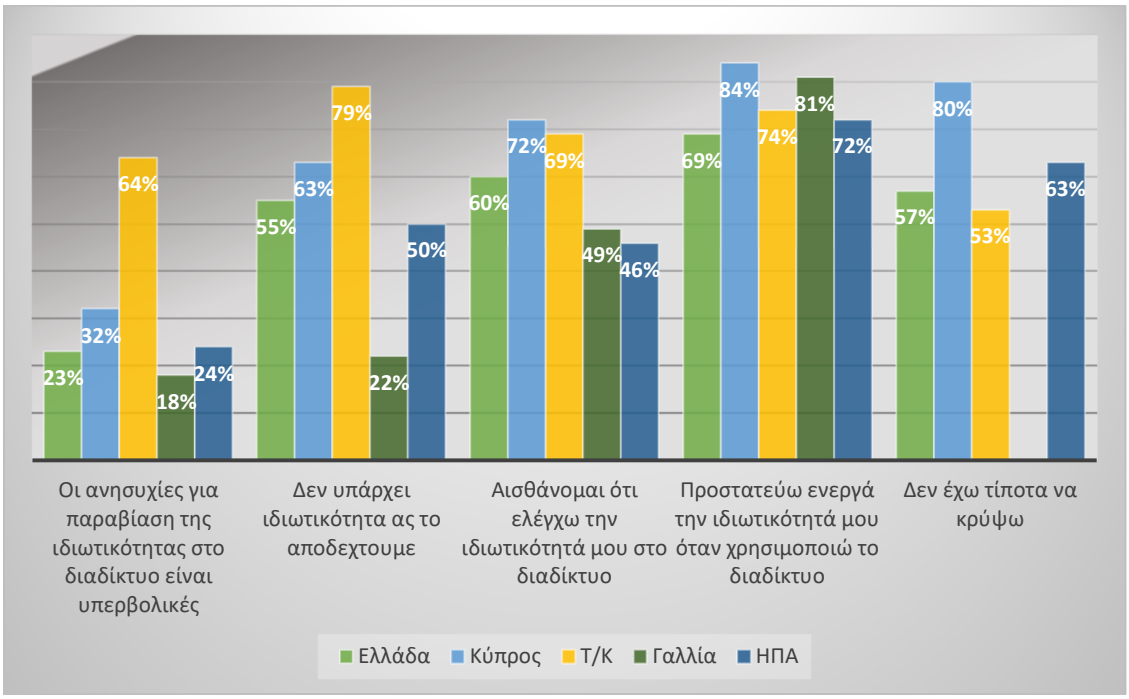
Γράφημα 5: Αποτελέσματα παραβιάσεων ιδιωτικότητας στο διαδίκτυο



Προστασία της διαδικτυακής ιδιωτικότητας: Στάσεις και συμπεριφορές

Η έρευνα του WIP αποκαλύπτει ότι οι στάσεις και οι συμπεριφορές των ατόμων σχετικά με την προστασία της διαδικτυακής ιδιωτικότητας ποικίλλουν από χώρα σε χώρα (Γράφημα 6).

Γράφημα 6: Στάσεις σχετικά με την διαδικτυακή ιδιωτικότητα



Τουλάχιστον το 72% των συμμετεχόντων σε όλες τις χώρες δηλώνουν ότι *προστατεύουν ενεργά* την ιδιωτικότητά τους. Η σύγχυση, όμως, και πιθανότατα η έλλειψη επίγνωσης των ερωτηθέντων φανερώνεται στις μεγάλες διακυμάνσεις που παρουσιάζουν στις άλλες ερωτήσεις της έρευνας. Ενώ το 72% των Αμερικανών απαντά ότι παίρνει μέτρα για να προστατεύσει την ιδιωτικότητά του, τελικά μόνο το 46% νιώθει ότι μπορεί να ελέγξει τις πληροφορίες που παρέχει διαδικτυακά. Και από το 84% των Ελληνοκυπρίων που ομοίως δηλώνει ότι προστατεύει την ιδιωτικότητά του, στην ερώτηση αν νιώθει ότι μπορεί τελικά να την ελέγξει το ποσοστό μειώνεται στο 72%. Την ίδια αβεβαιότητα έχουν και οι Γάλλοι συμμετέχοντες, οι οποίοι δηλώνουν ότι, αν και υιοθετούν στρατηγικές προστασίας της ιδιωτικότητάς τους (ποσοστό 81%), μόνο σε ποσοστό 49% νιώθουν ότι πράγματι μπορεί να την ελέγξουν. Οι Έλληνες συμμετέχοντες

παρουσιάζονται σχεδόν εξίσου σίγουροι για το πόσο ενεργά *προστατεύουν* την ιδιωτικότητά τους (69%) και το πόσο *αισθάνονται* ότι την ελέγχουν (60%). Ωστόσο, έχουν αποδεχτεί ότι «*δεν υπάρχει καμία ιδιωτικότητα*» (ποσοστό 55%). Με αυτήν τη θέση συμφωνούν οι ερωτηθέντες από τις περισσότερες χώρες που συμμετείχαν στην έρευνα του WIP, με τους συμμετέχοντες από την Τ/Κ κοινότητα να το αποδέχονται σε ποσοστό 79%, τους Ελληνοκύπριους σε ποσοστό 63% και τους Αμερικανούς σε ποσοστό 50%. Μόνο στη Γαλλία αυτή η πρόταση δεν βρήκε μεγάλη ανταπόκριση, καθώς οι Γάλλοι συμμετέχοντες αποδέχονται ότι δεν υπάρχει ιδιωτικότητα μόνο σε ποσοστό 22%, είτε γιατί συμφωνούν ότι πράγματι δεν υπάρχει, είτε γιατί δεν θέλουν να αποδεχτούν την απουσία της παρά το ότι μόνο οι μισοί ερωτηθέντες νιώθουν ότι μπορούν να ελέγξουν την ιδιωτική διαδικτυακή ζωή τους.

«*Δεν έχω τίποτα να κρύψω*»

Στην ερώτηση σχετικά με το αν οι ανησυχίες για την παραβίαση της ιδιωτικότητας στο διαδίκτυο είναι υπερβολικές, οι ερωτηθέντες από τις περισσότερες συμμετέχουσες χώρες δεν συμφωνούν με αυτήν τη θέση, με την Ελλάδα (23%) και τη Γαλλία (18%) να δίνουν τα χαμηλότερα ποσοστά συμφωνίας, ενώ ακολουθούν οι ΗΠΑ (24%) και η Κύπρος (32%). Εξαίρεση αποτελούν οι Τουρκοκύπριοι που σε ποσοστό 64% πιστεύουν ότι η συζήτηση για τη διαδικτυακή ιδιωτικότητα έχει μεγαλοποιηθεί παρά το ότι εκείνοι που δηλώνουν ότι δεν έχουν *τίποτα να κρύψουν* είναι λιγότεροι (53%). Οι πιο «αθώοι» από τους ερωτηθέντες είναι οι Ελληνοκύπριοι που δηλώνουν σε ποσοστό 80% ότι δεν έχουν τίποτα να κρύψουν, ενώ την ίδια άνετη στάση έχει και το 63% των Αμερικανών. Από τη θέση «*δεν έχω τίποτα να κρύψω*» οι Γάλλοι συμμετέχοντες σημείωσαν μια ενδιαφέρουσα αποστασιοποίηση, καθώς δεν έδωσαν καμία απάντηση γι' αυτό το θέμα, πράγμα που κατά πάσα πιθανότητα υπονοεί όχι τόσο ότι έχουν κάτι να κρύψουν αλλά ότι δεν θεωρούν τη δήλωση αυτή σχετική με το πρόβλημα.

Η υιοθέτηση της στάσης «*δεν έχω τίποτα να κρύψω*» φανερώνει μια σχεδόν σιωπηλή παραδοχή ότι ο ψηφιακός εαυτός των χρηστών είναι πιθανότατα αντικείμενο παρακολούθησης, αλλά αφού δεν έχουν τίποτα να κρύψουν τότε και η επιτήρησή τους

δεν θα είναι βλαπτική. Οι άνθρωποι υποθέτουν ότι οι πληροφορίες τους ή θα γίνουν αντικείμενο στοχοποίησης από εταιρίες για να τους αποστέλλονται διαφημίσεις, τις οποίες απλώς θα αγνοήσουν χωρίς καμία επίπτωση στην ιδιωτικότητά τους. Επίσης, μπορεί να εκτεθούν σε λίγους αξιωματούχους της ασφάλειας του κράτους και καθώς δεν θεωρούν εαυτούς ενόχους για οτιδήποτε δεν ενοχλούνται αν το αντάλλαγμα είναι η συμμετοχή σε μια υπηρεσία ή μια διαδικτυακή δραστηριότητα (Solove, 2007). Με άλλα λόγια, το «*δεν έχω τίποτα να κρύψω*» προκύπτει από τη συγκριτική αξία της ιδιωτικότητας σε σχέση με την ασφάλεια. Το 2005 ο Posner έγραφε: «*η συλλογή και επεξεργασία δεδομένων από μηχανές δεν μπορεί να θεωρηθεί ότι παραβιάζει την ιδιωτικότητα. Εξάλλου ο υπολογιστής δεν είναι ένα νοήμον ον. Εξαιτίας του τεράστιου όγκου τους, τα δεδομένα «κοσκινίζονται» από υπολογιστές που αναζητούν μόνο ονόματα, τηλέφωνα ή διευθύνσεις που μπορεί να έχουν κάποια αξία για την ασφάλεια και δεν επιτρέπουν σε κανέναν άνθρωπο να έχει πρόσβαση σε αυτά*».[20] Ο Bernal (2018: 71-77), ωστόσο, καταρρίπτει αυτόν το «μύθο της ουδετερότητας» καθώς η αθωότητα της «*τεχνικής, αυτόματης και παθητικής*» διεργασίας που επιτελεί ένα δίκτυο ή ένας αλγόριθμος παύει να ισχύει από τη στιγμή που η επεξεργασία της παραγόμενης πληροφορίας οδηγεί σε αποφάσεις και σκοπούς που τουλάχιστον ο αρχικός ιδιοκτήτης της πληροφορίας δεν ελέγχει.

Η διάδοση και επικράτηση της στάσης «*δεν έχω τίποτα να κρύψω*» ενέχει τρία προβλήματα. Πρώτον, προϋποθέτει ότι η ιδιωτικότητα αφορά το να μπορεί κανείς να κρύψει κάτι κακό (Posner, 1978· Schneier, 2006· Bernal, 2018). Δεύτερον, συρρικνώνει την προβληματική για την παρακολούθηση και την εκμετάλλευση των προσωπικών δεδομένων στο άσχετο θέμα του αν έχει κάποιος να κρύψει κάτι και την εκτρέπει από τα πραγματικά ερωτήματα που είναι :

- Πόσο υπόλογοι είναι οι παρατηρητές έναντι των παρατηρούμενων;
- Οι συλλέκτες δεδομένων έχουν τη συναίνεση εκείνων από τους οποίους παίρνουν τα δεδομένα;

[20] Posner, R. (2005). «Our domestic intelligence crisis». *Washington Post*, 21 Δεκεμβρίου 2005, https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/ (πρόσβαση Ιανουάριος 2020).

- Ποια σχέση υπάρχει ανάμεσα στις εταιρίες εξόρυξης δεδομένων, τις πλατφόρμες κοινωνικής δικτύωσης και τις υπηρεσίες παρακολούθησης;
- Έχει υπάρξει δημόσιος διάλογος σχετικά με την εφαρμογή τρόπων παρακολούθησης και ελέγχου των δεδομένων των ατόμων;
- Ποιος ελέγχει τους συλλέκτες δεδομένων και ποιοι είναι οι ιδιοκτήτες όλων των δεδομένων που αναλύονται (Richards and King, 2014);

Το τρίτο πρόβλημα αφορά τη λανθασμένη υπόθεση των ανθρώπων που πιστεύουν ότι, επειδή δεν «έχουν τίποτα να κρύψουν», θα είναι μόνιμα «αθώοι», παραμελώντας την εκδοχή στην οποία η ψηφιακή τους ύπαρξη μπορεί να γίνει αντικείμενο ενοχοποίησης στα χέρια οποιουδήποτε έχει κάποια σκοπιμότητα. Η Shephard (2016) παρατηρεί ότι όταν «*ένα άτομο χάνει τον έλεγχο των πληροφοριών του, ομοίως χάνει και τον έλεγχο των δυνητικών μεταμορφώσεων αυτών των πληροφοριών*».[21] Σε αυτό συμφωνεί και η Ακριβοπούλου (2011), η οποία επισημαίνει ότι από νομικής σκοπιάς τον μεγαλύτερο κίνδυνο εγκυμονεί η δυνατότητα επεξεργασίας, σύγκρισης και ταυτοποίησης των πληροφοριών που καθίστανται ευκολότερες από τη σύγχρονη πληροφοριακή τεχνολογία, θέτοντας εν κινδύνω πτυχές της ταυτότητας, της ατομικότητας και της διαφορετικότητάς των ατόμων (Poullet and Dinant, 2006). Ακριβώς αυτή η επεξεργασία που υπάρχει ως λειτουργική οντότητα (Haggerty and Erickson, 2000) και συντελείται μέσα από τη σύγκλιση άλλοτε διακριτών συστημάτων παρακολούθησης σε μια «συγκέντρωση επιτήρησης» (surveillant assemblage), παραπέμπει στις «assemblages» (συγκεντρώσεις) των Deleuze και Guattari (1987), «πολλαπλότητες ετερογενών αντικειμένων» που αποσπούν τα ανθρώπινα σώματα από τα γήινα για να τα διαχωρίσουν σε μια σειρά διακριτών ροών και να τα επανασυναρμολογήσουν σε διαφορετικές τοποθεσίες ως διακριτούς «δεδομενικούς» σωσίες.

Αν η κύρια υπόθεση κάτω από τον ισχυρισμό «δεν έχω τίποτα να κρύψω» είναι «*αν δεν έχεις τίποτα να κρύψεις δεν έχεις και τίποτα να φοβάσαι*», υπονοεί ότι οι καλοί άνθρωποι δεν έχουν ανάγκη την ιδιωτικότητα, εφόσον δεν έχουν τίποτα να κρύψουν,

[21] Shephard, N. (2016). «Big data and sexual surveillance», *APC Issue Papers*, http://www.apc.org/sites/default/files/BigDataSexualSurveillance_0.pdf (πρόσβαση Φεβρουάριος 2020).

και οι κακοί άνθρωπο δεν την αξίζουν, εφόσον προφανώς αυτό που θέλουν να κρύψουν είναι κάτι επιβλαβές. «*Το άτομο έχει ανάγκη την ιδιωτικότητα από αυτούς που μπορούν να του ασκήσουν εξουσία*» σημειώνει ο Bernal (2018: 145), τονίζοντας ότι ένας από τους πιο διαδομένους μύθους είναι ότι η ιδιωτικότητα αποτελεί «ατομικό» και όχι κοινωνικό δικαίωμα, διαφορετικό από το δικαίωμα στην ελευθερία του λόγου ή το δικαίωμα του συναθροίζεσθαι και θα πρέπει να υποχωρεί προκειμένου να εξυπηρετούνται συλλογικότερα δικαιώματα όπως η ασφάλεια. Ο Schneier (2006) διευκρινίζει ότι η ιδιωτικότητα είναι στην πραγματικότητα προϋπόθεση της ασφάλειας, καθώς προστατεύει τα άτομα ακριβώς από τους κινδύνους της παρακολούθησης και του ελέγχου, διαφυλάσσει την ελευθερία του λόγου και την ελεύθερη συναναστροφή και αποτρέπει από την κατάχρηση εξουσίας, ενώ, σύμφωνα με τον Solove (2006), αυτός ο εύκολος υποβιβασμός της ιδιωτικότητας σε εγωιστικό πρόταγμα υπονομεύει το θεμελιώδη ρόλο των ατομικών δικαιωμάτων εν σχέσει προς τη συνολική ευημερία των κοινωνιών πυροδοτώντας μια ένταση ανάμεσα στο κοινωνικό και το ιδιωτικό.[22]

«Αποκαλύπτεται» μια κοινωνία όπου η προστασία σταδιακά περιορίζεται, αποστερείται ζώνες ιδιωτικότητας μέσα στις οποίες όλοι έχουν δικαίωμα να αποσύρονται, απαρατήρητοι και απομονωμένοι. Κι αυτό, όπως υποστηρίζουν ο Cohen (2013) και ο Berlin (2002), οδηγεί σε ανελεύθερες, δυσλειτουργικές κοινωνίες ίσως όχι τόσο «οργουελικές» (Πετρίδης, 2020) όσο «καφκικές» (Solove, 2006), όπου οι άνθρωποι δεν παρακολουθούνται απλά, αλλά μετασχηματίζονται σε δεδομενοποιμένους «άλλους» με χαρακτηριστικά και ιδιότητες που και οι ίδιοι δεν αναγνωρίζουν. Τέλος, αν η ψηφιακή ιδιωτικότητα γίνεται αντιληπτή μόνο ως ατομική επιλογή, η συζήτηση παραλείπει όλα εκείνα τα επίπεδα που υπερβαίνουν την ικανότητα του ατόμου να πάρει συνειδητές αποφάσεις σχετικά με τον πληροφοριακό εαυτό του και να ελέγξει από μονό του τον «δεδομενικό σωσία», τον οποίο δημιουργούν αόρατες, ανεξέλεγκτες και πολύ ισχυρότερες δομές εξουσίας (Mai, 2016).

[22] Πρβλ. το αφιερωματικό τεύχος #26 της επιθεώρησης *Επιστήμη και Κοινωνία* για τη διάκριση δημόσιου και ιδιωτικού (2010-2011) σε επιμέλεια Ν. Δεμερτζή και Ι. Παπαδόπουλου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνόγλωσση

Ακριβοπούλου, Χ. (2011). «Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή». *Θεωρία και Πράξη Διοικητικού Δικαίου*, 7: 679-691. https://www.constitutionalism.gr/2213-to-dikaiwma-stin-prostasia-twn-proswpikwn-dedomenw/ (πρόσβαση Φεβρουάριος 2020).

Ανθόπουλος, Χ. (2007). «Το δικαίωμα στη δημόσια ανωνυμία. Προστασία προσωπικών δεδομένων, ελευθερία του συνέρχεσθαι και ηλεκτρονικός έλεγχος των δημόσιων υπαίθριων συναθροίσεων». ΕΔΔ, 721: 719-728.

Δουζίνας, Κ. (2020). «Η βιοπολιτική της πανδημίας**».** Στο Π. Καπόλα, Γ. Κουζέλης και Ο. Κωνσταντάς (επιμ.), *Αποτυπώσεις σε στιγμές κινδύνου*. Εταιρεία Μελέτης των Επιστημών του Ανθρώπου. Αθήνα: Εκδ. Νήσος.

Επιστήμη και Κοινωνία (2010-2011). Διάκριση δημόσιου και ιδιωτικού. τχ. #26 https://ejournals.epublishing.ekt.gr/index.php/sas/issue/view/69/showToc

Κιουπκιολής, Α. (2020). «Ιοί της βιοεξουσίας και αντι-ηγεμονικές εναλλακτικές μιας δημοκρατίας των Κοινών». Στο Π. Καπόλα, Γ. Κουζέλης και Ο. Κωνσταντάς (επιμ.), *Αποτυπώσεις σε στιγμές κινδύνου*. Εταιρεία Μελέτης των Επιστημών του Ανθρώπου. Αθήνα: Εκδ. Νήσος.

Πετρίδης, Π. (2020). «Πορτρέτα της Κίνας, δυτικές δημοκρατίες και επιτήρηση της πληροφορίας. Στο Π. Καπόλα, Γ. Κουζέλης και Ο. Κωνσταντάς (επιμ.), *Αποτυπώσεις σε στιγμές κινδύνου*. Εταιρεία Μελέτης των Επιστημών του Ανθρώπου. Αθήνα: Εκδ. Νήσος.

Σπουρδαλάκης, Μ. (2020). «Η μετά κορωνοϊού - Δημοκρατία ή θα είναι σοσιαλιστική ή δεν θα υπάρχει». Στο Π. Καπόλα, Γ. Κουζέλης και Ο. Κωνσταντάς (επιμ.), *Αποτυπώσεις σε στιγμές κινδύνου*. Εταιρεία Μελέτης των Επιστημών του Ανθρώπου. Αθήνα: Εκδ. Νήσος.

Τζαρέλας, Δ. (2020). «Η επιστροφή του κράτους εν μέσω πανδημίας». Στο Π. Καπόλα, Γ. Κουζέλης και Ο. Κωνσταντάς (επιμ.), *Αποτυπώσεις σε στιγμές κινδύνου*. Εταιρεία Μελέτης των Επιστημών του Ανθρώπου. Αθήνα: Εκδ. Νήσος.

Ξενόγλωσση

Acquisti, A. and Grossklags, J. (2007). «What can behavioral economics teach us about privacy. Στο Acquisti A., Gritzalis S., Lambrinoudakis C., di Vimercati S. (eds), *Digital privacy: theory, technology, and practices* (σελ. 363-77). Auerbach Publications.

Acquisti, A., Taylor, C. and Wagman, L. (2016). «The economics of privacy». *Journal of Economic Literature,* 54 (2): 442-92.

Amoore, L., and De Goede, M. (2005). «Governance, risk and dataveillance in the war on terror». *Crime, Law and Social Change,* 43: 149-173.

Ariely, D. and Berns, G.S. (2010). «Neuromarketing: the hope and hype of neuroimaging in business». *Nature Reviews*. *Neuroscience*, 11 (4): 284-292.

Berlin, I. (2002). «Two concepts of liberty». Στο I. Berlin, *Liberty* (σελ. 118-172). Oxford: Oxford University Press (1η έκδοση 1958).

Bernal, P. (2018). *The Internet, Warts and All. Free Speech, Privacy and Truth*. Cambridge University Press.

Boyd, d. and Crawford, K. (2012). «Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon». *Information, Communication & Society*, 15 (5): 662-79.

Brown, B. (2001). «Studying the internet experience». *Hp Laboratories Technical Report HPL* 49. https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf (πρόσβαση Φεβρουάριος 2020).

Bustos de, C.M. and Izquierdo-Castillo, L. (2019). «Who will control the media? The impact of GAFAM on the media industries in the digital economy*». Revista Latina de Comunicación Social*, 74: 803-821.

Cadwalladr, C. and Graham-Harrison, E. (2018). «Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach». *The Guardian*, 17 Μαρτίου 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (πρόσβαση Φεβρουάριος 2020).

Cammaerts, B. (2008). «Critiques on the participatory potentials of Web 2.0». *Communication, Culture and Critique,* 1 (4): 358-77.

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira, R. (2013). «Your browsing behavior for a Big Mac: economics of personal information online». Στο *Proceedings of the 22nd international conference on World Wide Web (*σελ. 189-200). Rio de Janeiro, Brazil.

Clarke, R. (1994). «Dataveillance by governments: The technique of computer matching». *Information Technology & People,* 7 (2): 46-85.

Clarke, R. (1988). «Information technology and dataveillance». *Communication. ACM 31* (5): 498-512, http://www.rogerclarke.com/DV/CACM88.html [πρόσβαση Φεβρουάριος 2020].

Cohen, J.E. (2013). «What privacy is for». *Harvard Law Review*, 126: 1904–1933.

Conrad, K. (2009). «Surveillance, gender, and the virtual body in the information age». *Surveillance & Society* 6(4): 380–387

Cooke, T. N. (2020). «Metadata, Jailbreaking, and the Cybernetic Governmentality of OS: Or, the need to distinguish digital privacy from digital privacy». *Surveillance & Society,* 18(1): 90-103. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index [πρόσβαση Απρίλιος 2020].

Crouch, C. (2004). *Post Democracy*. Polity.

Curran, D. (2018). «Are you ready? Here is all the data Facebook and Google have on you». *The Guardian*, 30 Μαρτίου 2018, https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [πρόσβαση Μάρτιος 2020]

Davenport, T. H. and Beck, J. C. (2013). *The Attention Economy: Understanding the New Currency of Business*. Cambridge, MA: Harvard Business Press.

Debatin, B., Lovejoy, J.P, Horn, A.K. and Hughes, B.N (2009). «Facebook and online privacy: attitudes, behaviors, and unintended consequences». *Journal of Computer-Mediated Communication,* 15 (1): 83-108.

Deleuze, G. and Guattari, F. (1987). *A Thousand Plateaus*. Minneapolis: University of Minnesota Press.

Demertzis, N. and Tsekeris, C. (2018). «Multifaceted European Public Sphere - Socio-Cultural Dynamics». Στο B. Cammaerts, N. Anstead and R. Stupart, *Media@LSE Working Paper Series.* Media and Communications, Media@LSE, London School of Economics and Political Science

Derikx, S., De Reuver, M., Kroesen, M., and Bouwman, H. (2015). «Buying-off privacy concerns for mobility services in the internet-of-things era: a discrete choice experiment on the case of mobile insurance». Στο Proceedings of the 28th Bled eConference, http://aisel.aisnet.org/bled2015/28 (πρόσβαση Φεβρουάριος 2020).

Dinev, T. and Hart P. (2008). «An extended privacy calculus model for e-commerce transactions». *Information Systems Research,* 17(1): 61-80.

Egelman, S., Felt, A.P. and Wagner, D. (2012). «Choice architecture and smartphone privacy: there's a price for that». Στο *Proceedings of the 11th annual workshop on the economics of information security*. Berlin, Germany.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. (2011). «Negotiating privacy concerns and social capital needs in a social media environment». *Privacy online*. Berlin Heidelberg: Springer, 19-32.

Eubanks, V. (2018). *Automating Inequality How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Publishing Group.

Finucane, M.L, Alhakami, A., Slovic, P. and Johnson, S.M. (2000). «The Affect Heuristic in Judgment of Risks and Benefits». *Journal of Behavioral Decision Making,* 13 (1): 1-17.

Flick, C. (2016). «Informed consent and the Facebook emotional manipulation study». *Research Ethics,* 12 (1): 14–28.

Foa, R. S. and Mounk, Y. (2017). «The Signs of Deconsolidation». *Journal of Democracy,* 28 (1): 5-15.

Fuchs, C. (2012). «The political economy of privacy on Facebook». *Television & New Media,* 13 (2): 139-159.

Fuchs, C. (2014). «Social Media and the public sphere». tripleC: Communication, Capitalism & Critique, *Journal for a Global Sustainable Information Society,* 12 (1): 57-101.

Ganesh, M. I., Deutch, J. and Schulte, J. (2016). «Privacy, anonymity, visibility: dilemmas in tech use by marginalised communities». Brighton: IDS, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/12110/TacticalTech_Online_FINAL3.pdf [πρόσβαση Φεβρουάριος 2020].

Gross, J.A. (2020). «Government okays mass surveillance of Israelis' phones to curb coronavirus». *Times of Israel*, 15 Μαρτίου 2020, https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/ [πρόσβαση Απρίλιος 2020]

Hache, A. and Jansen, F. (2018). «Privacy, surveillance and data tracking: why does it matter for human rights defenders? ». *Free media: issues, challenges and proposals*, Ιούλιος 2018, https://www.ritimo.org/Privacy-Surveillance-and-Data-Tracking-Why-Does-it-Matter-for-Human-Rights#nb20 [πρόσβαση Φεβρουάριος 2020].

Haggerty, K.D. and Ericson, R.V. (2000). «The surveillant assemblage». *British Journal of Sociology,* 51 (4): 605-622.

Hayden, M. (2014). General Michael Hayden Beyond Snowden: An NSA Reality Check. *World Affairs,* 176 (5): 13-23.

Helbing, D. (2015). *Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society*. Springer.

Heller, C. (2011). *Post-Privacy: Prima leben ohne Privatsphäre*. München: Beck.

Hindman, M. (2009). *The myth of digital democracy*. Princeton, NJ: Princeton University Press.

Hsu, T. and Celia Kang, C. (2018). «Demands grow for Facebook to explain its privacy policies». *New York Times*, 26 Μαρτίου 2018, https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge-analytica.html [πρόσβαση Μάρτιος 2020].

Jaworski, J. (2011). «Identifying web users on the base of their browsing patterns». *International Journal of Computational Intelligence Systems,* 4 (5): 1062-106.

Keyes, R. (2004). *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*, St. Martin's Press.

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

Kramer, A.D.I., Guillory, J. and Hancock, J. (2014). «Experimental evidence of massive scale emotional contagion through social networks». *Proceedings of the National Academy of Sciences,* 111 (24): 8788–90.

Laudon, K. (1997). «Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information». New York University Stern School of Business, Working Paper IS-97-4.

Lee, H., Park, H., Kim, J. (2013). «Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk». *International Journal of Human-Computer Studies* 71 (9): 862-77.

Lupton, D. (2014). *Digital Sociology*. London: Routledge.

Lyon, D. (2001a). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (2001b). «Facing the Future: Seeking ethics for everyday surveillance». *Ethics and Information Technology*, 3 (3): 171-180.

Lyon, D. (2014). «Surveillance, Snowden, and Big Data: Capacities, consequences, critique». *Big Data & Society*, 1-13.

Madden, M. (2014). «Public perceptions of privacy and security in the post-snowden era». Pew Research Center. https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ (πρόσβαση Φεβρουάριος 2020).

Mai, J. E. (2016). «Big data privacy: The datafication of personal information». *The Information Society,* 32 (3): 192-199

Manovich, L. (2011). «Trending: The promises and the challenges of big social data». Στο M. K. Gold (ed.), *Debates in the Digital Humanities* (σελ. 1-17). Minneapolis: University of Minnesota Press.

Mayer-Schonberger, V. and Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. New York, NY: Houghton Mifflin Harcourt.

McIntyre, L. (2018). *Post Truth*. The MIT Press Essential Knowledge series.

Meinert, D. B., Peterson, D. K., Criswell, J. R., and Crossland, M. D. (2006). «Privacy policy statements and consumer willingness to provide personal information». *Journal of Electronic Commerce in Organizations,* 4(1): 1-17.

Mosco, V. (2009). *The Political Economy of Communication*. London: Sage.

Mosco, V. (2014). *To the Cloud: Big Data in a Turbulent World*. Boulder, CA: Paradigm Books.

Ngwenyama, O. and Klein, S. (2018). «Phronesis, argumentation and puzzle solving in IS Research: Illustrating an approach to Phronetic IS Research Practice». *European Journal of Information Systems,* 27(3): 347-366

Nield, D. (2019). «All the ways Google tracks you—and how to stop it». *The Wired*, 27 Μαΐου 2019. https://www.wired.com/story/google-tracks-you-privacy/ [πρόσβαση Απρίλιος 2020].

Noble, S.U. (2018). *Algorithms of Oppression How Search Engines Reinforce Racism*. NYU Press.

Norberg, P.A, Horne, D.R and Horne, D.A. (2007). «The privacy paradox: personal information disclosure intentions versus behaviors*». Journal of Consumer Affaires,* 41 (1) : 100-126.

Norval, A., and Prasopoulou, E. (2017). «"Public Faces? A critical exploration of the diffusion of face recognition technologies in online social networks». *New Media & Society,* 19(4): 637-654.

o' Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

Oetzel, M.C and Gonja, T. (2011). «The online privacy paradox: a social representations perspective». Proceedings of CHI'11 extended abstracts on human factors in computing systems, 7–12 Μαΐου, Vancouver, Canada.

Park, Y.J., Chung, J.E and Shin, D.H. (2018). «The structuration of digital ecosystem, privacy, and big data intelligence». *American Behavioral Scientist*, SAGE Publications, 1-19.

Posner, R. (1978). «The right of privacy». *Georgia Law Review,* 12: 393-428.

Posner, R. (2005). «Our domestic intelligence crisis». *Washington Post*, 21 Δεκεμβρίου 2005, https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/ (πρόσβαση Ιανουάριος 2020).

Poullet, Y. and Dinant, J.M. (2006). «The internet and private life in Europe». Στο Kenyon, A. T. and Richardson, M., *New dimensions in privacy law: international and comparative prospectives* (σελ. 60-90). Cambridge University Press.

Rainie L, and Smith, A. (2012). «Social networking sites and politics», 12 Μαρτίου 2012. https://www.pewresearch.org/internet/2012/03/12/social-networking-sites-and-politics [πρόσβαση Απρίλιος 2020].

Reportes without Borders (2014). *Enemies of the Internet 2014 Report*, https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf [πρόσβαση Μάρτιος 2020].

Richards, B. (2007). *Emotional Governance: Politics, Media and Terror*. Basingstoke: Palgrave Macmillan.

Richards, N. M. and King, J. H. (2014). «What's up with big data ethics?», *Forbes*, 28 Μαρτίου 2014, https://www.forbes.com/sites/oreillymedia/2014/03/28/whats-up-with-big-data-ethics/#75f4830d3591 [πρόσβαση Φεβρουάριος 2020]

Rule, J. B., McAdam, D., Stearns, L. and Uglow, D. (1983). «Documentary identification and mass surveillance in the United States». *Social Problems,* 31(2): 222-234.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.

Schneier, B. (2006). «The Eternal Value of Privacy». *The Wired*, May 18 Μαΐου 2006, http://www.wired.com/news/columns/1,70886-0.html (πρόσβαση Φεβρουάριος 2020).

Schuster, S., Van den Berg, M., Larrucea, X., Slewe, T. and Ide-Kostic, P. (2017). «Mass surveillance and technological policy options: Improving security of private communications». *Computer Standards & Interfaces,* 50: 76-82.

Sennett, R. (1993). *The Fall of Public Man*. London: Faber and Faber.

Shephard, N. (2016). «Big data and sexual surveillance». APC Issue Papers, http://www.apc.org/sites/default/files/BigDataSexualSurveillance_0.pdf (πρόσβαση Φεβρουάριος 2020)

Shorey, S. and Howard, P. N. (2016). Automation, big data, and politics: A research review. *International Journal of Communication,* 10 (2016): 5032-55.

Singer, N. and Sang-Hun, C. (2020). «As Coronavirus surveillance escalates, personal privacy plummets». *The New York Times*, 23 Μαρτίου 2020, https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html (πρόσβαση Απρίλιος 2020)

Smith, D. (2020). «Google keeps a frightening amount of data on you. Here's how to find and delete it». *Cnet*. 7 Μαρτίου 2020. https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/ (πρόσβαση Απρίλιος 2020)

Smith, G. J. (2016). «Surveillance, Data and Embodiment: On the Work of Being Watched». *Body & Society,* 22 (2): 108-139.

Solove, D. J. (2007). «"I've got nothing to hide" and other misunderstandings of privacy». *San Diego Law Review,* 44: 745.

Solove, D. (2006). «A taxonomy of privacy», *University Pennsylvania Law Review*, 154 (3): 477-560.

Spiekermann, S., Grossklags, J., Berendt, B. (2001). «E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior". *Proceedings of the 3rd ACM conference on electronic commerce*. Florida, USA, 38-47.

Srnicek, N. (2017). *Platform Capitalism*. Polity Press.

Steidl, P. (2012). *Neurobranding*. CreateSpace Independent Publishing Platform.

Stein, A. (2020). «How to restore data privacy after the coronavirus pandemic». *World Economic Forum*, 31 Μαρτίου 2020. https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic [πρόσβαση Απρίλιος 2020]

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. and Lampe, C. (2012). «Privacy in Interaction: exploring disclosure and social capital inFacebook». *Proceedings of the 6th international conference on weblogs and social media* (ICWSM 2012), Dublin, Ireland.

Taddicken, M. (2014). «The ''privacy paradox'' in the social web: the impact of privacy concerns, individual characteristics and the perceived social relevance on different forms of self-disclosure». *Journal of Computer-Mediated Communication,* 19 (2): 248–73.

TRUSTe (2014). US Consumer Confidence Privacy Report Consumer Opinion and Business Impact. Διαθέσιμο http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf, πρόσβαση Φεβρουάριος 2020

Tzogopoulos, G.N. (2020). «The Internet in the coronavirus era». *The Begin Sadat Center for Strategic Studies*, 30 Μαρτίου 2020, https://besacenter.org/perspectives-papers/coronavirus-internet/ [πρόσβαση Απρίλιος 2020]

van der Schyff, K., Krauss, K.E.M. and Kroeze, J.H. (2018). «Facebook and dataveillance: Demonstrating a multimodal discourse analysis». *Twenty-fourth Americas Conference on Information Systems,* New Orleans.

Van Dijck, J. (2014). «Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology». *Surveillance & Society,* 12 (2): 197.

Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*, Oxford: Oxford University Press.

Watson, C. (2018). «The key moments from Mark Zuckerberg's testimony to Congress». *The Guardian*, 11 Απρίλιου 2018, https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments πρόσβαση Φεβρουάριος 2020

Wilken, R. (2014). «Places Nearby: Facebook as a location-based social media platform». *New Media & Society,* 16 (7): 1087-1103.

Wilson, D. and Valacich, J.S. (2012). «Unpacking the privacy paradox: irrational decision-making within the privacy calculus. In: *Proceedings of the 33rd international conference on information systems* (ICIS2012), 16-19 Δεκεμβρίου, Florida, USA.

Wouters, C. (2007). *Informalization: Manners and emotions since 1890*. London: Sage.

Zafeiropoulou, A.M, Millard, D.E, Webber, C. and O'Hara, K. (2013). «Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? ». Proceedings of the 5th annual ACMWeb Science Conference, May 2–4, Paris, France.

Zurawicki, L. (2010). *Neuromarketing: Exploring the brain.*