ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΣΥΓΧΡΟΝΕΣ ΔΗΜΟΣΙΟΓΡΑΦΙΚΕΣ ΣΠΟΥΔΕΣ

Μεταπτυχιακή Διπλωματική Εργασία

Χρήση Πλατφορμών Ασφαλούς Επικοινωνίας από Δημοσιογράφους

Μαρία – Αλεξάνδρα Σεβαστάκη

Επιβλέπων καθηγητής: Ανδρέας Βέγλης

Αθήνα, Ιούλιος 2024

Χρήση Πλατφορμών Ασφαλούς Επικοινωνίας από Δημοσιογράφους

Μαρία – Αλεξάνδρα Σεβαστάκη

Επιτροπή Επίβλεψης Μεταπτυχιακής Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής:	Συν-Επιβλέπουσα Καθηγήτρια:
Ανδρέας Βέγλης	Γεωργία Γιολτζίδου
Καθηγητής, ΑΠΘ	Μέλος ΣΕΠ, ΕΑΠ

Αθήνα, Ιούλιος 2024

Ευχαριστώ πολύ τον καθηγητή Ανδρέα Βέγλη, επιβλέποντα της μεταπτυχιακής μου εργασίας για την εμπιστοσύνη που μου έδειξε, δίνοντάς μου την ευκαιρία να συνεργασθώ μαζί του καθώς και για την πολύτιμη βοήθεια και την καθοδήγησή του.

Ευχαριστώ την οικογένειά μου και ιδιαίτερα τον σύζυγό μου Θεόδωρο Αλεξάκη για την αμέριστη στήριξή τους σε όλη τη διάρκεια των σπουδών μου.

Περίληψη

Ο τομέας της Δημοσιογραφίας αποτελεί τον ακρογωνιαίο λίθο μιας δημοκρατικής κοινωνίας και διακρίνεται από το βάθος και τη δέσμευσή της στην αποκάλυψη της αλήθειας, ειδικά σε περιπτώσεις όπου στερείται η διαφάνεια, συμβάλλοντας έτσι στην έγκυρη ενημέρωση του πολίτη.

Στην ψηφιακή εποχή, η ασφάλεια της επικοινωνίας είναι πρωταρχικής σημασίας, ιδιαίτερα στον τομέα της Δημοσιογραφίας όπου η προστασία των πηγών και των ευαίσθητων πληροφοριών είναι ζωτικής σημασίας. Η παρούσα μεταπτυχιακή διπλωματική εργασία εξετάζει τη χρήση ασφαλών πλατφορμών επικοινωνίας από δημοσιογράφους, εστιάζοντας στο πώς αυτά τα εργαλεία επηρεάζουν τις εργασιακές πρακτικές τους και την ασφάλεια των επικοινωνιών τους. Η εργασία διερευνά τον βαθμό στον οποίο οι δημοσιογράφοι υιοθετούν ασφαλείς πλατφόρμες, τις προκλήσεις που αντιμετωπίζουν και την αποτελεσματικότητα αυτών των τεχνολογιών στη διαφύλαξη των επικοινωνιών τους.

Για τη συλλογή εμπειρικών δεδομένων, διανεμήθηκε σε δημοσιογραφικές ενώσεις ένα ερωτηματολόγιο που περιελάμβανε 33 ερωτήσεις. Το ερωτηματολόγιο διερεύνησε διάφορες πτυχές της ασφαλούς επικοινωνίας, συμπεριλαμβανομένων των πλατφορμών που χρησιμοποιούνται, τη συχνότητα χρήσης, την αξιοπιστία και ασφάλεια και τυχόν εμπόδια στην υιοθέτηση. Επιπλέον, εξέτασε την επίγνωση των πιθανών απειλών από τους δημοσιογράφους και τα μέτρα που λαμβάνουν για τον μετριασμό αυτών.

Τα συμπεράσματα που εξήχθησαν αποκαλύπτουν τις ανησυχίες των δημοσιογράφων σχετικά με τους κινδύνους και τις προκλήσεις της ψηφιακής εποχής. Επιπλέον, υπάρχει ευρεία επίγνωση της σημασίας των ασφαλών πλατφορμών με τα ποσοστά υιοθέτησης να ποικίλλουν αναλόγως των τεχνικών γνώσεων, των αναγκών αλλά και των χαρακτηριστικών αυτών των πλατφορμών. Ωστόσο, υπάρχουν αξιοσημείωτες ανησυχίες σχετικά με την ασφάλεια που παρέχουν, τις λειτουργίες τους και τις τεχνικές προκλήσεις που σχετίζονται με αυτές.

Η παρούσα εργασία συμβάλλει στην κατανόηση της ασφαλούς επικοινωνίας στη Δημοσιογραφία παρέχοντας μια λεπτομερή ανάλυση των τρεχουσών πρακτικών, προκλήσεων και πιθανών λύσεων.

Λέξεις – Κλειδιά

Πλατφόρμες ασφαλούς επικοινωνίας, Δημοσιογραφία, Διαδίκτυο, Ασφαλής επικοινωνία, Πληροφοριοδότες, Ψηφιακές προκλήσεις

Use of Secure Communication Platforms by Journalists

Maria – Alexandra Sevastaki

Abstract

The field of Journalism is the cornerstone of a democratic society and is distinguished by its depth and commitment to uncovering the truth, especially in cases where transparency is lacking, thus contributing to valid citizen information.

In the digital age, communication security is paramount, especially in the field of Journalism where protecting sources and sensitive information is vital. This master's thesis examines the use of secure communication platforms by journalists, focusing on how these tools affect their work practices and the security of their communications. The paper explores the extent to which journalists are adopting secure platforms, the challenges they face and the effectiveness of these technologies in safeguarding their communications.

To collect empirical data, a questionnaire including 33 questions was distributed to journalistic associations. The questionnaire explored various aspects of secure communication, including platforms used, frequency of use, reliability and security, and any barriers to adoption. In addition, it examined journalists' awareness of potential threats and the measures they take to mitigate them.

The conclusions drawn reveal the concerns of journalists about the risks and challenges of the digital age. Additionally, there is widespread awareness of the importance of secure platforms with adoption rates varying according to the technical know-how, needs, and features of these platforms. However, there are notable concerns about the security they provide, their functions, and the technical challenges associated with them.

This master thesis contributes to the understanding of secure communication in journalism by providing a detailed analysis of current practices, challenges and potential solutions.

Keywords

Secure communication platforms, Journalism, Internet, Secure communication, Whistleblowers, Digital challenges

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες & Ακρωνύμια

ΕΑΠ	Ελληνικό Ανοικτό Πανεπιστήμιο
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΗΕΑ	Ένωσις Συντακτών Ημερήσιων Εφημερίδων Αθηνών
ΕΣΗΕΜ-Θ	Ένωση Συντακτών Ημερήσιων Εφημερίδων Μακεδονίας – Θράκης
ΕΣΗΕΘΣΤΕ-Ε	Ένωση Συντακτών Ημερήσιων Εφημερίδων Θεσσαλίας – Στερεάς Ελλάδας – Εύβοιας
ΕΣΗΕΠΗΝ	Ένωση Συντακτών Ημερησίων Εφημερίδων Πελοποννήσου-Ηπείρου-Νήσων
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΜΜΕ	Μέσα Μαζικής Ενημέρωσης
ΝΠΔΔ	Νομικό Πρόσωπο Δημοσίου Δικαίου
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΠΟΕΣΥ	Πανελλήνια Ομοσπονδία Ενώσεων Συντακτών
ΤΝ	Τεχνητή Νοημοσύνη
AI	Artificial Intelligence
CERN	Conseil Européen pour la Recherche Nucléaire
CIMA	Center for International Media Assistance
CPJ	Committee to Protect Journalists
EMFA	European Media Freedom Act
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ICIJ	International Consortium of Investigative Journalists
IP	Internet Protocol
MIT	Massachusetts Institute of Technology

MoJo	Mobile Journalism
NSA	National Security Agency
ITU	International Telecommunication Union
RSF	Reporters Sans Frontières
VoIP	Voice over IP
VPN	Virtual Private Network
2FA	Two-Factor Authentication

1 Εισαγωγή

Αν μπορούσαν να προσδοθούν δύο βασικά χαρακτηριστικά στον 21ο αιώνα, το ένα θα ήταν η ραγδαία εξέλιξη της τεχνολογίας και το δεύτερο η μαζική προσλαμβάνουσα πληροφορία. Τα Μέσα Μαζικής Ενημέρωσης (ΜΜΕ) αποτελούν την κύρια πηγή μετάδοσης πληροφοριών στο ευρύ κοινό και εκφραστές των ΜΜΕ είναι οι επαγγελματίες δημοσιογράφοι. Στο δυναμικό τοπίο της σύγχρονης Δημοσιογραφίας, η έλευση των ψηφιακών τεχνολογιών έχει αναδείξει πολλές ευκαιρίες μα συνάμα και προκλήσεις. Προκλήσεις που αφορούν την προστασία των πηγών τους, των ευαίσθητων δεδομένων αλλά και των καναλιών επικοινωνίας τους, όσον αφορά τη δημοσίευση μιας είδησης, του δημοσιογραφικού τους δηλαδή υλικού. Σε μια εποχή που χαρακτηρίζεται από διάχυτη ψηφιακή επιτήρηση και απειλές για την ελευθερία του Τύπου, ο ρόλος των ασφαλών πλατφορμών στη Δημοσιογραφία έχει καταστεί πρωταρχικής σημασίας. Ο στόχος των πλατφορμών αυτών είναι η διατήρηση της ακεραιότητας των δημοσιογράφων αλλά και η προστασία ευαίσθητων πληροφοριών. Το σημερινό λοιπόν ταχέως εξελισσόμενο ψηφιακό τοπίο, επιβάλλει δημοσιογραφική εντιμότητα και διαφύλαξη των πηγών, επαγγελματικές έννοιες που είναι ολοένα και περισσότερο συνυφασμένες με την αναγκαιότητα ασφαλών πλατφορμών επικοινωνίας.

Οι δημοσιογράφοι, επιφορτισμένοι με το καθήκον να αποκαλύπτουν αλήθειες και να λογοδοτούν, αντιμετωπίζουν ολοένα και αυξανόμενες προκλήσεις, όσον αφορά την προστασία ευαίσθητων πληροφοριών από την παρακολούθηση, τη λογοκρισία και οποιοδήποτε άλλο πιθανόν κακόβουλο παράγοντα. Ως απάντηση, η υιοθέτηση ασφαλών αλλά και φιλικών προς τον χρήστη εργαλείων επικοινωνίας, έχει αναδειχθεί ως ζωτικό συστατικό της σύγχρονης δημοσιογραφικής πρακτικής. Τέτοιες πλατφόρμες περιλαμβάνουν μια σειρά εργαλείων και τεχνολογιών που έχουν σχεδιασθεί για να προστατεύουν την επικοινωνία, την αποθήκευση δεδομένων και τη συνεργασία, χρησιμοποιώντας συχνά κρυπτογράφηση, πρωτόκολλα ελέγχου ταυτότητας και χαρακτηριστικά ανωνυμίας. Με τη χρήση σύγχρονων εργαλείων ασφαλούς επικοινωνίας, οι δημοσιογράφοι μπορούν να θωρακίζουν τις πηγές τους, να επικοινωνούν εμπιστευτικά, να μετριάζουν τους κινδύνους λογοκρισίας και να τηρούν τις αρχές της διαφάνειας και της λογοδοσίας σε μια εποχή γεμάτη ψηφιακές ευπάθειες.

Η χρήση πλατφορμών ασφαλούς επικοινωνίας ήρθε ως απάντηση στις προκλήσεις και στους κινδύνους που επέφερε η ψηφιακή εποχή ιδιαίτερα στο κομμάτι της παρακολούθησης των επικοινωνιών. Με την πάροδο του χρόνου, η χρήση τέτοιων εργαλείων υιοθετήθηκε από όλο και περισσότερους επαγγελματίες του χώρου της Δημοσιογραφίας Η πιο αντιπροσωπευτική ομάδα είναι οι επονομαζόμενοι πληροφοριοδότες ή Whistleblowers, όπως είναι ευρέως γνωστοί παγκοσμίως, οι οποίοι είναι άτομα που αποκαλύπτουν εμπιστευτικές ή απόρρητες πληροφορίες για το δημόσιο συμφέρον. Στην προσπάθεια τους αυτή έχουν αναζητήσει ασφαλείς πλατφόρμες για να μοιράζονται πληροφορίες με δημοσιογράφους, ελαχιστοποιώντας τον κίνδυνο εντοπισμού τους. Αξίζει επίσης να γίνει αναφορά σε Διεθνείς οργανισμούς, όπως η Επιτροπή Προστασίας των Δημοσιογράφων - Committee to Protect Journalists (CPJ) και οι Δημοσιογράφοι Χωρίς Σύνορα - (Reporters Sans Frontières (RSF), που έχουν μεριμνήσει σχετικά με τη σημασία της ψηφιακής ασφάλειας στη Δημοσιογραφία και έχουν παράσχει πόρους και υποστήριξη σε δημοσιογράφους που αντιμετώπιζαν τον οποιοδήποτε κίνδυνο. Επιπλέον, κυβερνητικές πρωτοβουλίες διαφάνειας, όπως το Άρθρο 14 σύμφωνα με το Σύνταγμα της Ελλάδας που αφορά την ελευθερία του Τύπου (Βουλή των Ελλήνων, 2019) ο πρόσφατος ευρωπαϊκός νόμος που εγκρίθηκε από το συμβούλιο της Ευρωπαϊκής Ένωσης στις 26 Μαρτίου 2024 σχετικά με την ελευθερία των Μέσων Ενημέρωσης - European Media Freedom Act (EMFA) (Council of the EU, 2024) όπως επίσης και ο νόμος περί ελευθερίας της Πληροφόρησης - Freedom of Information Act (FOIA) (Freedom of Information Act, 2024) στις Ηνωμένες Πολιτείες έχουν διευκολύνει τη δημοσιοποίηση κυβερνητικών εγγράφων και δεδομένων σε δημοσιογράφους με ασφαλή και διαφανή τρόπο. Τέλος, κρίσιμο ρόλο στη δημιουργία και τη βελτίωση πλατφορμών προσαρμοσμένων στις ανάγκες των δημοσιογράφων και των ειδησεογραφικών οργανισμών έχουν και συνεχίζουν να διαδραματίζουν οι προγραμματιστές τεχνολογίας καθώς και οι ακαδημαϊκές και ερευνητικές κοινότητες παγκοσμίως, οι οποίοι μελετούν την ψηφιακή ασφάλεια και συνεισφέρουν τα μέγιστα με τις πολύτιμες γνώσεις και συστάσεις τους.

Στο πλαίσιο αυτό, στην παρούσα εργασία, το βασικό ερώτημα που διερευνάται είναι η χρήση των πλατφορμών ασφαλούς επικοινωνίας από τους δημοσιογράφους. Η απάντηση σε αυτό το ερώτημα δεν είναι άμεση και ξεκάθαρη αφού εμπεριέχει

διαφορετικούς παράγοντες που πρέπει να ληφθούν υπόψη. Αρχικά, εξετάζεται η αναγκαιότητα των πλατφορμών αυτών και ποιοι είναι οι λόγοι που οδήγησαν στην ανάπτυξή τους αλλά και στην καθιέρωσή τους ως μέσο επικοινωνίας. Η απάντηση σε αυτό το σκέλος του ερευνητικού ερωτήματος της παρούσας εργασίας δίδεται μέσω του επόμενου κεφαλαίου στο οποίο υπάρχει ενδελεχής βιβλιογραφική έρευνα, η οποία εκκινεί από την καθιέρωση του Διαδικτύου έως τις προκλήσεις που αντιμετωπίζουν οι δημοσιογράφοι και οι πληροφοριοδότες στη σύγχρονη ψηφιακή εποχή. Στη συνέχεια, στο πλαίσιο της παρούσας εργασίας, αναπτύχθηκε σχετικό ερωτηματολόγιο, το οποίο διανεμήθηκε ηλεκτρονικά σε Έλληνες δημοσιογράφους, με σκοπό τη χαρτογράφηση της χρήσης αλλά και της γνώσης γενικότερα τόσο των πλατφορμών ασφαλούς επικοινωνίας όσο και γενικότερα την ασφάλεια στην επικοινωνία τους στο πλαίσιο άσκησης του δημοσιογραφικού επαγγέλματος. Μέσω λοιπόν της συλλογής των αποτελεσμάτων, τα οποία παρουσιάζονται αναλυτικά στο Κεφάλαιο 5, η παρούσα εργασία καλείται να δώσει μια σφαιρική απάντηση και να παράξει χρήσιμα συμπεράσματα στο ερώτημα σχετικά με τη χρήση πλατφορμών ασφαλούς επικοινωνίας στη Δημοσιογραφία.

Λόγω του εύρους του συγκεκριμένου ερευνητικού ερωτήματος και με δεδομένο ότι ο κλάδος της Δημοσιογραφίας αλλά και της τεχνολογίας εξελίσσονται συνεχώς και με ταχείς ρυθμούς, τα συμπεράσματα που αναφέρονται στην παρούσα εργασία δεν είναι καθολικά καθώς υπεισέρχονται κάποιοι περιοριστικοί παράγοντες. Αρχικά, το ερωτηματολόγιο απευθύνθηκε μόνο σε Έλληνες δημοσιογράφους και έγινε καταγραφή απαντήσεων που αφορά αποκλειστικά την ελληνική Δημοσιογραφία. Επομένως, τα συμπεράσματα που παρατίθενται στο πλαίσιο της παρούσας εργασίας δεν είναι καθολικά και ίσως δεν είναι τα ίδια ή σχετικά σε άλλες χώρες. Επιπλέον, με τη ραγδαία εξέλιξη και τη γιγάντωση της αγοράς και άρα της προσφοράς λύσεων ασφαλούς επικοινωνίας ήταν αδύνατο να εξετασθούν όλες οι διαθέσιμες πλατφόρμες που υπάρχουν. Έτσι, έγινε μια σταχυολόγηση αυτών βάσει της δημοφιλίας τους αλλά και σχετικής έρευνας που πραγματοποιήθηκε στο πλαίσιο της παρούσας μελέτης. Περισσότερες πληροφορίες για κάθε μία από τις πλατφόρμες που επιλέχθηκαν υπάρχουν στο Κεφάλαιο 3 του παρόντος. Τέλος, η εξαγωγή συμπερασμάτων βασίζεται αποκλειστικά στη βιβλιογραφική έρευνα και στις απαντήσεις που έδωσε το

συγκεκριμένο δείγμα συμμετεχόντων που απάντησε το ερωτηματολόγιο που αναπτύχθηκε για τους σκοπούς της παρούσας εργασίας.

1.1 Στόχοι της εργασίας

Σκοπός της παρούσας ερευνητικής εργασίας είναι η εύρεση, ανάλυση και παραγωγή χρήσιμων συμπερασμάτων αναφορικά με τα χαρακτηριστικά και τις προκλήσεις της σύγχρονης ψηφιακής εποχής καθώς και της χρήσης πλατφορμών επικοινωνίας από τους δημοσιογράφους. Οι πλατφόρμες αυτές αποτελούν βασικό εργαλείο στην κατεύθυνση της ασφαλούς επικοινωνίας για την προστασία ευαίσθητων πληροφοριών αλλά και την προστασία των επαγγελματικών πηγών στον χώρο της Δημοσιογραφίας. Τα κεφάλαια που ακολουθούν και αναπτύσσονται, στοχεύουν στο να τονίσουν την ανάγκη για την ύπαρξη αυτών των πλατφορμών αλλά και τον ουσιαστικό ρόλο τους στην υποστήριξη της δημοσιογραφικής ηθικής, την προώθηση της ελευθερίας του Τύπου και την ενίσχυση των βασικών αρχών και των θεμελίων των δημοκρατικών κοινωνιών στην ψηφιακή εποχή. Πολύτιμος αρωγός αυτής της εργασίας αποτέλεσε το ερωτηματολόγιο 33 ερωτήσεων κλειστού και ανοιχτού τύπου που διαμορφώθηκε με το λογισμικό Google Forms και διαμοιράσθηκε σε δημοσιογραφικές ενώσεις.

1.2 Δομή

Στο παρόν κεφάλαιο δόθηκαν κάποια εισαγωγικά στοιχεία, τέθηκε το βασικό ερευνητικό ερώτημα και οι περιορισμοί της παρούσας εργασίας. Επίσης, παρουσιάστηκε ο σκοπός της και η δομή της για την καλύτερη και πληρέστερη κατανόησή της. Έτσι, επιλέχθηκαν και υπογραμμίσθηκαν οι βασικές πληροφορίες της εργασίας.

Το δεύτερο κεφάλαιο αποτελεί το πιο θεωρητικό κομμάτι της παρούσας εργασίας καθώς σε αυτό αποτυπώνεται και αναπτύσσεται το σύνολο της βιβλιογραφικής έρευνας που πραγματοποιήθηκε προκειμένου να ενισχύσει και να υποστηρίξει τη συγγραφή της με επιστημονικά δεδομένα.

Στο τρίτο κεφάλαιο γίνεται επισκόπηση των πλατφορμών επικοινωνίας Nextcloud, Wickr, Proton Mail, Signal, Threema, Wire, WhatsApp, SecureDrop, GlobaLeaks, OnionShare, Tresorit και Telegram.

Στο τέταρτο κεφάλαιο παρουσιάζεται αναλυτικά η μεθοδολογία που ακολουθήθηκε για την προετοιμασία, σχεδιασμό και υλοποίηση του ερευνητικού τμήματος της παρούσας. Επεξηγείται η σχεδίαση του ερωτηματολογίου και δίνονται σημαντικές πληροφορίες σχετικά με τον διαμοιρασμό του σε επαγγελματίες δημοσιογράφους και δημοσιογραφικές ενώσεις.

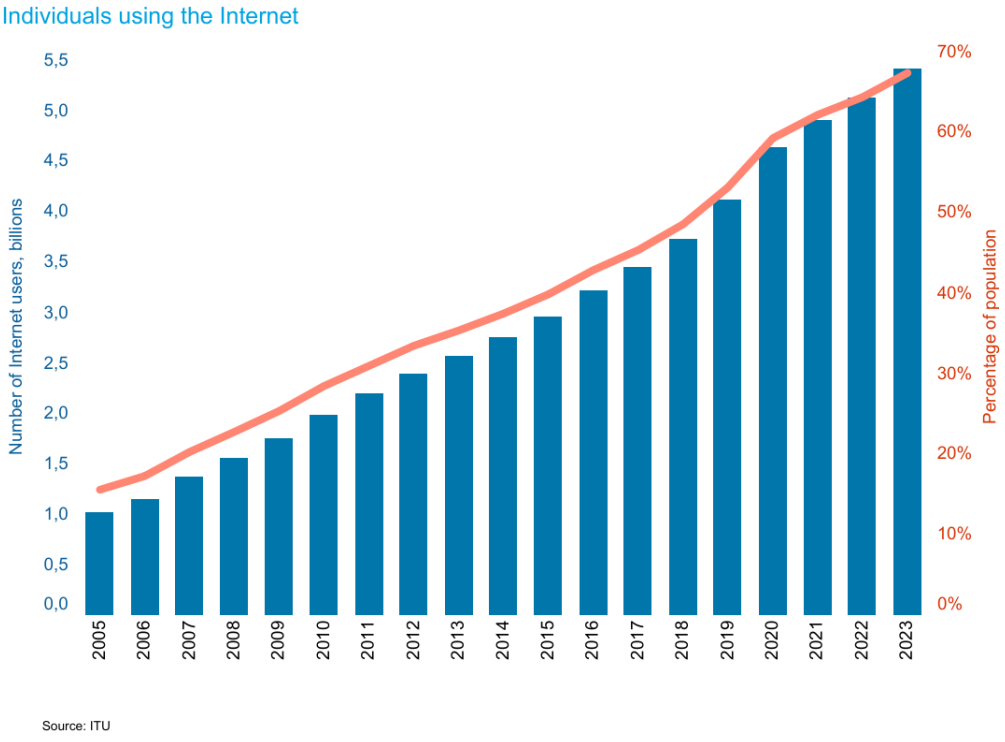
Στο πέμπτο κεφάλαιο ακολουθεί η λογική συνέχεια του τέταρτου, ήτοι η ποσοτική ανάλυση των δοθεισών απαντήσεων του ερωτηματολογίου καθώς και ο σχολιασμος των αποτελεσμάτων της έρευνας.

Στο έκτο και καταληκτικό κεφάλαιο της παρούσας παρουσιάζονται πιθανές μελλοντικές επεκτάσεις στο συγκεκριμένο ερευνητικό πεδίο καθώς και τα βασικά συμπεράσματα που παρήχθησαν από την εκπόνηση της συγκεκριμένης εργασίας.

2 Βιβλιογραφική Έρευνα

2.1 Διαδίκτυο και Μετάδοση της Πληροφορίας

Το Διαδίκτυο αποτελεί πλέον ένα εργαλείο καθώς και βασική ανάγκη για το μεγαλύτερο μέρος του πληθυσμού. Αυτό συνέβαλε στο να αλλάξει άρδην η καθημερινότητα σε ένα ευρύ φάσμα από τον επαγγελματικό τομέα μέχρι τη διασκέδαση των ανθρώπων. Έτσι, δεν έμεινε ανεπηρέαστος και ο τρόπος με τον οποίο οι πληροφορίες και οι ειδήσεις παράγονται, μεταδίδονται και καταναλώνονται παγκοσμίως. Η ραγδαία αυτή εξάπλωση του Διαδικτύου αποτυπώνεται και στην Εικόνα 1, η οποία παρουσιάζει το σύνολο των χρηστών του Διαδικτύου από το 2005 έως το 2023. Το 2023 το ποσοστό αυτό ανήλθε στο 67% του παγκόσμιου πληθυσμού, σύμφωνα με το International Telecommunication Union (ITU) (International Telecommunication Union (ITU), 2024).



Εικόνα 1. Χρήστες του διαδικτύου σε εκατομμύρια ανά έτος 2005-2023 (International Telecommunication Union (ITU), 2024)

Έτσι, από την προ-ψηφιακή εποχή, κατά την οποία η παραγωγή και η μετάδοση ειδήσεων και πληροφοριών ήταν αργή και αρκετά περιορισμένη, πραγματοποιήθηκε

μια ραγδαία έως και βίαιη μετάβαση στην ψηφιακή πραγματικότητα στην οποία καθοριστικό ρόλο διαδραμάτισε η εξάπλωση και η εδραίωση του Διαδικτύου και των εργαλείων που το συνοδεύουν (π.χ., κοινωνικά δίκτυα, ηλεκτρονική αλληλογραφία, κ.α.).

2.1.1 Η εποχή πριν το Διαδίκτυο

Πριν το Διαδίκτυο, η ροή της πληροφορίας καθοριζόταν κυρίως από τα παραδοσιακά μέσα - όπως αποκαλούνται - και πιο συγκεκριμένα τις εφημερίδες, την τηλεόραση και το ραδιόφωνο. Αυτά τα κανάλια πληροφοριών, όπως συμβαίνει στις περισσότερες περιπτώσεις ακόμα και σήμερα, ανήκουν σε ένα περιορισμένο αριθμό ιδιοκτητών και οργανισμών, οι οποίοι έχουν καταφέρει να τα συγκεντρώσουν. Έτσι, όπως είναι αναμενόμενο, η συγκέντρωση αυτή των μέσων διάδοσης πληροφορίας κάτω από συγκεκριμένους οργανισμούς και πρόσωπα οδηγεί πολλές φορές στην επιβολή συγκεκριμένων κατευθύνσεων που εξυπηρετούν συμφέροντα, επηρεάζοντας σημαντικά την κοινή γνώμη. Αυτό έχει ως αποτέλεσμα, η μετάδοση της πληροφορίας να απαιτεί χρόνο προκειμένου να συσσωρευτεί, να επεξεργαστεί και να μεταδοθεί με τον τρόπο που θα εξυπηρετούσε καλύτερα τα συμφέροντα του εκάστοτε οργανισμού (Briggs & Burke, 2009; Pavlik, 2008).

Πιο συγκεκριμένα, οι εφημερίδες και τα περιοδικά αποτελούν τα βασικά έντυπα μέσα που χρησιμοποιούνται ακόμα και σήμερα για τη συγκέντρωση και τη μετάδοση πληροφοριών. Ωστόσο, ο κύκλος από τη συλλογή μέχρι και τη δημοσίευση πληροφοριών στα έντυπα μέσα είναι χρονοβόρος και πολλές φορές απαιτεί μέχρι και ολόκληρες εβδομάδες (Briggs & Burke, 2009).

Από την άλλη, η τηλεόραση και το ραδιόφωνο διαθέτουν συνεχόμενη ροή μεταδόσεων και συνήθως πιο άμεση ενημέρωση συγκριτικά με τα έντυπα μέσα. Και σε αυτή την κατηγορία όμως υπάρχουν περιορισμοί καθώς το πρόγραμμα μεταδόσεων είναι καθορισμένο και περιλαμβάνει πέρα από ενημερωτικές εκπομπές και ψυχαγωγικές (Briggs & Burke, 2009; Pavlik, 2008).

Ένας ακόμα περιορισμός των παραδοσιακών μέσων είναι η τοπικότητα των ειδήσεων. Συνήθως, οι ειδήσεις και οι πληροφορίες που μεταδίδονται αφορούν αποκλειστικά εγχώρια ζητήματα με αποτέλεσμα η ενημέρωση για παγκόσμια

γεγονότα ή πληροφορίες που αφορούν διαφορετικές χώρες να είναι ελάχιστες αναλογικά με αυτές που αφορούν την εγχώρια καθημερινότητα (Pavlik, 2008).

2.1.2 Η επανάσταση του Διαδικτύου και η άμεση πρόσβαση στην πληροφορία

Η έλευση και η εδραίωση του Διαδικτύου σε όλες σχεδόν τις εκφάνσεις της καθημερινότητας έχει οδηγήσει σε μια σειρά από ραγδαίες αλλαγές στον τομέα του διαμοιρασμού πληροφοριών. Οι αλλαγές αυτές έγκεινται κυρίως στα ακόλουθα:

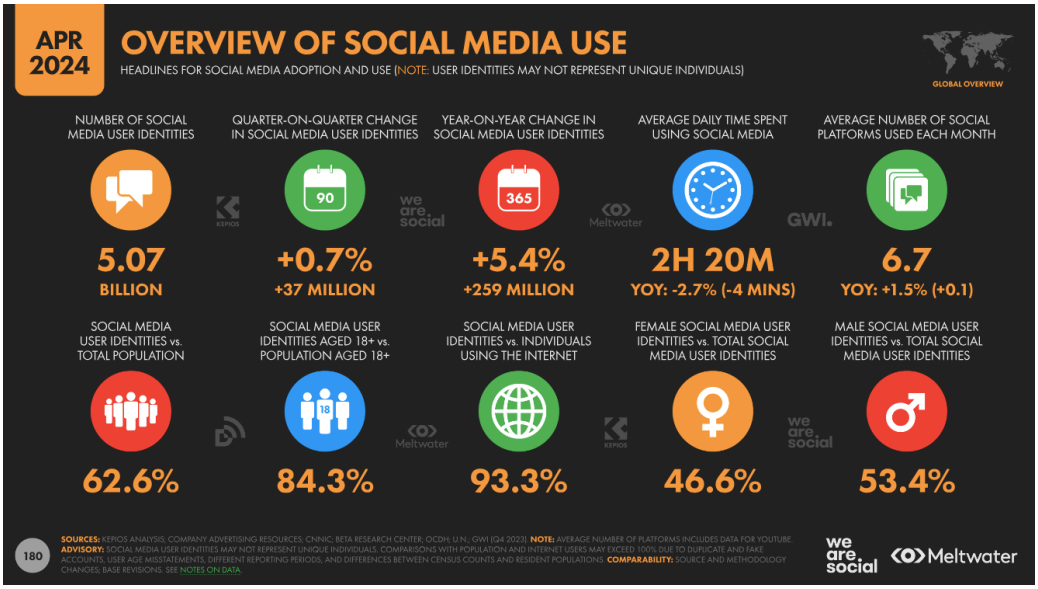
- **Ταχύτητα και προσβασιμότητα**: Οι πληροφορίες πλέον είναι διαθέσιμες σε πραγματικό χρόνο. Οι ειδησεογραφικοί ιστότοποι, τα ιστολόγια καθώς και οι πλατφόρμες μέσων κοινωνικής δικτύωσης είναι σε θέση να μεταδίδουν και να παρέχουν ενημερώσεις μέσα σε δευτερόλεπτα από την εκδήλωση ενός γεγονότος ή ακόμα και σε ζωντανή μετάδοση (Castells, 2009).
- **Παγκόσμια Απήχηση**: Οι γεωγραφικοί περιορισμοί πλέον δεν υφίστανται καθώς μέσω του Διαδικτύου είναι δυνατή η παραγωγή, η μετάδοση και η αναπαραγωγή πληροφοριών από οποιοδήποτε σε οποιοδήποτε σημείο στον κόσμο (Benkler, 2006).
- **Αποκέντρωση:** Πλέον η διαχείριση της πληροφορίας δεν εναποτίθεται μόνο σε έναν περιορισμένο αριθμό οργανισμών και ατόμων που διαχειρίζονται τα παραδοσιακά μέσα, όπως αναφέρθηκε προηγουμένως. Οποιοσδήποτε μπορεί να παράξει, να μεταδώσει και να αναπαράξει περιεχόμενο και πληροφορίες ακόμα και σε ζωντανή μετάδοση. Αυτό οδηγεί σε αποκέντρωση στη διαχείριση των πληροφοριών (Shirky, 2008).

2.1.3 Τα κοινωνικά δίκτυα και η δημοκρατικοποίηση της πληροφορίας

Παράλληλα με την άνοδο και τη διάδοση του Διαδικτύου εμφανίστηκαν οι πλατφόρμες κοινωνικής δικτύωσης και πλέον αποτελούν αναπόσπαστο κομμάτι στην καθημερινότητα των περισσότερων. Μέσω των πλατφορμών κοινωνικής δικτύωσης όπως το Facebook, το X (πρώην Twitter), το Instagram κ.α. οι άνθρωποι ενημερώνονται, ψυχαγωγούνται αλλά και παράγουν οι ίδιοι περιεχόμενο καθημερινά. Έτσι, κάθε χρήστης δύναται σε πραγματικό χρόνο και χωρίς να χάσει καθόλου χρόνο, σχεδόν στιγμιαία, να μεταδώσει κάποια πληροφορία δημιουργώντας έτσι μια νέα εποχή αλλά και κουλτούρα στον διαμοιρασμό πληροφοριών (Kaplan & Haenlein, 2010).

Έτσι, ακόμα και οι δημοσιογράφοι μπορούν να αντλήσουν περιεχόμενο από τα μέσα κοινωνικής δικτύωσης και να δημοσιεύσουν πληροφορίες αλλά και ειδήσεις, ακόμα και σε πραγματικό χρόνο. Χρήστες με μεγάλο κοινό και αριθμό ακολούθων μπορούν να μεταδώσουν περιεχόμενο, το οποίο να έχει απήχηση σε χιλιάδες ή ακόμα και εκατομμύρια κόσμο σχεδόν ακαριαία. Επιπλέον, η μετάδοση πληροφορίας δεν είναι μονόδρομη όπως με τα παραδοσιακά μέσα αφού πλέον οι χρήστες των κοινωνικών δικτύων μπορούν να αλληλεπιδράσουν με τις αναρτήσεις υπό μορφή σχολιασμού, αναδημοσίευσης ή και απάντησης σε σχόλια άλλων χρηστών, δημιουργώντας έτσι μια διαδραστική ροή στη μετάδοση περιεχομένου (Kietzmann, Hernmkens, McCarthy, & Silvestre, 2011). Οι πτυχές αυτές των κοινωνικών δικτύων και τα χαρακτηριστικά που προσέφεραν στον τομέα των πληροφοριών ήταν κάτι που φάνταζε αδύνατο με τα παραδοσιακά μέσα.

Η επίδραση των κοινωνικών δικτύων είναι εμφανής μελετώντας τα στατιστικά στην Εικόνα 2. Σύμφωνα με τα στατιστικά που παρατίθενται από την ιστοσελίδα Smart Insights (Chaffey, 2024) οι χρήστες των κοινωνικών δικτύων μέχρι και τον Απρίλιο 2024 αγγίζουν τα 5.07 δισεκατομμύρια παγκοσμίως. Αυτό μεταφράζεται περίπου στο 63% του παγκόσμιου πληθυσμού με τη σημείωση ότι αυτά τα 5.07 δισεκατομμύρια είναι οι διαφορετικές ταυτότητες χρηστών στα κοινωνικά δίκτυα, ωστόσο κάποιος χρήστης μπορεί να διαθέτει παραπάνω του ενός λογαριασμούς. Ενδιαφέρον παρουσιάζει το στατιστικό ότι καθημερινά ο μέσος χρήστης αφιερώνει πάνω από 2 ώρες στα κοινωνικά δίκτυα. Τέλος, η κατανομή μεταξύ ανδρών και γυναικών είναι σχεδόν ίσοι αφού το 46,6% των λογαριασμών ανήκουν σε γυναίκες και το 53,4% σε άνδρες.



Εικόνα 2. Η χρήση των κοινωνικών δικτύων σε αριθμούς (Chaffey, 2024)

2.1.4 Η τεχνολογία της πληροφορίας και των επικοινωνιών στη Δημοσιογραφία

Η επανάσταση της υψηλής τεχνολογίας έχει αλλάξει σημαντικά τον τρόπο με τον οποίο το κοινό έχει πρόσβαση στις ειδησεογραφικές πληροφορίες με αποτέλεσμα τα ΜΜΕ να έχουν απολέσει μεγάλο μερίδιο από το παραδοσιακό μονοπώλιό τους. Τα ΜΜΕ και οι δημοσιογραφικές πρακτικές εν γένει, ωστόσο, άργησαν να προσαρμοσθούν στο Διαδίκτυο και στις παγκόσμιες επιπτώσεις που προκάλεσε η τεχνολογική «έκρηξη» (Kaul, 2013). Αξιοσημείωτο είναι ότι τις τελευταίες δεκαετίες οι δημοσιογράφοι στον Δυτικό Κόσμο επωφελήθηκαν από την τεράστια ανάπτυξη της τεχνολογίας της πληροφορίας και των επικοινωνιών ή ICTs (Information and Communication Technology), καθώς τα εργαλεία αυτά διευκόλυναν τις εργασιακές διεργασίες. Οι τεχνολογίες αυτές άλλαξαν ριζικά τη Δημοσιογραφία αναδιαμορφώνοντας τον τρόπο με τον οποίο συγκεντρώνονται, παράγονται και διανέμονται οι ειδήσεις. Πιο συγκεκριμένα, οι τεχνολογίες αυτές αναφέρονται σε όλα τα τεχνικά μέσα που χρησιμοποιούνται για τον χειρισμό πληροφοριών και προσφέρουν ουσιαστική βοήθεια στον τομέα της επικοινωνίας (Eurostat, 2023)

Όσον αφορά τα ICTs, καταρχάς οι δημοσιογράφοι χρησιμοποιούν διάφορα ψηφιακά μέσα για τη συλλογή πληροφοριών και τη συγγραφή ειδήσεων. Αυτό περιλαμβάνει smartphones, ψηφιακές συσκευές εγγραφής και φορητούς υπολογιστές, που τους επιτρέπουν να λειτουργούν πιο ευέλικτα ακόμα και σε απομακρυσμένες τοποθεσίες. Επίσης, πλατφόρμες όπως το X, το Facebook και το Instagram έχουν πλέον καταστεί

πολύ σημαντικά εργασιακά εργαλεία για τους δημοσιογράφους, όταν θέλουν να διαδώσουν άμεσα ένα έκτακτο γεγονός στο κοινό ή να επαληθεύσουν στοιχεία του ρεπορτάζ τους. Ένα ακόμα χαρακτηριστικό που κάνει τα ICTs αναγκαία μέσα, είναι ότι επιτρέπουν την παραγωγή πλούσιου, πολυμεσικού περιεχομένου. Οι δημοσιογράφοι μπορούν να δημιουργήσουν διαδραστικές ιστορίες που ενσωματώνουν βίντεο, ήχο και γραφικά, ενισχύοντας την εμπειρία αφήγησης και προσελκύοντας το κοινό πιο ουσιαστικά (Abosede Olubunmi, 2022).

2.2 Δημοσιογραφικές Αρχές και Μέθοδοι στην Ψηφιακή Εποχή

Αν και όπως αναφέρθηκε στις προηγούμενες παραγράφους το Διαδίκτυο άλλαξε ριζικά ακόμα και την ίδια τη Δημοσιογραφία, οι βασικές αρχές που τη διέπουν παραμένουν σε μεγάλο βαθμό οι ίδιες. Στις επόμενες παραγράφους γίνεται μια ανασκόπηση αυτών όπως παρατίθενται στη διεθνή βιβλιογραφία καθώς και των μεθόδων της ψηφιακής εποχής που συνεισφέρουν στην ορθή τήρησή τους.

2.2.1 Βασικές αρχές της Δημοσιογραφίας

Οι βασικές αρχές της Δημοσιογραφίας μπορούν να συνοψισθούν στις παρακάτω:

- **Ακρίβεια και εγκυρότητα:** Αποτελούν τη βάση της Δημοσιογραφίας. Στην ψηφιακή εποχή με δεδομένα την ταχύτητα και τον τεράστιο όγκο πληροφοριών που μεταδίδονται, η ακρίβεια και η εγκυρότητα των γεγονότων είναι πιο κρίσιμες από ποτέ (Graves, 2016; Silverman, et al., 2016).
    - **Έλεγχος γεγονότων:** Ο έλεγχος και η επαλήθευση των πληροφοριών αποτελεί βασικό μέλημα για τους σύγχρονους δημοσιογράφους. Έτσι, η επαλήθευση ενός γεγονότος από διαφορετικές πηγές, η συμβολή των ειδικών στην εκάστοτε θεματολογία αλλά και η χρήση σύγχρονων εργαλείων που αποσκοπούν στον έλεγχο της εγκυρότητας όπως το Snopes[1] και το FactCheck.org[2] αποτελούν βασικά εργαλεία της σύγχρονης Δημοσιογραφίας.
    - **Διορθώσεις και ανακλήσεις:** Το επάγγελμα της Δημοσιογραφίας συνήθως ασκείται κάτω από συνθήκες πίεσης, οι οποίες απαιτούν

[1] https://www.snopes.com/
[2] https://www.factcheck.org/

ταχύτητα στη μεταφορά πληροφοριών με αποτέλεσμα να μεταδίδονται ανακρίβειες ή εσφαλμένες πληροφορίες. Για τον λόγο αυτό και προκειμένου να μην διακυβεύεται η ακρίβεια και η εγκυρότητα αλλά και γενικότερα η εμπιστοσύνη στη Δημοσιογραφία, σε περιπτώσεις λαθών οι δημοσιογράφοι καλούνται να προβούν σε διορθώσεις και ενδεχομένως ανακλήσεις των πληροφοριών ή και απόψεών τους. Στην ψηφιακή εποχή, οι διαδικτυακές πλατφόρμες ειδήσεων καθώς και τα κοινωνικά δίκτυα επιτρέπουν διορθώσεις και ενημερώσεις των πληροφοριών σε πραγματικό χρόνο, δίνοντας έτσι τη δυνατότητα στους δημοσιογράφους να διορθώνουν άμεσα οποιαδήποτε ανακρίβεια, εξασφαλίζοντας με τον τρόπο αυτό την εμπιστοσύνη του κοινού.

- **Ανεξαρτησία:** Κάθε δημοσιογράφος οφείλει να διατηρεί την ανεξαρτησία του και να μην επηρεάζεται από εξωτερικούς παράγοντες ούτως ώστε να είναι σε θέση να παράσχει αντικειμενική ενημέρωση (Schiffrin, 2017; Kovach & Rosenstiel, 2021).
    - **Συντακτική ανεξαρτησία:** Η πλειοψηφία των δημοσιογραφικών οργανισμών διαχωρίζει το περιεχόμενό της προκειμένου να είναι ξεκάθαρο του τι αποτελεί δημοσιογραφική είδηση και τι διαφήμιση ή ανάρτηση περιεχόμενου με εταιρικά συμφέροντα. Με αυτόν τον τρόπο, εξασφαλίζεται η ανεξαρτησία των δημοσιογράφων του ομίλου/οργανισμού αλλά και τα όποια φαινόμενα σύγκρουσης συμφερόντων (Schiffrin, 2017).
    - **Διαφάνεια:** Η διαφάνεια αποτελεί βασικό στοιχείο για την τήρηση της αρχής της ανεξαρτησίας. Πολλές φορές, η αναφορά τυχόν αντικρουόμενων συμφερόντων καθώς και των φορέων χρηματοδότησης ενός δημοσιογραφικού οργανισμού εξασφαλίζει την απαραίτητη διαφάνεια προς το κοινό. Έτσι, αποφεύγονται τυχόν γκρίζες ζώνες και σκοτεινά σημεία, τα οποία μπορούν να οδηγήσουν σε απώλεια της εμπιστοσύνης του κοινού (Kovach & Rosenstiel, 2021).
- **Αμεροληψία:** Αποτελεί βασική αρχή της Δημοσιογραφίας καθώς σε ένα γεγονός που εκτυλίσσεται ο δημοσιογράφος είναι υποχρεωμένος να εξετάζει

και να παρουσιάζει όλες τις εμπλεκόμενες πλευρές χωρίς καμία προκατάληψη (Donsbach & Klett, 1993; Stroud, 2011).

- **Αντικειμενικό ρεπορτάζ:** Κάθε δημοσιογράφος οφείλει να χρησιμοποίει διαφορετικές πηγές προκειμένου να καλύπτει όλες τις οπτικές πάνω σε ένα ζήτημα. Έτσι, πρέπει να καταγράφει όλες τις απόψεις από όλους τους εμπλεκόμενους φορείς και να διασφαλίζει ότι εκφράζει κάθε μειονότητα ή περιθωριοποιημένη άποψη, απαλλάσσοντας έτσι το ρεπορτάζ από κάθε υποκειμενική ή προσωπική άποψη ή χροιά.
- **Ουδέτερη γλώσσα:** Η προσεκτική χρήση της γλώσσας, η οποία οφείλει να φέρει μια ουδέτερη και αντικειμενική χροιά, συνεισφέρει στη διατήρηση της αμεροληψίας. Έτσι, οι δημοσιογράφοι πρέπει να εκφέρουν ή να συντάσσουν λόγο απαλλαγμένο από κάθε επίκληση στο συναίσθημα προκειμένου να μην αποπροσανατολίζουν ή διαστρεβλώνουν την αντίληψη του κοινού για ένα γεγονός.

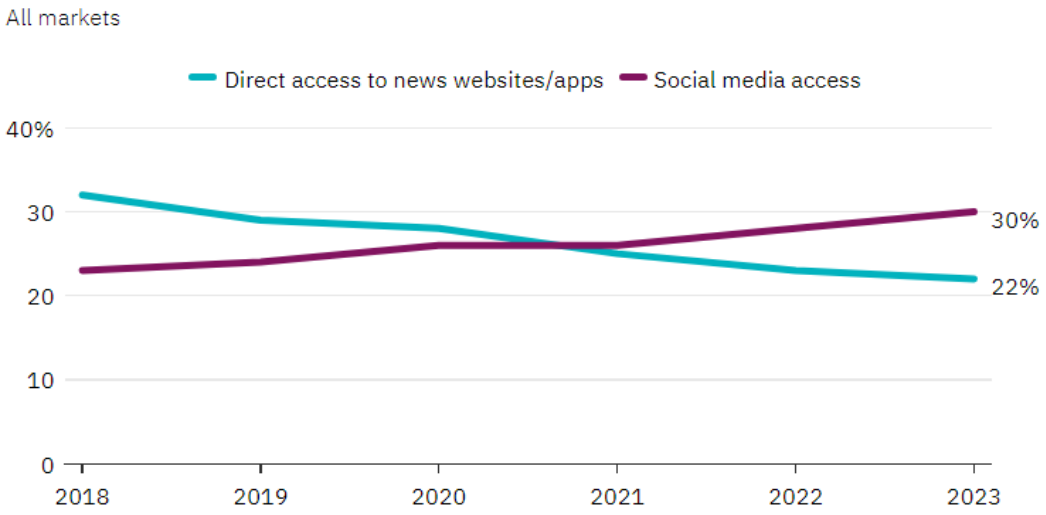
- **Λογοδοσία:** Όλοι οι δημοσιογράφοι πρέπει να δρουν και να ασκούν το επάγγελμά τους ως υπόλογοι απέναντι στο κοινό. Για τον λόγο αυτό, η Δημοσιογραφία πρέπει πάντα να ασκείται ακολουθώντας ισχυρά δεοντολογικά πρότυπα (Craft & Davis, 2021; Eberwein, Fengler, & Karmasin, 2017).
  - **Αρχές δεοντολογίας:** Οι περισσότεροι δημοσιογραφικοί οργανισμοί είναι θιασώτες αυστηρών δεοντολογικών αρχών που ορίζονται από δημοσιογραφικές ενώσεις (ΕΣΗΕΑ) (ΕΣΗΕΑ, 1998) καθώς και από νομοθεσίες είτε σε εθνικό ή διεθνές επίπεδο (Eberwein, Fengler, & Karmasin, 2017).
  - **Συμμετοχή του κοινού:** Η συμμετοχή του κοινού καθώς και η αποδοχή ήταν ανέκαθεν ζητούμενο στη Δημοσιογραφία. Ωστόσο, παλαιότερα κάτι τέτοιο ήταν εφικτό μόνο σε περιορισμένο βαθμό και συνήθως ετεροχρονισμένα. Με την έλευση του Διαδικτύου και τη ραγδαία ανάπτυξή του, η συμμετοχή του κοινού είναι άμεση καθώς μπορεί μέσω των διαδικτυακών πλατφορμών να παρέχει σχολιασμό, κριτική και να συζητούν ακόμα και σε πραγματικό χρόνο με τους

δημοσιογράφους, οι οποίοι μπορούν να παράσχουν διευκρινίσεις, απόψεις και γεγονότα (Bélair-Gagnon, Nelson, & Lewis, 2018).

2.2.2 Μέθοδοι και νέες μορφές Δημοσιογραφίας

Μία νέα μορφή Δημοσιογραφίας που εμφανίστηκε με την ανάπτυξη των ψηφιακών μέσων, είναι η Δημοσιογραφία των κινητών ή όπως είναι διεθνώς αναγνωρίσιμος ο όρος Mobile Journalism (MoJo). Πρόκειται για έναν αναπτυσσόμενο τομέα, στον οποίο οι δημοσιογράφοι χρησιμοποιούν κινητές συσκευές για την επεξεργασία, την αναφορά και τη δημοσίευση ειδήσεων. Αυτού του είδους η Δημοσιογραφία καθιστά τη συλλογή ειδήσεων οικονομικά αποδοτική και γρήγορη, ειδικά σε τοποθεσίες που είναι δύσκολο να προσεγγιστούν με παραδοσιακό εξοπλισμό. Τέλος, όσον αφορά τα ψηφιακά εργαλεία και μέσα έχει παρατηρηθεί ότι συνεισφέρουν στην ταχεία εξακρίβωση των γεγονότων χρησιμοποιώντας διάφορες διαδικτυακές βάσεις δεδομένων, υπηρεσίες επαλήθευσης και εργαλεία ελέγχου γεγονότων (Abosede Olubunmi, 2022).

Στον απόηχο της εξέλιξης των έξυπνων κινητών τηλεφώνων και του MoJo έχει αναπτυχθεί η τάση της συνεχούς ζωντανής ενημέρωσης. Έτσι, οι δημοσιογράφοι καλούνται πλέον να ανταπεξέλθουν σε ένα άκρως ανταγωνιστικό περιβάλλον με μεγάλη πίεση για την κάλυψη γεγονότων με ταχύτητα και ακρίβεια. Στην κατεύθυνση αυτή, ιστοσελίδες με συνεχή ροή νέων πραγματοποιούν συνεχώς ενημερώσεις και λειτουργούν με το μοντέλο 24/7 ούτως ώστε να μην χάνεται καμία ενημέρωση, ακόμα και για το ίδιο θέμα, τροποποιώντας κατάλληλα τα άρθρα τους (Thurman & Walters, 2013). Τα κοινωνικά δίκτυα από τη μεριά τους διαδραματίζουν καθοριστικό ρόλο στην ενημέρωση των πολιτών και πολλές φορές η ροή ειδήσεων και ενημερώσεων λαμβάνει χώρα σε αυτά είτε με τη μορφή αναρτήσεων κειμένου είτε και ακόμα με τη δημοσιοποίηση οπτικοακουστικού υλικού (βίντεο και φωτογραφίες) (Humayun & Ferrucci, 2022). Σύμφωνα με τη μελέτη του Nic Newman (Newman, 2024) το 2023 το 30% των πολιτών ενημερώνονται από τα κοινωνικά δίκτυα. Αυτή η αυξητική τάση επικρατεί τα τελευταία χρόνια καθιστώντας έτσι τα κοινωνικά δίκτυα ως ένα μέσο, το οποίο εξελίσσεται σε έναν κόμβο ενημέρωσης, ψυχαγωγίας, εργασίας και πολλά ακόμη. Στην Εικόνα 3 φαίνεται η εξέλιξη του ποσοστού των ατόμων που ενημερώνονται από τα κοινωνικά δίκτυα σε σχέση με αυτούς που ενημερώνονται από τις δημοσιογραφικές ιστοσελίδες από το 2018 μέχρι και το 2023.



Εικόνα 3. Ποσοστό πολιτών που ενημερώνονται από τα κοινωνικά δίκτυα (μοβ γραμμή) και αυτών που ενημερώνονται από τις δημοσιογραφικές ιστοσελίδες (κυανή γραμμή) (Newman, 2024)

Έτσι, οι δημοσιογράφοι πλέον είναι σχεδόν αναγκασμένοι να παρακολουθούν τα κοινωνικά δίκτυα για τυχόν ειδήσεις που ενδεχομένως να προκύψουν από το περιεχόμενο που αναρτάται συνεχώς αλλά και να ενημερώνουν οι ίδιοι τα κοινωνικά δίκτυα καθώς η απήχηση θα είναι μεγαλύτερη στο ευρύ κοινό. Για το πρώτο σκέλος που αφορά την παρακολούθηση των ενημερώσεων των κοινωνικών δικτύων πλατφόρμες όπως το XPro[3] (πρώην TweetDeck), το Hootsuite[4], κ.α. αποτελούν χρήσιμα εργαλεία για τους δημοσιογράφους καθώς τους επιτρέπουν σε πραγματικό χρόνο να παρακολουθούν σχεδόν το σύνολο των αναρτήσεων στα κοινωνικά δίκτυα αναζητώντας συγκεκριμένες λέξεις κλειδιά ή ξαφνικές ειδήσεις που τις εντοπίζουν λόγω της ταχείας διάδοσής τους στα κοινωνικά δίκτυα.

Μία ακόμα μορφή Δημοσιογραφίας, η οποία ανθίζει και διευκολύνεται με την ανάπτυξη των ψηφιακών τεχνολογιών, είναι η ερευνητική Δημοσιογραφία. Η ερευνητική Δημοσιογραφία εστιάζει στην αποκάλυψη της αλήθειας, όποια και αν είναι αυτή σε ευαίσθητα θέματα κυρίως κοινωνικά, όπως η διαφθορά και η κατάχρηση εξουσίας. Αν και σαν μορφή Δημοσιογραφίας δεν είναι νέα, καθώς υπήρχε από παλαιότερα, τα μέσα και οι μέθοδοι που χρησιμοποιούνται πλέον έχουν αλλάξει ριζικά (Bounegru & Gray, 2021). Πιο συγκεκριμένα, η ραγδαία αύξηση των

[3] https://pro.twitter.com/
[4] https://www.hootsuite.com/platform/integrations

διαθέσιμων δεδομένων λόγω της ψηφιοποίησης σχεδόν όλων των διαδικασιών και των συναλλαγών των πολιτών καθώς και η διαθεσιμότητα ισχυρών εργαλείων ανάλυσης δεδομένων όπως το Microsoft Excel ή και των γλωσσών προγραμματισμού R και Python θέτει τους σύγχρονους δημοσιογράφους σε θέση να ανακαλύψουν μοτίβα και πιθανές συσχετίσεις που χωρίς αυτά θα ήταν υπερβολικά δύσκολο έως και αδύνατο να γίνει (Ausserhofer, Gutounig, Oppermann, Matiasek, & Goldgruber, 2017). Μέσα από αυτές τις αναλύσεις και με τη χρήση αποθετηρίων ανοικτών δεδομένων καθώς και συνεργατικών έργων, όπως το opentender.eu[5], η ερευνητική Δημοσιογραφία αναπτύσσεται και ανθίζει όσο ποτέ άλλοτε. Έτσι, συνδυάζοντας δεδομένα, εργαλεία καθώς και γνώση διαφορετικών ειδικοτήτων, ο δημοσιογράφος μπορεί να ανακαλύψει στοιχεία και να φέρει στο φως ειδήσεις και γεγονότα που παλαιότερα θα ήταν σχεδόν αδύνατο λόγω της πολυπλοκότητας της έρευνας που απαιτείται.

Η πρόσβαση σε ηλεκτρονικούς υπολογιστές και έξυπνα κινητά τηλέφωνα στο μεγαλύτερο κομμάτι του πληθυσμού παγκοσμίως έχει προσδώσει τα απαραίτητα εργαλεία στους δημοσιογράφους να συνοδεύουν την οποιαδήποτε είδηση με εικόνες, βίντεο, ήχο ή κάποια διαδραστικά πολυμέσα (van der Nat, Müller, & Bakker, 2021). Έτσι, πέρα από τα παραδοσιακά οπτικοακουστικά μέσα, πλατφόρμες όπως το Tableau[6], το Flourish[7], το D3.js[8] δίνουν τη δυνατότητα στους δημοσιογράφους να δημιουργήσουν διαδραστικά γραφήματα, χάρτες και γενικά γραφικά που θα κερδίσουν την προσοχή του κοινού. Επιπλέον, η παραγωγή βίντεο και podcasts δρουν ως αρωγός στην προσπάθεια του εκάστοτε δημοσιογράφου να διεισδύσει σε ετερογενή κοινά και να αυξήσει την επιδραστικότητά του (Mihajlov Prokopovic, 2021).

2.3 Προκλήσεις της Νέας Εποχής στη Δημοσιογραφία

2.3.1 Οι απειλές και οι προκλήσεις της ψηφιακής εποχής

Η νέα ψηφιακή εποχή, όπως παρουσιάσθηκε προηγουμένως, έχει επιφέρει ριζικές αλλαγές στη Δημοσιογραφία, δημιουργώντας νέες μορφές αυτής αλλά και

[5] https://opentender.eu/gr?lang=el
[6] https://www.tableau.com/
[7] https://flourish.studio/
[8] https://d3js.org/

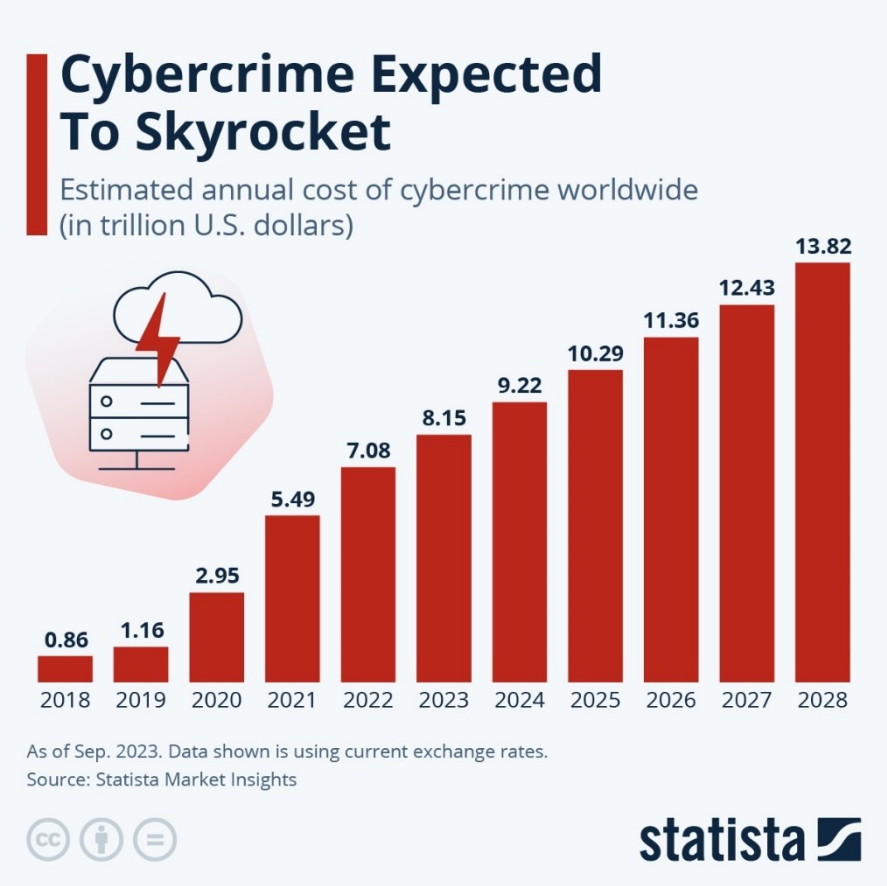
προσφέροντας εργαλεία που βοηθούν τους δημοσιογράφους στην καθημερινότητά τους. Ωστόσο, η εποχή της πληροφορίας έχει δημιουργήσει πολλές προκλήσεις για κάθε επάγγελμα και η Δημοσιογραφία δεν θα μπορούσε να εξαιρεθεί. Η στροφή προς το ψηφιακά μέσα έχει διαταράξει επιπλέον και τα παραδοσιακά μοντέλα εσόδων για τη Δημοσιογραφία, όπως οι πωλήσεις έντυπων και οι διαφημίσεις. Πολλοί ειδησεογραφικοί οργανισμοί βασίζονται πλέον σε ψηφιακές συνδρομές, paywalls και διαφοροποιημένες ροές εσόδων, συμπεριλαμβανομένων εκδηλώσεων και περιεχομένου που χορηγείται. Αυτές οι τεχνολογικές αλλαγές απαιτούν από τους δημοσιογράφους να προσαρμόζουν συνεχώς τις δεξιότητες και τις στρατηγικές τους για να χρησιμοποιούν αποτελεσματικά νέα εργαλεία και πλατφόρμες, διατηρώντας παράλληλα τη δημοσιογραφική τους ακεραιότητα.

Στον απόηχο των τεχνολογικών αλλαγών, η ασφάλεια των πληροφοριών - Information Security (InfoSec) – αποτελεί εδώ και κάποια χρόνια πρωτεύον πεδίο ενδιαφέροντος για τη Δημοσιογραφία, ειδικά μετά τις αποκαλύψεις του Edward Snowden, ενός Αμερικανού τεχνικού της Υπηρεσίας Εθνικής Ασφάλειας (NSA) των ΗΠΑ που έγινε ευρέως γνωστός το 2013 καθώς διέρρευσε απόρρητες πληροφορίες από την κυβέρνηση των ΗΠΑ (Ray, Edward Snowden, 2024). Η υπόθεση ανέδειξε μια σειρά ζητημάτων, όπως η μυστική χρήση της κυβερνητικής εξουσίας, η ιδιωτικότητα στην ψηφιακή εποχή, η ηθική της πληροφορίας και ο ρόλος που μπορούν να παίξουν το Διαδίκτυο και τα ανώνυμα προγράμματα περιήγησης στον σκοτεινό ιστό (dark web) όπως το Tor - σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο - στη διευκόλυνση τέτοιων καταγγελιών (Veglis, 2023; Kaspersky, 2024).

Επιπλέον, οι ανταποκριτές συχνά καταπιάνονται με ευαίσθητες πληροφορίες, καθιστώντας τους ίδιους, στόχους κυβερνοεπιθέσεων. Αυτό μπορεί να περιλαμβάνει ηλεκτρονικό ψάρεμα (phishing), κακόβουλο λογισμικό και απόπειρες παραβίασης των επικοινωνιών τους για την αποκάλυψη πηγών ή μη δημοσιευμένου υλικού. Πολλοί δημοσιογράφοι που ασχολούνται με την ερευνητική Δημοσιογραφία βιώνουν σημαντική παρενόχληση στο Διαδίκτυο, η οποία μπορεί να κλιμακωθεί σε πραγματικές απειλές. Το εξελισσόμενο ψηφιακό τοπίο απαιτεί συνεχή προσαρμογή και επαγρύπνηση, ιδίως όσον αφορά τους νομικούς κινδύνους και την ασφάλεια στον κυβερνοχώρο (Goodwin, Woolbright, & Tomé, 2022).

Πέρα όμως από πρακτικούς κινδύνους που ελλοχεύουν στην ψηφιακή εποχή και αφορούν στην εισροή εσόδων, στην παραβίαση της ιδιωτικότητας αλλά και τεχνικούς κινδύνους όπως η εγκατάσταση κακόβουλου λογισμικού, υπάρχουν και πιο έμμεσοι κίνδυνοι. Οι κίνδυνοι αυτοί συνδέονται άμεσα με την έκρηξη των πληροφοριών και την παραπληροφόρηση είτε αυτή είναι εσκεμμένη είτε ακούσια. Οι δημοσιογράφοι καθημερινά έρχονται σε επαφή με έναν τεράστιο όγκο πληροφοριών, τις οποίες πρέπει να αξιολογούν ώστε να ανακαλύπτουν και να μεταφέρουν τις κατάλληλες ειδήσεις. Πολλές φορές, οι πληροφορίες αυτές είναι λανθασμένες ή ανακριβείς και οδηγούν σε παραπληροφόρηση του κοινού. Δεδομένων λοιπόν των συνθηκών πίεσης για την ταχεία δημοσίευση μιας είδησης, πολλές φορές δεν αφιερώνεται ο κατάλληλος χρόνος για την επαλήθευση αυτών των πληροφοριών (Caled & Silva , 2021). Επιπλέον, όπως αναφέρεται σε έρευνα του MIT, η διάδοση μιας ψευδούς είδησης πολλές φορές «ταξιδεύει» έως και έξι φορές ταχύτερα σε σχέση με μια έγκυρη (Vosoughi, Roy, & Aral, 2018). Αυτό έχει ως αποτέλεσμα, οι ψευδείς ειδήσεις να κατακλύζουν γρήγορα το κοινό δημιουργώντας έτσι λανθασμένες εντυπώσεις. Η έκρηξη αυτή των πληροφοριών, η οποία συνοδεύεται πολλές φορές και από έκρηξη στη μεταφορά ψευδών ειδήσεων, έχει ως αποτέλεσμα στην απώλεια της εμπιστοσύνης του κοινού σε δημοσιογράφους και δημοσιογραφικούς οργανισμούς.

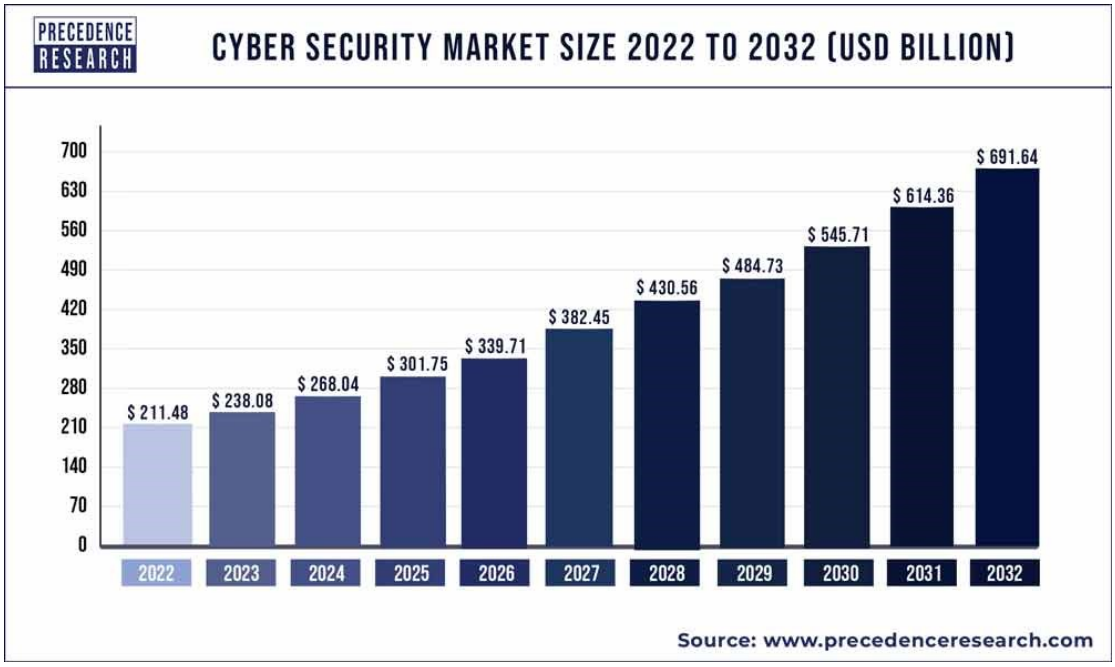
Η ταχύτατη ανάπτυξη των ψηφιακών μέσων συνοδεύεται παράλληλα και με την ταχύτατη αύξηση των ψηφιακών απειλών και επιθέσεων. Η αυξητική αυτή τάση, η οποία απέκτησε σχεδόν εκθετικό ρυθμό αύξησης από την εποχή του Covid-19 μέχρι και σήμερα, προβλέπεται να συνεχισθεί και τα επόμενα 4 χρόνια. Σύμφωνα με το Statista Market Insights, το κόστος σε δολάρια αυτών των επιθέσεων τα επόμενα τέσσερα χρόνια αναμένεται να αυξηθεί από 9,22 τρισεκατομμύρια δολάρια σε 13,82 τρισεκατομμύρια δολάρια σε παγκόσμιο επίπεδο (Fleck, 2024). Η τάση αυτή του κόστος σε δολάρια ανά έτος από το 2018 μέχρι και την πρόβλεψη για το 2028 απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 4. Εκτίμηση κόστους σε δολάρια ανά έτος σε παγκόσμιο επίπεδο (Fleck, 2024)

2.3.2 Αντιμετώπιση των προκλήσεων

Με την ολοένα ταχεία και αναπτυσσόμενη τεχνολογική πρόοδο, όπως παρουσιάσθηκε προηγουμένως, αυξάνονται και οι κίνδυνοι που δημιουργούνται από ψηφιακές απειλές. Ακολουθώντας τους ολοένα αυξανόμενους κινδύνους που υπάρχουν στα ψηφιακά εργαλεία και μέσα, η αγορά που αφορά λύσεις κυβερνοασφάλειας, κερδίζει όλο και περισσότερα έσοδα και ενδιαφέρον σε παγκόσμιο επίπεδο. Σύμφωνα με την έκθεση από το Precedence Research αναμένεται το 2032 τα έσοδα της αγοράς που αφορούν την κυβερνοασφάλεια να φτάσουν τα 691,64 δισεκατομμύρια δολάρια σε παγκόσμιο επίπεδο (Precedence Research, 2023). Η αυξητική τάση αυτή και η πρόβλεψη απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 5. Μέγεθος αγοράς σε δισεκατομμύρια δολάρια στον τομέα της κυβερνοασφάλειας από το 2022 έως το 2032 (Precedence Research, 2023)

Η Δημοσιογραφία ακολουθεί αυτή την τάση αυξανόμενου ενδιαφέροντος στις λύσεις κυβερνοασφάλειας. Έτσι, οι δημοσιογράφοι επιδεικνύουν πλέον ιδιαίτερο ενδιαφέρον στην εξεύρεση λύσεων προκειμένου να προστατεύσουν την εργασία τους και κυρίως τις πηγές τους. Πιο συγκεκριμένα, και λαμβάνοντας υπόψη τις περιπτώσεις παραβίασης της ιδιωτικότητας - όπως στην υπόθεση του Edward Snowden - η χρήση και η υιοθέτηση ισχυρών εργαλείων κρυπτογράφησης για τους σκοπούς της επικοινωνίας έχει καταστεί επείγον και επιτακτικό ζήτημα για δημοσιογράφους σε όλο τον κόσμο (Veglis, 2023; Di Salvo, 2022).

Οι δημοσιογράφοι πλέον χρησιμοποιούν κατά κόρον ηλεκτρονικούς υπολογιστές, έξυπνα κινητά τηλέφωνα και tablets για την καταγραφή, συγγραφή και δημοσίευση ειδήσεων. Έτσι, πέρα από την κρυπτογράφηση στις επικοινωνίες τους, που αποτελεί βασικό εργαλείο σε ανταλλαγή ηλεκτρονικών μηνυμάτων οποιασδήποτε μορφής, υπάρχουν και άλλα τεχνικά μέσα και μέθοδοι που μπορούν να επωφεληθούν οι δημοσιογράφοι ώστε να εξασφαλίσουν την προστασία των επικοινωνιών τους. Πιο συγκεκριμένα, τα Εικονικά Ιδιωτικά Δίκτυα – Virtual Private Networks (VPNs) - προστατεύουν την έκθεση των ηλεκτρονικών συσκευών στο Διαδίκτυο. Μέσω αυτών, ο χρήστης αποκρύπτει στοιχεία του όπως η κίνηση των δεδομένων του, η διαδικτυακή του διεύθυνση IP αλλά μπορεί και να συνδεθεί απομακρυσμένα και με

ασφάλεια σε ένα ιδιωτικό δίκτυο, όπως για παράδειγμα του οργανισμού του ή του χώρου εργασίας του. Επιπλέον, όλοι οι χρήστες συσκευών που είναι διασυνδεδεμένες στο Διαδίκτυο οφείλουν να έχουν τις συσκευές ενημερωμένες με τις τελευταίες εκδόσεις λογισμικού έτσι ώστε να διαθέτουν τη μέγιστη δυνατή προστασία από τυχόν κενά ασφαλείας. Στην κατεύθυνση αυτή, πέρα από τα ενημερωμένα με τις τελευταίες εκδόσεις τους (λειτουργικές ενημερώσεις και ενημερώσεις ασφαλείας) λογισμικά συστήματα, υπάρχουν και λειτουργικά συστήματα (Tails OS[9], Debian OS[10], Kali Linux[11], Linux OS[12], κ.α.), τα οποία προσφέρουν επιπλέον ασφάλεια και προστασία και προτείνονται σε όσους εργάζονται με ευαίσθητα δεδομένα που δεν πρέπει να διαρρεύσουν, όπως οι δημοσιογράφοι (Veglis, 2023). Επιπλέον αυτών, η δικτυακή ασφάλεια απαιτεί τη δημιουργία ασφαλών δικτύων με κατάλληλη προστασία, ρυθμίζοντας τείχη προστασίας (firewalls), έλεγχο πρόσβασης (access control) καθώς και διάφορα φίλτρα επιτήρησης της δικτυακής κίνησης (π.χ. SPAM filters, ransomware protection, κ.α.) (Oluwafemi Olaoye & Adedokun, 2023).

Στον απόηχο όλων αυτών των ραγδαίων εξελίξεων και αλλαγών αλλά και των προκλήσεων που παρουσιάσθηκαν, πέρα από τα τεχνικά μέσα, κρίθηκε απαραίτητη και η προσαρμογή των νομικών πλαισίων. Έτσι, σε πολλές χώρες, -συμπεριλαμβανομένης της Ελλάδας- το ψηφιακό περιεχόμενο υπόκειται σε αυστηρούς κανονισμούς στους οποίους καλούνται να συμμορφωθούν όλοι όσοι παράγουν και μεταδίδουν ψηφιακό περιεχόμενο οποιασδήποτε μορφής. Θεμέλιος λίθος της τρέχουσας νομοθεσίας είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, ο οποίος καθορίζει τον τρόπο με τον οποίο τα προσωπικά δεδομένα μπορούν να χρησιμοποιηθούν συμπεριλαμβανομένου και του κλάδου της Δημοσιογραφίας (ΕυρωπαΪκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016). Στην Ελλάδα, σύμφωνα με τον Νόμο 4624/2019 που δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως στις 29 Αυγούστου 2019, οι δημοσιογράφοι πρέπει να τηρούν τις ισχύουσες διατάξεις και τους κανονισμούς όταν χειρίζονται προσωπικές πληροφορίες (Αρχή Προστασίας Δεδομένων Προσωπικού

[9] https://tails.net
[10] https://www.debian.org
[11] https://www.kali.org
[12] https://www.linux.org

Χαρακτήρα, 2019). Επιπλέον της προστασίας των προσωπικών δεδομένων, το ψηφιακό περιεχόμενο υπόκειται επίσης στους νόμους περί πνευματικής ιδιοκτησίας. Οι δημοσιογράφοι πρέπει να διασφαλίζουν ότι το περιεχόμενο που χρησιμοποιούν ή παράγουν δεν παραβιάζει τους νόμους περί πνευματικών δικαιωμάτων, οι οποίοι επιβάλλονται αυστηρά στην Ελλάδα και την ΕΕ. Στην Ελλάδα θεμελιώδης νόμος για την πνευματική ιδιοκτησία ή πνευματικά δικαιώματα είναι πλέον ο νόμος 4996/2022 (ΦΕΚ Α'218, 24/11/2022) (Ελληνική Δημοκρατία (α), 2022). Η εγχώρια νομοθεσία παρέχει ένα πλαίσιο που μπορεί να προστατεύσει αλλά και να περιορίσει τη δημοσιογραφική δραστηριότητα. Το αυστηρό νομικό πλαίσιο τόσο σε εγχώριο όσο και σε ευρωπαϊκό επίπεδο σχετικά με το ψηφιακό περιεχόμενο, μπορεί να επιφέρει ποινικές κυρώσεις, συμπεριλαμβανομένης της φυλάκισης και των προστίμων, καθιστώντας τους δημοσιογράφους υπόλογους σχετικά με τις πληροφορίες που δημοσιεύουν στο Διαδίκτυο.

Με την αυξανόμενη ανάγκη προστασίας των εμπιστευτικών πληροφοριών, οι δημοσιογράφοι πρέπει να είναι ικανοί στη χρήση ψηφιακών εργαλείων που διασφαλίζουν την ασφάλεια και την αξιοπιστία των δεδομένων τους. Οφείλουν επαγγελματικά να είναι εξοπλισμένοι με γνώσεις και εργαλεία για να αντιμετωπίζουν αποτελεσματικά αυτές τις απειλές, διατηρώντας παράλληλα το επίπεδο ηθικής τους ακέραιο και προστατεύοντας τις πηγές τους και τον εαυτό τους.

2.4 Πληροφοριοδότες στη Δημοσιογραφία

Οι ριζικές αλλαγές, οι προκλήσεις, τα νέα εργαλεία αλλά και το νομικό πλαίσιο της σύγχρονης εποχής έχουν επηρεάσει σε σημαντικό βαθμό και την έννοια της ασφάλειας, η οποία πλέον έγκειται κυρίως στον ψηφιακό κόσμο αλλά και τον ρόλο των πληροφοριοδοτών ή whistleblowers, όπως είναι διεθνώς γνωστοί.

2.4.1 Ο ρόλος των πληροφοριοδοτών, οι προκλήσεις και οι απειλές

Οι πληροφοριοδότες διαδραματίζουν σημαντικό ρόλο στη Δημοσιογραφία καθώς πολλές φορές αποκαλύπτουν γεγονότα και πληροφορίες που αφορούν τη διαφθορά, την κατάχρηση εξουσίας ή τα κακώς κείμενα ισχυρών ατόμων ή οργανισμών στην κοινωνία που διαφορετικά θα έμεναν κρυφά. Έτσι, η συνεισφορά τους είναι καθοριστικής σημασίας σε κάθε κοινωνία καθώς λειτουργούν ως ρυθμιστικοί παράγοντες. Πιο συγκεκριμένα, οι πληροφοριοδότες συμβάλλουν στη διαφάνεια και

την απόδοση ευθυνών καθώς αποκαλύπτουν γεγονότα που πολλές φορές αφορούν σημαίνοντα πρόσωπα και οργανισμούς. Επίσης, η δράση τους συνήθως είναι συνυφασμένη με το κοινό συμφέρον καθώς οι πληροφορίες που παρέχουν, επωφελούν την κοινωνία ως σύνολο με τον όποιο κίνδυνο μπορεί αυτό να συνεπάγεται για τους ίδιους τους πληροφοριοδότες (Kleinig, 2024; Ryle, 2018). Η δράση τους λοιπόν αυτή τους καθιστά καταλύτες σε σημαντικές αλλαγές που μπορούν να επέλθουν σε μια κοινωνία είτε αυτές έχουν να κάνουν με τον ανασχηματισμό της είτε με την πολιτική.

Η δράση των πληροφοριοδοτών έχει ως αποτέλεσμα να αντιμετωπίζουν αρκετούς κινδύνους τόσο σε νομικό επίπεδο, όσο και σε προσωπικό, εργασιακό αλλά και ψυχολογικό (Anvari, Wenzel, Woodyatt, & Haslam, 2019). Πολλές φορές η αποκάλυψη πληροφοριών οδηγεί επίσης και στην παραβίαση προσωπικών και ευαίσθητων δεδομένων με αποτέλεσμα ο πληροφοριοδότης να διώκεται ποινικά με κατηγορίες που αφορούν κατασκοπεία, κλοπή ή διαρροή απόρρητων πληροφοριών όπως τις περιπτώσεις του Edward Snowden (Ray, Edward Snowden, 2024) και της Chelsea Manning (Ray, Chelsea Manning: United States Army intelligence analyst, 2024). Επίσης, όταν οι πληροφορίες αφορούν εταιρικά δεδομένα είναι πολύ πιθανό ένας πληροφοριοδότης να κατηγορηθεί για παραβίαση της εμπιστευτικότητας ή του συμβολαίου του με αποτέλεσμα να οδηγηθεί στη δικαιοσύνη με βαρύτατες συνέπειες. Οι προεκτάσεις όμως των συνεπειών πολλές φορές δεν περιορίζονται μόνο σε νομικό επίπεδο αλλά και σε εργασιακό. Έτσι, δεν είναι απίθανο πολλές φορές ένας πληροφοριοδότης που θα αποκαλυφθεί η ταυτότητά του να αντιμετωπίσει αντίποινα σε επαγγελματικό επίπεδο όπως απόλυση, επιβλαβή φήμη και γενικότερα απομόνωση και καταστροφή της καριέρας του/της. Ένα βήμα παραπέρα, υπάρχουν ακραίες περιπτώσεις που πληροφοριοδότες παρακολουθούνται και ενδεχομένως να δέχονται απειλές ακόμα και για την ίδια τους τη ζωή (HR future, 2024). Όλα τα παραπάνω έχουν ως αποτέλεσμα οι πληροφοριοδότες να έχουν ψυχολογικές συνέπειες στην καθημερινότητά τους και να έρχονται αντιμέτωποι με καταστάσεις άγχους και πίεσης για τις κυρώσεις που ενδεχομένως να έρθουν μετά την αποκάλυψη συγκεκριμένων πληροφοριών και εφόσον η ταυτότητά τους αποκαλυφθεί. Σε πιο σοβαρές περιπτώσεις, δεν αποκλείεται να εμφανίσουν και μορφές κατάθλιψης και απομόνωσης (van der Velden, Pecoraro, Houwerzijl, & van der Meulen, 2019).

Οι απειλές και οι προκλήσεις που αντιμετωπίζουν οι πληροφοριοδότες και οι δημοσιογράφοι λόγω της ψηφιοποίησης της σύγχρονης εποχής είναι ποικίλες και συχνά μπορούν να οδηγήσουν σε παραβίαση της εμπιστευτικότητας ή ακόμα και της ασφάλειας τόσο των πληροφοριών όσο των ίδιων των ατόμων. Μια βασική απειλή στην ψηφιακή εποχή είναι ότι πλέον η παρακολούθηση των ηλεκτρονικών επικοινωνιών και της ανταλλαγής πληροφοριών είναι πιο εύκολη από ποτέ. Έτσι, ιδιωτικές εταιρείες ή ακόμα και κυβερνήσεις πολλές φορές χρησιμοποιώντας διάφορες προφάσεις όπως η εσωτερική ασφάλεια, η παρακολούθηση της συμπεριφοράς του καταναλωτικού κοινού κ.α. έχουν πρόσβαση και παρακολουθούν τις επικοινωνίες με αποτέλεσμα πολλές φορές να αποκτούν πρόσβαση σε ευαίσθητες πληροφορίες και προσωπικά δεδομένα, τα οποία μπορούν να οδηγήσουν σε ταυτοποίηση προσώπων και ενδεχομένως σε δυσάρεστες συνέπειες για αυτά (Townend & Danbury, 2017). Πέρα όμως από τον κίνδυνο της παρακολούθησης λόγω συμφερόντων που υπάρχουν, οι δημοσιογράφοι και οι πληροφοριοδότες αποτελούν πόλο έλξης και στόχο για επίδοξους hackers, οι οποίοι με διάφορα μέσα και μεθόδους όπως phishing, ransomware, κ.α. αποσκοπούν στο να αποκτήσουν πρόσβαση σε προσωπικές ή εμπιστευτικές πληροφορίες τις οποίες θα μπορούσαν να εκμεταλλευτούν προς όφελός τους (Deibert, 2017).

2.4.2 Χαρακτηριστικές περιπτώσεις πληροφοριοδοτών

2.4.2.1 Chelsea Manning

Η Chelsea Manning, πρώην αναλύτρια πληροφοριών του Στρατού των Ηνωμένων Πολιτειών της Αμερικής, έγινε γνωστή το 2010, όταν διέρρευσε ένα τεράστιο πλήθος απόρρητων στρατιωτικών εγγράφων στο WikiLeaks[13]. Αυτά τα έγγραφα, γνωστά αργότερα ως Ημερολόγια Πολέμου του Ιράκ και Αφγανικό Ημερολόγιο Πολέμου, περιελάμβαναν ευαίσθητες πληροφορίες σχετικά με τις επιχειρήσεις του στρατού των ΗΠΑ στο Ιράκ και το Αφγανιστάν, αποκαλύπτοντας περιπτώσεις απωλειών αμάχων, φιλικά πυρά και άλλες αμφιλεγόμενες ενέργειες. Επιπλέον, η Manning κυκλοφόρησε μια σειρά από διπλωματικά τηλεγραφήματα των ΗΠΑ, τα οποία παρείχαν μια άνευ προηγουμένου ματιά στις εσωτερικές λειτουργίες της αμερικάνικης διπλωματίας. Η πιο αξιοσημείωτη δημοσίευση ήταν το βίντεο "Collateral Murder", το οποίο

[13] https://wikileaks.org

απεικόνιζε μια επίθεση με ελικόπτερο των ΗΠΑ στη Βαγδάτη με πολλά θύματα, συμπεριλαμβανομένων δύο δημοσιογράφων του Reuters. Οι διαρροές της Manning πυροδότησαν εκτεταμένη συζήτηση σχετικά με τη διαφάνεια της κυβέρνησης, τη στρατιωτική ηθική και τη μεταχείριση των πληροφοριοδοτών (Ray, Chelsea Manning: United States Army intelligence analyst, 2024).

Οι επιπτώσεις για τη Chelsea Manning ήταν άμεσες και σοβαρές. Το 2010, συνελήφθη και κατηγορήθηκε για 22 αδικήματα, συμπεριλαμβανομένης της παροχής βοήθειας στον εχθρό, μια κατηγορία που μπορεί να την οδηγούσε να καταδικαστεί σε θάνατο. Τελικά, καταδικάστηκε σε 35 χρόνια φυλάκιση, τη μεγαλύτερη ποινή που επιβλήθηκε ποτέ για διαρροή πληροφοριών της κυβέρνησης των ΗΠΑ στα μέσα ενημέρωσης. Η μεταχείρισή της κατά τη διάρκεια του προδικαστικού περιορισμού προκάλεσε σημαντική κριτική από οργανώσεις ανθρωπίνων δικαιωμάτων και ομάδες υπεράσπισης. Κρατήθηκε στην απομόνωση για μεγάλα χρονικά διαστήματα, οδηγώντας σε καταγγελίες για απάνθρωπη μεταχείριση. Τον Ιανουάριο του 2017, αφού εξέτισε επτά χρόνια, η ποινή της Manning τροποποιήθηκε από τον Πρόεδρο Barack Obama σε μία από τις τελευταίες του πράξεις στην εξουσία, επιτρέποντάς της να αποφυλακισθεί τον Μάιο του 2017 (BBC, 2017).

Η υπόθεση της Manning είχε βαθύ αντίκτυπο στον δημόσιο διάλογο σχετικά με τη διαφάνεια της κυβέρνησης και τα δικαιώματα των πληροφοριοδοτών. Επιπλέον, επεσήμανε τις σκληρές ποινές που αντιμετωπίζουν όσοι αποκαλύπτουν κυβερνητικές πληροφορίες και πυροδότησε μια ευρύτερη συζήτηση σχετικά με την ισορροπία μεταξύ της εθνικής ασφάλειας και του δικαιώματος του κοινού στη γνώση. Η Manning έγινε από τότε υπέρμαχος της διαφάνειας, της κυβερνητικής λογοδοσίας και των δικαιωμάτων. Η υπόθεσή της συνεχίζει να χρησιμεύει ως σημείο αναφοράς σε συζητήσεις σχετικά με την ηθική της καταγγελίας, τη μεταχείριση ατόμων υπό κρατική κράτηση και τον ρόλο των μέσων ενημέρωσης στον έλεγχο της εξουσίας (Munro, 2018).

2.4.2.2 Edward Snowden

Ο Edward Snowden, πρώην συνεργάτης της Υπηρεσίας Εθνικής Ασφάλειας της Αμερικής (NSA), έγινε παγκοσμίως γνωστός το 2013, όταν διέθεσε απόρρητες πληροφορίες της NSA που αφορούσαν δραστηριότητες παρακολούθησης. Οι αποκαλύψεις του Snowden κατέδειξαν την ύπαρξη πολυάριθμων προγραμμάτων

παγκόσμιας επιτήρησης και παρακολούθησης, πολλά από τα οποία χρησιμοποιούνται από την ίδια την NSA και συνεργαζόμενες εταιρείες τηλεπικοινωνιών, με την υποστήριξη των ευρωπαϊκών κυβερνήσεων. Τα έγγραφα που διέρρευσαν αποκαλύπτουν ότι η NSA είχε τη δυνατότητα να παρακολουθεί και να συλλέγει τεράστιες ποσότητες δεδομένων τόσο από τις εγχώριες όσο και από τις διεθνείς επικοινωνίες, συμπεριλαμβανομένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails), των τηλεφωνικών κλήσεων και της δραστηριότητας στο Διαδίκτυο, συχνά χωρίς εντάλματα. Οι αποκαλύψεις του Snowden πυροδότησαν μια παγκόσμια συζήτηση για την ιδιωτική ζωή, την επιτήρηση της κυβέρνησης και την ισορροπία μεταξύ εθνικής ασφάλειας και ατομικών ελευθεριών (Greenwald, 2014).

Ο αντίκτυπος των διαρροών του Snowden ήταν βαθύς και πολύπλευρος. Στις ΗΠΑ, οδήγησε σε σημαντική δημόσια κατακραυγή και την απαίτηση για μεγαλύτερη διαφάνεια και εποπτεία των υπηρεσιών πληροφοριών. Οι αποκαλύψεις του οδήγησαν σε αρκετές νομικές προκλήσεις και επανεξέταση των νόμων επιτήρησης και παρακολούθησης στις Ηνωμένες Πολιτείες Αμερικής, με αποκορύφωμα τη θέσπιση του νόμου περί ελευθερίας των ΗΠΑ το 2015 (US Congress, 2015), γεγονός που αποσκοπούσε να περιορίσει ορισμένες από τις πρακτικές ανεξέλεγκτης συλλογής δεδομένων της NSA. Σε παγκόσμιο επίπεδο, οι αποκαλύψεις του Snowden δημιούργησαν τριβές στις διπλωματικές σχέσεις μεταξύ των Ηνωμένων Πολιτειών Αμερικής και των συμμάχων τους, πολλοί από τους οποίους εμπλέκονταν στις δραστηριότητες παρακολούθησης. Επιπλέον, οι διαρροές προκάλεσαν έναν παγκόσμιο διάλογο και προβληματισμό για την ψηφιακή ιδιωτικότητα και τις ηθικές επιπτώσεις της κυβερνητικής επιτήρησης, επηρεάζοντας τις εταιρείες τεχνολογίας να υιοθετήσουν ισχυρότερες πρακτικές κρυπτογράφησης για την προστασία των δεδομένων των χρηστών.

Σε προσωπικό επίπεδο, ο Edward Snowden ήρθε αντιμέτωπος με βαρύτατες συνέπειες. Μετά τις διαρροές, κατηγορήθηκε για πολλαπλά κακουργήματα βάσει του νόμου περί κατασκοπείας, συμπεριλαμβανομένης της κλοπής της κυβερνητικής περιουσίας και της μη εξουσιοδοτημένης επικοινωνίας των ευαίσθητων εθνικών πληροφοριών. Αντιμετωπίζοντας επικείμενη σύλληψη (Younger, 2020), ο Snowden έφυγε στο Χονγκ Κονγκ και στη συνέχεια έλαβε άσυλο στη Ρωσία, όπου παραμένει μέχρι και σήμερα. Ζώντας στην εξορία, ο Snowden εξακολουθεί να αποτελεί ένθερμο

υποστηρικτή για τη διαφάνεια και τα δικαιώματα ιδιωτικής ζωής, συχνά παραθέτοντας τις απόψεις του που σχετίζονται με την επιτήρηση της κυβέρνησης και τις πολιτικές ελευθερίες ακόμα και την TN (Roytburg, 2024). Η περίπτωσή του παραμένει ένα από τα σημαντικότερα γεγονότα καταγγελίας στη σύγχρονη ιστορία, υπογραμμίζοντας την πολύπλοκη αλληλεπίδραση μεταξύ της κρατικής ασφάλειας και της ατομικής ιδιωτικής ζωής στην ψηφιακή εποχή.

2.4.2.3 Panama papers

Τα έγγραφα του Παναμά ή Panama papers, όπως είναι παγκοσμίως γνωστά, είναι μία από τις σημαντικότερες και πιο μεγάλες διαρροές οικονομικών δεδομένων στην ιστορία, αποκαλύπτοντας την εκτεταμένη χρήση υπεράκτιων φορολογικών τοποθεσιών (offshore tax havens) από τους πλέον πλούσιους και ισχυρούς παγκοσμίως προκειμένου να αποκρύψουν τα περιουσιακά τους στοιχεία. Τα συγκεκριμένα έγγραφα κυκλοφόρησαν τον Απρίλιο του 2016 από τη Διεθνή Κοινοπραξία Διερευνητικών Δημοσιογράφων (International Consortium of Investigative Journalists, ICIJ). Τα έγγραφα του Παναμά περιείχαν 11,5 εκατομμύρια έγγραφα από τη δικηγορική εταιρεία του Παναμά Mossack Fonseca & Co και περιέγραφαν λεπτομερώς τις οικονομικές δραστηριότητες περισσότερων από 214.000 υπεράκτιων οντοτήτων. Η διαρροή αυτή εξέθεσε τον κρυμμένο πλούτο των πολιτικών, των δημόσιων υπαλλήλων, των επιχειρηματικών ηγετών και των διασημοτήτων, αποκαλύπτοντας έναν σύνθετο ιστό φοροδιαφυγής, νομιμοποίηση εσόδων από παράνομες δραστηριότητες και διαφθορά που συνέβαινε σε όλο τον κόσμο (Harding, 2016).

Οι αποκαλύψεις από τα έγγραφα του Παναμά είχαν βαθιές επιπτώσεις τόσο σε παγκόσμια όσο και σε εγχώρια κλίμακα. Σε πολιτικό επίπεδο εμπλέκονταν πρόσωπα υψηλού προφίλ, συμπεριλαμβανομένου του τότε υπουργού της Ισλανδίας Sigmundur Davíð Gunnlaugsson, ο οποίος παραιτήθηκε μετά από τις διαρροές. Άλλα αξιοσημείωτα στοιχεία που αναφέρονταν στα έγγραφα περιελάμβαναν συνεργάτες του Ρώσου Προέδρου Vladimir Putin, μέλη της οικογένειας του Κινέζου πρωθυπουργού Li Keqiang και πολλούς πολιτικούς από το Ηνωμένο Βασίλειο, την Αργεντινή, την Ουκρανία ακόμα και την Ελλάδα καθώς και άλλες χώρες (Lusher, 2016). Οι διαρροές προκάλεσαν τη δημόσια οργή και οδήγησαν σε έρευνες με

ζητούμενο περισσότερη διαφάνεια καθώς και μεταρρυθμίσεις στα χρηματοπιστωτικά συστήματα για την πρόληψη αντίστοιχων καταχρήσεων.

Σε οικονομικό επίπεδο, τα έγγραφα του Παναμά ανέδειξαν συστημικά ζητήματα στο παγκόσμιο χρηματοπιστωτικό σύστημα που επιτρέπουν τη δημιουργία και τη διατήρηση των υπεράκτιων φορολογικών εδρών. Τέτοιου είδους δραστηριότητες πολλές φορές προσφέρουν μυστικότητα και ευνοϊκές φορολογικές συνθήκες, επιτρέποντας σε άτομα και εταιρείες να αποφεύγουν τους φόρους και τους κανονισμούς στις χώρες τους. Οι αντιδράσεις που προκλήθηκαν από τις διαρροές οδήγησαν σε αυξημένο έλεγχο της χρηματοδότησης των offshore εταιρειών, προτρέποντας τις κυβερνήσεις και τους διεθνείς οργανισμούς να εφαρμόσουν αυστηρότερους κανονισμούς και να περιορίσουν τις παράνομες/παράτυπες οικονομικές δραστηριότητες. Τα έγγραφα του Παναμά όχι μόνο αποκάλυψαν ατοπήματα σε ατομικό επίπεδο, αλλά υπογράμμισαν κυρίως την ανάγκη για μια ισχυρή παγκόσμια συνεργασία σχετικά με την αντιμετώπιση των προκλήσεων που θέτει η οικονομική μυστικότητα και την εξασφάλιση ενός πιο διαφανούς και δίκαιου χρηματοπιστωτικού συστήματος (Fitzgibbon & Hudson, 2021).

2.4.3 Μέτρα για την προστασία των πληροφοριοδοτών

Λόγω της ευαίσθητης και επικίνδυνης φύσης της δραστηριότητας των πληροφοριοδοτών είναι επιτακτική ανάγκη να υπάρχουν μέτρα για την προστασία τους. Τα μέτρα αυτά μπορούν να είναι σε επίπεδο νομικό, οργανισμών και τεχνολογικά. Σε νομικό επίπεδο η προστασία των πληροφοριοδοτών έγκειται στο κομμάτι της ελευθερίας του λόγου αλλά και στην προστασία της ιδιωτικότητας. Όπως, παρουσιάσθηκε στο κεφάλαιο 2.3.2, η αντιμετώπιση των προκλήσεων στην ψηφιακή εποχή επαφίεται σε νομικό επίπεδο με τη θέσπιση μέτρων και νόμων που αφορούν την προστασία της ιδιωτικότητας – όπως το GDPR – και την ελευθερία του λόγου. Πιο συγκεκριμένα στην Ελλάδα, ο Νόμος 4990/2022 διασφαλίζει ένα ολοκληρωμένο πλαίσιο προστασίας για τα πρόσωπα που αναφέρουν παραβιάσεις του ενωσιακού δικαίου – του δικαίου της Ευρωπαϊκής Ένωσης - το οποίο περιλαμβάνει ένα σύνολο νομικών κανόνων και αρχών που καθορίζουν τη λειτουργία και τις εξουσίες της Ευρωπαϊκής Ένωσης (Ελληνική Δημοκρατία (β), 2022). Πέρα όμως από αυτό, επιβάλλεται σε επίπεδο εταιρικό και οργανισμών να υποστηρίζονται μέτρα και πολιτικές που προστατεύουν τους πληροφοριοδότες όπως πολιτική για να μην

υπάρχουν αντίποινα ακόμα και εντός ενός οργανισμού ούτως ώστε οποιοσδήποτε να μπορεί να εκφραστεί ελεύθερα αλλά και την ύπαρξη μηχανισμών υποστήριξης όταν απαιτείται. Οι μηχανισμοί αυτοί μπορούν να αφορούν τη νομική, οικονομική αλλά και ψυχολογική υποστήριξη ατόμων που παρέχουν πληροφορίες και ενδεχομένως να αντιμετωπίσουν εχθρική συμπεριφορά από αυτούς που θίγονται τα συμφέροντά τους. Στην Ελλάδα αποτελεί μια πολύ αξιόλογη προσπάθεια προς την κατεύθυνση αυτή η Τεχνική Έκθεση για την Προστασία των Πληροφοριοδοτών που ενεργούν προς το Δημόσιο Συμφέρον. Η συγκεκριμένη έκθεση έχει συνταχθεί από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) και περιλαμβάνει 56 συστάσεις που βασίζονται σε καλές πρακτικές άλλων κρατών μελών του ΟΟΣΑ. Οι προτάσεις αυτές αποσκοπούν στη δημιουργία ενός ευνοϊκού περιβάλλοντος για τους πληροφοριοδότες προκείμενου να καταγγέλλουν τα κακώς κείμενα που ζημιώνουν το κοινό συμφέρον (ΟΟΣΑ, 2020).

Κορωνίδα όμως των μέτρων και των μέσων που αφορούν την προστασία των πληροφοριοδοτών είναι τα τεχνολογικά και τεχνικά μέσα που έχουν στη φαρέτρα τους προκειμένου να είναι ασφαλείς. Μια χαρτογράφηση των μέσων αυτών παρουσιάσθηκε στο κεφάλαιο 2.3.2. Τα μέσα αυτά όπως VPN, ασφαλή λειτουργικά συστήματα, ενημερώσεις λογισμικού κ.α. αποτελούν βασικά εργαλεία για την ασφαλή ανταλλαγή πληροφοριών. Ένα από τα βασικά αυτά εργαλεία που χρησιμοποιούν οι πληροφοριοδότες είναι οι πλατφόρμες ασφαλούς επικοινωνίας, οι οποίες αποτελούν και το βασικό αντικείμενο της παρούσας εργασίας. Τα βασικά χαρακτηριστικά τους και πολλές από τις ίδιες τις πλατφόρμες παρουσιάζονται με λεπτομέρεια στο επόμενο κεφάλαιο. Βασικός λόγος για τον οποίο οι δημοσιογράφοι και οι πληροφοριοδότες τους χρειάζονται τεχνολογίες και εργαλεία για την ασφαλή τους επικοινωνία είναι η προστασία και η ανωνυμία τους.

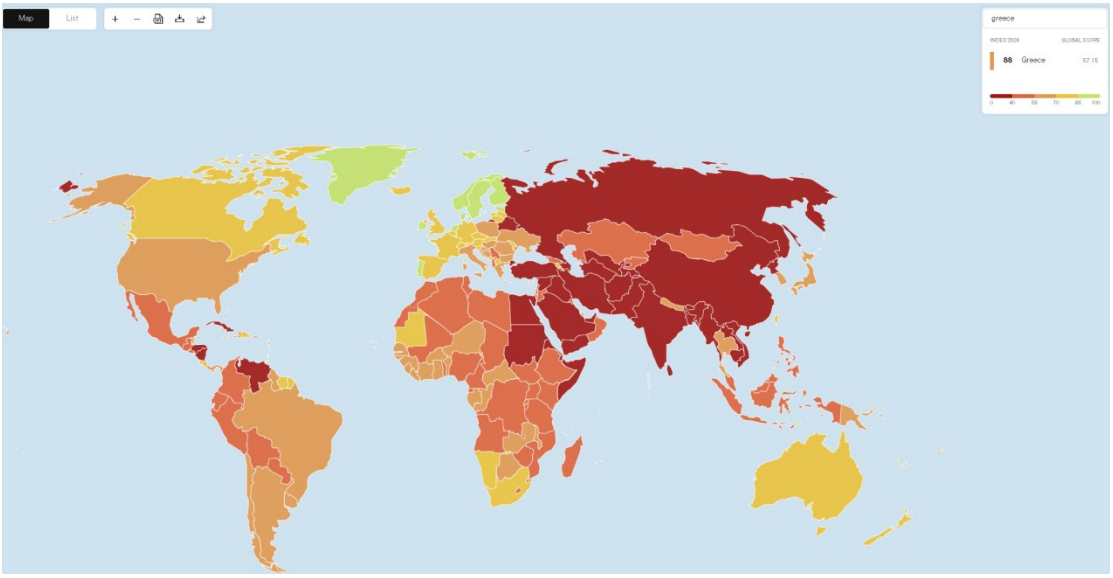
3 Πλατφόρμες Ασφαλούς Επικοινωνίας

3.1 Γενικά Στοιχεία

Σε μια εποχή όπου οι πληροφορίες είναι ταυτόχρονα ένα ισχυρό εργαλείο αλλά και ένα τρωτό σημείο, οι πλατφόρμες ασφαλούς επικοινωνίας αποτελούν βασικό μέσο και εργαλείο για τους δημοσιογράφους αλλά και τους πληροφοριοδότες. Η ψηφιακή εποχή, όπως παρουσιάσθηκε και στο προηγούμενο κεφάλαιο έχει αλλάξει άρδην την επικοινωνία και έχει φέρει σημαντικές αλλαγές στη Δημοσιογραφία στο σύνολό της. Αυτό όμως, όπως ήδη παρουσιάσθηκε, έχει επιφέρει και νέους κινδύνους και απειλές για τους δημοσιογράφους όπως παρακολούθηση και παραβίαση δεδομένων. Αυτό έχει ως αποτέλεσμα να θέτουν σε κίνδυνο την εμπιστευτικότητα των πηγών και την ακεραιότητα των ευαίσθητων πληροφοριών. Ως απάντηση σε αυτές τις απειλές και προκειμένου να θωρακισθούν όσο το δυνατόν απέναντί τους, οι δημοσιογράφοι βασίζονται όλο και περισσότερο σε πλατφόρμες ασφαλούς επικοινωνίας, οι οποίες προσφέρουν ισχυρή κρυπτογράφηση, ανωνυμία καθώς και άλλα προηγμένα χαρακτηριστικά ασφαλείας. Αυτά τα εργαλεία όχι μόνο προστατεύουν τους ίδιους τους δημοσιογράφους, αλλά προστατεύουν και τις πηγές τους, διασφαλίζοντας με αυτόν τον τρόπο την ελεύθερη ροή πληροφοριών σε ένα τοπίο γεμάτο με ψηφιακούς κινδύνους (Internet Society, 2022; Abellán, 2021).

Η ασφαλής επικοινωνία και ειδικότερα στον τομέα της Δημοσιογραφίας είναι υψίστης σημασίας. Σε αρκετές χώρες ανά τον κόσμο, οι δημοσιογράφοι αντιμετωπίζουν συνεχείς απειλές από αυταρχικά καθεστώτα, εγκληματικές οργανώσεις, ακόμη και εταιρικές οντότητες που επιδιώκουν να ελέγξουν ή να καταστείλουν ρεπορτάζ που ενδεχομένως θίγουν συγκεκριμένα συμφέροντα. Χαρακτηριστικά παραδείγματα αποτελούν η Κίνα και το Χονγκ Κονγκ, τα οποία όπως αναφέρεται στη μελέτη του Tsui, (Tsui, The importance of digital security to securing press freedom, 2018) το 2018 κατατάσσονταν 176 και 70 στους 180 αντίστοιχα. Σύμφωνα με τον ιστότοπο Reporters without borders στην κατάταξη για την ελευθερία του Τύπου, η Ελλάδα βρίσκεται στην 88η θέση ενώ το 2023 ήταν στην 107η αντίστοιχα η Κίνα βρίσκεται πλέον στην 172η θέση και προηγείται μόνο των χωρών Μπαχρέιν, Βιετνάμ, Τουρκμενιστάν, Ιράν, Βόρεια Κορέα, Αφγανιστάν, Συρία και Ερυθραία (Reporters without borders, 2024). Παρά τη βελτίωση στην κατάταξη

της Ελλάδας, σε ευρωπαϊκό επίπεδο βρίσκεται στην τελευταία θέση. Στην παρακάτω εικόνα, φαίνεται με χρωματικό κώδικα η κατάταξη των χωρών στην ελευθερία του Τύπου, όπου όσο πιο βαθύ κόκκινο χρώμα τόσο πιο χαμηλά στην κατάταξη βρίσκεται η εκάστοτε χώρα.



Εικόνα 6. Κατάταξη των χώρων στην ελευθερία του Τύπου (Reporters without borders, 2024)

Επομένως, είναι πασιφανές ότι σε χώρες με απολυταρχικά καθεστώτα, εταιρικούς κολοσσούς, με αυστηρά θρησκευτικά πρότυπα (π.χ. Ισλάμ) και χαμηλό βιοτικό επίπεδο, η ελευθερία του Τύπου βρίσκεται σε δυσμενή θέση (Tsui, The importance of digital security to securing press freedom, 2018), (Tsui & Lee, How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom, 2019). Η λίστα με την κατάταξη όλων των χωρών όπως αυτή προκύπτει από το Reporters without borders (Reporters without borders, 2024) είναι διαθέσιμη στο Παράρτημα 1: Ελευθερία του Τύπου – Κατάταξη χωρών.

Οι πλατφόρμες αυτές, οι οποίες αναλύονται αργότερα στο παρόν κεφάλαιο, παρέχουν στους δημοσιογράφους τα μέσα για να επικοινωνούν εμπιστευτικά και με ασφάλεια με τους πληροφοριοδότες τους. Αυτές οι πλατφόρμες χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο, πράγμα που σημαίνει ότι μόνο οι χρήστες που επικοινωνούν μπορούν να διαβάσουν τα μηνύματα, αποτρέποντας ουσιαστικά σε τρίτους ενδεχόμενη υποκλοπή της επικοινωνίας. Αυτό το επίπεδο ασφάλειας είναι απαραίτητο για την προστασία ευαίσθητων πληροφοριών και τη διατήρηση της

εμπιστοσύνης των πηγών που ενδέχεται να διακινδυνεύσουν την ασφάλειά τους για να παρέχουν πολύτιμες πληροφορίες (Media Defence, 2022).

Επιπλέον, πλατφόρμες ασφαλούς επικοινωνίας είναι ζωτικής σημασίας για τη διασφάλιση της ακεραιότητας της Δημοσιογραφίας. Η ερευνητική Δημοσιογραφία, ειδικότερα, περιλαμβάνει συχνά χειρισμό εξαιρετικά ευαίσθητων δεδομένων που, εάν παραβιασθούν, θα μπορούσαν να οδηγήσουν σε σοβαρές συνέπειες. Οι διαρροές τέτοιων πληροφοριών όχι μόνο θέτουν σε κίνδυνο πηγές, αλλά υπονομεύουν επίσης την αξιοπιστία των δημοσιογράφων και των ειδησεογραφικών οργανισμών που εκπροσωπούν. Οι πλατφόρμες αυτές λοιπόν συμβάλλουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου και μηνύματα κειμένου, διατηρώντας έτσι την ακεραιότητα της δημοσιογραφικής έρευνας. Αυτό, δημιουργεί ένα αίσθημα ασφάλειας στους δημοσιογράφους προκειμένου να μπορέσουν να συνεχίσουν τις έρευνες σε βάθος χωρίς τον συνεχή φόβο κάποιας ενδεχόμενης παραβίασης ή διαρροής (Višňovský & Radošinská, 2016).

Ο ρόλος αυτών των πλατφορμών αυτών εκτείνεται πέρα από την απλή προστασία της επικοινωνίας μεταξύ των δημοσιογράφων και των πηγών τους. Διαδραματίζουν επίσης κρίσιμο ρόλο στον συντονισμό των δημοσιογραφικών προσπαθειών, ειδικά σε περιπτώσεις που απαιτείται συνεργασία μεταξύ ανθρώπων που βρίσκονται σε διαφορετικές γεωγραφικές περιοχές ή/και οργανισμούς. Οι πλατφόρμες ασφαλούς επικοινωνίας επιτρέπουν στους δημοσιογράφους να μοιράζονται πληροφορίες, να συζητούν στρατηγικές και να συντονίζουν τις δραστηριότητές τους χωρίς να εκτίθενται στους κινδύνους που συνδέονται με μη κρυπτογραφημένα ή μη ασφαλή κανάλια. Αυτό είναι ιδιαίτερα σημαντικό σε περιπτώσεις όπως αυτές που παρουσιάσθηκαν στα κεφάλαια 2.4.2.1, 2.4.2.2 και 2.4.2.3. Σε τέτοιες περιπτώσεις, απαιτείται η συνεργασία δημοσιογράφων από όλο τον κόσμο προκειμένου να αποκαλύψουν κακώς κείμενα ή πολύπλοκα δίκτυα διαφθοράς και αθέμιτες χρηματοοικονομικές πρακτικές (Internet Society, 2022).

Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, το ίδιο κάνουν και οι μέθοδοι ψηφιακής παρακολούθησης και κυβερνοεπιθέσεων. Οι δημοσιογράφοι πρέπει να παραμείνουν μπροστά σε αυτές τις απειλές ενημερώνοντας συνεχώς τα εργαλεία αλλά και τις πρακτικές για την ασφάλειά τους, χρησιμοποιώντας τα πιο προηγμένα

διαθέσιμα εργαλεία. Η κατάρτιση και η ευαισθητοποίηση για αυτά τα ζητήματα είναι επίσης βασικά στοιχεία προς αυτή την κατεύθυνση. Έτσι, οι δημοσιογράφοι πρέπει να εκπαιδεύονται σχετικά με τη σημασία της ψηφιακής ασφάλειας και πώς να χρησιμοποιούν αποτελεσματικά αυτές τις πλατφόρμες. Οι οργανισμοί των μέσων ενημέρωσης πρέπει να επενδύσουν τόσο στην τεχνολογία όσο και στην εκπαίδευση του προσωπικού τους για να εξασφαλίσουν ότι οι δημοσιογράφοι τους είναι κατάλληλα εξοπλισμένοι προκειμένου να χειριστούν τις συνεχώς εξελισσόμενες απειλές στην ψηφιακή εποχή. Με αυτόν τον τρόπο, όχι μόνο προστατεύουν τα δικά τους συμφέροντα αλλά και υποστηρίζουν τις θεμελιώδεις αρχές ενός ελεύθερου και ανεξάρτητου Τύπου (Abellán, 2021; O'Driscoll, 2023).

Οι ασφαλείς πλατφόρμες επικοινωνίας είναι απαραίτητες για τη σύγχρονη Δημοσιογραφία. Προστατεύουν το απόρρητο των πηγών, διατηρούν την ακεραιότητα της ερευνητικής διαδικασίας και διευκολύνουν την ασφαλή συνεργασία μεταξύ των δημοσιογράφων. Καθώς οι ψηφιακές απειλές συνεχίζουν να αυξάνονται, η εδραίωση τέτοιου είδους ψηφιακών εργαλείων αλλά και πρακτικών κυβερνοασφάλειας θα αποτελούν όλο και περισσότερο απαραίτητα εργαλεία στη φαρέτρα των δημοσιογράφων. Επενδύοντας σε αυτές τις τεχνολογίες αλλά και στην κατάλληλη εκπαίδευση και ενημέρωση, οι δημοσιογράφοι μπορούν να συνεχίσουν να εκτελούν το κρίσιμο έργο τους χωρίς να θέσουν σε κίνδυνο την ασφάλεια των πηγών τους ή την ακεραιότητα των πληροφοριών τους (O'Driscoll, 2023).

Στις επόμενες παραγράφους του παρόντος κεφαλαίου θα γίνει ανάλυση των δώδεκα εργαλείων ασφαλούς επικοινωνίας για δημοσιογράφους που τέθηκαν ως ερώτημα στο ερωτηματολόγιο που διαμοιράσθηκε. Τα εργαλεία αυτά είναι τα εξής: Nextcloud, Wickr, Proton Mail, Signal, Threema, Wire, WhatsApp, SecureDrop, GlobaLeaks, OnionShare, Tresorit και Telegram.

3.2 Nextcloud

Το Nextcloud είναι γερμανική εταιρεία λογισμικού με έδρα τη Στουτγκάρδη και δημιουργήθηκε τον Ιούνιο του 2016 από τον Frank Karlitschek και από έμπειρους επιχειρηματίες και μηχανικούς με στόχο να δώσουν στους χρήστες τη δυνατότητα να ανακτήσουν τον έλεγχο των δεδομένων και της επικοινωνίας τους. Το Nextcloud είναι μια πλατφόρμα συνεργασίας και επικοινωνίας, η οποία επιτρέπει σε ομάδες

χρηστών να έχουν πρόσβαση, να μοιράζονται και να επεξεργάζονται τα έγγραφά τους, συνομιλώντας και συμμετέχοντας σε βιντεοκλήσεις και διαχειρίζοντας την αλληλογραφία και το ημερολόγιό τους (calendar) μέσω κινητών, υπολογιστών και διεπαφή χρήστη (web interface) (Nextcloud, 2024).

Εικόνα 7. Λογότυπο Nextcloud

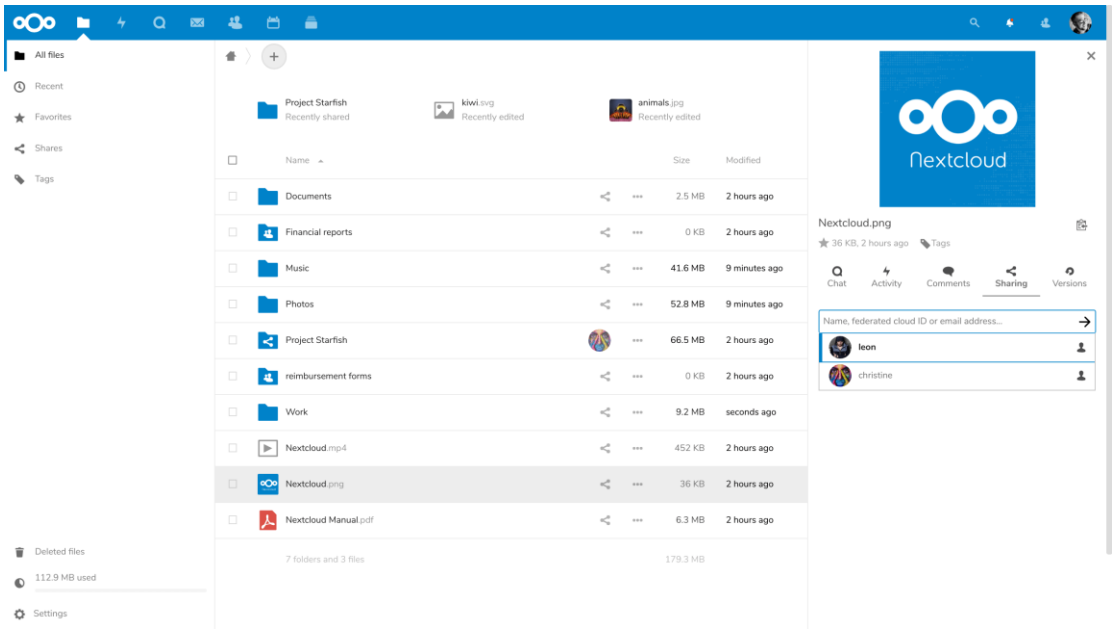
Το Nextcloud αποτελεί λογισμικό ανοιχτού κώδικα (Open-source software) που παρέχει έναν ασφαλή και ευέλικτο τρόπο αποθήκευσης και κοινής χρήσης αρχείων. Επιτρέπει στον χρήστη να διαχειρίζεται τον δικό του χώρο αποθήκευσης είτε τοπικά σε ιδιωτικό διακομιστή (server) είτε στο υπολογιστικό νέφος (cloud). Οι χρήστες μπορούν να αποθηκεύουν και να συγχρονίζουν τα αρχεία τους σε πολλές συσκευές και να μοιράζονται αρχεία.

Επιπλέον, το Nextcloud περιλαμβάνει εργαλεία συνεργασίας, όπως το Nextcloud Talk για βιντεοκλήσεις και συνομιλία, καθώς και συνεργατική επεξεργασία εγγράφων με ενσωμάτωση εργαλείων γραφείου όπως το ONLYOFFICE[14] ή το Collabora Online[15]. Συγχρονίζεται άριστα με τις εφαρμογές ημερολογίου και επαφών και επίσης προσφέρει τη δυνατότητα να συνδεθεί με διακομιστές email για διαχείριση απευθείας από την πλατφόρμα.

Στον τομέα της ασφάλειας, το Nextcloud δίνει ιδιαίτερη έμφαση ενσωματώνοντας λειτουργίες όπως έλεγχος ταυτότητας δύο παραγόντων (2FA), ενσωματωμένη σάρωση ιών, κρυπτογράφηση και πρόληψη περιστατικών παραβίασης. Το Nextcloud είναι δημοφιλές τόσο στους μεμονωμένους χρήστες που αναζητούν έλεγχο του απορρήτου των δεδομένων τους όσο και στους οργανισμούς που αναζητούν ένα

[14] https://www.onlyoffice.com/
[15] https://www.collaboraoffice.com/

συνεργατικό εργαλείο που μπορούν να φιλοξενήσουν στη δική τους υποδομή για να συμμορφωθούν με τους κανονισμούς ασφάλειας δεδομένων και διατήρησης της ιδιωτικότητας ακολουθώντας την πολιτική για μηδενικές διαρροές δεδομένων (Zero Data Leaks) (Cadet, 2023).



Εικόνα 8. Nextcloud περιβάλλον χρήστη

3.3 Wickr

Η Wickr είναι αμερικανική εταιρεία λογισμικού με έδρα τη Νέα Υόρκη και αποτελεί μια ασφαλή πλατφόρμα ανταλλαγής μηνυμάτων καθώς δίνει μεγάλη έμφαση στο απόρρητο των χρηστών. Το Wickr είναι ευρέως γνωστό ότι παρέχει ισχυρή κρυπτογράφηση από άκρο σε άκρο για όλα τα μηνύματα, διασφαλίζοντας ότι μόνο οι προβλεπόμενοι παραλήπτες μπορούν να διαβάσουν το περιεχόμενο. Τα μηνύματα και τα αρχεία που αποστέλλονται μέσω Wickr δύναται να ρυθμιστούν ώστε να αυτοκαταστρέφονται μετά από μια καθορισμένη περίοδο, ενισχύοντας το απόρρητο, αποτρέποντας τη μακροπρόθεσμη αποθήκευση ευαίσθητων πληροφοριών (AWS Wickr, 2022).

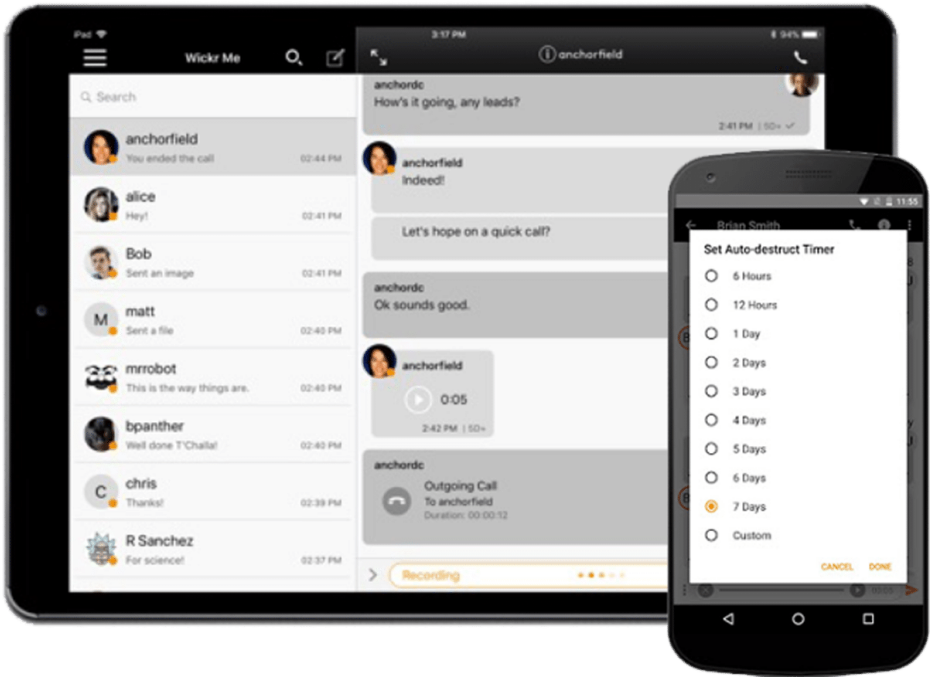
Εικόνα 9. Λογότυπο Wickr

Επιπλέον, το Wickr δεν διατηρεί μεταδεδομένα για επικοινωνίες, που σημαίνει ότι δεν αποθηκεύει πληροφορίες σχετικά με το ποιος επικοινώνησε με ποιον, πότε ή πού. Επίσης, το Wickr υποστηρίζει ομαδικές συνομιλίες και ασφαλείς κλήσεις φωνής και βίντεο, καθιστώντας το, κατάλληλο εργαλείο τόσο για προσωπική όσο και για επαγγελματική χρήση. Οι χρήστες μπορούν να μοιράζονται με ασφάλεια αρχεία, φωτογραφίες και βίντεο με το ίδιο επίπεδο κρυπτογράφησης με τα μηνύματα κειμένου.

Η Wickr προσφέρει λύσεις προσαρμοσμένες για εταιρική χρήση, συμπεριλαμβανομένων των Wickr Pro και Wickr Enterprise, οι οποίες παρέχουν πρόσθετες λειτουργίες για τις επιχειρήσεις, όπως ασφαλείς διαχειριστικούς ελέγχους και ενοποίηση με άλλα εταιρικά εργαλεία.

Το ιδιαίτερα σημαντικό χαρακτηριστικό της Wickr είναι ότι χρησιμοποιεί ένα μοντέλο ασφάλειας μηδενικής εμπιστοσύνης (Zero Trust), διασφαλίζοντας ότι ακόμη και η ίδια η Wickr δεν μπορεί να έχει πρόσβαση στα δεδομένα χρήστη. Το Zero Trust είναι ένα πλαίσιο ασφαλείας που απαιτεί από όλους τους χρήστες, είτε εντός είτε εκτός του δικτύου του οργανισμού, να ελέγχονται, να είναι εξουσιοδοτημένοι και να επικυρώνονται συνεχώς πριν τους παραχωρηθεί ή διατηρηθεί η πρόσβαση σε εφαρμογές και δεδομένα (Raina, 2023).

Η εφαρμογή είναι διαθέσιμη σε πολλές πλατφόρμες, συμπεριλαμβανομένων των iOS, Android, Windows και Mac, επιτρέποντας στους χρήστες να επικοινωνούν με ασφάλεια σε διαφορετικές συσκευές. Το Wickr χρησιμοποιείται συχνά από άτομα και οργανισμούς που δίνουν προτεραιότητα στην ασφάλεια και το απόρρητο στις επικοινωνίες τους, συμπεριλαμβανομένων δημοσιογράφων, ακτιβιστών και επιχειρήσεων που χειρίζονται ευαίσθητες πληροφορίες.



Εικόνα 10. Wickr περιβάλλον χρήστη

3.4 Proton Mail

Το Proton Mail είναι μια ελβετική υπηρεσία κρυπτογραφημένης αλληλογραφίας από άκρο σε άκρο που ιδρύθηκε το 2014 από επιστήμονες του CERN με σκοπό την παροχή ενός καλύτερου Διαδικτύου με δεδομένη την προστασία της ιδιωτικότητας. Αξιοσημείωτο είναι ότι η Ελβετία έχει μερικούς από τους ισχυρότερους νόμους περί απορρήτου στον κόσμο (Proton Team, 2024). Αυτό το νομικό περιβάλλον παρέχει ένα επιπλέον επίπεδο προστασίας για τα δεδομένα των χρηστών. Παρά τα προηγμένα χαρακτηριστικά ασφάλειάς του, το Proton Mail προσφέρει μια φιλική προς τον χρήστη διεπαφή που μοιάζει με αυτή των συμβατικών υπηρεσιών email, διευκολύνοντας τους χρήστες να προσαρμοστούν (Proton, 2024).

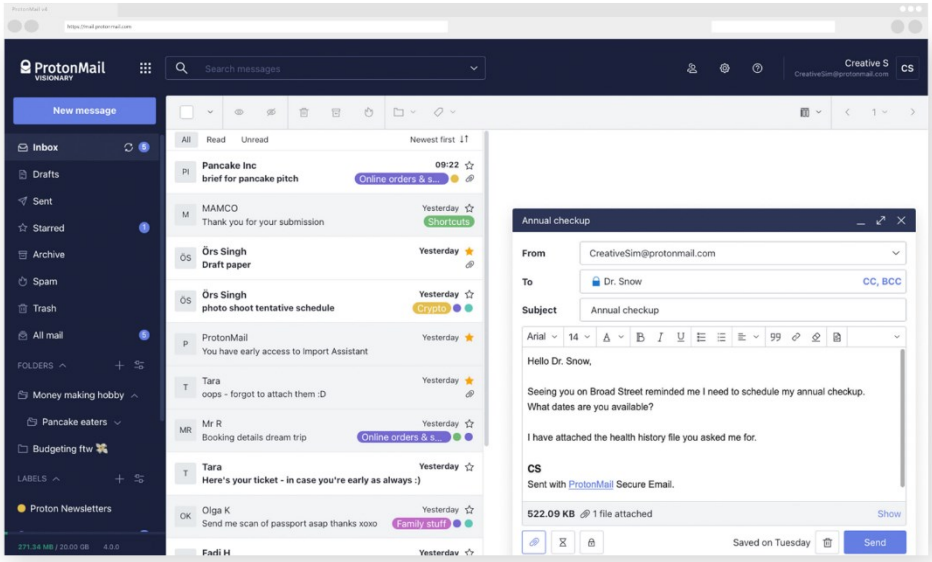
Εικόνα 11. Λογότυπο Proton Mail

Το Proton Mail χρησιμοποιεί κρυπτογράφηση από άκρο σε άκρο για να διασφαλίσει ότι μόνο ο αποστολέας και ο παραλήπτης μπορούν να διαβάσουν το περιεχόμενο του email. Αυτή η κρυπτογράφηση πραγματοποιείται αυτόματα και δεν απαιτεί πρόσθετη ρύθμιση από τον χρήστη. Επιπρόσθετα, η εταιρεία διασφαλίζει ότι ακόμη και οι διαχειριστές της υπηρεσίας δεν μπορούν να διαβάσουν τα emails των χρηστών. Αυτό επιτυγχάνεται μέσω κρυπτογράφησης που πραγματοποιείται από την πλευρά του πελάτη, που σημαίνει ότι τα emails κρυπτογραφούνται πριν φτάσουν στους διακομιστές της υπηρεσίας. Ένα επιπλέον σημαντικό στοιχείο είναι ότι οι αλγόριθμοι κρυπτογράφησης του Proton Mail είναι ανοιχτού κώδικα, επιτρέποντας τη διαφάνεια και την επαλήθευση των μέτρων ασφαλείας που ισχύουν (Pang, 2022).

Το Proton Mail δεν παρακολουθεί ούτε καταγράφει τη δραστηριότητα των χρηστών. Δίνει προτεραιότητα στο απόρρητο των χρηστών, χωρίς να διατηρεί διευθύνσεις IP ή οποιαδήποτε άλλη πληροφορία που μπορεί να οδηγήσει στην ταυτοποίηση προσώπων. Παρόμοια με το Wickr, οι χρήστες του Proton Mail μπορούν να ρυθμίσουν τα emails να αυτοκαταστρέφονται μετά από μια καθορισμένη περίοδο, διασφαλίζοντας ότι οι ευαίσθητες πληροφορίες δεν θα παραμείνουν προσβάσιμες επ' αόριστον. Αυτό το χαρακτηριστικό το καθιστά μια υπηρεσία πολύ φιλική προς τους δημοσιογράφους και τους πληροφοριοδότες τους καθώς η προστασία που προσφέρει

διασφαλίζει την απρόσκοπτη ανταλλαγή πληροφοριών χωρίς τον φόβο παραβίασης αυτών ή ταυτοποίησης των εμπλεκόμενων μερών (Wolford, 2023).

Τέλος, να υπογραμμισθεί ότι το Proton Mail επιτρέπει στους χρήστες να στέλνουν κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου σε διευθύνσεις που δεν ανήκουν στο Proton Mail. Οι παραλήπτες λαμβάνουν έναν σύνδεσμο προς το κρυπτογραφημένο μήνυμα και μια ξεχωριστή επικοινωνία με έναν κωδικό πρόσβασης για την αποκρυπτογράφησή του.



Εικόνα 12. Proton Mail περιβάλλον χρήστη

3.5 Signal

Το Signal είναι μια δωρεάν εφαρμογή ανταλλαγής μηνυμάτων ανοιχτού κώδικα (free open-source messaging app) που αναπτύχθηκε από τον μη κερδοσκοπικό οργανισμό Signal Foundation, με έδρα το Σαν Φρανσίσκο και εστιάζει στο απόρρητο και στην ασφάλεια. Είναι διαθέσιμο για πλατφόρμες Android, iOS και επιτραπέζιους υπολογιστές (Windows, macOS, Linux). Το Signal χρησιμοποιεί κρυπτογράφηση από άκρο σε άκρο προκειμένου να διασφαλίσει ότι τα μηνύματα, οι φωνητικές κλήσεις, οι βιντεοκλήσεις και τα κοινόχρηστα αρχεία θα είναι προσβάσιμα μόνο στους προβλεπόμενους παραλήπτες. Υποστηρίζει κρυπτογραφημένες ομαδικές συνομιλίες και ομαδικές κλήσεις, επιτρέποντας σε πολλούς χρήστες να επικοινωνούν με ασφάλεια. Οι χρήστες μπορούν να αναμεταδώσουν τις φωνητικές τους κλήσεις μέσω των διακομιστών του Signal για να αποφύγουν την αποκάλυψη της διεύθυνσης IP

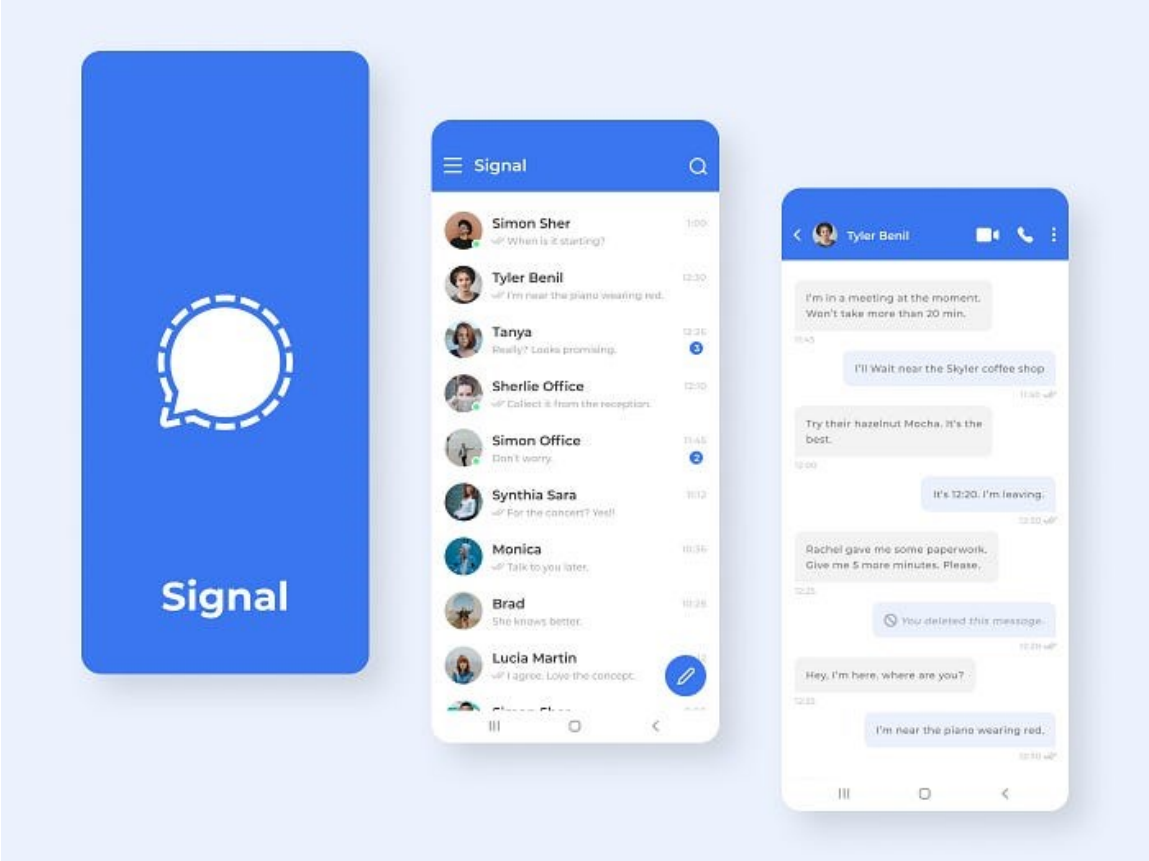
τους στις επαφές τους (Marlinspike, Signal 2.0: Private messaging comes to the iPhone, 2015).

Εικόνα 13. Λογότυπο Signal

Όλες οι επικοινωνίες μέσω του Signal είναι κρυπτογραφημένες από άκρο σε άκρο, πράγμα που σημαίνει ότι μόνο ο αποστολέας και ο παραλήπτης μπορούν να διαβάσουν τα μηνύματα. Αυτό το πρωτόκολλο κρυπτογράφησης (Signal Protocol) έχει σχεδιασθεί με τέτοιο τρόπο ώστε να εμποδίζει τρίτα μέρη - συμπεριλαμβανομένων των προγραμματιστών της εφαρμογής- να έχουν πρόσβαση στο περιεχόμενο των επικοινωνιών. Επιπροσθέτως, το Signal επιτρέπει στους χρήστες να ανακαλύψουν ποιες από τις επαφές τους χρησιμοποιούν την εφαρμογή. Σε υποστηριζόμενες συσκευές, μπορεί να ενεργοποιήσει μια λειτουργία πληκτρολογίου ανώνυμης περιήγησης για να εμποδίσει το πληκτρολόγιο να μάθει συνήθειες πληκτρολόγησης. Ένα ακόμα χαρακτηριστικό του Signal που το κάνει ενδιαφέρον είναι ότι οι χρήστες μπορούν να ρυθμίσουν τα μηνύματα να διαγράφονται αυτόματα μετά από ένα καθορισμένο χρονικό διάστημα. Αυτή η δυνατότητα βοηθά στη διατήρηση του απορρήτου διασφαλίζοντας την ακεραιότητα των ευαίσθητων πληροφοριών. Επιπλέον, το Signal περιλαμβάνει λειτουργίες για τη βελτίωση της ασφάλειας, όπως την αποτροπή στιγμιότυπων οθόνης εντός της εφαρμογής σε ορισμένες συσκευές και χρησιμοποιεί αριθμούς ασφαλείας για να επαληθεύσει την ασφάλεια των επικοινωνιών σας με συγκεκριμένες επαφές. Εάν για παράδειγμα αλλάξει ο αριθμός ασφαλείας μιας επαφής, μπορεί να υποδεικνύει ότι το κλειδί κρυπτογράφησης της επαφής έχει αλλάξει (Marlinspike, Advanced cryptographic ratcheting, 2013).

Ένα πολύ σημαντικό στοιχείο αποτελεί το γεγονός ότι το Signal δεν εμφανίζει διαφημίσεις, ούτε παρακολουθεί τη δραστηριότητα των χρηστών. Χρηματοδοτείται από δωρεές και επιχορηγήσεις, ιδίως από το Signal Foundation, διασφαλίζοντας την ανεξαρτησία του από εμπορικά συμφέροντα (Acton, 2018).

Ο τρόπος λειτουργίας του είναι απλός. Οι χρήστες εγγράφονται με τον αριθμό τηλεφώνου τους, ο οποίος χρησιμεύει ως μοναδικό αναγνωριστικό τους. Η εφαρμογή αποθηκεύει μόνο τον αριθμό τηλεφώνου που χρησιμοποιήθηκε για την εγγραφή καθώς και τον τελευταίο χρόνο σύνδεσης.



Εικόνα 14. Signal περιβάλλον χρήστη

3.6 Threema

Το Threema είναι μια ασφαλής εφαρμογή ανταλλαγής μηνυμάτων, παρόμοια με το Signal. Αναπτύχθηκε από την Threema GmbH στην Ελβετία και κυκλοφόρησε το 2012 και πλέον απαριθμεί περί τα δώδεκα εκατομμύρια χρήστες παγκοσμίως. Έχει σχεδιασθεί για να διασφαλίζει ότι οι επικοινωνίες των χρηστών προστατεύονται από υποκλοπές και μη εξουσιοδοτημένη πρόσβαση. Το Threema είναι ευρέως γνωστό για

την ισχυρή δέσμευσή του στο απόρρητο και την ασφάλεια, καθιστώντας το μια δημοφιλή επιλογή μεταξύ των χρηστών που ανησυχούν για το ψηφιακό τους απόρρητο (Threema (a), 2024).

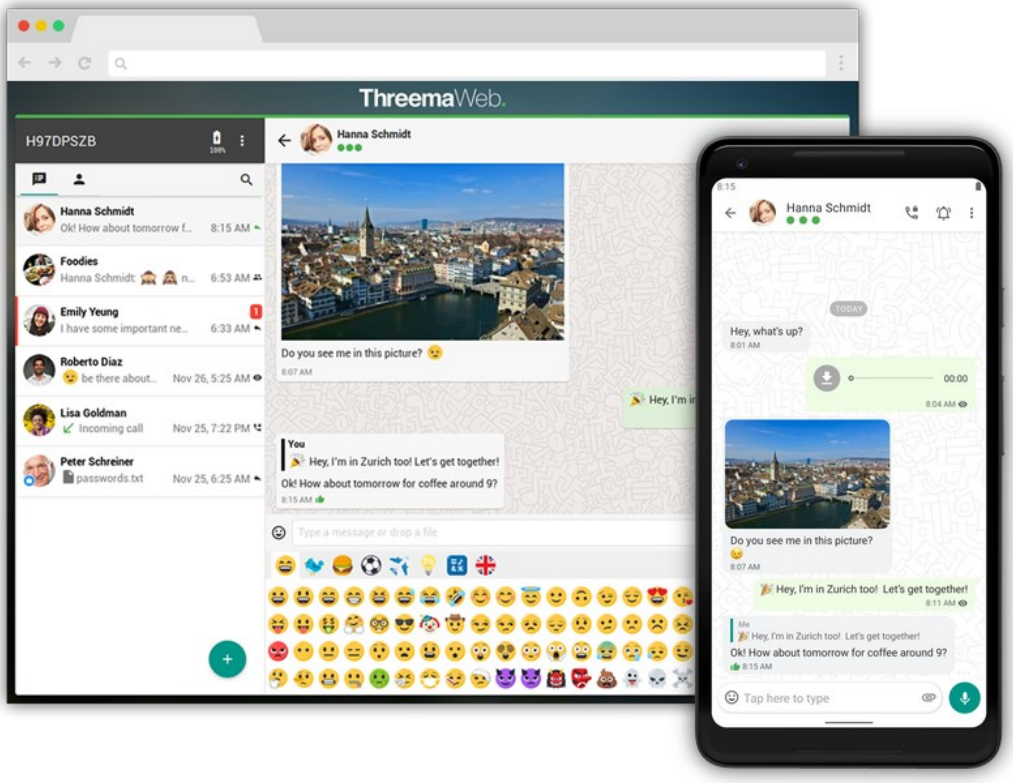
Εικόνα 15. Λογότυπο Threema

Είναι μια εφαρμογή επί πληρωμή, που σημαίνει ότι οι χρήστες πρέπει να την αγοράσουν από το εκάστοτε κατάστημα εφαρμογών (app store). Αυτό το επιχειρηματικό μοντέλο υποστηρίζει τις λειτουργίες της εφαρμογής χωρίς να βασίζεται σε διαφημίσεις ή δεδομένα χρήστη (Threema (b), 2024). Είναι διαθέσιμο σε Android, iOS και ως εφαρμογή Ιστού, επιτρέποντας στους χρήστες να έχουν πρόσβαση στα μηνύματά τους σε διαφορετικές συσκευές. Το Threema προσφέρει μια διεπαφή ιστού που επιτρέπει στους χρήστες να έχουν πρόσβαση στα μηνύματά τους από έναν υπολογιστή, συγχρονίζοντας με την εφαρμογή για κινητά.

Το Threema χρησιμοποιεί κρυπτογράφηση από άκρο σε άκρο για την ασφάλεια όλων των μορφών επικοινωνίας, συμπεριλαμβανομένων των μηνυμάτων κειμένου, των φωνητικών κλήσεων, των βιντεοκλήσεων, των ομαδικών συνομιλιών και της μεταφοράς αρχείων διαφόρων τύπων και μεγεθών. Επίσης, το Threema επιτρέπει στους χρήστες να χρησιμοποιούν την εφαρμογή ανώνυμα. Σε αντίθεση με πολλές άλλες εφαρμογές ανταλλαγής μηνυμάτων, δεν απαιτεί αριθμό τηλεφώνου ή διεύθυνση email για εγγραφή. Οι χρήστες αναγνωρίζονται από ένα αναγνωριστικό Threema που δημιουργείται τυχαία. Οι χρήστες εγγράφονται δημιουργώντας ένα τυχαίο Threema ID, το οποίο χρησιμεύει ως το μοναδικό τους αναγνωριστικό. Όσον αφορά την επαλήθευση, το Threema επιτρέπει στους χρήστες να επαληθεύουν την ταυτότητα των επαφών τους σαρώνοντας έναν κωδικό QR, ενισχύοντας την ασφάλεια των επικοινωνιών. Οι χρήστες του Threema, όπως και στις άλλες εφαρμογές που προαναφέρθηκαν, μπορούν να ρυθμίσουν τα μηνύματα ώστε να διαγράφονται

αυτόματα μετά από μια καθορισμένη περίοδο, διασφαλίζοντας ότι οι ευαίσθητες πληροφορίες δεν θα παραμένουν προσπελάσιμες επ' άπειρον (Threema (c), 2024).

Πολύ ενδιαφέρον χαρακτηριστικό της εφαρμογής, αποτελεί η ενσωματωμένη λειτουργία δημιουργίας δημοσκοπήσεων και ερευνών σε ομαδικές συνομιλίες, καθιστώντας το χρήσιμο για την οργάνωση εκδηλώσεων και τη συλλογή απόψεων. Ξεχωριστό στοιχείο αποτελεί το πρωτόκολλο κρυπτογράφησης που χρησιμοποιεί το Threema που είναι το NaCl (Βιβλιοθήκη Δικτύωσης και Κρυπτογραφίας), διασφαλίζοντας έτσι ισχυρή ασφάλεια για όλες τις επικοινωνίες. Τέλος, να υπογραμμισθεί ότι το Threema συλλέγει ελάχιστα δεδομένα χρήστη. Η εφαρμογή δεν αποθηκεύει μεταδεδομένα που σχετίζονται με επικοινωνίες και διασφαλίζει ότι τα δεδομένα αποθηκεύονται με τρόπο που προστατεύει το απόρρητο των χρηστών. Τα δεδομένα όπως και τα μηνύματα αποθηκεύονται τοπικά στη συσκευή του χρήστη και όχι στους διακομιστές του Threema (Threema (c), 2024).



Εικόνα 16. Threema περιβάλλον χρήστη

3.7 Wire

Το Wire είναι μια ασφαλής εφαρμογή ανταλλαγής μηνυμάτων που δημιουργήθηκε από την Wire Swiss GmbH, μια εταιρεία λογισμικού με εγκαταστάσεις στο Βερολίνο της Γερμανίας, το Τσουγκ της Ελβετίας και το Σαν Φρανσίσκο των ΗΠΑ (Wire (a), 2024). Η εφαρμογή Wire επιτρέπει στους χρήστες να ανταλλάσσουν κρυπτογραφημένα από άκρη σε άκρη μηνύματα, καθώς και να πραγματοποιούν κλήσεις (φωνητικές και βιντεοκλήσεις), διασφαλίζοντας ότι μόνο οι προβλεπόμενοι παραλήπτες μπορούν να διαβάσουν ή να αποκτήσουν πρόσβαση στο περιεχόμενο (Wire (b), 2024).

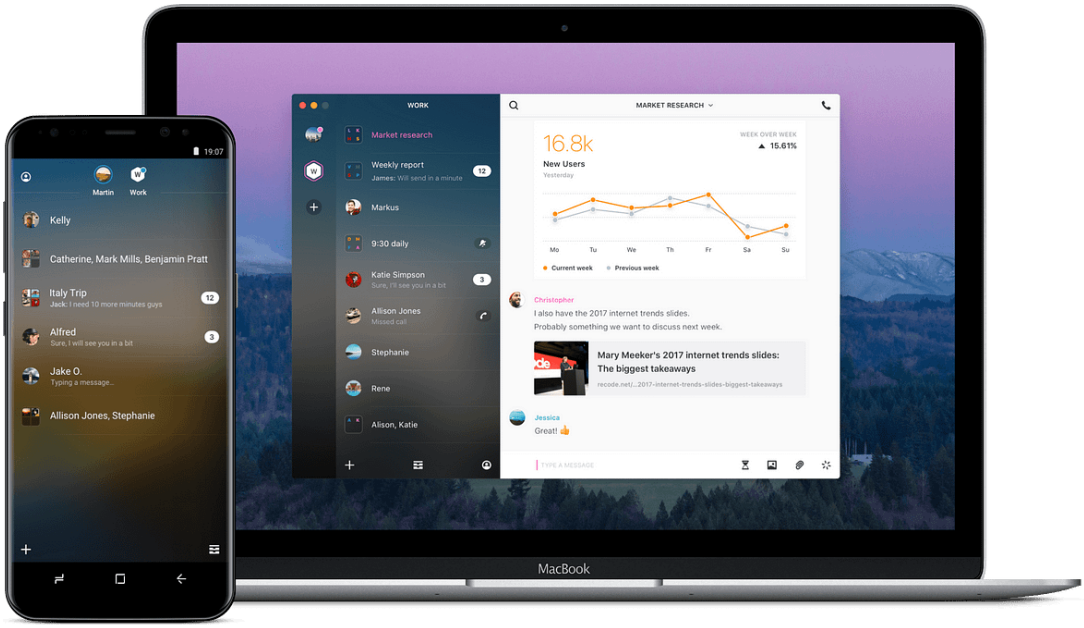
Εικόνα 17. Λογότυπο Wire

Το Wire είναι διαθέσιμο σε πολλές πλατφόρμες, συμπεριλαμβανομένων των Windows, macOS, iOS, Android και προγραμμάτων περιήγησης ιστού, επιτρέποντας στους χρήστες να παραμένουν συνδεδεμένοι σε όλες τις συσκευές.

Επιπλέον, το Wire έχει σχεδιαστεί με ιδιαίτερη έμφαση στο απόρρητο των χρηστών. Δεν κρατάει δεδομένα για την παρακολούθηση της συμπεριφοράς των χρηστών και τηρεί αυστηρές πολιτικές προστασίας δεδομένων (Wire (c), 2024). Η εφαρμογή Wire παρέχει εξειδικευμένες λύσεις για επιχειρήσεις, συμπεριλαμβανομένων εργαλείων ασφαλούς επικοινωνίας για ομάδες, συμμόρφωση με ρυθμιστικά πρότυπα και ενσωμάτωση σε διάφορες εταιρικές πλατφόρμες συνεργασίας. Αποτελεί μια δημοφιλή επιλογή σε περιπτώσεις που απαιτείται η ασφαλής ανταλλαγή πληροφοριών όπως μεταξύ δημοσιογράφων και πληροφοριοδοτών, οργανισμών αλλά και αξιωματούχων και υπηρεσιών επιβολής του νόμου (Wire (d), 2024; Gierow, 2024). Παράλληλα, επιτρέπει τη δημιουργία δωματίων επισκεπτών, όπου μπορούν να προσκληθούν εξωτερικοί χρήστες για ασφαλή επικοινωνία χωρίς να απαιτείται

λογαριασμός Wire. Για πρόσθετη ασφάλεια, το Wire προσφέρει την επιλογή αποστολής μηνυμάτων που διαγράφονται αυτόματα μετά από μια καθορισμένη περίοδο (Wire (b), 2024).

Συμπερασματικά, το Wire λόγω των ισχυρών χαρακτηριστικών ασφαλείας του και της δέσμευσής του στο απόρρητο των χρηστών, καθώς και για το γεγονός ότι πληροί διεθνή πρότυπα, όσον αφορά την προστασία και την ασφάλεια των δεδομένων, αποτελεί μία επιλογή για επικοινωνία τόσο σε προσωπικό όσο και σε επαγγελματικό πλαίσιο (Gierow, 2024).



Εικόνα 18. Wire περιβάλλον χρήστη

3.8 WhatsApp

Το WhatsApp είναι μία από τις πιο δημοφιλείς εφαρμογές επικοινωνίας της Meta Platforms (πρώην Facebook) που επιτρέπει στους χρήστες να στέλνουν μηνύματα κειμένου, να πραγματοποιούν φωνητικές κλήσεις και βιντεοκλήσεις και να μοιράζονται εικόνες, έγγραφα και άλλα μέσα. Το WhatsApp χρησιμοποιείται ευρέως σε όλο τον κόσμο λόγω της ευκολίας στη χρήση του, το ισχυρό σύνολο λειτουργιών και την ασφάλεια που παρέχει η κρυπτογράφηση από άκρο σε άκρο. Ενδεικτικό είναι ότι χρησιμοποιείται από περισσότερα από 2 δισεκατομμύρια ανθρώπους σε πάνω από 180 χώρες σε όλο τον κόσμο (WhatsApp (a), 2024).

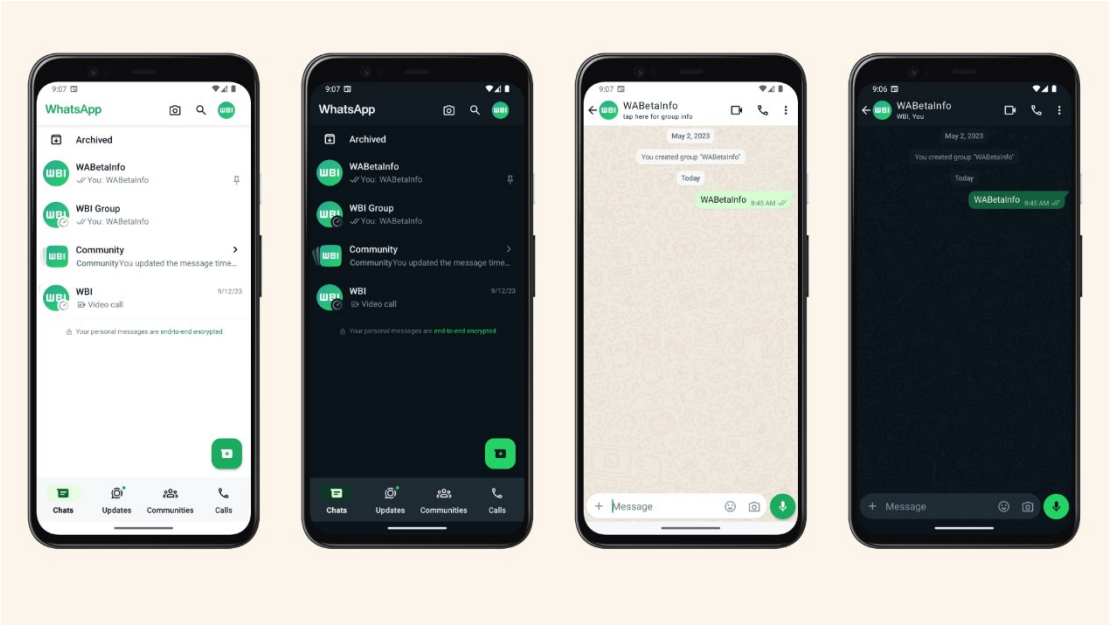
Εικόνα 19. Λογότυπο Whatsapp

Το WhatsApp επιτρέπει στους χρήστες να στέλνουν μηνύματα κειμένου άμεσα και γρήγορα σε άλλους χρήστες του WhatsApp, είτε μεμονωμένα είτε σε ομαδικές συνομιλίες (WhatsApp (b), 2024). Οι χρήστες μπορούν να δημιουργήσουν ομαδικές συνομιλίες με έως και 1024 συμμετέχοντες (WhatsApp (c), 2024). Ένα ενδιαφέρον χαρακτηριστικό του WhatssApp είναι οι λίστες εκπομπής (broadcast lists). Οι λίστες εκπομπής είναι αποθηκευμένες λίστες επαφών που επιτρέπουν στον εκάστοτε χρήστη να στέλνει μηνύματα σε πολλές επαφές ταυτόχρονα χωρίς να έχει πρόσβαση ο ένας στις πληροφορίες του άλλου (WhatsApp (d), 2024).

Όλες οι επικοινωνίες στο WhatsApp, συμπεριλαμβανομένων των μηνυμάτων, των κλήσεων, των φωτογραφιών και των βίντεο, προστατεύονται με κρυπτογράφηση από άκρο σε άκρο, διασφαλίζοντας ότι μόνο ο αποστολέας και ο παραλήπτης μπορούν να τις διαβάσουν ή να τις ακούσουν. Πολύ ενδιαφέρον χαρακτηριστικό της εφαρμογής είναι ότι οι χρήστες μπορούν να δημοσιεύουν ενημερώσεις κατάστασης, οι οποίες είναι ορατές στις επαφές τους για 24 ώρες. Αυτές οι ενημερώσεις μπορεί να περιλαμβάνουν κείμενο, φωτογραφίες, βίντεο και GIF (WhatsApp, 2023).

Όσον αφορά τις επιχειρήσεις η εφαρμογή προσφέρει το WhatsApp Business, η οποία είναι μια έκδοση της εφαρμογής που έχει σχεδιασθεί για μικρές επιχειρήσεις και διαθέτει λειτουργίες όπως αυτοματοποιημένες απαντήσεις, εταιρικά προφίλ και στατιστικά μηνυμάτων (WhatsApp Business, 2024).

Το WhatsApp είναι διαθέσιμο σε πολλές πλατφόρμες, συμπεριλαμβανομένων των iOS, Android, Windows Phone και μπορεί να χρησιμοποιηθεί σε tablet και υπολογιστές μέσω του WhatsApp Web ή της εφαρμογής επιτραπέζιου υπολογιστή. Τέλος, οι χρήστες του WhatsApp μπορούν να δημιουργήσουν αντίγραφα ασφαλείας του ιστορικού συνομιλιών τους στο Google Drive[16] ή στο iCloud[17], καθιστώντας εύκολη την επαναφορά των συνομιλιών κατά την εναλλαγή συσκευών (WhatsApp, 2021).



Εικόνα 20. Whatsapp περιβάλλον χρήστη

3.9 SecureDrop

Το SecureDrop είναι ένα σύστημα υποβολής καταγγελιών ανοιχτού κώδικα σχεδιασμένο για ασφαλή και ανώνυμη επικοινωνία μεταξύ δημοσιογράφων και πληροφοριοδοτών. Αρχικά αναπτύχθηκε από τον Αμερικανό προγραμματιστή Aaron Swartz και τώρα ανήκει στο Freedom of the Press Foundation. To Freedom of the Press Foundation (FPF) είναι ένας μη κερδοσκοπικός οργανισμός που προστατεύει, υπερασπίζεται και ενδυναμώνει τη Δημοσιογραφία δημοσίου συμφέροντος στον 21ο αιώνα (Freedom of the Press Foundation, 2024).

[16] https://www.google.com/
[17] https://www.icloud.com/

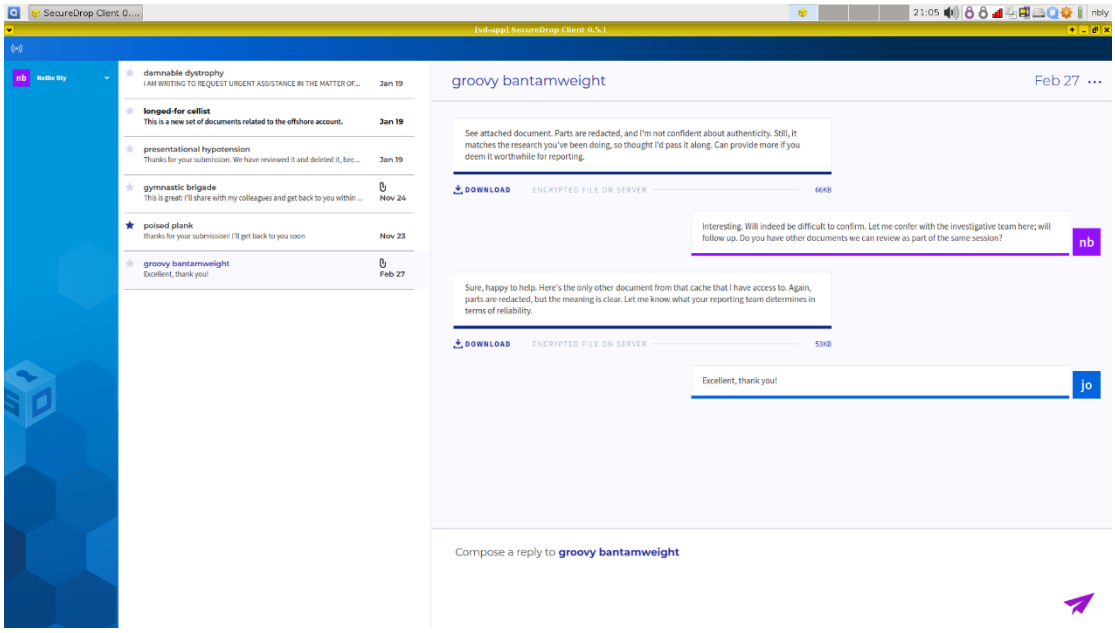
Εικόνα 21. Λογότυπο SecureDrop

Το SecureDrop αποτελεί ένα πολύ σημαντικό εργαλείο για την ερευνητική Δημοσιογραφία καθώς αποσκοπεί στην προστασία της ταυτότητας των πληροφοριοδοτών και στη διασφάλιση της ασφάλειας των πληροφοριών που μεταδίδονται. Οι πληροφοριοδότες έχουν πρόσβαση στο SecureDrop μέσω του δικτύου Tor προκειμένου να εξασφαλίσουν την ανωνυμία. Αυτό έχει ως αποτέλεσμα την απόκρυψη των διευθύνσεων IP τους και κρυπτογράφηση της συχνότητάς τους. Οι πληροφοριοδότες μπορούν να ανεβάζουν έγγραφα και να στέλνουν μηνύματα σε δημοσιογράφους χρησιμοποιώντας μια διεπαφή ιστού που παρέχεται από το SecureDrop. Αυτή η διεπαφή έχει σχεδιασθεί ούτως ώστε να είναι φιλική προς τον χρήστη και ασφαλή. Κάθε υποβολή είναι κρυπτογραφημένη με ένα δημόσιο κλειδί (public key), διασφαλίζοντας ότι μόνο οι προβλεπόμενοι παραλήπτες μπορούν να αποκρυπτογραφήσουν και να διαβάσουν τις πληροφορίες (SecureDrop (a), 2024).

Από την πλευρά τους, οι δημοσιογράφοι έχουν επίσης πρόσβαση στο σύστημα SecureDrop μέσω Tor. Χρησιμοποιούν έναν ασφαλή σταθμό εργασίας (συνήθως έναν υπολογιστή εγκατεστημένο σε ασφαλές περιβάλλον) για τη λήψη και την αποκρυπτογράφηση των καταγγελιών. Αυτή η διαδικασία ελαχιστοποιεί τον κίνδυνο έκθεσης ευαίσθητων πληροφοριών σε εξωτερικές απειλές. Η πρόσβαση στο σύστημα SecureDrop απαιτεί συχνά έλεγχο ταυτότητας δύο παραγόντων, προσθέτοντας ένα επιπλέον επίπεδο ασφάλειας (SecureDrop (a), 2024).

Τόσο οι πληροφοριοδότες όσο και οι δημοσιογράφοι παραμένουν ανώνυμοι. Οι πηγές προσδιορίζονται με μοναδικά «κωδικά» ονόματα και οι διευθύνσεις IP τους αποκρύπτονται από το Tor. Το SecureDrop προστατεύει τους πληροφοριοδότες από αντίποινα διατηρώντας την ανωνυμία τους αλλά παράλληλα παρέχει στους δημοσιογράφους μια ασφαλή μέθοδο να λαμβάνουν ευαίσθητες πληροφορίες. Βέβαια, η χρήση του απαιτεί τεχνικές γνώσεις για εγκατάσταση, διαμόρφωση και

συντήρηση της πλατφόρμας. Το SecureDrop χρησιμοποιείται ευρέως από μεγάλους ειδησεογραφικούς οργανισμούς και ομάδες ανθρωπίνων δικαιωμάτων για τη διευκόλυνση της ασφαλούς επικοινωνίας και την προστασία της δημοσιογραφικής ακεραιότητας (SecureDrop (b), 2024).



Εικόνα 22. SecureDrop περιβάλλον χρήστη

3.10 GlobaLeaks

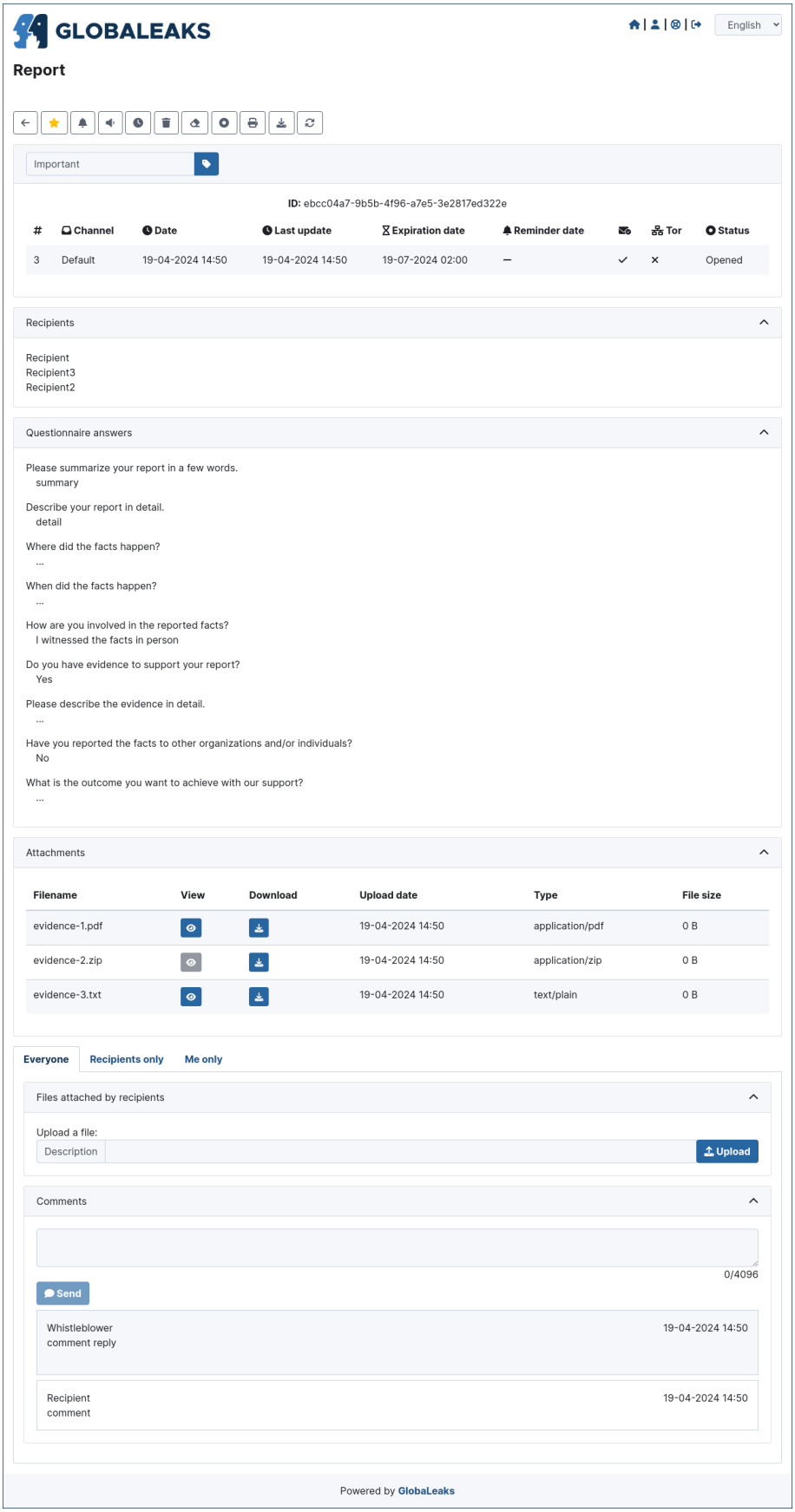
Το GlobaLeaks είναι μια πλατφόρμα καταγγελίας ανοιχτού κώδικα που έχει σχεδιαστεί για να παρέχει ασφαλή και ανώνυμα κανάλια σε άτομα προκειμένου να αναφέρουν κακώς κείμενα, διαφθορά ή άλλη ανήθικη συμπεριφορά. Το GlobaLeaks αναπτύχθηκε αρχικά στην Ιταλία. Το έργο συντονίζεται από τη Whistleblowing Solutions Impresa Sociale S.r.l. (WBS), μια καινοτόμα κοινωνική επιχείρηση με έδρα την Ιταλία και υποστηρίζεται από το Κέντρο Διαφάνειας και Ψηφιακών Ανθρωπίνων Δικαιωμάτων Hermes, μια μη κερδοσκοπική ένωση με έδρα επίσης την Ιταλία. Το Hermes Center ιδρύθηκε από μια ομάδα Ιταλών ακτιβιστών, δικηγόρων και υπερασπιστών ψηφιακών δικαιωμάτων για την ανάπτυξη και εφαρμογή τεχνολογιών ανοιχτού κώδικα που υποστηρίζουν την ελευθερία του λόγου και την προστασία των ανθρωπίνων δικαιωμάτων στην ψηφιακή εποχή (GlobaLeaks (a), 2024).

Εικόνα 23. Λογότυπο GlobaLeaks

Παρέχοντας έναν ασφαλή και ανώνυμο τρόπο αναφοράς ζητημάτων, το GlobaLeaks συμβάλλει στην προώθηση της διαφάνειας και της λογοδοσίας σε οργανισμούς και ιδρύματα. Το GlobaLeaks δίνει προτεραιότητα στην ασφάλεια και την ανωνυμία των καταγγελιών, χρησιμοποιώντας κρυπτογράφηση και άλλα προηγμένα μέτρα ασφαλείας για την προστασία της ταυτότητας των χρηστών και των πληροφοριών που παρέχουν (GlobaLeaks (b), 2024).

Η πλατφόρμα είναι εξαιρετικά προσαρμόσιμη, επιτρέποντας στους οργανισμούς να προσαρμόσουν το λογισμικό στις συγκεκριμένες ανάγκες και απαιτήσεις τους. Αυτό περιλαμβάνει την προσαρμογή των φορμών υποβολής, των ροών εργασίας και των συστημάτων ειδοποιήσεων. Το GlobaLeaks υποστηρίζει πολλές γλώσσες, καθιστώντας το προσβάσιμο σε ένα ευρύ φάσμα χρηστών σε όλο τον κόσμο. Η πλατφόρμα έχει σχεδιαστεί για να είναι φιλική προς τον χρήστη, διασφαλίζοντας ότι τόσο οι καταγγέλλοντες όσο και οι διαχειριστές μπορούν να τη χρησιμοποιούν αποτελεσματικά χωρίς να απαιτούνται εκτεταμένες τεχνικές γνώσεις (GlobaLeaks (c), 2024).

Συνολικά, το GlobaLeaks είναι ένα ισχυρό εργαλείο για οργανισμούς που επιθυμούν να εφαρμόσουν ή να βελτιώσουν τα συστήματα καταγγελίας και αναφοράς τους, ενισχύοντας μια κουλτούρα διαφάνειας και ηθικής συμπεριφοράς. Η χρήση του επεκτείνεται σε διάφορες περιπτώσεις όπως η καταπολέμηση της διαφθοράς (GlobaLeaks (d), 2024), η εταιρική υπευθυνότητα (GlobaLeaks (e), 2024), η προστασία των ανθρώπινων δικαιωμάτων (GlobaLeaks (f), 2024) και η ερευνητική Δημοσιογραφία (GlobaLeaks (g), 2024). Δύναται να βοηθήσει εταιρείες και οργανισμούς να συμμορφωθούν με διάφορες νομικές και κανονιστικές απαιτήσεις που σχετίζονται με τους μηχανισμούς καταγγελίας και αναφοράς.



Εικόνα 24. GlobaLeaks περιβάλλον χρήστη

3.11 OnionShare

Το OnionShare είναι ένα εργαλείο ανοιχτού κώδικα που επιτρέπει στους χρήστες να μοιράζονται ανώνυμα και με ασφάλεια αρχεία, να φιλοξενούν ιστότοπους και να συνομιλούν χρησιμοποιώντας το δίκτυο Tor. Το OnionShare αξιοποιεί τις υπηρεσίες του Tor για να εξασφαλίσει κρυπτογράφηση και ανωνυμία από άκρο σε άκρο παρέχοντας έτσι προστασία στους χρήστες και διατηρώντας ασφαλές το απόρρητό τους (Higgins, 2014).

Εικόνα 25. Λογότυπο OnionShare

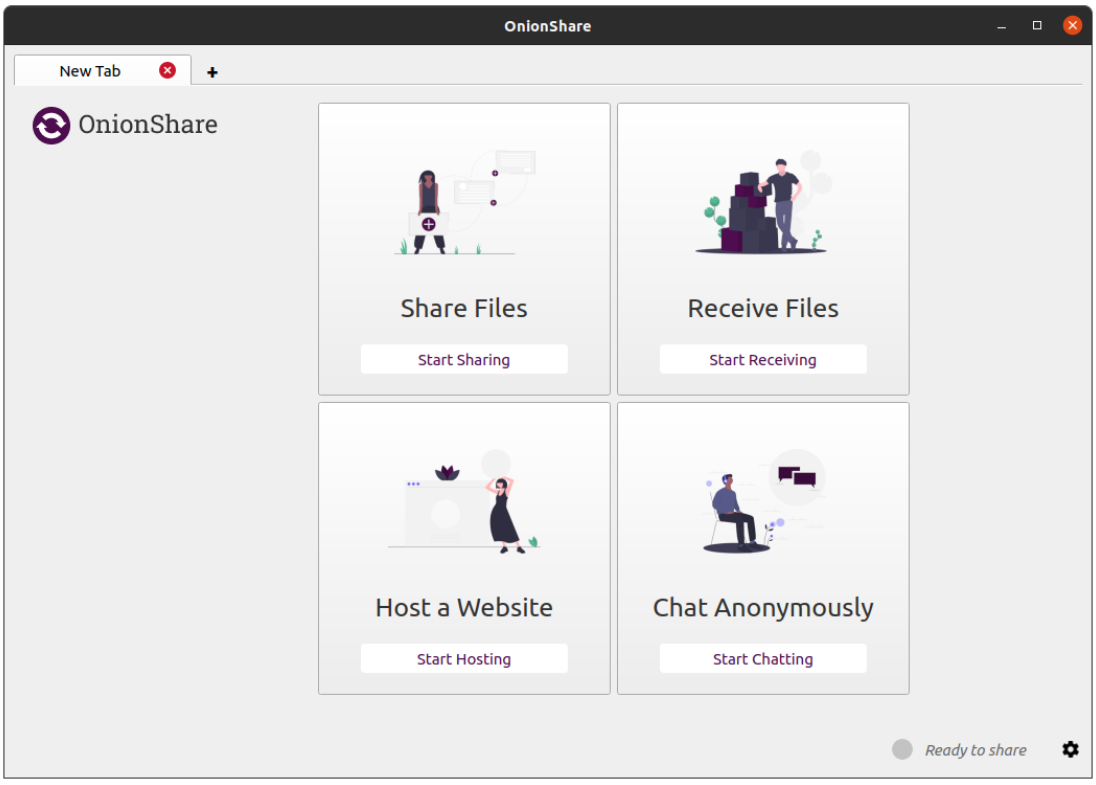
Οι χρήστες μπορούν να μοιράζονται αρχεία δημιουργώντας έναν διακομιστή web (Web Server) στον υπολογιστή τους, ο οποίος είναι προσβάσιμος μέσω μιας διεύθυνσης Tor onion. Αυτό διασφαλίζει ότι η διαδικασία κοινής χρήσης αρχείων παραμένει ανώνυμη και ασφαλής. Το OnionShare περιλαμβάνει επίσης μια λειτουργία λήψης αρχείων (Receive Files) επιτρέποντας στους χρήστες να λαμβάνουν αρχεία με ασφάλεια. Αυτό είναι ιδιαίτερα χρήσιμο για τη ρύθμιση ενός ανώνυμου αποθετηρίου, όπου άλλοι μπορούν να ανεβάζουν αρχεία απευθείας στο σύστημα. Το εργαλείο μπορεί να χρησιμοποιηθεί για τη φιλοξενία ιστοτόπων ανώνυμα, καθιστώντας το χρήσιμο για τη ρύθμιση κρυφών υπηρεσιών ή την κοινή χρήση περιεχομένου χωρίς να αποκαλύπτεται η ταυτότητα του κάθε χρήστη (Lee, 2024).

Το OnionShare υποστηρίζει πρόσκαιρες, ανώνυμες αίθουσες συνομιλίας που δεν καταγράφουν κανένα μήνυμα, παρέχοντας ένα ασφαλές περιβάλλον για ιδιωτικές συνομιλίες. Διαθέτει τη λειτουργία “Public Mode”, η οποία επιτρέπει τη δημιουργία δημόσιων διευθύνσεων OnionShare χωρίς slugs (τμήμα σε μια διεύθυνση URL που επιτρέπει την καλύτερη αναζήτηση), αποτρέποντας τον τερματισμό λειτουργίας του διακομιστή λόγω επαναλαμβανόμενων σφαλμάτων “404”. Οι χρήστες μπορούν να ενεργοποιήσουν τις μόνιμες διευθύνσεις να διατηρούν την ίδια διεύθυνση ακόμα και

μετά την επανεκκίνηση του διακομιστή, κάτι που είναι χρήσιμο για τη διατήρηση σταθερών σημείων πρόσβαση (Lee, 2024).

Το OnionShare είναι διαθέσιμο για Windows, macOS, Linux και έχει εκδόσεις για κινητά για Android και iOS. Έρχεται προεγκατεστημένο σε λειτουργικά συστήματα με επίκεντρο το απόρρητο όπως το QubesOS, το Tails και το ParrotOS.

Το εργαλείο διαθέτει διεπαφή με καρτέλες που επιτρέπει την ταυτόχρονη εκτέλεση πολλαπλών υπηρεσιών, όπως κοινή χρήση αρχείων, λήψη αρχείων, φιλοξενία ιστοτόπων και συνομιλία. Το OnionShare συνεχίζει να εξελίσσεται, με τακτικές ενημερώσεις και βελτιώσεις που στοχεύουν στη βελτίωση της λειτουργικότητας και της ασφάλειάς του. Το έργο διατηρείται ενεργά και υποστηρίζεται από μια κοινότητα προγραμματιστών.



Εικόνα 26. OnionShare περιβάλλον χρήστη

3.12 Tresorit

Το Tresorit είναι μια cloud υπηρεσία αποθήκευσης αρχείων που εστιάζει στην ασφάλεια και το απόρρητο. Ιδρύθηκε το 2011 και έχει την έδρα της στην Ελβετία. Η Ελβετία βοηθά την Tresorit να επωφεληθεί από τους ισχυρούς νόμους περί

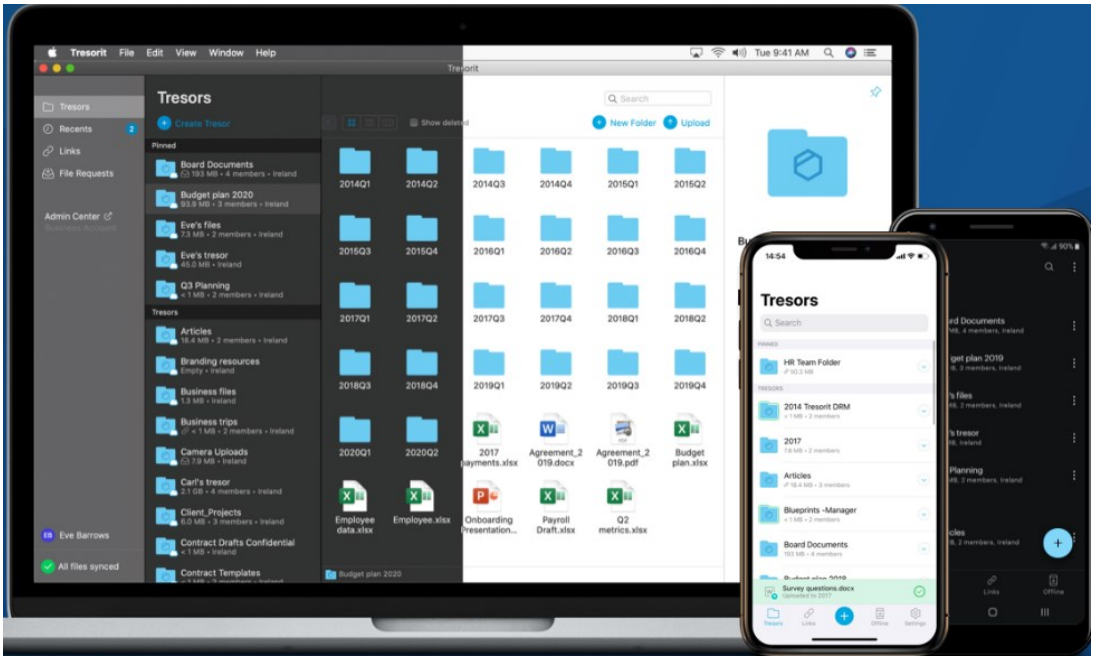
απορρήτου της χώρας και τη φήμη για την ασφάλεια των δεδομένων που τη συνοδεύει (Tresorit, 2024).

Εικόνα 27. Λογότυπο Tresorit

Το Tresorit επιτρέπει στους χρήστες να μοιράζονται αρχεία και φακέλους με ασφάλεια, διατηρώντας την κρυπτογράφηση κατά τη διαδικασία μεταφοράς. Τα αρχεία κρυπτογραφούνται στη συσκευή του χρήστη πριν μεταφορτωθούν στους διακομιστές του Tresorit, διασφαλίζοντας ότι μόνο ο χρήστης και όσοι μοιράζονται τα αρχεία μπορούν να έχουν πρόσβαση στα δεδομένα. Οι χρήστες μπορούν να έχουν πρόσβαση στα αρχεία τους από διάφορες συσκευές, συμπεριλαμβανομένων των Windows, macOS, Linux, iOS και Android. Το Tresorit προσφέρει εργαλεία για ομαδική συνεργασία, όπως κοινόχρηστους φακέλους και διαχείριση αδειών χρήστη, επιτρέποντας την ασφαλή ομαδική εργασία (Tresorit Team, 2023).

Το Tresorit συμμορφώνεται με διάφορους διεθνείς κανονισμούς προστασίας δεδομένων, συμπεριλαμβανομένου του GDPR. Επιπλέον, το Tresorit λειτουργεί σύμφωνα με μια πολιτική μηδενικής γνώσης (Zero-Knowledge Policy) που σημαίνει ότι η εταιρεία δεν έχει πρόσβαση σε κλειδιά ή δεδομένα κρυπτογράφησης (encryption keys or data) χρηστών, διασφαλίζοντας τη μέγιστη προστασία της ιδιωτικότητας (Lám, 2023). Το Tresorit περιλαμβάνει λειτουργίες όπως έλεγχο ταυτότητας δύο παραγόντων (2FA) – ο έλεγχος ταυτότητας δύο παραγόντων (2FA) είναι μια μέθοδος διαχείρισης ταυτοτήτων και πρόσβασης που απαιτεί δύο μορφές ταυτοποίησης για την πρόσβαση σε πόρους και δεδομένα.

Το Tresorit είναι ιδιαίτερα δημοφιλές εργαλείο μεταξύ των επιχειρήσεων και των ατόμων που δίνουν προτεραιότητα στην ασφάλεια και το απόρρητο δεδομένων στις cloud λύσεις αποθηκευτικού χώρου.



Εικόνα 28. Tresorit περιβάλλον χρήστη

3.13 Telegram

Το Telegram είναι μια υπηρεσία άμεσων μηνυμάτων, VoIP (Voice over IP) και βιντεοκλήσεων. Το Telegram ξεκίνησε το 2013 από τα αδέρφια Nikolai και Pavel Durov. Ο Parev Durov είναι γνωστός για την ίδρυση του ρωσικού κοινωνικού δικτύου VK (Matthias, 2024).

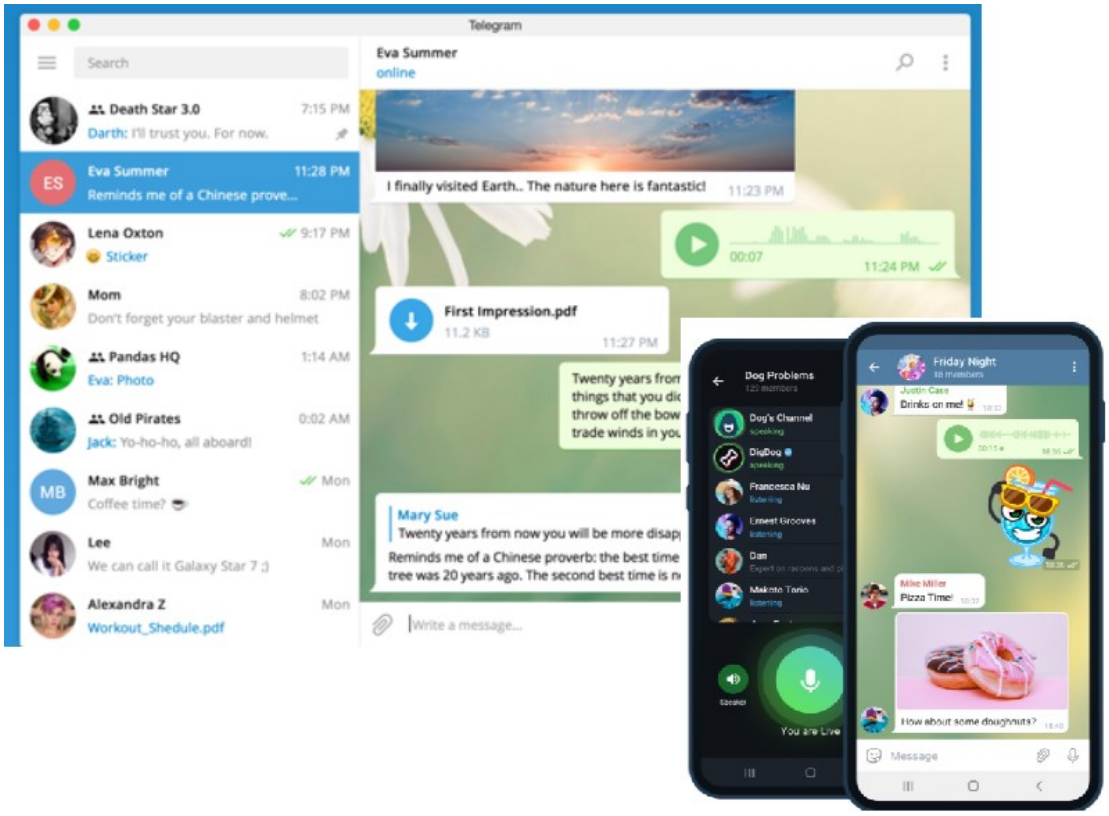
Εικόνα 29. Λογότυπο Telegram

Το Telegram επιτρέπει στους χρήστες να στέλνουν μηνύματα κειμένου, φωνητικά μηνύματα, αρχεία πολυμέσων και έγγραφα οποιουδήποτε τύπου με ασφαλή τρόπο. Όλα τα μηνύματα και τα πολυμέσα αποθηκεύονται στο cloud, επιτρέποντας στους χρήστες να έχουν πρόσβαση στις συνομιλίες και τα αρχεία τους από διαφορετικές συσκευές. Υποστηρίζει κρυπτογράφηση από άκρο σε άκρο για τις «μυστικές συνομιλίες» του (secret chats), διασφαλίζοντας ότι τα μηνύματα μπορούν να διαβαστούν μόνο από τον αποστολέα και τον παραλήπτη Το Telegram υποστηρίζει μεγάλες ομαδικές συνομιλίες -έως 200.000 μέλη- και δημόσια ή ιδιωτικά κανάλια, όπου οι χρήστες μπορούν να μεταδίδουν μηνύματα σε απεριόριστους συνδρομητές (Telegram, 2024).

Επιπλέον, προσφέρει μια ισχυρή Διεπαφή Προγραμματισμού Εφαρμογών API (Application Programming Interface) (Telegram, 2024) που επιτρέπει στους προγραμματιστές να δημιουργούν bots - συντομογραφία για το robot - τα οποία είναι λογισμικό που λειτουργεί ως «πράκτορας» (agent) για έναν χρήστη ή άλλο πρόγραμμα ή για την προσομοίωση μιας ανθρώπινης δραστηριότητας. Τα bots χρησιμοποιούνται συνήθως για την αυτοματοποίηση ορισμένων εργασιών, που σημαίνει ότι μπορούν να εκτελούνται χωρίς συγκεκριμένες οδηγίες από ανθρώπους για διάφορους σκοπούς, όπως υποστήριξη πελατών, ενημερώσεις ειδήσεων και πολλά άλλα (Lutkevich & Gillis, 2022).

Το Telegram είναι διαθέσιμο σε πολλές πλατφόρμες, συμπεριλαμβανομένων των iOS, Android, Windows, macOS και Linux, καθώς και μέσω προγραμμάτων περιήγησης ιστού. Η συγκεκριμένη πλατφόρμα δίνει έμφαση στο απόρρητο και την ασφάλεια των χρηστών, προσφέροντας λειτουργίες όπως μηνύματα που καταστρέφονται (self-destructing messages) κλειδώματα κωδικών πρόσβασης και τη δυνατότητα διαγραφής μηνυμάτων από όλες τις συσκευές.

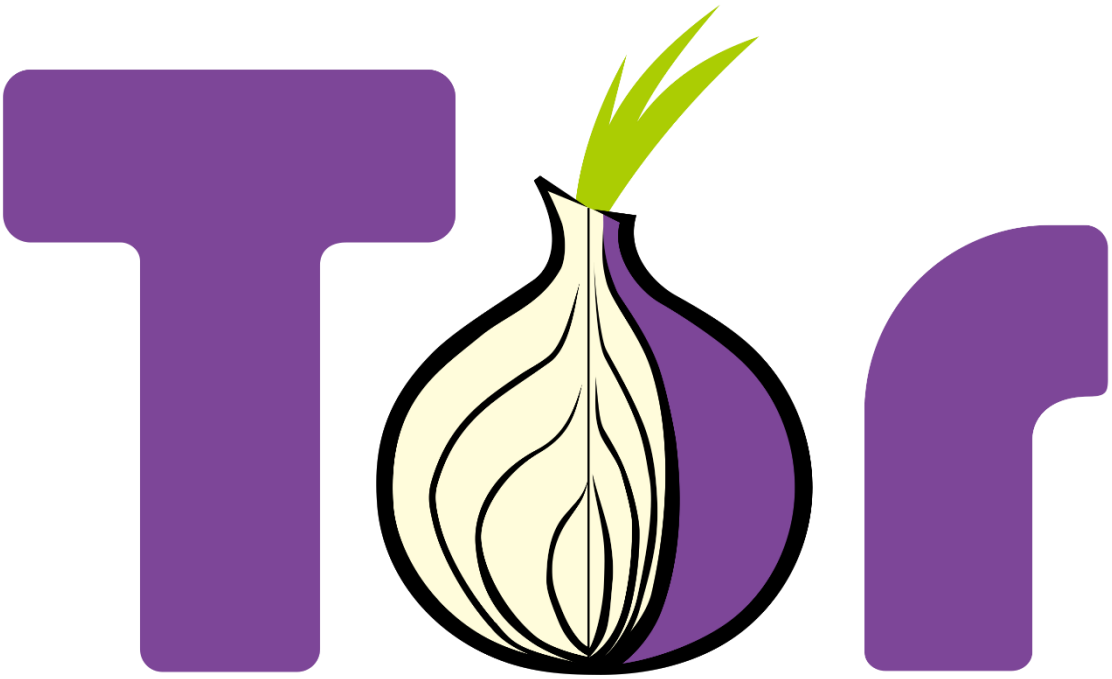
Το Telegram έχει κερδίσει δημοτικότητα λόγω της ταχύτητας, των χαρακτηριστικών ασφαλείας και της ευελιξίας του, καθιστώντας το μια προτιμώμενη εφαρμογή ανταλλαγής μηνυμάτων για πολλούς χρήστες σε όλο τον κόσμο.



Εικόνα 30. Telegram περιβάλλον χρήστη

3.14 Tor browser

Λαμβάνοντας υπόψη ότι αναφέρθηκε αρκετά φορές προηγουμένως η χρήση του Tor browser, κρίνεται σκόπιμο να γίνει μια επισκόπηση του εν λόγω λογισμικού. Το Tor browser είναι ένα πρόγραμμα περιήγησης ιστού που έχει σχεδιαστεί για να παρέχει ανώνυμη και ασφαλή περιήγηση στο Διαδίκτυο, δρομολογώντας την κυκλοφορία μέσω του δικτύου Tor. Είναι ένα εργαλείο για χρήστες που έχουν αυξημένες απαιτήσεις για απόρρητο και ασφάλεια, συμπεριλαμβανομένων δημοσιογράφων, ακτιβιστών και ατόμων σε περιοχές με αυστηρή λογοκρισία στο Διαδίκτυο.



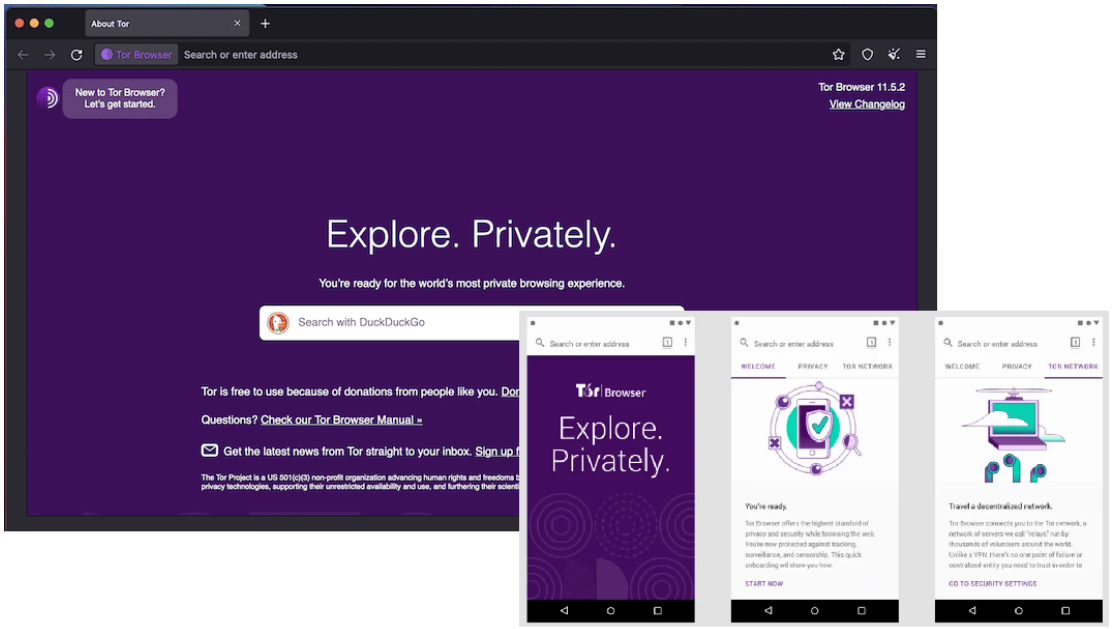
Εικόνα 31. Λογότυπο Tor browser

Το Tor, συντομογραφία του The Onion Router, είναι ένα αποκεντρωμένο δίκτυο που ανωνυμοποιεί την κίνηση που καταγράφεται κατά την περιήγηση στο Διαδίκτυο. Αυτό το επιτυγχάνει μεταβαίνοντας μέσω πολλών διακομιστών που λειτουργούν από εθελοντές και ονομάζονται κόμβοι ή αναμεταδότες, σε όλο τον κόσμο. Αυτή η διαδικασία κρυπτογραφεί τα δεδομένα πολλές φορές, όπως και τα στρώματα ενός κρεμμυδιού, παρέχοντας έτσι ισχυρή ανωνυμία και προστασία από την παρακολούθηση και την ανάλυση της διαδικτυακής κίνησης (Tor, 2024).

Η ανάγκη για εργαλεία προστασίας από παρακολουθήσεις έγινε κύρια ανησυχία χάρη στις αποκαλύψεις του Snowden το 2013, όπως παρουσιάσθηκε και στο Κεφάλαιο 2.4.2.2. Το Tor browser είχε καθοριστικό ρόλο στις αποκαλύψεις του Edward Snowden. Στη συγκεκριμένη υπόθεση ήταν αυταπόδεικτο ότι δεν υπήρξε παρακολούθηση του Tor browser καθώς αν κάτι τέτοιο είχε γίνει, θα ήταν αδύνατο να δημοσιευθούν τα έγγραφα με το περιεχόμενο που ήρθε στη δημοσιότητα (Tor, 2024). Η τεράστια δημοσιότητα που πήρε το όλο εγχείρημα του Tor αλλά και η αφοσίωση της ομάδας που το αναπτύσσουν για τη διασφάλιση της ιδιωτικότητας αλλά και την ελευθερία της έκφρασης στο Διαδίκτυο, έχει καταστήσει το Tor ένα από τα πιο διαδεδομένα και ισχυρά εργαλεία στον κόσμο, όταν έχει να κάνει με την ανώνυμη και χωρίς λογοκρισία πρόσβαση στο Διαδίκτυο.

Το βασικό χαρακτηριστικό του Tor browser είναι η εξασφάλιση της ανωνυμίας και του απορρήτου. Πιο συγκεκριμένα, το πρόγραμμα περιήγησης Tor αποκρύπτει τη διεύθυνση IP και τις διαδικτυακές δραστηριότητες, δυσκολεύοντας έτσι τους ιστότοπους καθώς και τρίτους από το να παρακολουθούν την κίνηση στο Διαδίκτυο. Επιπλέον, λόγω του τρόπου λειτουργίας του που περιγράφηκε παραπάνω με τους πολλαπλούς διακομιστές, ευνοεί τους χρήστες να παρακάμψουν οποιοδήποτε φραγμό και απαγορεύσεις πρόσβασης σε ιστοσελίδες, ειδικά σε χώρες, όπου υπάρχουν εκτεταμένοι περιορισμοί στο Διαδίκτυο. Με αυτόν τον τρόπο, επιτυγχάνεται παράκαμψη της λογοκρισίας που αποτελεί ζητούμενο στην αξιόπιστη Δημοσιογραφία. Η έμφαση στην ασφάλεια με την εφαρμογή πολλαπλών μέτρων αποτελεί βασικό χαρακτηριστικό του Tor browser. Έτσι, το Tor έχει σχεδιαστεί ώστε να εμποδίζει τους ιστότοπους να συλλέγουν δεδομένα περιήγησης, εφαρμόζοντας προηγμένες μεθόδους κρυπτογράφησης. Με αυτόν τον τρόπο, διασφαλίζεται η ανωνυμία και η προστασία των χρηστών αποκλείοντας πιθανές απειλές και κινδύνους που μπορούν να οδηγήσουν στην ταυτοποίηση ενός ατόμου (Tor project (a), 2024; Tor project (b), 2024).

Το Tor browser έχει αδιαμφισβήτητα πολλαπλά οφέλη και αποτελεί ένα αρκετά διαδεδομένο εργαλείο για ασφαλή περιήγηση στο Διαδίκτυο. Ωστόσο, έχει και κάποιους περιορισμούς. Η ταχύτητα περιήγησης πολλές φορές είναι πιο αργή από τους συμβατικούς περιηγητές λόγω της λειτουργίας που περιγράφηκε παραπάνω με τους πολλαπλούς διακομιστές. Επίσης, λόγω της σύνδεσης του Tor browser με το σκοτεινό Διαδίκτυο (Dark Web) και τη συσχέτιση αυτού με παράνομες δραστηριότητες, υπάρχουν ιστοσελίδες που αποκλείουν την επίσκεψη σε αυτές μέσω Tor ή ενδέχεται να αντιμετωπίζουν προβλήματα συμβατότητας.



Εικόνα 32. Tor browser περιβάλλον χρήστη

4 Μεθοδολογία

Στο παρόν κεφάλαιο γίνεται μια καταγραφή και παρουσίαση της μεθοδολογίας που ακολουθήθηκε για το ερευνητικό κομμάτι της εργασίας. Έτσι, αρχικά παρατίθενται κάποια γενικά στοιχεία και οι στόχοι που καλούνται να επιτευχθούν μέσω του συγκεκριμένου ερωτηματολογίου, στη συνέχεια γίνεται αναφορά στον σχεδιασμό του και καταληκτικά στο κοινό στο οποίο επικοινωνήθηκε.

4.1 Γενικά στοιχεία της μεθοδολογίας και στόχοι

Σε ερευνητικές εργασίες όπως αποτελεί και η παρούσα, ο διαμοιρασμός ερωτηματολογίων έχει ως στόχο να συνεισφέρει σε μεγάλο και σημαντικό βαθμό στη συγκέντρωση πληροφοριών από ένα σύνολο ατόμων, τα οποία έχουν τη δυνατότητα να εκφράσουν τη γνώμη τους ανώνυμα και ιδιωτικά χωρίς άγχος ή ανησυχία μήπως οι απόψεις τους κατηγορηθούν λόγω του ότι αντιβαίνουν με τη γενική σύμφωνη γνώμη. Τα ερευνητικά ερωτηματολόγια είναι απαραίτητα εργαλεία στην ακαδημαϊκή έρευνα, παρέχοντας έναν συστηματικό τρόπο συλλογής δεδομένων από έναν πληθυσμό-στόχο. Είναι ιδιαίτερα πολύτιμα στον τομέα της Δημοσιογραφίας, όπου η κατανόηση των πρακτικών επικοινωνίας είναι ζωτικής σημασίας.

Στο ταχέως εξελισσόμενο τοπίο της Δημοσιογραφίας, η χρήση ασφαλών πλατφορμών επικοινωνίας γίνεται όλο και πιο σημαντική. Οι δημοσιογράφοι βασίζονται σε αυτές τις πλατφόρμες για να προστατεύσουν τις πηγές τους και να διασφαλίσουν την εμπιστευτικότητα των ευαίσθητων πληροφοριών. Το ερευνητικό ερωτηματολόγιο στο πλαίσιο της παρούσας εργασίας έχει ως σκοπό να βοηθήσει στην κατανόηση ερωτημάτων και ζητημάτων όπως το πώς χρησιμοποιούνται αυτές οι πλατφόρμες, τις προκλήσεις που αντιμετωπίζουν και τον αντίκτυπο στις δημοσιογραφικές πρακτικές. Συλλέγοντας δεδομένα απευθείας από επαγγελματίες του χώρου της Δημοσιογραφίας καθίσταται δυνατό το να εντοπισθούν τάσεις, κενά στη γνώση και τομείς που χρήζουν βελτίωσης.

Ένα ορθά σχεδιασμένο ερωτηματολόγιο περιλαμβάνει έναν συνδυασμό τύπων ερωτήσεων, όπως πολλαπλής επιλογής ή δυαδικής επιλογής - κλειστού τύπου όπως ονομάζονται - καθώς και ανοιχτού τύπου – ελεύθερου κειμένου – για τη συλλογή περιεκτικών δεδομένων. Οι ερωτήσεις ανοιχτού τύπου επιτρέπουν στους ερωτηθέντες να παρέχουν λεπτομερείς, διακριτικές απαντήσεις, προσφέροντας πληροφορίες που

μπορεί να μην προκύψουν από ερωτήσεις κλειστού τύπου. Ωστόσο, οι ερωτήσεις ανοιχτού τύπου μπορεί να είναι χρονοβόρες για ανάλυση. Από την άλλη, οι ερωτήσεις κλειστού τύπου πολλαπλής επιλογής και της κλίμακας Likert (Robinson, 2014), είναι πιο εύκολο να ποσοτικοποιηθούν και να αναλυθούν στατιστικά. Οι ερωτήσεις πολλαπλής επιλογής παρέχουν προκαθορισμένες απαντήσεις, απλοποιώντας τη συλλογή και ανάλυση δεδομένων. Οι ερωτήσεις της κλίμακας Likert μετρούν την ένταση των απόψεων ή των συμπεριφορών των ερωτηθέντων, χρήσιμες για τη μέτρηση της στάσης π.χ., απέναντι σε ασφαλείς πλατφόρμες επικοινωνίας.

Σκοπός λοιπόν του ερωτηματολογίου που μοιράσθηκε στο πλαίσιο της παρούσας εργασίας ήταν να καταγράψει τις τάσεις και τις απόψεις των συμμετεχόντων σχετικά με τις πλατφόρμες ασφαλούς επικοινωνίας αλλά και σχετικά με τους κίνδυνους και τις προκλήσεις της νέας ψηφιακής εποχής. Έτσι, βάσει των δομημένων ερωτημάτων που τέθηκαν στο ερωτηματολόγιο, τα οποία είχαν μια λογική συνέχεια προκειμένου να βοηθήσουν την/τον ερωτηθείσα/ερωτηθέντα να απαντήσει εύκολα και γρήγορα, προέκυψαν σημαντικά στοιχεία, τα οποία θα παρουσιασθούν και θα αναλυθούν στο επόμενο κεφάλαιο.

4.2 Σχεδιασμός και υλοποίηση ερωτηματολογίου

Ο σχεδιασμός ενός ερωτηματολογίου έχει άμεση σχέση και εξάρτηση από το είδος των πληροφοριών που πρέπει να συλλεχθούν. Τα ποιοτικά ερωτηματολόγια σχεδιάζονται όταν προκύπτει ανάγκη συγκέντρωσης διερευνητικών δεδομένων ή επαλήθευσης - διάψευσης μιας υπόθεσης. Τα ποσοτικά ερωτηματολόγια σχεδιάζοντας σε περιπτώσεις που αφορούν επικύρωση ή έλεγχο οποιασδήποτε προηγηθείσας υπόθεσης που έχει δημιουργηθεί.

Το παρόν ερωτηματολόγιο δομήθηκε με συνολικά 33 ερωτήματα. Αρχικά, στις πρώτες επτά ερωτήσεις οι ερωτηθέντες κλήθηκαν να δώσουν κάποιες πληροφορίες σχετικά με δημογραφικά στοιχεία όπως φύλο, ηλικία, επίπεδο εκπαίδευσης, είδος επαγγελματικής ενασχόλησης καθώς και καλυπτόμενη θεματική κατηγορία στον χώρο εργασίας. Οι υπόλοιπες είκοσι έξι ερωτήσεις αποτέλεσαν το κυρίως «σώμα» του ερωτηματολογίου όπου ζητήθηκαν να δοθούν γενικές ειδικές απαντήσεις σχετικά με τις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιούν στον χώρο εργασίας

τους οι δημοσιογράφοι ή επαγγελματίες που έχουν συνάφεια με τον τομέα της Δημοσιογραφίας αλλά και σχετικά με τις συνήθειές τους και τις απόψεις τους αναφορικά με την ασφάλεια, τις προκλήσεις και τους κινδύνους της ψηφιακής εποχής.

Οι συμμετέχοντες ερωτήθηκαν αναφορικά με τη χρήση ή μη πλατφορμών ασφαλούς επικοινωνίας στην εργασία τους, τη συχνότητα χρήσης αυτών και συγκεκριμένα έγινε αναφορά στις δώδεκα που παρουσιάσθηκαν στο Κεφάλαιο 3: Nextcloud, Wickr, Proton Mail, Signal, Threema, Wire, WhatsApp, SecureDrop, GlobaLeaks, OnionShare, Tresorit και Telegram. Εν συνεχεία, οι συμμετέχοντες ερωτήθηκαν αναφορικά με τη γνώση περί της δυνατότητας κρυπτογράφησης στην αποστολή και λήψη emails αλλά και το αν γίνεται χρήση αυτού του επαγγελματικού εργαλείου. Επιπλέον, μέσω προκαθορισμένης λίστας απαντήσεων δόθηκαν απαντητικές διευκρινίσεις σχετικά με το ποιες λειτουργίες των πλατφορμών ασφαλούς επικοινωνίας βρίσκουν οι ερωτηθέντες πιο επωφελείς καθώς και ποιοι παράγοντες επηρέασαν την επιλογή τους για τη χρήση των πλατφορμών αυτών.

Σημαίνουσα βαρύτητα δόθηκε στο κομμάτι της ασφάλειας επικοινωνιών στον χώρο εργασίας. Οι ερωτηθέντες κλήθηκαν να αποτυπώσουν την άποψή τους σχετικά με το εάν πιστεύουν ότι τίθεται θέμα ασφαλείας επικοινωνιών στην άσκηση της Δημοσιογραφίας, με το πόσο βέβαιοι είναι όσον αφορά την ασφάλεια και την ιδιωτικότητα των πλατφορμών ασφαλούς επικοινωνίας που χρησιμοποιούν και με το ποιες προκλήσεις έρχονται αντιμέτωποι τη σύγχρονη εποχή οι δημοσιογράφοι. Εν συνεχεία, από το ερωτηματολόγιο εξήχθησαν συμπεράσματα σχετικά με την εμπειρία των ερωτηθέντων παραβίασης της επικοινωνίας στον εργασιακό βίο και αν αυτό το γεγονός έδρασε ως ανασταλτικός παράγοντας στην ορθή άσκηση των επαγγελματικών τους καθηκόντων.

Καταληκτικά, οι ερωτηθέντες έδωσαν τις απαντήσεις τους στο εάν γνωρίζουν αλλά και ποιες πρακτικές εφαρμόζουν προκειμένου να διασφαλίσουν την ασφαλή επικοινωνία και τη διαφύλαξη των πηγών τους στον χώρο εργασίας τους καθώς επίσης υπογράμμισαν τους τρόπους με τους οποίους επενδύουν στην επαγγελματική τους εκπαίδευση και κατάρτιση ούτως ώστε να αποκτήσουν και να εμπλουτίσουν τις γνώσεις τους σχετικά με την ασφαλή επικοινωνία και διαμοίραση πληροφοριών μέσω Διαδικτύου.

Έτσι, το ερωτηματολόγιο το οποίο αναπτύχθηκε για τις ανάγκες της παρούσας εργασίας είναι διαθέσιμο στο Παράρτημα 2: Ερωτηματολόγιο. Η δομή του ερωτηματολογίου συνοπτικά και οι ενότητες στις οποίες εντάχθηκαν οι 33 ερωτήσεις για τους συμμετέχοντες της έρευνας είναι οι παρακάτω:

1. **Εισαγωγή:** Αποτελεί την πρώτη σελίδα του ερωτηματολογίου στην οποία υπάρχει το καλωσόρισμα στη/στον συμμετέχουσα/συμμετέχοντα και κάποιες γενικές πληροφορίες σχετικά με το ερωτηματολόγιο, το πλαίσιο στο οποίο διαμοιράσθηκε, τα στοιχεία της εργασίας και του συγγραφέα αυτής καθώς και του επιβλέποντα καθηγητή. Επίσης, τονίζεται ότι η συμμετοχή είναι ανώνυμη και προστατευμένα με βάση τον νόμο 4624/2019 που αφορά την προστασία των προσωπικών δεδομένων.
2. **Προσωπικά στοιχεία:** Στην παρούσα ενότητα οι συμμετέχοντες κλήθηκαν να παράσχουν κάποιες γενικές πληροφορίες σχετικά με δημογραφικά τους στοιχεία όπως το φύλο, η ηλικία και το επίπεδο εκπαίδευσης. Επισημαίνεται ότι δεν ζητήθηκαν προσωπικά στοιχεία που μπορούσαν να οδηγήσουν με τον οποιοδήποτε τρόπο στην ταυτοποίηση ενός προσώπου διατηρώντας έτσι την ανωνυμία τους.
3. **Πληροφορίες σχετικά με τον τομέα απασχόλησής σας:** Συνεχίζοντας στην ενότητα αυτή ζητήθηκε από τους ερωτηθέντες να απαντήσουν σε μία σειρά ερωτήσεων σχετικά με την απασχόλησή τους όπως την ιδιότητά τους, τη σχέση εργασίας τους, η θεματολογία των ειδήσεων που καλύπτουν κ.α.
4. **Χρήση πλατφορμών ασφαλούς επικοινωνίας στην εργασία σας:** Η ενότητα αυτή του ερωτηματολόγιου αποτέλεσε το κύριο μέρος του καθώς οι συμμετέχοντες κλήθηκαν να απαντήσουν σχετικά με τις γνώσεις τους, τα χαρακτηριστικά των πλατφορμών ασφαλούς επικοινωνίας αλλά και το εάν και πόσο χρησιμοποιούν τέτοιες πλατφόρμες και αν θα τις πρότειναν.
5. **Ασφάλεια επικοινωνιών στην εργασία σας:** Στο συγκεκριμένο τμήμα του ερωτηματολόγιου έγινε καταγραφή των απόψεων σχετικά με τους κινδύνους και τις προκλήσεις στην ασφάλεια των επικοινωνιών στην εργασία τους.
6. **Εμπειρία από παραβίαση επικοινωνίας στην εργασία:** Η εν λόγω ενότητα είχε ως σκοπό να καταγράψει μέσω απλών ερωτημάτων την εμπειρία των ερωτηθέντων σχετικά με ενδεχόμενη παραβίαση της επικοινωνίας τους στο

πλαίσιο της εργασίας τους και κατά πόσο αυτό τους επηρέασε ή τους προβλημάτισε ούτως ώστε να εγκαταλείψουν κάποιο θέμα που ερευνούν, την επικοινωνία με συναδέλφους ή με τις πηγές τους ή να εγκαταλείψουν ακόμα και την ίδια τη Δημοσιογραφία.

7. **Εφαρμογή πρακτικών που διασφαλίζουν την ασφαλή επικοινωνία:** Συνεχίζοντας οι συμμετέχοντες απάντησαν σε δύο ερωτήσεις σχετικά με το εάν γνωρίζουν καλές πρακτικές που διασφαλίζουν την ασφαλή επικοινωνία στο Διαδίκτυο και αν χρησιμοποιούν κάποιες από αυτές στην εργασία τους.
8. **Κατοχή γνώσεων ασφαλούς επικοινωνίας και τρόπος απόκτησής τους:** Καταληκτικά, οι ερωτηθέντες κλήθηκαν να απαντήσουν αν έχουν κάποιες γνώσεις γενικότερα σχετικά με την ασφαλή επικοινωνία και την κοινή χρήση αρχείων μέσω Διαδικτύου καθώς και για το εάν θα ήθελαν να εφαρμόσουν ή εφαρμόζουν κάποιες πρακτικές για την απόκτηση γνώσης σχετικά με την ασφάλεια στις επικοινωνίες στο Διαδίκτυο.

4.3 Στοχευμένο κοινό και διαμοιρασμός

4.3.1 Δημοσιογραφικές ενώσεις

Τα ερωτηματολόγια μπορούν να διανεμηθούν με ποικίλους τρόπους όπως για παράδειγμα να σταλούν με ταχυδρομείο ή να επισυναφθούν ως συνημμένο μήνυμα ηλεκτρονικού ταχυδρομείου. Επίσης, μπορούν να δημοσιευθούν σε διάφορους ιστότοπους στο Διαδίκτυο ή ακόμα να δοθούν προσωπικά σε κάθε άτομο, όπως επίσης να διαμοιραστούν μέσα σε ένα ακροατήριο, σε άτομα δηλαδή που τυγχάνει να λαμβάνουν μέρος σε ένα συνέδριο ή μια ημερίδα. Στην προκειμένη περίπτωση, το ερωτηματολόγιο απεστάλη μέσω του ηλεκτρονικού ταχυδρομείου (επισυνάπτοντας τον σχετικό σύνδεσμο που οδηγούσε στην πλατφόρμα Google Forms) για λόγους ευχρηστίας και οικονομίας χρόνου.

Το κοινό στο οποίο διαμοιράσθηκε υπό τη μορφή Google Forms ήταν στοχευμένο και αποτελείτο από επαγγελματίες δημοσιογράφους και δημοσιογραφικές ενώσεις. Συγκεκριμένα, το ερωτηματολόγιο με αρωγό τον επιβλέποντα καθηγητή Ανδρέα Βέγλη προωθήθηκε στην Ένωση Συντακτών Ημερήσιων Εφημερίδων Μακεδονίας -

Θράκης (ΕΣΗΕΜ-Θ)[18], στην Ένωση Συντακτών Ημερήσιων Εφημερίδων Θεσσαλίας – Στερεάς Ελλάδας – Εύβοιας (ΕΣΗΕΘΣΤΕ-Ε)[19] και στην Ένωση Συντακτών Ημερησίων Εφημερίδων Πελοποννήσου - Ηπείρου - Νήσων (ΕΣΗΕΠΗΝ)[20].

Η Ένωση Συντακτών Ημερησίων Εφημερίδων Μακεδονίας-Θράκης είναι ένα από τα παλαιότερα σωματεία της Θεσσαλονίκης και η αρχαιότερη από τις σημερινές δημοσιογραφικές οργανώσεις της χώρας. Η πορεία της περιλαμβάνει σελίδες όχι μόνο επαγγελματικής, αλλά και εθνικής, κοινωνικής και πολιτιστικής προσφοράς. Μιας προσφοράς που είχε αρχίσει από άλλα συνδικαλιστικά όργανα δημοσιογράφων της Θεσσαλονίκης, τα οποία με άλλες επωνυμίες, αλλά με σχεδόν τα ίδια μέλη, είχαν εμφανιστεί από την περίοδο της τουρκικής κυριαρχίας και από τα πρώτα χρόνια της ελεύθερης ζωής της Θεσσαλονίκης. Η σημερινή δύναμη της ΕΣΗΕΜ-Θ είναι 874 μέλη, όλων των Μαζικών Μέσων Ενημερώσεως και από ολόκληρη τη Μακεδονία και τη Θράκη. Μεταξύ των σκοπών της Ένωσης, όπως αυτοί ορίζονται στο καταστατικό της, είναι «η ηθική και οικονομική συμβολή στη μελέτη των γενικότερων (πολιτιστικών, εκπαιδευτικών, οικονομικών, κοινωνικών, πληροφόρησης, ελευθερίας) προβλημάτων και επιδιώξεων του Τύπου και των ΜΜΕ στον ελλαδικό, βαλκανικό και διεθνή χώρο», καθώς και «η συμβολή στην εν γένει ανάπτυξη της χώρας και ειδικότερα της Μακεδονίας-Θράκης». Στο πλαίσιο αυτό, η ΕΣΗΕΜ-Θ αναπτύσσει σειρά δραστηριοτήτων, μεταξύ των οποίων η λειτουργία Κέντρου Τεκμηρίωσης στο βαλκανικό Κέντρο Τύπου, η συμμετοχή σε ευρωπαϊκά χρηματοδοτούμενα προγράμματα, η εκτεταμένη συνεργασία με φορείς και αρχές της Θεσσαλονίκης και της Μακεδονίας-Θράκης εν γένει. Παράλληλα, με την ίδρυση του Μορφωτικού της Ιδρύματος επαληθεύει τον ρόλο της ως πνευματικού φορέα και την πάγια μέριμνά της για τη δια βίου εκπαίδευση των μελών της (Ένωση Συντακτών Ημερησίων Εφημερίδων Μακεδονίας-Θράκης, 2024).

Η Ένωση Συντακτών Ημερήσιων Εφημερίδων Θεσσαλίας – Στερεάς Ελλάδας – Εύβοιας συνεστήθη βάσει του νόμου 1093 του 1938. Η ΕΣΗΕΘΣΤΕ-Ε πρωτοστάτησε στην καθιέρωση της κυριακάτικης αργίας με βάση τον νόμο 1092 του 1938 περί

[18] https://esiemth.gr
[19] https://www.pressunion.gr
[20] https://www.esiepin.gr

Τύπου. Στο άρθρο 37 οριζόταν σαφώς: «Καθιερούται η Κυριακή αργία δι᾽ άπαν το προσωπικόν των εκδιδομένων εντός των ορίων της Επικρατείας Ημερησίων Εφημερίδων». Η σημερινή μορφή της Ένωσης προέκυψε μετά από πολλές αναθεωρήσεις του καταστατικού της. Το1949 (8 Μαϊου) εγκρίνεται καινούργιο καταστατικό του σωματείου υπό την επωνυμία «Ένωσις Συντακτών Ημερησίων Εφημερίδων Θεσσαλίας, Στερεάς Ελλάδος και Ευβοίας» με έδρα τον Βόλο. Θα ακολουθήσουν στο δεύτερο μισό του εικοστού αιώνα αλλεπάλληλες τροποποιήσεις του καταστατικού και συγκεκριμένα το 1951, το 1957, το 1964, το 1973, το 1979, το 1986 και το 1997. Κατά το καταστατικό του 1997 η ΕΣΗΕΘΣΤΕ-Ε συμμετέχει ως ιδρυτικό μέλος στην Πανελλήνια Ομοσπονδία Ενώσεων Συντακτών (Π.Ο.Ε.Σ.Υ.), ύστερα από απόφαση της Συνέλευσης του Ιανουαρίου 1994. Με την ίδρυση της Π.Ο.Ε.Σ.Υ. ικανοποιήθηκε, κατά κάποιο τρόπο, ένα παλιό αίτημα της ΕΣΗΕΘΣΤΕ-Ε καθώς και των άλλων Ενώσεων Συντακτών της χώρας (ΕΝΩΣΗ ΣΥΝΤΑΚΤΩΝ ΗΜΕΡΗΣΙΩΝ ΕΦΗΜΕΡΙΔΩΝ ΘΕΣΣΑΛΙΑΣ - ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ - ΕΥΒΟΙΑΣ, 2024). Αυτή τη στιγμή με βάση τα επίσημα στοιχεία της Ένωσης στην ιστοσελίδα τους αριθμούν 186 μέλη και πληθώρα επαρχιακών και τοπικών μέσων.

Η αρχή της λειτουργίας της Ένωσης των Συντακτών των Ημερησίων Εφημερίδων Πελοποννήσου, Ηπείρου και Νήσων, της ΕΣΗΕΠΗΝ, δεν συνέπεσε με την πρώτη εμφάνιση της Δημοσιογραφίας στην Πάτρα και στην ευρύτερη περιοχή ή τουλάχιστον δεν την ακολούθησε, ύστερα από μικρό σχετικά χρονικό διάστημα. Σημειώθηκε 100 περίπου χρόνια μετά την κυκλοφορία της πρώτης ελληνικής εφημερίδας σ’ αυτόν το χώρο, του «Αχαϊκού Κήρυκος», του οποίου η έκδοση άρχισε τον Ιούνη του 1840. Το 1939 η «Ένωσις Συντακτών Πατρών» έπαψε να υπάρχει υποχρεωτικά και στη θέση της συγκροτήθηκε, με βάση το νόμο 1093 η ΕΣΗΕΠΗΝ. Από το 1950 και πέρα η διοίκηση της ΕΣΗΕΠΗΝ, απαλλαγμένη από τους περιορισμούς, που είχε επιβάλει στις ενέργειές της το ασφυκτικό εμπόλεμο κλίμα (γερμανική κατοχή και εμφύλιος πόλεμος), άρχισε να αναπτύσσει αξιόλογη δράση, η οποία είχε ως θετικό αποτέλεσμα, εκτός πολλών άλλων και τη σταδιακή βελτίωση των οικονομικών της Ένωσης. Σήμερα, η διοίκηση της ΕΣΗΕΠΗΝ που πρόκειται κυρίως για μια συνδικαλιστική ηγεσία, που, όπως και όλες οι προηγούμενες ηγεσίες της Ένωσης, επιχειρεί να εκφράζεται ως συνεργάτης και φίλος του κάθε μέλους της ΕΣΗΕΠΗΝ για την αποτελεσματικότερη προάσπιση των επαγγελματικών

δικαιωμάτων του κλάδου σε περιφερειακό επίπεδο και για την παράλληλη εφαρμογή από μέρους όλων των συντακτών της δημοσιογραφικής δεοντολογίας (Λάζαρης, 2024). Η ΕΣΗΕΠΗΝ περιλαμβάνει ΜΜΕ από την Ήπειρο και την Πελοπόννησο καθώς και όλων των νήσων συμπεριλαμβανομένης και της Κρήτης. Από τα νησιά εξαιρείται μόνο η Εύβοια, η οποία περιλαμβάνεται στην ΕΣΗΕΘΣΤΕ-Ε.

Κατ΄ επέκταση, οι ενώσεις αυτές το απέστειλαν στα μέλη τους. Η τελική ανταπόκριση ήταν στο σύνολο 51 συμπληρωμένα ερωτηματολόγια, αριθμός ικανός για εξαγωγή ποσοτικών και ποιοτικών αποτελεσμάτων.

4.3.2 Κοινή χρήση ερωτηματολογίου μέσω Google Forms

Η τεχνική υλοποίηση του ερωτηματολογίου έγινε μέσω της πλατφόρμας Google Forms. Οι βασικοί λόγοι που οδήγησαν σε αυτή την επιλογή ήταν η ευκολία στη χρήση της συγκεκριμένης πλατφόρμας, οι επιλογές δόμησης και ανάπτυξης των ερωτήσεων αλλά και οι δυνατότητες εξαγωγής των απαντήσεων και των στατιστικών.

Το Google Forms είναι μια διαδικτυακή εφαρμογή που αναπτύχθηκε από την Google και επιτρέπει στους χρήστες να δημιουργούν και να διανέμουν ερωτηματολόγια, έρευνες και φόρμες. Το Google Forms, που κυκλοφόρησε ως μέρος της σουίτας Google Drive το 2008, έχει υποστεί σημαντικές βελτιώσεις, καθιστώντας το ένα ισχυρό εργαλείο για τη συλλογή δεδομένων. Επιτρέπει στους χρήστες να σχεδιάζουν προσαρμοσμένες φόρμες, να τις μοιράζονται με τους ερωτηθέντες και να συλλέγουν απαντήσεις σε πραγματικό χρόνο. Η απλότητα και η προσβασιμότητά του έχουν συμβάλει στην ευρεία υιοθέτησή του σε διάφορους τομείς, από την εκπαίδευση έως τις επιχειρήσεις και την έρευνα (Schalk, 2021).

Ένα από τα βασικά χαρακτηριστικά του Google Forms είναι η πληθώρα επιλογών προσαρμογής του. Οι χρήστες μπορούν να δημιουργήσουν διαφορετικούς τύπους ερωτήσεων, συμπεριλαμβανομένων πολλαπλών επιλογών, πλαισίων ελέγχου, σύντομων απαντήσεων και γραμμικών κλιμάκων. Επιπλέον, η πλατφόρμα υποστηρίζει στοιχεία πολυμέσων, επιτρέποντας στους χρήστες να ενσωματώνουν εικόνες και βίντεο στις φόρμες τους. Αυτή η ευελιξία επιτρέπει τη δημιουργία ελκυστικών και διαδραστικών ερευνών προσαρμοσμένων σε συγκεκριμένες ερευνητικές ανάγκες.

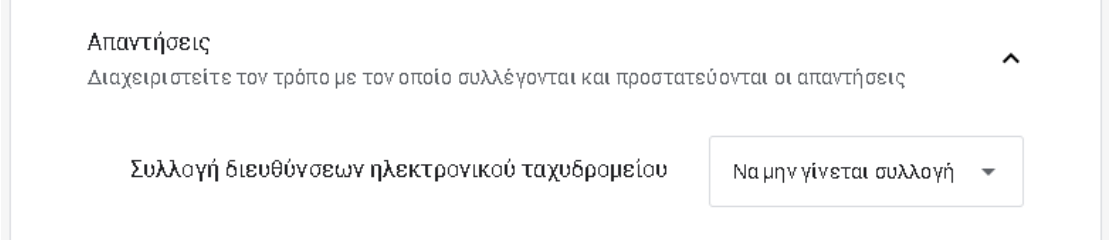
Το Google Forms ενσωματώνεται απρόσκοπτα με άλλες υπηρεσίες της Google, όπως τα Υπολογιστικά Φύλλα Google (Google Sheets) και το Google Drive. Αυτή η ενοποίηση διευκολύνει την αυτόματη συλλογή και οργάνωση των απαντήσεων σε δομημένη μορφή. Οι χρήστες μπορούν να αναλύσουν δεδομένα απευθείας στο Google Sheets, αξιοποιώντας ενσωματωμένες λειτουργίες και εργαλεία για ολοκληρωμένη ανάλυση δεδομένων. Επιπλέον, το Google Forms υποστηρίζει τη συνεργασία σε πραγματικό χρόνο, επιτρέποντας σε πολλούς χρήστες να εργάζονται σε μια φόρμα ταυτόχρονα.

Το Google Forms προσφέρει πολλά πλεονεκτήματα που το καθιστούν μια προτιμώμενη επιλογή για τη συλλογή δεδομένων. Πρώτον, η φιλική προς τον χρήστη διεπαφή διασφαλίζει ότι τόσο οι δημιουργοί όσο και οι ερωτηθέντες μπορούν να πλοηγηθούν στην πλατφόρμα με ευκολία. Ο διαισθητικός σχεδιασμός μειώνει την καμπύλη εκμάθησης, επιτρέποντας στους χρήστες να δημιουργούν και να διανέμουν γρήγορα φόρμες χωρίς εκτεταμένες τεχνικές γνώσεις.

Η προσβασιμότητα είναι ένα άλλο βασικό πλεονέκτημά του. Η πλατφόρμα είναι προσβάσιμη από οποιαδήποτε συσκευή με σύνδεση στο Διαδίκτυο, διασφαλίζοντας ότι οι ερωτηθέντες μπορούν να συμμετέχουν από οπουδήποτε στον κόσμο. Αυτό έχει ως αποτέλεσμα να διευκολύνει τη συλλογή απαντήσεων και να άρει τους γεωγραφικούς περιορισμούς. Επιπλέον, το γεγονός ότι παρέχεται δωρεάν μέσω του λογαριασμού Google, το κάνει μια δελεαστική επιλογή για τη δημιουργία και την εκτέλεση ερευνών που βασίζονται στη συλλογή απαντήσεων από το κοινό όπως στην παρούσα εργασία.

Η συλλογή και η ανάλυση δεδομένων σε πραγματικό χρόνο είναι ζωτικής σημασίας πλεονέκτημα του Google Forms. Μόλις οι ερωτηθέντες υποβάλουν τις απαντήσεις τους, τα δεδομένα είναι άμεσα διαθέσιμα για έλεγχο και ανάλυση. Αυτή η αμεσότητα επιτρέπει στους ερευνητές να παρακολουθούν τα ποσοστά απόκρισης, να εντοπίζουν τις τάσεις και να λαμβάνουν άμεσα αποφάσεις βάσει δεδομένων. Επιπλέον, το Google Forms παρέχει διάφορες επιλογές για την οπτικοποίηση δεδομένων, όπως γραφήματα και γραφήματα, που βοηθούν στην ερμηνεία και την παρουσίαση των αποτελεσμάτων.

Παρά τα πολυάριθμα πλεονεκτήματά του, το Google Forms έχει και ορισμένους περιορισμούς και προκλήσεις που πρέπει να αναφερθούν και να λάβουν υπόψη τους οι χρήστες. Ένα από τα κύρια ζητήματα είναι το απόρρητο και η ασφάλεια των δεδομένων. Ενώ η Google εφαρμόζει αυστηρά μέτρα ασφαλείας, η διαδικτυακή φύση του Google Forms εγείρει πιθανούς κινδύνους παραβιάσεων δεδομένων και μη εξουσιοδοτημένης πρόσβασης. Οι ερευνητές που χειρίζονται ευαίσθητες πληροφορίες πρέπει να εφαρμόζουν πρόσθετα πρωτόκολλα ασφαλείας για την προστασία των δεδομένων των ερωτώμενων. Στη συγκεκριμένη εργασία και στο ερευνητικό ερωτηματολόγιο που αναπτύχθηκε και διαμοιράσθηκε δεν ζητήθηκαν προσωπικά στοιχεία, τα οποία θα μπορούσαν να χρησιμοποιηθούν ώστε να ταυτοποιήσουν τους συμμετέχοντες. Επιπλέον, όλες οι απαντήσεις συλλέχθηκαν ανώνυμα χρησιμοποιώντας τη συγκεκριμένη επιλογή (να μην συλλέγονται ούτε οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των συμμετεχόντων) κατά την ανάπτυξη του ερωτηματολογίου στο Google Forms όπως φαίνεται στην Εικόνα 33.



Εικόνα 33. Επιλογή για να μην συλλέγονται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των συμμετεχόντων στο Google Forms

Οι περιορισμοί σχεδιασμού και προσαρμογής είναι μια άλλη πρόκληση που σχετίζεται με το Google Forms. Ενώ η πλατφόρμα προσφέρει διάφορους τύπους ερωτήσεων και υποστήριξη πολυμέσων, δεν διαθέτει προηγμένα χαρακτηριστικά σχεδιασμού που βρίσκονται σε εξειδικευμένο λογισμικό έρευνας. Έτσι, σε περιπτώσεις που οι χρήστες αναζητούν εξαιρετικά προσαρμοσμένες και οπτικά ελκυστικές φόρμες μπορεί να βρουν την εν λόγω πλατφόρμα κάπως περιορισμένη, όσον αφορά τις δυνατότητες σχεδιασμού. Στο πλαίσιο της παρούσας εργασίας, οι επιλογές που δινόταν από το Google Forms κάλυπταν επαρκώς τις ανάγκες.

Ένας ακόμα περιορισμός είναι η απαίτηση συνεχούς σύνδεσης στο Διαδίκτυο κατά τη διαδικασία απάντησης από τους συμμετέχοντες αλλά και από τον δημιουργό της φόρμας κατά τη διαδικασία δημιουργίας και επεξεργασίας της. Αυτό έχει ως

αποτέλεσμα σε περιοχές με περιορισμένη πρόσβαση στο Διαδίκτυο, να μην είναι δυνατή η συμμετοχή σε αυτό. Για τις ανάγκες του παρόντος, η φόρμα διαμοιράσθηκε σε κοινό που είχαν εύκολη πρόσβαση στο Διαδίκτυο. Ωστόσο, είχε προβλεφθεί ότι σε περίπτωση δυσκολίας εκτέλεσης του ερωτηματολόγιου λόγω τεχνικών προβλημάτων να δίνεται η δυνατότητα να μοιρασθεί μέσω αρχείου η φόρμα.

Συμπερασματικά, το Google Forms είναι ένα ισχυρό και ευέλικτο εργαλείο για τη συλλογή δεδομένων που απευθύνεται σε ένα ευρύ φάσμα χρηστών και εφαρμογών. Η φιλική προς τον χρήστη διεπαφή, η προσβασιμότητα και η σχέση κόστους-αποτελεσματικότητας το καθιστούν ελκυστική επιλογή για εκπαιδευτικούς, επιχειρήσεις και ερευνητές. Αν και έχει ορισμένους περιορισμούς και προκλήσεις, τα οφέλη συχνά υπερτερούν αυτών των μειονεκτημάτων. Καθώς η συλλογή ψηφιακών δεδομένων συνεχίζει να εξελίσσεται, το Google Forms παραμένει ένα σχετικό και πολύτιμο εργαλείο για τη συλλογή και την ανάλυση πληροφοριών με αποτελεσματικό και προσιτό τρόπο και για τους λόγους που αναλύθηκαν παραπάνω επιλέχθηκε για την εκτέλεση του ερωτηματολογίου της παρούσας εργασίας.

Η φόρμα διαμοιράσθηκε μέσω υπερσυνδέσμου που στάλθηκε στις δημοσιογραφικές ενώσεις που αναφέρθηκαν προηγουμένως και περιείχε διάφορες κατηγορίες ερωτήσεων όπως κλειστού τύπου με μία απάντηση (Εικόνα 35), ερώτηση κλειστού τύπου με δυνατότητα πολλαπλών απαντήσεων (Εικόνα 36), ερώτηση ανοικτού τύπου με δυνατότητα απάντησης με ελεύθερο κείμενο (Εικόνα 37) και ερωτήσεις κλειστού τύπου της κλίμακας Likert (Εικόνα 38).

Πλατφόρμες Ασφαλούς Επικοινωνίας στη Δημοσιογραφία

Αγαπητή κυρία/Αγαπητέ κύριε,

Το παρόν ερωτηματολόγιο δημιουργήθηκε στο πλαίσιο εκπόνησης της διπλωματικής μου εργασίας με θέμα "Χρήση πλατφορμών ασφαλούς επικοινωνίας από δημοσιογράφους" για την ολοκλήρωση του Μεταπτυχιακού Προγράμματος Σπουδών "Σύγχρονες Δημοσιογραφικές Σπουδές" στο Ελληνικό Ανοικτό Πανεπιστήμιο υπό την επίβλεψη του Καθηγητή Ανδρέα Βέγλη.

Για το εμπειρικό κομμάτι της εργασίας έχει συνταχθεί το παρόν ερωτηματολόγιο, το οποίο απευθύνεται στους επαγγελματίες του χώρου της Δημοσιογραφίας. Σκοπός του ερωτηματολογίου είναι η εύρεση, ανάλυση και παραγωγή χρήσιμων συμπερασμάτων αναφορικά με τη χρήση πλατφορμών επικοινωνίας από τους δημοσιογράφους και κατά πόσο ασφαλείς είναι σε επίπεδο ανάγκης για προστασία των ευαίσθητων πληροφοριών και των επαγγελματικών πηγών τους.

Η συμμετοχή στην έρευνα είναι ανώνυμη. Με σεβασμό στα προσωπικά σας δεδομένα, θα τηρηθεί η πλήρης εμπιστευτικότητα αυτών, ώστε να μην μπορούν να οδηγήσουν στην ταυτοποίησή σας. Οι πληροφορίες που θα συλλεχθούν θα χρησιμοποιηθούν αποκλειστικά και μόνο για τους σκοπούς της παρούσας έρευνας και κανείς άλλος, εκτός από την ερευνήτρια και τους δύο επιβλέποντες καθηγητές, δεν θα έχει πρόσβαση σε αυτές. Τα δεδομένα που θα συλλεχθούν θα υποβληθούν σε επεξεργασία σύμφωνα με την ελληνική νομοθεσία περί προστασίας των προσωπικών δεδομένων (ν.4624/2019). Η συμμετοχή σας στην έρευνα συνεπάγεται τη συμφωνία σας σε ενδεχόμενη μελλοντική δημοσίευση των αποτελεσμάτων της, με την προϋπόθεση ότι θα διατηρηθεί η ανωνυμία σας.

Σας ευχαριστώ εκ των προτέρων για τον χρόνο σας και την πολύτιμη συμβολή σας στην επιτυχή ολοκλήρωση της παρούσας εργασίας.

Με εκτίμηση,

Μαρία-Αλεξάνδρα Σεβαστάκη

E-mail: std520990@ac.eap.gr

smarianta@gmail.com Εναλλαγή λογαριασμού

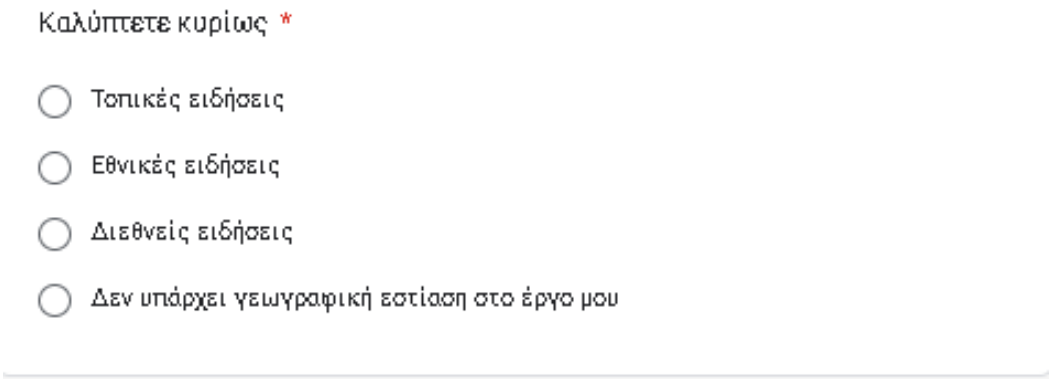
Δεν κοινοποιήθηκε

Επόμενο

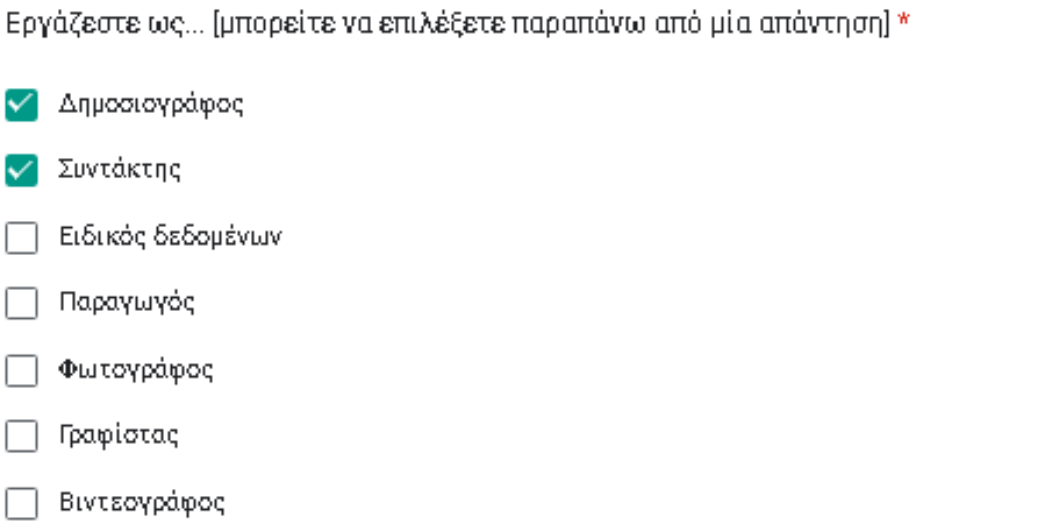
Σελίδα 1 από 9

Εκκαθάριση φόρμας

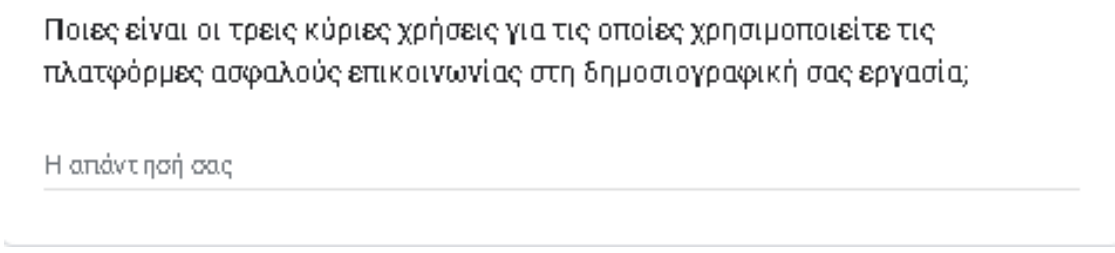
Εικόνα 34. Εισαγωγική σελίδα ερωτηματολογίου στο Google Forms



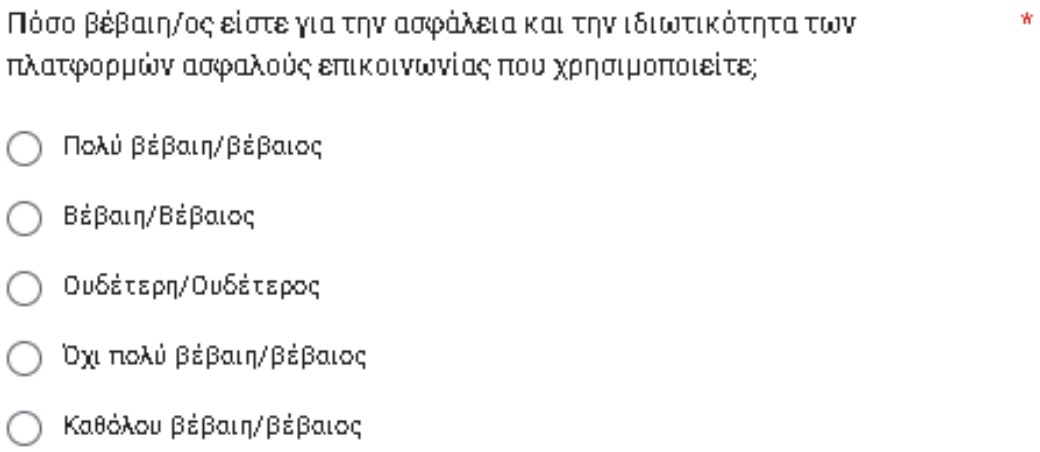
Εικόνα 35. Ερώτηση κλειστού τύπου με δυνατότητα επιλογής μόνο μίας απάντησης



Εικόνα 36. Ερώτηση κλειστού τύπου με δυνατότητα επιλογής πολλαπλών απαντήσεων



Εικόνα 37. Ερώτηση ανοικτού τύπου με δυνατότητα απάντησης με ελεύθερο κείμενο



Εικόνα 38. Ερώτηση τύπου κλίμακας Likert

5 Αποτελέσματα της έρευνας

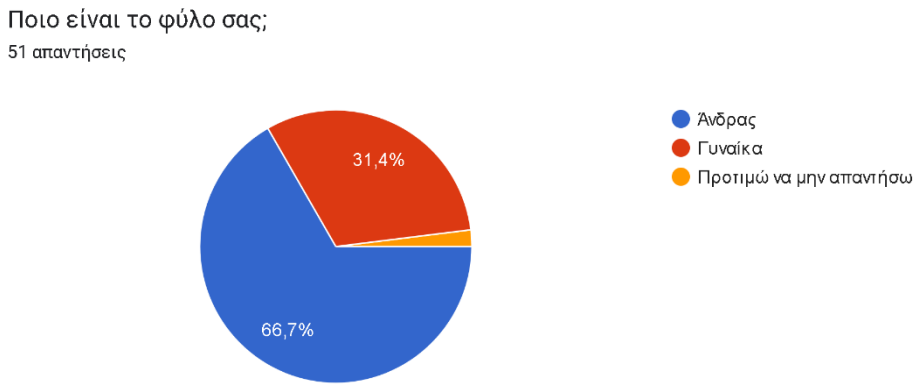
Το ερωτηματολόγιο που υπάρχει στο Παράρτημα 2: Ερωτηματολόγιο απαντήθηκε στο σύνολό του από 51 συμμετέχοντες. Στις επόμενες παραγράφους γίνεται μια λεπτομερής ποσοτική ανάλυση των απαντήσεων αυτών. Παράλληλα παρατίθεται σχετικός σχολιασμός και συμπεράσματα που εξήχθησαν από αυτή την ερευνητική διαδικασία.

5.1 Ποσοτική Ανάλυση

Η ποσοτική ανάλυση και η παράθεση αριθμητικών δεδομένων και στατιστικών αποτελεί το πρώτο βήμα για την ερμηνεία των απαντήσεων του ερωτηματολογίου.

5.1.1 Δημογραφικά στοιχεία

Αρχικά, όπως φαίνεται και παρακάτω, στην Εικόνα 39 τα 2/3 του συνόλου ήταν άνδρες ενώ μόλις μία απάντηση ήταν «Προτιμώ να μην απαντήσω». Σε απόλυτους αριθμούς οι συμμετέχοντες κατανέμονται σε:



Εικόνα 39. Κατανομή συμμετεχόντων ανά φύλο

Πίνακας 1. Κατανομή συμμετεχόντων ανά φύλο σε απόλυτα νούμερα

Ποιο είναι το φύλο σας;	
Απαντήσεις	**Σύνολο**
Άνδρας	**34**
Γυναίκα	16

Προτιμώ να μην απαντήσω	1

Η ηλικιακή κατανομή των συμμετεχόντων ήταν μοιρασμένη όπως φαίνεται στην Εικόνα 40. Η κυρίαρχη κλάση ήταν 45-54 ετών, η οποία ακολουθείτο από τις κλάσεις μεγαλύτεροι των 54 και 35-44. Χαρακτηριστικό είναι ότι στην ηλικιακή ομάδα 18-24 δεν υπήρχε καμία απάντηση. Αναλυτικότερα οι απαντήσεις μοιράστηκαν ως εξής:

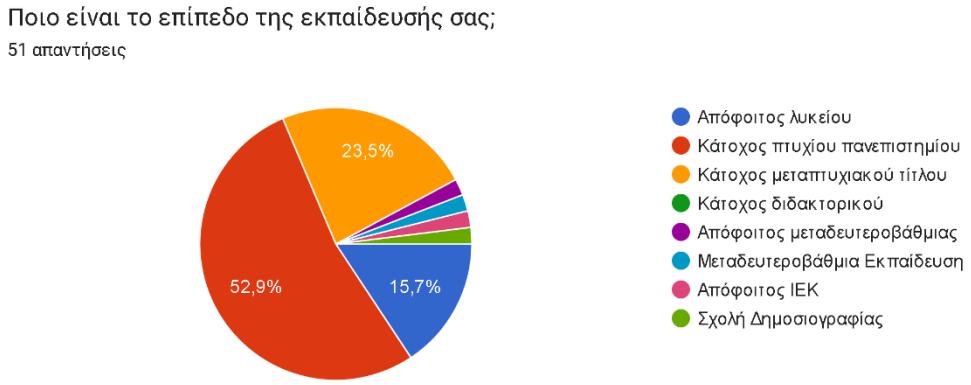
Εικόνα 40. Ηλικιακή κατανομή συμμετεχόντων

Πίνακας 2. Ηλικιακή κατανομή συμμετεχόντων σε απόλυτα νούμερα

Σε ποια ηλικιακή ομάδα ανήκετε;	
Απαντήσεις	**Σύνολο**
18-24	0
25-34	4
35-44	12
45-54	**21**
>54	14

Σχετικά με το επίπεδο εκπαίδευσης η επικρατούσα κλάση των συμμετεχόντων ήταν «Κάτοχος πτυχίου πανεπιστημίου», η οποία ακολουθείτο από αυτή της «Κάτοχος μεταπτυχιακού τίτλου» και αμέσως μετά «Απόφοιτος λυκείου. Η κατανομή των

απαντήσεων σε ποσοστά στην Εικόνα 41 και σε απόλυτα νούμερα φαίνεται στον Πίνακα 3.



Εικόνα 41. Κατανομή των συμμετεχόντων με βάση το επίπεδο εκπαίδευσης

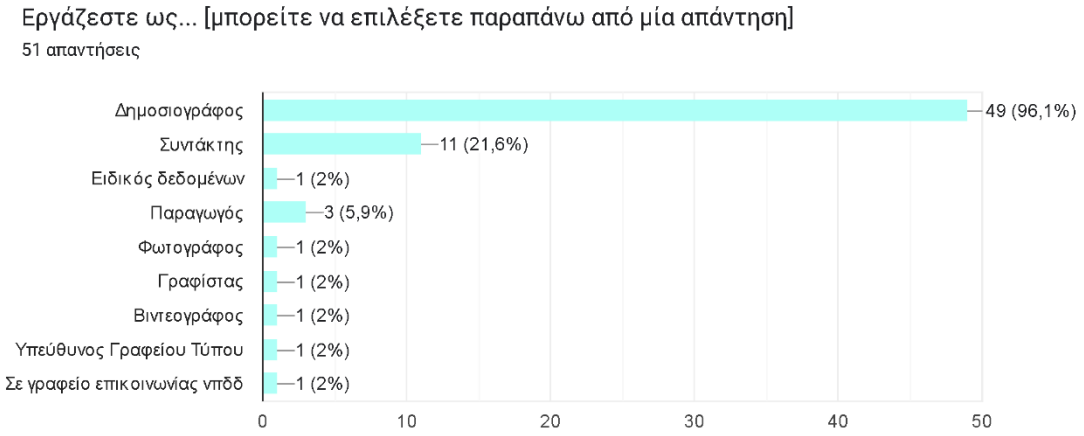
Πίνακας 3. Κατανομή των συμμετεχόντων με βάση το επίπεδο εκπαίδευσης σε απόλυτα νούμερα

Ποιο είναι το επίπεδο της εκπαίδευσής σας;	
Απαντήσεις	**Σύνολο**
Απόφοιτος λυκείου	8
Κάτοχος πτυχίου πανεπιστημίου	**27**
Κάτοχος μεταπτυχιακού τίτλου	12
Κάτοχος διδακτορικού	0
Απόφοιτος μεταδευτεροβάθμιας	1
Μεταδευτεροβάθμια εκπαίδευση	1
Απόφοιτος ΙΕΚ	1
Σχολή Δημοσιογραφίας	1

5.1.2 Τομέας απασχόλησης

Οι συμμετέχοντες στο ερωτηματολόγιο στη συνέχεια ερωτήθηκαν σχετικά με τα στοιχεία της απασχόλησής τους. Η πλειοψηφία των συμμετεχόντων και σε ποσοστό πάνω από 95% δήλωσαν ότι έχουν ως κύρια ή δευτερεύουσα ιδιότητα αυτή του

δημοσιογράφου. Της δημοσιογραφικής ιδιότητας έπεται αυτή του συντάκτη την οποία δήλωσαν το 21,6% των συμμετεχόντων. Η κατανομή των απαντήσεων σχετικά με την απασχόληση των συμμετεχόντων σε ποσοστό φαίνεται στην Εικόνα 42 ενώ σε απόλυτα νούμερα στον Πίνακα 4.

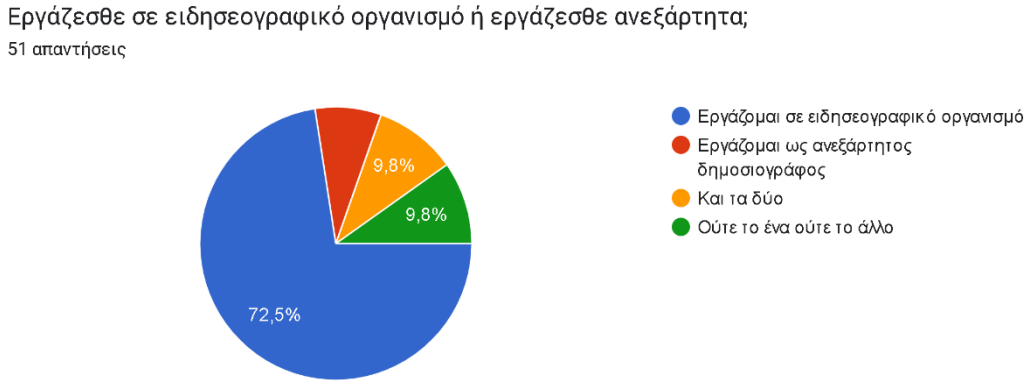


Εικόνα 42. Κατανομή των συμμετεχόντων με βάση την ιδιότητα της απασχόλησής τους

Πίνακας 4. Κατανομή των συμμετεχόντων με βάση την ιδιότητα της απασχόλησής τους σε απόλυτα νούμερα

Εργάζεσθε ως... [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Δημοσιογράφος	**50**
Συντάκτης	11
Ειδικός δεδομένων	1
Παραγωγός	3
Φωτογράφος	1
Γραφίστας	1
Βιντεογράφος	1
Υπεύθυνος σε γραφείο τύπου (Άλλο)	1
Σε γραφείο επικοινωνίας ΝΠΔΔ (Άλλο)	1

Στη συνέχεια, οι ερωτηθέντες κλήθηκαν να απαντήσουν για τη σχέση εργασίας τους. Αν εργάζονται σε δημοσιογραφικό οργανισμό ή ανεξάρτητα. Η πλειοψηφία αυτών σε ποσοστό 72,5% απάντησε ότι εργάζεται σε ειδησεογραφικό οργανισμό ενώ το εναπομείναν ποσοστό μοιράστηκε σχεδόν ισομερώς στις υπόλοιπες απαντήσεις όπως φαίνεται στην Εικόνα 43 και στον Πίνακα 5.



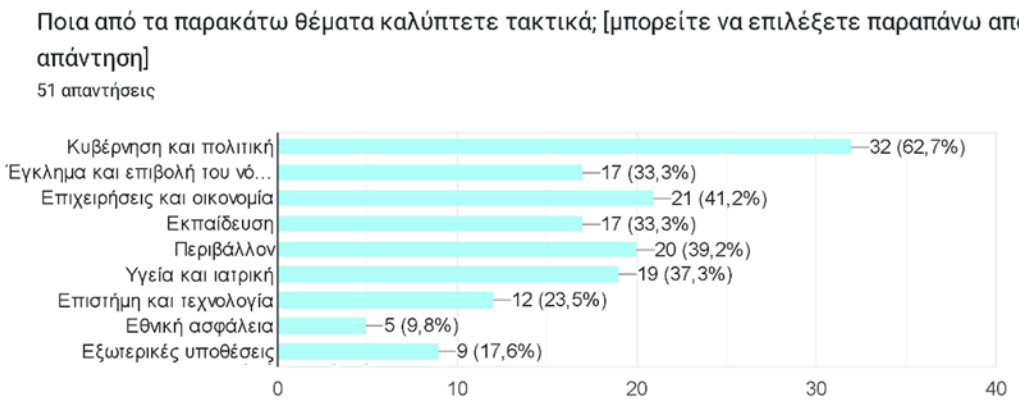
Εικόνα 43. Κατανομή των συμμετεχόντων με βάση τη σχέση εργασίας τους

Πίνακας 5. Κατανομή των συμμετεχόντων με βάση τη σχέση εργασίας τους σε απόλυτα νούμερα

Εργάζεσθε σε ειδησεογραφικό οργανισμό ή εργάζεσθε ανεξάρτητα;	
Απαντήσεις	**Σύνολο**
Σε ειδησεογραφικό οργανισμό	**37**
Ανεξάρτητος δημοσιογράφος	4
Και τα δύο	5
Ούτε το ένα ούτε το άλλο	5

Η θεματολογία που καλύπτουν οι περισσότεροι από τους συμμετέχοντες έχει να κάνει με την κυβέρνηση και την πολιτική. Βέβαια, οι περισσότεροι συμμετέχοντες δήλωσαν ότι ασχολούνται με παραπάνω του ενός θεματικές ενότητες. Έτσι, πέρα από τα κυβερνητικά θέματα και την πολιτική που είναι η δημοφιλέστερη κατηγορία, αρκετοί από τους συμμετέχοντες δήλωσαν ότι ασχολούνται και με το αστυνομικό ρεπορτάζ, την οικονομία, την εκπαίδευση, το περιβάλλον, την υγεία, την επιστήμη, την εθνική

ασφάλεια και τις εξωτερικές υποθέσεις. Η λεπτομερής κατανομή των απαντήσεων φαίνεται στην Εικόνα 44 και στον Πίνακα 6.



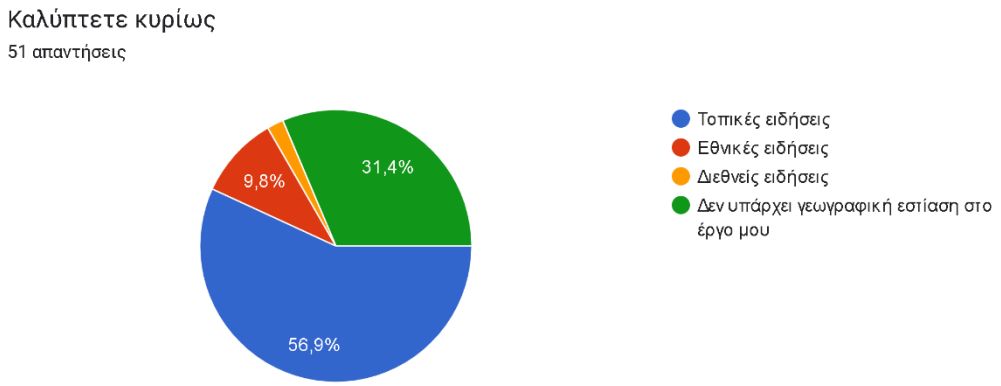
Εικόνα 44. Απαντήσεις με βάση τη θεματολογία που καλύπτουν

Πίνακας 6. Απαντήσεις με βάση τη θεματολογία που καλύπτουν σε απόλυτα νούμερα

Ποια από τα παρακάτω θέματα καλύπτετε τακτικά; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Κυβέρνηση και πολιτική	**32**
Έγκλημα και επιβολή του νόμου	17
Επιχειρήσεις και οικονομία	21
Εκπαίδευση	17
Περιβάλλον	20
Υγεία και ιατρική	19
Επιστήμη και τεχνολογία	12
Εθνική ασφάλεια	5
Εξωτερικές υποθέσεις	9
Ορθόδοξη εκκλησία (Άλλο)	1
Αθλητικά (Άλλο)	2

Επαρχιακό ρεπορτάζ (Άλλο)	1
Κοινωνικά ζητήματα (Άλλο)	1
Αθλητικά (Άλλο)	2
Επικοινωνία ΝΠΔΔ (Άλλο)	1
Ελεύθερο ρεπορτάζ (Άλλο)	1
Πολιτισμός (Άλλο)	2

Ένα ακόμα χαρακτηριστικό σχετικά με την απασχόληση των συμμετεχόντων, το οποίο έρχεται να συμπληρώσει τη θεματολογία με την οποία ασχολούνται, είναι η γεωγραφική κάλυψη των ειδήσεων που μεταφέρουν. Έτσι οι περισσότεροι και σε ποσοστό 56,9% ασχολούνται με ειδήσεις σε τοπικό επίπεδο ενώ το 31,4% δήλωσε ότι δεν έχουν συγκεκριμένη γεωγραφική κάλυψη. Τα αναλυτικά αποτελέσματα φαίνονται στην Εικόνα 45 και στον Πίνακα 7.



Εικόνα 45. Κατανομή των απαντήσεων με βάση τη γεωγραφική κάλυψη των ειδήσεων που μεταφέρουν

Πίνακας 7. Κατανομή απαντήσεων με βάση τη γεωγραφική κάλυψη των ειδήσεων που μεταφέρουν σε απόλυτα νούμερα

Καλύπτετε κυρίως	
Απαντήσεις	**Σύνολο**
Τοπικές ειδήσεις	**29**

Εθνικές ειδήσεις	5
Διεθνείς ειδήσεις	1
Δεν υπάρχει γεωγραφική εστίαση	16

5.1.3 Χρήση των πλατφορμών ασφαλούς επικοινωνίας

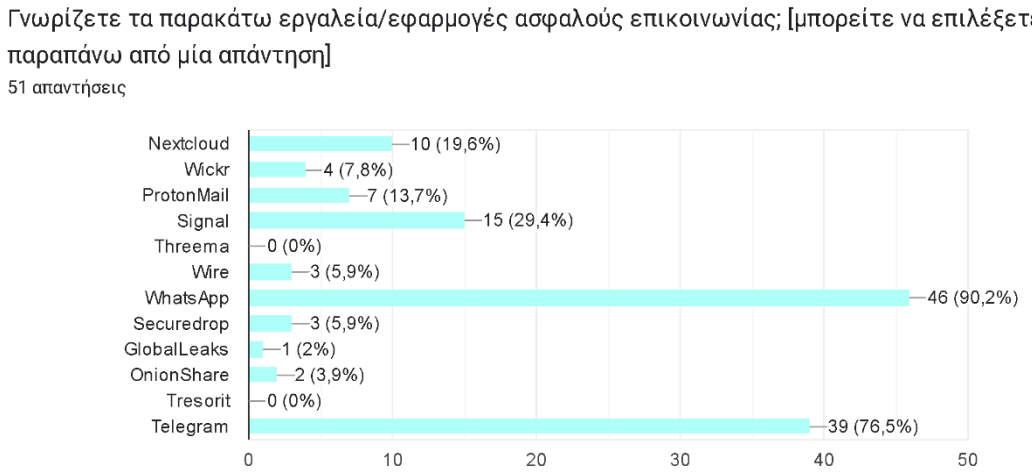
Το επόμενο μέρος του ερωτηματολογίου στο οποίο κλήθηκαν να απαντήσουν οι συμμετέχοντες αφορά τη χρήση πλατφορμών ασφαλούς επικοινωνίας στην εργασία τους. Οι πλατφόρμες αυτές παρουσιάσθηκαν λεπτομερώς στο Κεφάλαιο 3. Το 62,7% απάντησε ότι χρησιμοποιεί τέτοιες πλατφόρμες για την άσκηση του δημοσιογραφικού επαγγέλματος.

Εικόνα 46. Ποσοστό συμμετεχόντων με βάση το αν χρησιμοποιούν ή όχι πλατφόρμες ασφαλούς επικοινωνίας

Πίνακας 8. Κατανομή απαντήσεων με βάση το αν χρησιμοποιούν ή όχι πλατφόρμες ασφαλούς επικοινωνίας απόλυτα νούμερα

Χρησιμοποιείτε αυτή τη στιγμή κάποια πλατφόρμα ασφαλούς επικοινωνίας για τη δημοσιογραφική σας εργασία;	
Απαντήσεις	**Σύνολο**
Ναι	**32**
Όχι	19

Οι συμμετέχοντες στη συνέχεια κλήθηκαν να απαντήσουν αν γνωρίζουν κάποιες από τις πλατφόρμες ασφαλούς επικοινωνίας που παρουσιάσθηκαν στο Κεφάλαιο 3. Η συντριπτική πλειοψηφία (90,2%) γνωρίζει την εφαρμογή WhatsApp και ακολουθεί με αρκετά υψηλό ποσοστό το Telegram. Η αναλυτική κατανομή των αποτελεσμάτων στη συγκεκριμένη ερώτηση φαίνεται στην Εικόνα 47 και στον Πίνακα 9.



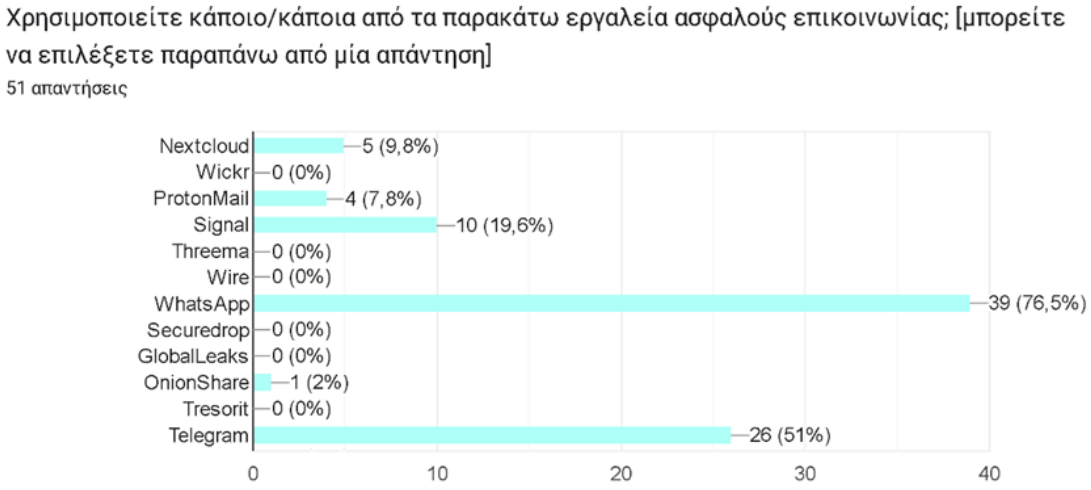
Εικόνα 47. Ποσοστό επί των συμμετεχόντων που γνωρίζουν την κάθε πλατφόρμα

Πίνακας 9. Αριθμός συμμετεχόντων που γνωρίζει την κάθε πλατφόρμα ασφαλούς επικοινωνίας

Γνωρίζετε τα παρακάτω εργαλεία/εφαρμογές ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Nextcloud	10
Wickr	4
Proton Mail	7
Signal	15
Threema	0
Wire	3
WhatsApp	46
SecureDrop	3

GlobaLeaks	1
OnionShare	2
Tresorit	0
Telegram	39

Στη συνέχεια, πέρα από τις πλατφόρμες που γνωρίζουν, ζητήθηκε από τους συμμετέχοντες να απαντήσουν ποιες από τις παραπάνω πλατφόρμες ή και από άλλες που δεν αναφέρθηκαν προηγουμένως, χρησιμοποιούν στην εργασία τους. Έτσι, και πάλι η πλειοψηφία των ερωτηθέντων σε ποσοστό 76,5% χρησιμοποιούν το WhatsApp, το 51% χρησιμοποιούν το Telegram ενώ υπήρχαν απαντήσεις για Viber, Facebook Messenger, WeTransfer, Botim και imo messenger. Τα αναλυτικά αποτελέσματα για το ποιες πλατφόρμες χρησιμοποιούν οι συμμετέχοντες στην έρευνα φαίνονται στην Εικόνα 48 και στον Πίνακα 10.

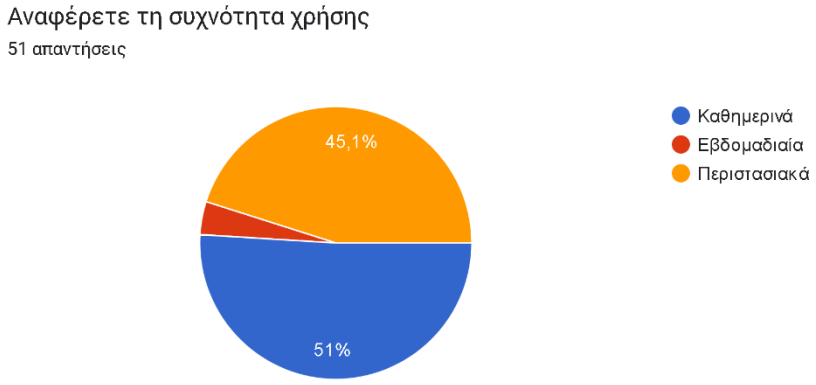


Εικόνα 48. Ποσοστό ανά πλατφόρμα επί των συμμετεχόντων

Πίνακας 10. Αριθμός συμμετεχόντων που χρησιμοποιεί την κάθε πλατφόρμα ασφαλούς επικοινωνίας

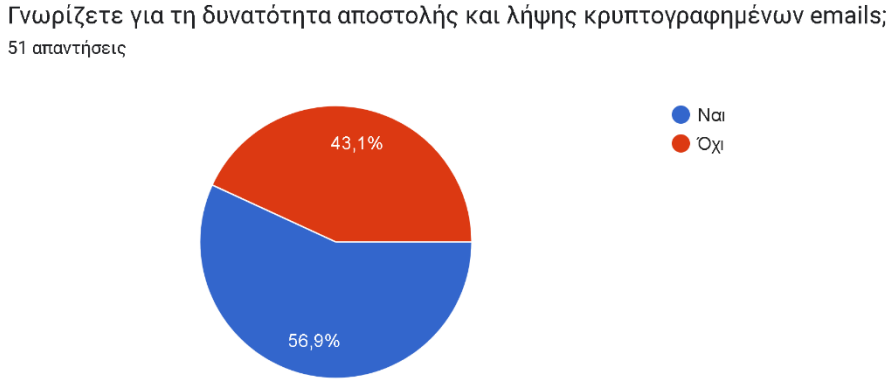
Χρησιμοποιείτε κάποιο/κάποια από τα παρακάτω εργαλεία ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Nextcloud	5
Wickr	0
Proton Mail	4
Signal	10
Threema	0
Wire	0
WhatsApp	39
SecureDrop	0
GlobaLeaks	0
OnionShare	1
Tresorit	0
Telegram	26
Viber (Άλλο)	5
Zoom (Άλλο)	1
Botim (Άλλο)	1
Iom (Άλλο)	1
We transfer (Άλλο)	1
Facebook messenge (Άλλο)	1
Κανένα (Άλλο)	3

Από όσους απάντησαν ότι χρησιμοποιούν πλατφόρμες ασφαλούς επικοινωνίας για στην εργασία τους το 51% απάντησε ότι το κάνει καθημερινά, το 45,1% περιστασιακά και το 3,9% εβδομαδιαία όπως φαίνεται στην Εικόνα 49.



Εικόνα 49. Κατανομή απαντήσεων σχετικά με τη συχνότητα χρήσης

Συνεχίζοντας στο κομμάτι της χρήσης των πλατφορμών ασφαλούς επικοινωνίας, οι ερωτηθέντες της έρευνας απάντησαν στην ερώτηση αν ήταν ενήμεροι για τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails. Το 56,9% απάντησε ότι γνωρίζει για τη δυνατότητα αυτή ενώ το 43,1% δεν ήταν ενημερωμένο σχετικά. Η ανάλυση των απαντήσεων της συγκεκριμένης ερώτησης φαίνεται στην Εικόνα 50 και στον Πίνακα 11.

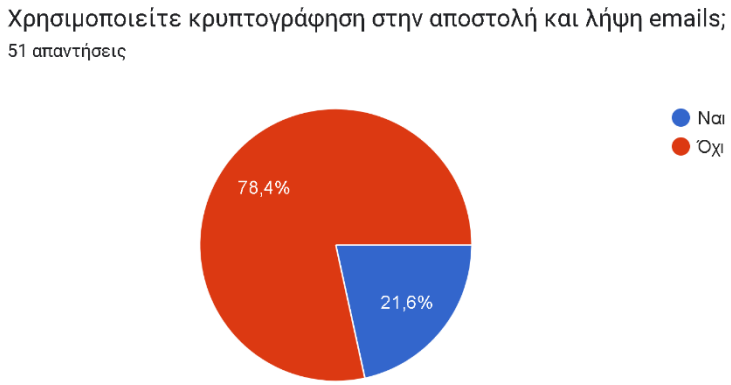


Εικόνα 50. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το εάν γνωρίζουν ή όχι τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails

Πίνακας 11. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν γνωρίζουν ή όχι τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails

Γνωρίζετε για τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails;	
Απαντήσεις	**Σύνολο**
Ναι	**29**
Όχι	22

Ως άμεση απόρροια της προηγούμενης ερώτησης, οι συμμετέχοντες στην έρευνα κλήθηκαν να απαντήσουν στο εάν χρησιμοποιούν κρυπτογράφηση κατά την ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Με εμφανή διαφορά η συντριπτική πλειοψηφία σε ποσοστό (78,4%) απάντησε ότι δεν χρησιμοποιεί κρυπτογράφηση και μόλις το 21,6% απάντησε θετικά. Στην Εικόνα 49 και στον Πίνακα 12 φαίνονται αναλυτικά η κατανομή των απαντήσεων στην εν λόγω ερώτηση.

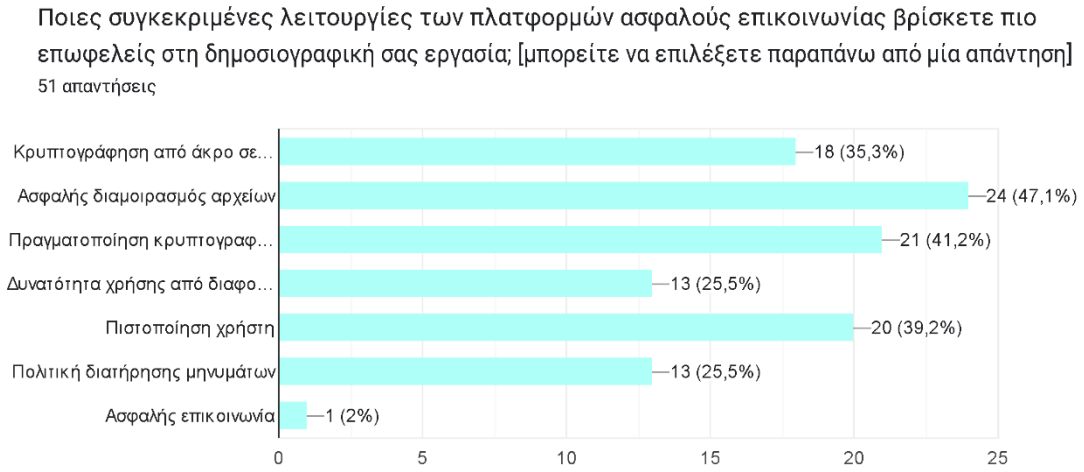


Εικόνα 51. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το εάν χρησιμοποιούν ή όχι κρυπτογράφηση στα emails

Πίνακας 12. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν χρησιμοποιούν ή όχι κρυπτογράφηση στα emails

Χρησιμοποιείτε κρυπτογράφηση στην αποστολή και λήψη emails;	
Απαντήσεις	**Σύνολο**
Ναι	11
Όχι	**40**

Προκειμένου να γίνει μια καταγραφή για το ποια χαρακτηριστικά είναι αυτά που θα ήθελαν να έχει μια πλατφόρμα ασφαλούς επικοινωνίας προκειμένου να τη χρησιμοποιήσουν στη δουλειά τους, κλήθηκαν να επιλέξουν από μία λίστα αυτών. Έτσι, ανάμεσα σε όλα, ο ασφαλής διαμοιρασμός αρχείων, η πραγματοποίηση κρυπτογραφημένων κλήσεων, η πιστοποίηση χρήστη καθώς και η κρυπτογράφηση από άκρο σε άκρο συγκέντρωσαν την πλειοψηφία των απαντήσεων, όπως φαίνεται και στην Εικόνα 52 αλλά και στον Πίνακα 13.



Εικόνα 52. Κατανομή απαντήσεων σε ποσοστό για τα σημαντικότερα χαρακτηριστικά μιας πλατφόρμας ασφαλούς επικοινωνίας

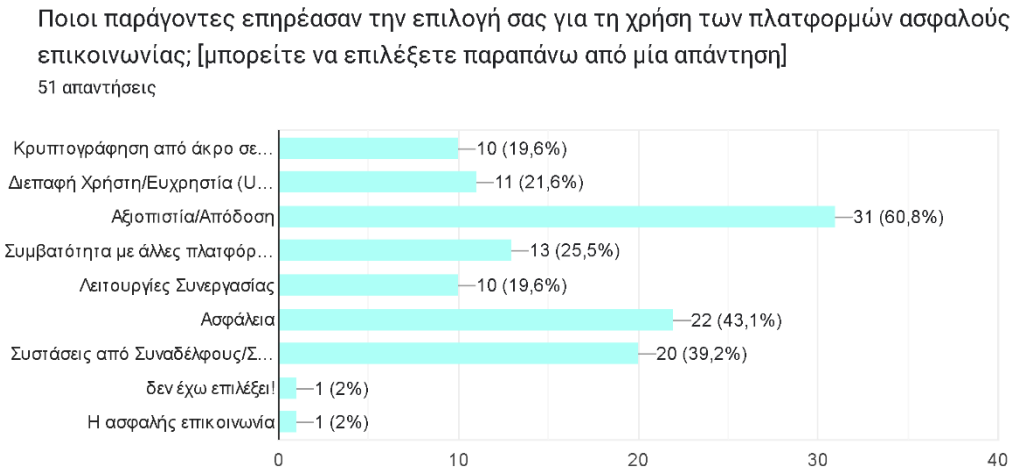
Πίνακας 13. Κατανομή σε πλήθος των απαντήσεων για τα σημαντικότερα χαρακτηριστικά μιας πλατφόρμας ασφαλούς επικοινωνίας

Ποιες συγκεκριμένες λειτουργίες των πλατφορμών ασφαλούς επικοινωνίας βρίσκετε πιο επωφελείς στη δημοσιογραφική σας εργασία;	
Απαντήσεις	**Σύνολο**
Κρυπτογράφηση από άκρο σε άκρο	18
Ασφαλής διαμοιρασμός αρχείων	**24**
Πραγματοποίηση κρυπτογραφημένων κλήσεων (ήχος και βίντεο)	21
Δυνατότητα χρήσης από διαφορετικές	13

συσκευές (cross platform compatibility)	
Πιστοποίηση χρήστη	20
Πολιτική διατήρησης μηνυμάτων	13
Ασφαλής επικοινωνία (Άλλο)	1

Η επόμενη ερώτηση ήταν ελεύθερου τύπου και οι συμμετέχοντες της έρευνας κλήθηκαν να αναφέρουν τις τρεις βασικές χρήσεις, οι οποίες τους οδηγούν να χρησιμοποιούν πλατφόρμες ασφαλούς επικοινωνίας. Καθώς η ερώτηση αυτή είχε ελεύθερο χαρακτήρα δεν υπήρξαν αμιγώς ποσοτικά αποτελέσματα. Ωστόσο, η κυρίαρχη απάντηση ήταν η ασφαλής επικοινωνία με πηγές και συναδέλφους καθώς και ο διαμοιρασμός αρχείων.

Στη συνέχεια, ζητήθηκε από τους συμμετέχοντες να απαντήσουν ποια είναι τελικά τα χαρακτηριστικά που επηρεάζουν στην επιλογή μιας πλατφόρμας ασφαλούς επικοινωνίας. Για την απάντησή τους δόθηκε μία λίστα χαρακτηριστικών από τα οποία η αξιοπιστία/απόδοση κρίνεται ως το σημαντικότερο από το 60,8% των ερωτηθέντων με την ασφάλεια και τις συστάσεις από συναδέλφους να ακολουθούν με 43,1% και 39,2% αντίστοιχα. Η λεπτομερής απεικόνιση των απαντήσεων για την εν λόγω ερώτηση φαίνεται στην Εικόνα 53 και στον Πίνακα 14Πίνακας 14.



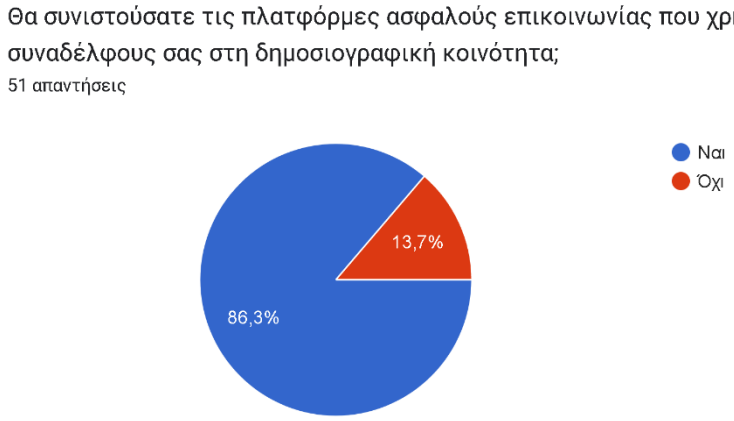
Εικόνα 53. Κατανομή σε ποσοστό των παραγόντων που επηρέασαν στην επιλογή μιας πλατφόρμας

Πίνακας 14. Κατανομή σε πλήθος των απαντήσεων για τους σημαντικότερους που επηρέασαν στην επιλογή μιας πλατφόρμας

Ποιοι παράγοντες επηρέασαν την επιλογή σας για τη χρήση των πλατφορμών ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Κρυπτογράφηση από άκρο σε άκρο	10
Διεπαφή Χρήστη/Ευχρηστία (User Interface)	11
Αξιοπιστία απόδοση	**31**
Συμβατότητα με άλλες πλατφόρμες	13
Λειτουργίες συνεργασίας	10
Ασφάλεια	23
Συστάσεις από συναδέλφους	20
Δεν έχω επιλέξει (Άλλο)	1

Σε ακόμα μία ερώτηση ελεύθερου τύπου ζητήθηκε από τους ερωτηθέντες να αναφέρουν ποιες βελτιώσεις θα ήθελαν να δουν στις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιούν. Λόγω της φύσης και του τύπου της ερώτησης, δεν είναι δυνατή η εξαγωγή ποσοτικής ανάλυσης. Ωστόσο, είναι φανερό ότι η πλειοψηφία των απαντήσεων εστιάζει στην ασφάλεια και θα επιθυμούσαν να βελτιωθεί στο μέλλον.

Ολοκληρώνοντας το συγκεκριμένο τμήμα του ερωτηματολογίου, περιείχε την ερώτηση εάν οι συμμετέχοντες θα πρότειναν τη χρήση πλατφορμών ασφαλούς επικοινωνίας που χρησιμοποιούν σε συναδέλφους τους στη δημοσιογραφική κοινότητα. Η συντριπτική πλειοψηφία και σε ποσοστό 86,3% απάντησε ναι όπως φαίνεται και στην Εικόνα 54 αλλά και στον Πίνακα 15.



Εικόνα 54. Κατανομή σε ποσοστό των ερωτηθέντων σχετικά με το αν θα συνιστούσαν τις πλατφόρμες που χρησιμοποιούν

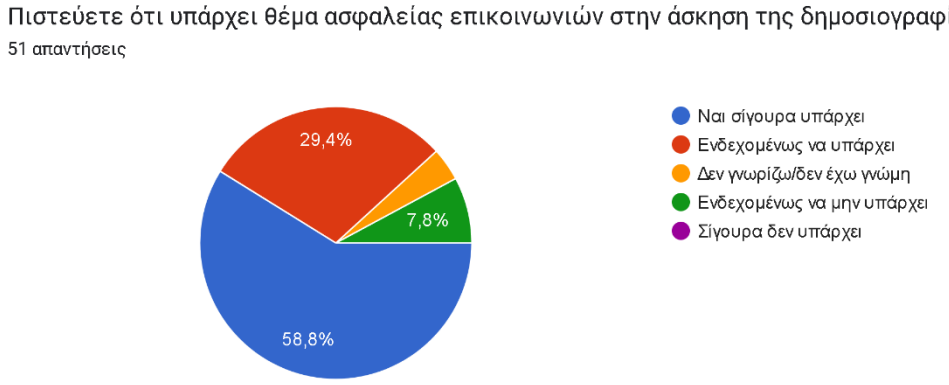
Πίνακας 15. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν θα συνιστούσαν ή όχι τις πλατφόρμες που χρησιμοποιούν

Θα συνιστούσατε τις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιείτε στους συναδέλφους σας στη δημοσιογραφική κοινότητα;	
Απαντήσεις	**Σύνολο**
Ναι	**44**
Όχι	7

5.1.4 Ασφάλεια επικοινωνιών στη Δημοσιογραφία

Το συγκεκριμένο τμήμα του ερωτηματολογίου συγκέντρωσε απαντήσεις ως προς την ασφάλεια των επικοινωνιών γενικότερα στη Δημοσιογραφία. Έτσι, κατέγραψε τις απόψεις των συμμετεχόντων, οι οποίες παρουσιάζονται σε ποσοτικό επίπεδο στις επόμενες παραγράφους.

Αρχικά, τέθηκε το ζήτημα στους ερωτηθέντες κατά πόσο πιστεύουν εάν υπάρχει ζήτημα ασφάλειας των επικοινωνιών στο επάγγελμα της Δημοσιογραφίας. Η πλειοψηφία με ποσοστό 58,8% δήλωσαν βέβαιοι ότι υπάρχει ενώ ένα 29,4% δήλωσε ότι πιθανόν υπάρχει. Τα ποσοστά αλλά και το πλήθος των απαντήσεων ανά επιλογή φαίνονται παρακάτω στην Εικόνα 55 και στον Πίνακα 16 αντίστοιχα.



Εικόνα 55. Κατανομή απαντήσεων σε ποσοστό ανά επιλογή σχετικά με το εάν πιστεύουν ότι υπάρχει ζήτημα ασφάλειας των επικοινωνιών στη Δημοσιογραφία

Πίνακας 16. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν πιστεύουν ότι υπάρχει ζήτημα ασφάλειας των επικοινωνιών στη Δημοσιογραφία

Πιστεύετε ότι υπάρχει θέμα ασφαλείας επικοινωνιών στην άσκηση της Δημοσιογραφίας;	
Απαντήσεις	**Σύνολο**
Ναι σίγουρα υπάρχει	**30**
Ενδεχομένως να υπάρχει	15
Δεν γνωρίζω/δεν έχω γνώμη	2
Ενδεχομένως να μην υπάρχει	4
Σίγουρα δεν υπάρχει	0

Εστιάζοντας περαιτέρω στις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιούν οι συμμετέχοντες στην έρευνα, ερωτήθηκαν κατά πόσο αισθάνονται βέβαιοι για την ασφάλεια και την ιδιωτικότητά τους, όταν τις χρησιμοποιούν. Τα αποτελέσματα εδώ δείχνουν ότι δεν αισθάνονται και πολύ βέβαιοι με ποσοστό 41,2% ενώ το 23,5% είχαν ουδέτερη στάση με το 15,7% να είναι καθόλου βέβαιο για την ασφάλεια αυτών και το 17,6% βέβαιοι και μόλις ένας από τους συμμετέχοντες αισθάνεται πολύ βέβαιος ή βέβαιη. Αναλυτικά τα αποτελέσματα αυτά παρουσιάζονται στην Εικόνα 56 και στον Πίνακα 17 παρακάτω.

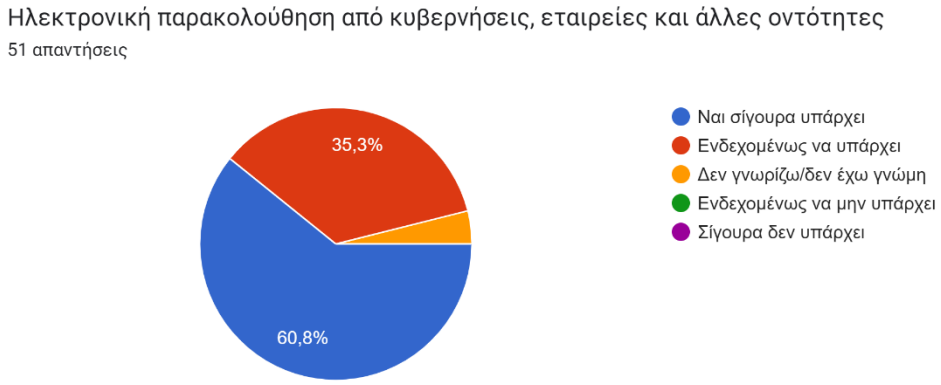
Εικόνα 56. Κατανομή απαντήσεων σε ποσοστό ανά επίπεδο βεβαιότητας για την ασφάλεια των πλατφορμών ασφαλούς επικοινωνίας

Πίνακας 17. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν επίπεδο βεβαιότητας για την ασφάλεια των πλατφορμών ασφαλούς επικοινωνίας

Πόσο βέβαιη/ος είστε για την ασφάλεια και την ιδιωτικότητα των πλατφορμών ασφαλούς επικοινωνίας που χρησιμοποιείτε;	
Απαντήσεις	**Σύνολο**
Πολύ βέβαιη/βέβαιος	1
Βέβαιη/Βέβαιος	9
Ουδέτερη/Ουδέτερος	12
Όχι πολύ βέβαιη/βέβαιος	**21**
Καθόλου βέβαιη/βέβαιος	8

Στη συνέχεια, εξερευνήθηκαν οι προκλήσεις που αντιμετωπίζουν οι δημοσιογράφοι στη σύγχρονη εποχή. Για τον λόγο αυτόν, τέθηκαν μία σειρά από ερωτήσεις που αποσκοπούσαν στο να καταγράψουν τη γνώμη όσων συμμετείχαν σχετικά με το αν πιστεύουν πως υπάρχουν συγκεκριμένες προκλήσεις που τους τέθηκαν ως ερώτημα. Έτσι, αρχικά στην ερώτηση αν θεωρούν πως υπάρχει ηλεκτρονική παρακολούθηση από κυβερνήσεις, εταιρείες αλλά και άλλους οργανισμούς ή οντότητες, το 60,8% απάντησε πως σίγουρα υπάρχει και το 35,3% ότι ενδεχομένως υπάρχει. Μόλις ένα

3.9% απάντησε ότι δεν γνωρίζει ή δεν έχει άποψη σχετικά με αυτό. Αυτά παρουσιάζονται αναλυτικά στην Εικόνα 57 και στον Πίνακα 18.



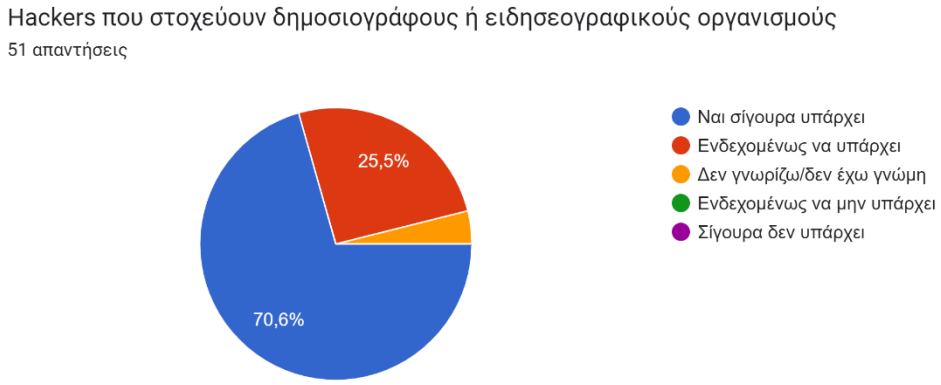
Εικόνα 57. Κατανομή απαντήσεων σε ποσοστό ανά επίπεδο βεβαιότητας για το αν θεωρούν ότι υπάρχει ηλεκτρονική παρακολούθηση από κυβερνήσεις, εταιρείες και άλλες οντότητες

Πίνακας 18. Κατανομή σε πλήθος των απαντήσεων σχετικά με το επίπεδο βεβαιότητας για το αν θεωρούν ότι υπάρχει ηλεκτρονική παρακολούθηση από κυβερνήσεις, εταιρείες και άλλες οντότητες

Οι δημοσιογράφοι αντιμετωπίζουν σήμερα σημαντικές προσκλήσεις. Πιστεύετε ότι υπάρχουν οι παρακάτω προκλήσεις; **Ηλεκτρονική παρακολούθηση από κυβερνήσεις, εταιρείες και άλλες οντότητες**	
Απαντήσεις	**Σύνολο**
Ναι σίγουρα υπάρχει	**31**
Ενδεχομένως να υπάρχει	18
Δεν γνωρίζω/δεν έχω γνώμη	2
Ενδεχομένως να μην υπάρχει	0
Σίγουρα δεν υπάρχει	0

Στην ερώτηση αν πιστεύουν πως hackers στοχεύουν δημοσιογράφους ή ειδησεογραφικούς οργανισμούς, η τάση των απαντήσεων είναι όμοια με προηγουμένως με το 70,6% να απαντά ότι σίγουρα υπάρχουν τέτοιες επιθέσεις και το 25,5% ότι ενδεχομένως υπάρχει αυτός ο κίνδυνος. Και πάλι ένα μόλις 3,9% δεν

εξέφρασε γνώμη για το συγκεκριμένο ζήτημα. Τα παραπάνω απεικονίζονται με λεπτομέρεια στην Εικόνα 58 και στον Πίνακα 19.



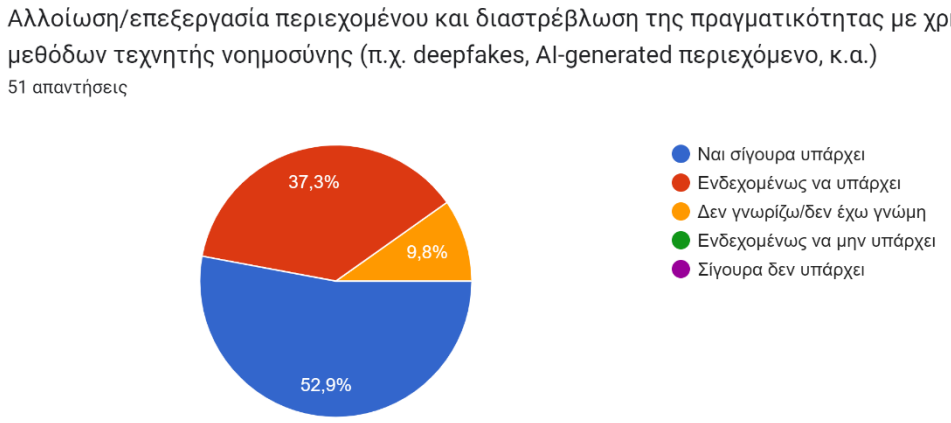
Εικόνα 58. Κατανομή απαντήσεων σε ποσοστό ανά επίπεδο βεβαιότητας για το αν θεωρούν ότι υπάρχει απειλή από hackers που στοχεύουν δημοσιογράφους και ειδησεογραφικούς οργανισμούς

Πίνακας 19. Κατανομή σε πλήθος των απαντήσεων σχετικά με το επίπεδο βεβαιότητας για το αν υπάρχει απειλή από hackers που στοχεύουν δημοσιογράφους και ειδησεογραφικούς οργανισμούς

Οι δημοσιογράφοι αντιμετωπίζουν σήμερα σημαντικές προσκλήσεις. Πιστεύετε ότι υπάρχουν οι παρακάτω προκλήσεις; **Hackers που στοχεύουν δημοσιογράφους ή ειδησεογραφικούς οργανισμούς**	
Απαντήσεις	**Σύνολο**
Ναι σίγουρα υπάρχει	**36**
Ενδεχομένως να υπάρχει	13
Δεν γνωρίζω/δεν έχω γνώμη	2
Ενδεχομένως να μην υπάρχει	0
Σίγουρα δεν υπάρχει	0

Συνεχίζοντας, το 52,9% απάντησε στην ερώτηση του αν υπάρχει ο κίνδυνος αλλοίωσης του περιεχομένου που οδηγεί σε διαστρέβλωση της πραγματικότητας με χρήση μεθόδων τεχνητής νοημοσύνης (ΤΝ) (π.χ. deepfake, AI-generated περιεχόμενο, κ.α.) πως θεωρεί βέβαιο ότι υπάρχει, με το 37,3% να απαντά ότι

ενδεχομένως υπάρχει. Το 9,8% ανέφερε ότι δεν γνωρίζει ή δεν έχει άποψη για το συγκεκριμένο θέμα. Αναλυτική απεικόνιση των απαντήσεων υπάρχει στην Εικόνα 59 και στον Πίνακα 20.



Εικόνα 59. Κατανομή απαντήσεων σε ποσοστό ανά επίπεδο βεβαιότητας για το αν θεωρούν ότι υπάρχει ο κίνδυνος αλλοίωσης του περιεχομένου με χρήση μεθόδων τεχνητής νοημοσύνης

Πίνακας 20. Κατανομή σε πλήθος των απαντήσεων σχετικά με το αν θεωρούν ότι υπάρχει ο κίνδυνος αλλοίωσης του περιεχομένου με χρήση μεθόδων τεχνητής νοημοσύνης

Οι δημοσιογράφοι αντιμετωπίζουν σήμερα σημαντικές προσκλήσεις. Πιστεύετε ότι υπάρχουν οι παρακάτω προκλήσεις; **Αλλοίωση/επεξεργασία περιεχομένου και διαστρέβλωση της πραγματικότητας με χρήση μεθόδων τεχνητής νοημοσύνης (π.χ. deepfakes, AI-generated περιεχόμενο, κ.α.)**	
Απαντήσεις	**Σύνολο**
Ναι σίγουρα υπάρχει	**27**
Ενδεχομένως να υπάρχει	19
Δεν γνωρίζω/δεν έχω γνώμη	5
Ενδεχομένως να μην υπάρχει	0
Σίγουρα δεν υπάρχει	0

Τέλος, οι ερωτηθέντες κλήθηκαν να επιλέξουν ποια από τις δύο επόμενες προτάσεις είναι πιο κοντά σε αυτό που και οι ίδιοι πιστεύουν:

- Για τους σημερινούς δημοσιογράφους, τα οφέλη της ψηφιακής επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα, υπερτερούν των κινδύνων
- Για τους σημερινούς δημοσιογράφους, οι κίνδυνοι της ψηφιακής επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα υπερτερούν των πλεονεκτημάτων

Το 74,5% συμφώνησε με την πρώτη πρόταση ότι τα οφέλη υπερτερούν των κινδύνων ενώ το 25,5% πιστεύει ότι οι κίνδυνοι είναι περισσότεροι από τα οφέλη.

Εικόνα 60. Κατανομή σε ποσοστό των απαντήσεων σχετικά με την άποψη των συμμετεχόντων στο ερώτημα αν τα οφέλη της ψηφιακής εποχής υπερτερούν των κινδύνων

Πίνακας 21. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν θα συνιστούσαν ή όχι τις πλατφόρμες που χρησιμοποιούν

Ποια από τις ακόλουθες δηλώσεις έρχεται πιο κοντά στη δική σας άποψη, ακόμη και αν καμία από τις δύο δεν είναι ακριβώς σωστή;	
Απαντήσεις	**Σύνολο**
Για τους σημερινούς δημοσιογράφους, τα οφέλη της ψηφιακής επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα, υπερτερούν των κινδύνων	**38**
Για τους σημερινούς δημοσιογράφους, οι κίνδυνοι της ψηφιακής επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα υπερτερούν των πλεονεκτημάτων	13

5.1.5 Εμπειρίες από παραβίαση επικοινωνίας στην εργασία

Σε αυτό το τμήμα του ερευνητικού ερωτηματολογίου οι συμμετέχοντες κλήθηκαν να απαντήσουν σε ερωτήματα που αφορούσαν τις εμπειρίες τους από ενδεχόμενη παραβίαση στην εργασία τους. Έτσι, αρχικά το 47,1% απάντησε ότι έχει βιώσει ή έχει υποψιαστεί παραβίαση της επικοινωνίας του στην εργασία του. Με το 33,3% να απαντάει ότι δεν έχει βιώσει ή υποψιαστεί κάποια παραβίαση της επικοινωνίας του με το 19,6% να αναφέρει ότι δεν γνωρίζει. Η οπτικοποίηση των αποτελεσμάτων φαίνεται παρακάτω στην Εικόνα 61 και στον Πίνακα 22.

Εικόνα 61. Κατανομή απαντήσεων σε ποσοστό σχετικά με το ερώτημα αν έχουν βιώσει ή υποψιαστεί παραβίαση της επικοινωνίας τους στην εργασία

Πίνακας 22. Κατανομή σε πλήθος των απαντήσεων σχετικά με το ερώτημα αν έχουν βιώσει ή υποψιαστεί παραβίαση της επικοινωνίας τους στην εργασία

Έχετε βιώσει ή υποψιαστεί ότι έχετε υποστεί παραβίαση επικοινωνίας στην εργασία σας;	
Απαντήσεις	**Σύνολο**
Ναι	**24**
Όχι	17
Δεν γνωρίζω	10

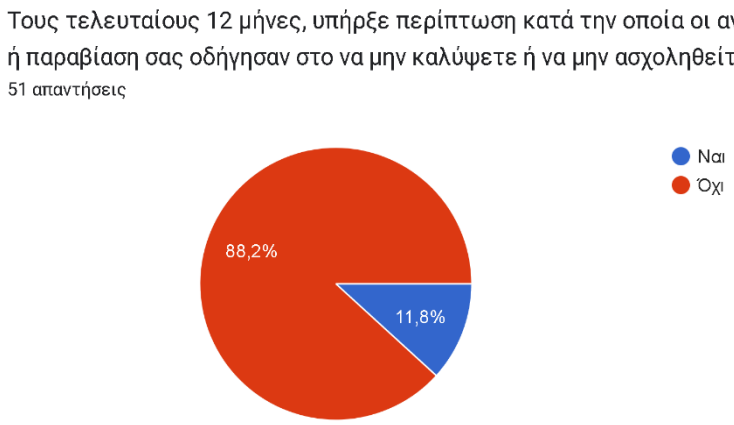
Οι συμμετέχοντες του ερωτηματολογίου στη συνέχεια ανέφεραν τις ανησυχίες τους σχετικά με τις διαδικασίες στις οποίες πιστεύουν ότι είναι πιο πιθανή η παραβίαση

των επικοινωνιών τους. Έτσι, από τους 24 συμμετέχοντες που απάντησαν ότι έχουν βιώσει ή υποπτευθεί παραβίαση των επικοινωνιών τους στον Πίνακα 23, φαίνεται ποιοι από αυτούς και σε ποιες διαδικασίες/χρήσεις τους θεωρούν ότι υπήρξε αυτή η παραβίαση.

Πίνακας 23. Κατανομή σε πλήθος των απαντήσεων σχετικά με τις διαδικασίες στις οποίες θεωρούν οι συμμετέχοντες ότι έχουν υποστεί παραβίαση επικοινωνιών

Αν απαντήσατε ναι στην προηγούμενη ερώτηση, ποιες από τις παρακάτω διαδικασίες αφορά; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Χρήση του διαδικτύου για συλλογή πληροφοριών	8
Αποθήκευση ή κοινή χρήση δυνητικά ευαίσθητων εγγράφων	4
Επικοινωνία με άλλους δημοσιογράφους, συντάκτες ή παραγωγούς	8
Επικοινωνία με πηγές	**11**

Καταγράφοντας λοιπόν τις όποιες ανησυχίες για την παραβίαση των επικοινωνιών τους, οι συμμετέχοντες στο ερευνητικό ερωτηματολόγιο ερωτηθήκαν εάν κατά τους 12 τελευταίους μήνες η οποιαδήποτε ανησυχία για ενδεχομένη παρακολούθηση τους οδήγησε στην απόφαση να μην καλύψουν ή να μην ασχοληθούν με κάποιο συγκεκριμένο θέμα. Η συντριπτική πλειοψηφία απάντησε ότι κάτι τέτοιο δεν συνέβη σε ποσοστό 88,2% με μόλις ένα 11,2% να απαντάει θετικά.



Εικόνα 62. Κατανομή σε ποσοστό των ερωτηθέντων στο ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται δεν ασχολήθηκαν με ένα θέμα

Πίνακας 24. Κατανομή σε πλήθος των απαντήσεων σχετικά με το ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται δεν ασχολήθηκαν με ένα θέμα

Τους τελευταίους 12 μήνες, υπήρξε περίπτωση κατά την οποία οι ανησυχίες για παρακολούθηση ή παραβίαση σας οδήγησαν στο να μην καλύψετε ή να μην ασχοληθείτε με ένα συγκεκριμένο θέμα;	
Απαντήσεις	**Σύνολο**
Ναι	6
Όχι	**45**

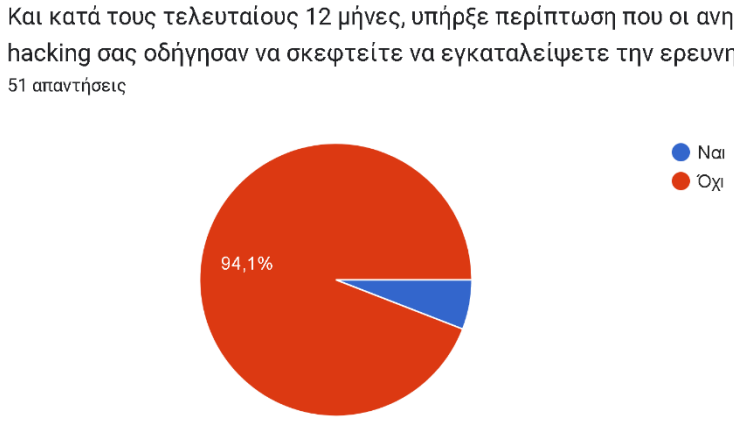
Συνεχίζοντας, τέθηκε το ερώτημα εάν υπό τον φόβο της παρακολούθησης των επικοινωνιών τους τελευταίους 12 μήνες δεν πραγματοποίησαν κάποια επικοινωνία με μια συγκεκριμένη πηγή τους. Και σε αυτή την ερώτηση, η πλειοψηφία σε ποσοστό 80,4% απάντησε αρνητικά. Τα αναλυτικά αποτελέσματα στο παρόν ερώτημα φαίνονται στην Εικόνα 63 και στον Πίνακα 25.

Εικόνα 63. Κατανομή σε ποσοστό των ερωτηθέντων στο ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται δεν επικοινώνησαν με κάποια συγκεκριμένη πηγή

Πίνακας 25. Κατανομή σε πλήθος των απαντήσεων σχετικά με το ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται δεν επικοινώνησαν με κάποια συγκεκριμένη πηγή

Τους τελευταίους 12 μήνες, υπήρξε περίπτωση που οι ανησυχίες για παρακολούθηση ή παραβίαση σας οδήγησαν στο να μην απευθυνθείτε σε μια συγκεκριμένη πηγή;	
Απαντήσεις	**Σύνολο**
Ναι	10
Όχι	**41**

Το τελευταίο ερώτημα, το οποίο αφορούσε την ανησυχία για ενδεχομένη παρακολούθηση των συμμετεχόντων κατά την επικοινωνία τους, είχε να κάνει με το εάν ο φόβος αυτός τους οδήγησε ποτέ να σκεφθούν να εγκαταλείψουν την ερευνητική Δημοσιογραφία. Το 94,1% απάντησε ότι δεν σκέφτηκε τους τελευταίους δώδεκα μήνες να εγκαταλείψει το δημοσιογραφικό του έργο. Παρακάτω στην Εικόνα 64 και στον Πίνακα 26 φαίνονται τα αναλυτικά αποτελέσματα.



Εικόνα 64. Κατανομή σε ποσοστό των ερωτηθέντων στο ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται σκέφθηκαν να παρατήσουν τη Δημοσιογραφία

Πίνακας 26. Κατανομή σε πλήθος των απαντήσεων σχετικά με το ερώτημα εάν λόγω ανησυχίας ότι παρακολουθούνται σκέφθηκαν να παρατήσουν τη Δημοσιογραφία

Και κατά τους τελευταίους 12 μήνες, υπήρξε περίπτωση που οι ανησυχίες για παρακολούθηση ή hacking σας οδήγησαν να σκεφτείτε να εγκαταλείψετε την ερευνητική Δημοσιογραφία;	
Απαντήσεις	**Σύνολο**
Ναι	10
Όχι	**41**

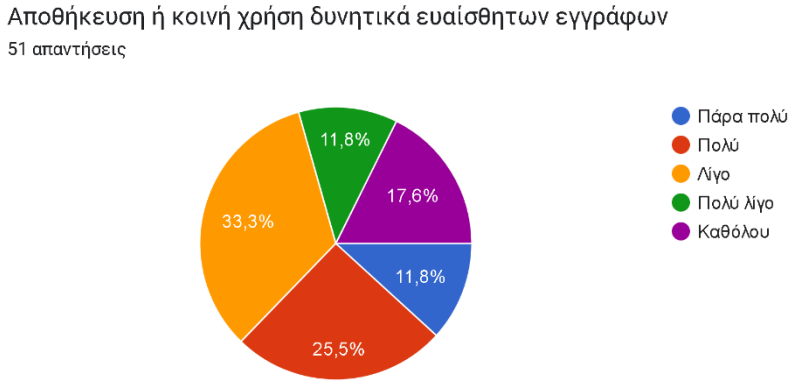
Έχοντας καταγράψει τις ανησυχίες των ερωτηθέντων σχετικά με ενδεχόμενη παραβίαση των επικοινωνιών τους τελευταίους δώδεκα μήνες, το επόμενο σύνολο ερωτήσεων είχε ως στόχο να καταγράψει τις συνήθειές τους και κατά πόσο αυτές έχουν αλλάξει ή όχι το τελευταίο έτος. Αρχικά, ερωτήθηκαν κατά πόσο έχει αλλάξει ο τρόπος με τον οποίο χρησιμοποιούν το Διαδίκτυο για να ερευνήσουν οποιοδήποτε θέμα. Το 33,3% απάντησε ότι έχει αλλάξει πολύ ο τρόπος ενώ τα υπόλοιπα 2/3 των ερωτηθέντων σχεδόν ισοκατανεμήθηκαν στις υπόλοιπες απαντήσεις. Τα αναλυτικά αποτελέσματα απεικονίζονται στην Εικόνα 65 και στον Πίνακα 27.

Εικόνα 65. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που χρησιμοποιούν το Διαδίκτυο για έρευνα

Πίνακας 27. Κατανομή σε πλήθος των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που χρησιμοποιούν το Διαδίκτυο για έρευνα

Τους τελευταίους 12 μήνες, πόσο, αν όχι καθόλου, έχετε αλλάξει τον τρόπο με τον οποίο... **Χρησιμοποιείτε το διαδίκτυο για να ερευνήσετε ιστορίες**	
Απαντήσεις	**Σύνολο**
Πάρα πολύ	8
Πολύ	**17**
Λίγο	9
Πολύ λίγο	7
Καθόλου	10

Συνεχίζοντας, η επόμενη ερώτηση αφορούσε το εάν έχει αλλάξει καθόλου ο τρόπος που αποθηκεύουν ή διαμοιράζονται αρχεία με ευαίσθητες πληροφορίες. Το 33,3% απάντησε λίγο ενώ το 25,5% πολύ με το εναπομείναν ποσοστό να μοιράζεται στις υπόλοιπες τρεις κλάσεις.

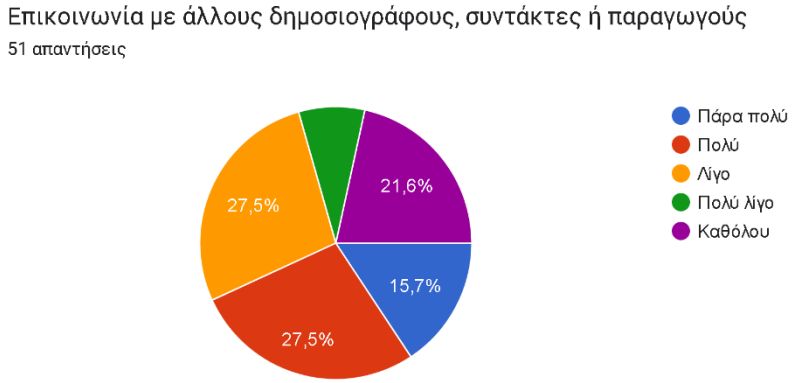


Εικόνα 66. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που αποθηκεύουν ή διαμοιράζονται ευαίσθητα έγγραφα

Πίνακας 28. Κατανομή σε πλήθος των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που αποθηκεύουν ή διαμοιράζονται ευαίσθητα έγγραφα

Τους τελευταίους 12 μήνες, πόσο, αν όχι καθόλου, έχετε αλλάξει τον τρόπο με τον οποίο... **Αποθηκεύετε ή κάνετε κοινή χρήση δυνητικά ευαίσθητων εγγράφων**	
Απαντήσεις	**Σύνολο**
Πάρα πολύ	6
Πολύ	13
Λίγο	**17**
Πολύ λίγο	6
Καθόλου	9

Στο ίδιο σύνολο ερωτήσεων, οι συμμετέχοντες του ερωτηματολογίου κλήθηκαν να απαντήσουν εάν έχει αλλάξει ο τρόπος επικοινωνίας τους με τους συναδέλφους τους, τους συντάκτες ή τους παραγωγούς. Ένα 27,5% των συμμετεχόντων απάντησε πολύ ενώ άλλο ένα 27,5% απάντησε λίγο. Πολύ κοντά βρίσκεται και η απάντηση «Καθόλου» με 21,6%. Η αναλυτική καταγραφή αυτών των απαντήσεων φαίνεται παρακάτω στην Εικόνα 67 και στον Πίνακα 29.

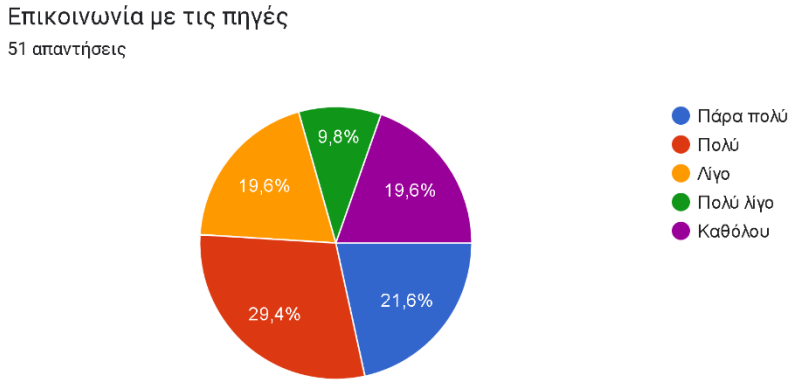


Εικόνα 67. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που επικοινωνούν με συναδέλφους ή άλλους επαγγελματίες του χώρου

Πίνακας 29. Κατανομή σε πλήθος των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που επικοινωνούν με συναδέλφους ή άλλους επαγγελματίες του χώρου

Τους τελευταίους 12 μήνες, πόσο, αν όχι καθόλου, έχετε αλλάξει τον τρόπο με τον οποίο... **Επικοινωνείτε με άλλους δημοσιογράφους, συντάκτες ή παραγωγούς**	
Απαντήσεις	**Σύνολο**
Πάρα πολύ	8
Πολύ	**14**
Λίγο	**14**
Πολύ λίγο	4
Καθόλου	11

Τέλος, το συγκεκριμένο τμήμα του ερωτηματολογίου κατέγραψε κατά πόσο έχει αλλάξει τους τελευταίους δώδεκα μήνες ο τρόπος επικοινωνίας των συμμετεχόντων με τις πηγές τους. Το 29,4% απάντησε ότι έχει αλλάξει πολύ και ακολουθεί το 21,6% που απάντησε πάρα πολύ. Τα αποτελέσματα σε ποσοστό και σε πλήθος απαντήσεων φαίνονται παρακάτω στην Εικόνα 68 και στον Πίνακα 30 αντίστοιχα.



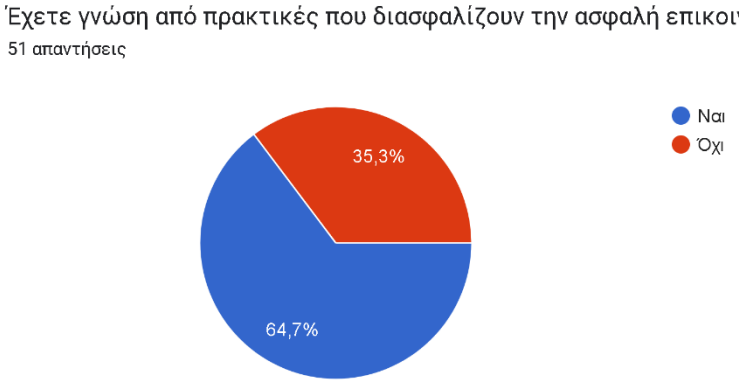
Εικόνα 68. Κατανομή σε ποσοστό των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που επικοινωνούν με τις πηγές τους

Πίνακας 30. Κατανομή σε πλήθος των απαντήσεων σχετικά με το κατά πόσο έχει αλλάξει ο τρόπος που επικοινωνούν με τις πηγές τους

Τους τελευταίους 12 μήνες, πόσο, αν όχι καθόλου, έχετε αλλάξει τον τρόπο με τον οποίο... **Επικοινωνείτε με πηγές**	
Απαντήσεις	**Σύνολο**
Πάρα πολύ	11
Πολύ	**15**
Λίγο	10
Πολύ λίγο	5
Καθόλου	10

5.1.6 Πρακτικές που διασφαλίζουν την ασφαλή επικοινωνία

Σε αυτό το σύντομο τμήμα του ερωτηματολογίου οι συμμετέχοντες ερωτήθηκαν εάν έχουν γνώση από τέτοιες πρακτικές και εάν όντως εφαρμόζουν κάποιες από αυτές. Έτσι, το 64,7% απάντησε ότι γνωρίζει τέτοιες πρακτικές και το 35,3% απάντησε ότι δεν έχει γνώση.



Εικόνα 69. Κατανομή απαντήσεων σε ποσοστό σχετικά με το ερώτημα εάν υπάρχει γνώση σχετικά με πρακτικές ασφαλούς επικοινωνίας

Πίνακας 31. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν έχουν γνώση για πρακτικές ασφαλούς επικοινωνίας

Έχετε γνώση από πρακτικές που διασφαλίζουν την ασφαλή επικοινωνία;	
Απαντήσεις	**Σύνολο**
Ναι	**33**
Όχι	18

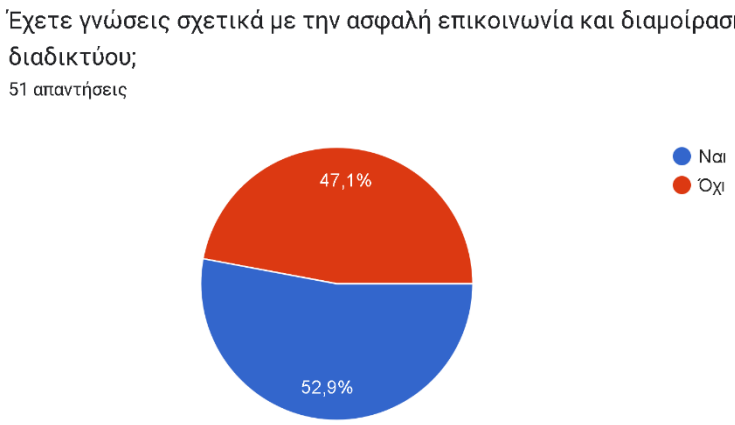
Οι 33 συμμετέχοντες που απάντησαν ότι έχουν γνώση στη συνέχεια ερωτήθηκαν εάν χρησιμοποιούν και κάποιες από αυτές για την ασφαλή τους επικοινωνία. Τα αποτελέσματα της συγκεκριμένης ερώτησης φαίνονται παρακάτω στον Πίνακα 32. Παρατηρείται ότι οι περισσότεροι συμμετέχοντες προσπαθούν να χρησιμοποιούν αρκετές πρακτικές ασφαλούς επικοινωνίας. Η δημοφιλέστερη είναι χρήση ισχυρών κωδικών και η λιγότερη δημοφιλής έχει να κάνει με την εκπαίδευση και την ενημέρωση σχετικά με τις κυβερνοαπειλές.

Πίνακας 32. Κατανομή σε πλήθος των απαντήσεων σχετικά με τις πρακτικές ασφαλούς επικοινωνίας που χρησιμοποιούν

Χρησιμοποιείτε κάποια από τα παρακάτω πρακτικές για ασφαλή επικοινωνία; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]	
Απαντήσεις	**Σύνολο**
Χρήση κρυπτογράφησης σε emails, μηνύματα, κ.λπ.	16
Χρήση ισχυρών κωδικών	**26**
Χρήση ταυτοποίησης δύο παραγόντων (2 Factor Authentication – 2FA)	17
Χρήση συσκευών με ισχυρή ασφάλεια	8
Αποφυγή χρήσης επισφαλών δημόσιων δικτύων (Wi-Fi σε καφέ, εστιατόρια, δημόσιους χώρους)	19
Συνεχής πραγματοποίηση ενημερώσεων ασφαλείας των εφαρμογών	17
Χρήση antivirus	23
Εκπαίδευση και ενημέρωση σχετικά με τις κυβερνοαπειλές	4

5.1.7 Γνώσεις και απόκτηση αυτών γύρω από την ασφαλή επικοινωνία

Στο τελευταίο τμήμα του ερωτηματολογίου, οι συμμετέχοντες κλήθηκαν να απαντήσουν εάν έχουν γνώσεις γύρω από την ασφαλή επικοινωνία και τον διαμοιρασμό πληροφοριών μέσω του Διαδικτύου. Το 52,9% απάντησε θετικά σε αυτό και το 47,1% αρνητικά όπως φαίνεται και στην Εικόνα 70.

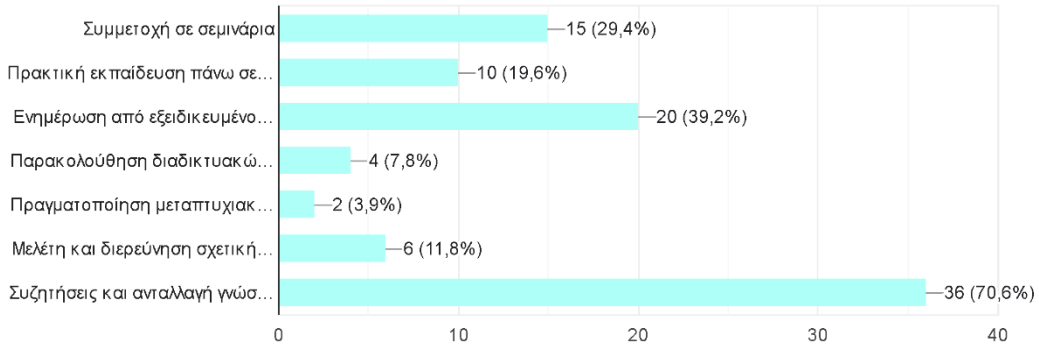


Εικόνα 70. Κατανομή απαντήσεων σε ποσοστό με βάση το ερώτημα εάν έχουν γνώσεις σχετικά με την ασφαλή επικοινωνία και το διαμοιρασμό πληροφοριών μέσω διαδικτύου

Πίνακας 33. Κατανομή σε πλήθος των απαντήσεων σχετικά με το εάν έχουν γνώση για πρακτικές ασφαλούς επικοινωνίας

Έχετε γνώσεις σχετικά με την ασφαλή επικοινωνία και διαμοίραση πληροφοριών μέσω Διαδικτύου;	
Απαντήσεις	**Σύνολο**
Ναι	**27**
Όχι	24

Τέλος, οι συμμετέχοντες του ερωτηματολογίου κλήθηκαν να δηλώσουν ποιες δράσεις ή πρακτικές εφαρμόζουν ή θα ήταν διατεθειμένοι να εφαρμόσουν προκειμένου να αποκτήσουν γνώση για ασφαλή διαμοιρασμό αρχείων και πληροφοριών μέσω Διαδικτύου. Οι περισσότεροι απάντησαν ότι η συζήτηση και η ανταλλαγή γνώσεων και εμπειριών αποτελεί μια τέτοια πρακτική ενώ αρκετοί δήλωσαν ότι θα τους ενδιέφερε η συμμετοχή σε ενημερώσεις από εξειδικευμένους ιστότοπους και η συμμετοχή σε σεμινάρια. Η ανάλυση των απαντήσεων φαίνεται στην Εικόνα 69.



Εικόνα 71. Κατανομή απαντήσεων σχετικά με τις πρακτικές και δράσεις που έχουν εφαρμόσει ή θα εφάρμοζαν προκειμένου να αποκτήσουν γνώσεις για την ασφαλή επικοινωνία και διαμοιρασμό πληροφοριών μέσω Διαδικτύου

5.2 Σχολιασμός αποτελεσμάτων και συμπεράσματα

Έχοντας παρουσιάσει προηγουμένως τα ποσοτικά αποτελέσματα της έρευνας, στο παρόν γίνεται ενδελεχής σχολιασμός αυτών και εξάγονται χρήσιμα συμπεράσματα. Ξεκινώντας από τα δημογραφικά, παρατηρείται από το δείγμα που απάντησε στο ερωτηματολόγιο ότι οι άνδρες είναι δύο προς μία γυναίκα στον δημοσιογραφικό χώρο. Αυτό καταδεικνύει ότι συντηρείται μια τάση, η οποία υπήρχε παλαιότερα κατά την οποία ο δημοσιογραφικός χώρος είναι κυρίως ανδροκρατούμενος. Ωστόσο, αυτό ίσως έρχεται σε άμεση σύνδεση και με την ηλικιακή κατανομή των συμμετεχόντων, η οποία μοιράζεται σε ποσοστό άνω του 92% σε ηλικίες μεγαλύτερες των 35 ετών και σε ποσοστό κοντά στο 70% σε ηλικίες άνω των 45 ετών. Έτσι, στο δείγμα των συμμετεχόντων, παρατηρούμε ότι υπάρχουν κυρίως έμπειροι δημοσιογράφοι, οι οποίοι στο μεγαλύτερο ποσοστό (άνω του 75%) είναι τουλάχιστον κάτοχοι πανεπιστημιακού τίτλου.

Προχωρώντας, η πλειοψηφία των συμμετεχόντων είναι δημοσιογράφοι που εργάζονται σε ειδησεογραφικό οργανισμό. Αυτό έχει ως αποτέλεσμα, πέρα από τις προσωπικές προτιμήσεις τους στη θεματολογία, να ασχολούνται με θέματα που επιθυμεί ή εξυπηρετεί κυρίως ο ειδησεογραφικός οργανισμός που εργάζονται. Έτσι, η πλειοψηφία των συμμετεχόντων που εργάζεται και σε ειδησεογραφικό οργανισμό, καταπιάνεται περισσότερο με θέματα πολιτικής και αστυνομικό ρεπορτάζ. Στον αντίποδα, παρατηρούμε ότι όσοι εργάζονται είτε ανεξάρτητα αποκλειστικά είτε σε συνδυασμό με άλλη εργασία, καταπιάνονται και με διαφορετικής θεματολογίας

θέματα όπως αθλητικά, πολιτισμό, εκκλησία, περιβάλλον, επιστήμη και τεχνολογία κ.α. Επιπλέον, παρατηρείται ένα ευρύτερο φάσμα θεματολογίας στις γυναίκες δημοσιογράφους συγκριτικά με τους άνδρες, οι οποίοι συνήθως εστιάζουν σε εσωτερικά ζητήματα όπως η πολιτική και η οικονομία. Ως απόρροια της κάλυψης κυρίως ειδήσεων που αφορούν την πολιτική και εσωτερικές υποθέσεις αλλά και το κοινό στο οποίο απεστάλη το ερωτηματολόγιο παρατηρείται ότι πάνω από τους μισούς συμμετέχοντες ασχολούνται με τοπικές ειδήσεις ενώ με διεθνείς αποκλειστικά ειδήσεις μόλις ένα 2%.

Σχετικά με τη χρήση πλατφορμών ασφαλούς επικοινωνίας, παρατηρούμε ότι το 62,7% απάντησε θετικά στο αν χρησιμοποιούν τέτοιες πλατφόρμες. Εδώ, αξίζει να σημειωθεί ότι το ποσοστό αυτό είναι σχετικά μειωμένο στους άνδρες και ανέρχεται σε 59% σχεδόν ενώ στις γυναίκες αυτό το ποσοστό είναι σημαντικά υψηλότερο στο 75%. Επομένως, αυτό ενδέχεται να οφείλεται ότι οι γυναίκες εισήλθαν αργότερα στη Δημοσιογραφία από τους άνδρες με αποτέλεσμα να είναι πιο δεκτικές σε νέες τεχνολογίες και εργαλεία. Αυτό απεικονίζεται και στις γνώσεις γύρω από τις διαθέσιμες πλατφόρμες, όπου αν και μικρότερο δείγμα αυτών των γυναικών, είχε απαντήσεις που εμπεριείχαν επτά από τις δώδεκα πλατφόρμες που ερωτήθηκαν. Στους άνδρες έχουμε έντεκα από τις δώδεκα αλλά το δείγμα είναι αρκετά μεγαλύτερο από αυτών των γυναικών. Επιπλέον, στο παρόν ερώτημα οι πλατφόρμες που είναι πιο διαδεδομένες είναι αυτές των άμεσων μηνυμάτων που παρέχονται χωρίς χρέωση όπως το Signal, WhatsApp και Telegram. Η δημοφιλία των προαναφερθέντων πλατφορμών επιβεβαιώνεται και από το ποσοστό που απάντησε ότι τις χρησιμοποιεί, το οποίο είναι αρκετά μεγαλύτερο από τις υπόλοιπες επιλογές. Αξίζει δε να σημειωθεί ότι μόνο τρεις συμμετέχοντες απάντησαν ότι δεν χρησιμοποιούν καμία πλατφόρμα από αυτές. Το κοινό χαρακτηριστικό αυτών των τριών απαντήσεων είναι ότι αφορούν άνδρες μεγαλύτερης ηλικίας, γεγονός που δικαιολογεί εν μέρει τη δυσκολία ή την άρνηση υιοθέτησης νέων μέσων και εργαλείων στην εργασία τους. Στη συχνότητα χρήσης των πλατφορμών αυτών και πάλι, το ποσοστό καθημερινής χρήσης είναι μεγαλύτερο στις γυναίκες από το αντίστοιχο των ανδρών, οι οποίοι κάνουν πιο αραιή χρήση.

Αξιοσημείωτο είναι ότι το 56,9% γνωρίζει τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails αλλά μόλις το 21,6% κάνει χρήση αυτής της δυνατότητας.

Αυτό πολλές φορές οφείλεται στα διαθέσιμα εργαλεία που έχει ένας δημοσιογράφος, στην ενημέρωση που του παρέχεται για τους κινδύνους αλλά και στον ίδιο καθώς και στο κατά πόσο ανησυχεί για την ιδιωτικότητα των πληροφοριών που μοιράζεται. Στη συγκεκριμένη ερώτηση αν και τα ποσοστά τόσο σε άντρες όσο και γυναίκες είναι χαμηλά, οι γυναίκες κάνουν χρήση στο 31% ενώ οι άνδρες στο 11%. Χαρακτηριστικό είναι ότι από όσους απάντησαν ότι χρησιμοποιούν κρυπτογραφημένα emails πάνω από το 50% ανήκει στην ηλικιακή ομάδα 35-44 γεγονός που φανερώνει ότι λόγω της εμπειρίας τους αλλά και το νεαρό της ηλικίας έχουν τη διάθεση να στραφούν σε νέα εργαλεία και τεχνολογίες. Επίσης, χαρακτηριστικό είναι ότι όσοι χρησιμοποιούν κρυπτογραφημένα emails, έχουν δηλώσει ότι εργάζονται σε ειδησεογραφικό οργανισμό. Αυτό πρακτικά καταδεικνύει ότι πολλές φορές οι οργανισμοί αυτοί επιβάλλουν τη χρήση τέτοιων εργαλείων στους συνεργάτες τους, υπό τον φόβο οποιασδήποτε παραβίασης, κάτι που σε ατομικό επίπεδο πολλές φορές παραμελείται.

Σχετικά με τις κύριες χρήσεις για τις οποίες χρησιμοποιούν τις πλατφόρμες ασφαλούς επικοινωνίας, στο σύνολό τους οι ερωτηθέντες απάντησαν για την επικοινωνία τους με συναδέλφους και πηγές καθώς και για τον ασφαλή διαμοιρασμό αρχείων. Επιπλέον, υπήρχαν απαντήσεις που αφορούσαν την αναζήτηση πληροφοριών πέρα από τα συμβατικά μέσα αλλά και τον συντονισμό συνεργατικών προσπαθειών, όταν μια είδηση ή ένα θέμα απαιτεί ομαδική εργασία και συνεχή ροή. Ταυτόχρονα, τα βασικά χαρακτηριστικά που επηρεάζουν την επιλογή μιας τέτοιας πλατφόρμας από έναν δημοσιογράφο, σύμφωνα με τα αποτελέσματα της έρευνας, είναι η αξιοπιστία και η απόδοση, η ασφάλεια αλλά και οι συστάσεις από συναδέλφους τους. Αυτό ήταν αναμενόμενο, καθώς η σωστή λειτουργία αλλά και η ασφάλεια αποτελούν βασικά στοιχεία για την άσκηση του δημοσιογραφικού επαγγέλματος, το οποίο σε πολλές περιπτώσεις διαχειρίζεται ευαίσθητες πληροφορίες. Από την άλλη, η σύσταση από συναδέλφους αποτελεί σημαντικό κριτήριο καθώς σε πολλές περιπτώσεις η εμπειρία χρήσης αλλά και η ανάγκη για συνεργατική εργασία απαιτεί τη χρήση κοινής πλατφόρμας. Όσον αφορά τις επιθυμητές βελτιώσεις που θα ήθελαν οι χρήστες, η επιπλέον ασφάλεια είναι βασικό χαρακτηριστικό, το οποίο επιζητούν οι χρήστες. Αυτό μπορεί να επιτευχθεί με πιο αυστηρά φίλτρα ασφαλείας, με συχνές ενημερώσεις των εφαρμογών και με καλύτερες διαδικασίες ταυτοποίησης των χρηστών. Επιπλέον, πολλοί χρήστες θα ήθελαν καλύτερες δυνατότητες διαμοιρασμού αρχείων (π.χ.

μεγαλύτερα αρχεία, καλύτερη ποιότητα) και βελτιώσεις στην εμπειρία χρήσης όπως συμβατότητα με λειτουργικά συστήματα και διαλειτουργικότητα με άλλες πλατφόρμες.

Είναι άξιο αναφοράς ότι το 86,3% θα συνιστούσε τις πλατφόρμες ασφαλούς επικοινωνίας σε συναδέλφους του. Το μικρό ποσοστό που απάντησε ότι δεν θα συνιστούσε της πλατφόρμας είναι στην πλειοψηφία του άτομα ηλικίας άνω των 45 που δεν χρησιμοποιούν οι ίδιοι κάποια πλατφόρμα επομένως, όπως είναι λογικό, δεν μπορούν να τη συστήσουν κιόλας σε κάποιο συνάδελφό τους. Αυτό το μεγάλο ποσοστό που θα συνιστούσε τις πλατφόρμες έρχεται σε πλήρη συμφωνία με το γεγονός ότι πάνω από το 85% πιστεύει ότι υπάρχει κίνδυνος με την ασφάλεια των επικοινωνιών στη Δημοσιογραφία. Ωστόσο, η συντριπτική πλειοψηφία παρόλο που θεωρεί ότι η ασφαλής επικοινωνία είναι ένα μείζον ζήτημα και θεωρεί ότι θα έπρεπε οι δημοσιογράφοι να χρησιμοποιούν τέτοιου είδους πλατφόρμες, δεν είναι πεπεισμένοι για την ασφάλεια που παρέχουν αυτές.

Στο κομμάτι των προκλήσεων είναι ιδιαίτερα ενδιαφέρον ότι τόσο για τον κίνδυνο παρακολουθήσεων από κυβερνήσεις, οργανισμούς, κ.λπ., τον κίνδυνο επίθεσης από hackers αλλά και της αλλοίωσης περιερχομένου μέσω εργαλείων τεχνητής νοημοσύνης, δεν απάντησε κανένας συμμετέχοντας ή συμμετέχουσα ότι δεν είναι υπαρκτοί. Έτσι, οι προκλήσεις της ψηφιακής εποχής είναι κάτι που προβληματίζει τους δημοσιογράφους. Παρά, λοιπόν τον προβληματισμό για τις προκλήσεις και τους κινδύνους που αντιμετωπίζουν οι δημοσιογράφοι στο ψηφιακό τοπίο που έχει επικρατήσει, το 74,5% αυτών πιστεύει ότι τα οφέλη της ψηφιακής επικοινωνίας υπερτερούν των κινδύνων. Παρότι, όπως έχει ήδη αναφερθεί ότι οι γυναίκες δείχνουν μια τάση να υιοθετούν πιο εύκολα τις νέες τεχνολογίες στη Δημοσιογραφία με βάση πάντα το συγκεκριμένο δείγμα που απάντησε το ερευνητικό ερωτηματολόγιο της παρούσας εργασίας, περίπου το 44% αυτών απάντησαν ότι θεωρούν ότι οι κίνδυνοι υπερτερούν των οφελών στην ψηφιακή εποχή. Κατά αντιστοιχία, το ποσοστό στους άνδρες είναι μόλις 14,7%.

Το 47,1% των ερωτηθέντων απάντησε ότι έχει βιώσει ή υποπτευθεί παραβίαση της επικοινωνίας του στην εργασία του/της, το 19,6% ότι δεν γνωρίζει και μόλις το 1/3 ότι δεν έχει βιώσει ή δεν έχει υποπτευθεί. Το ποσοστό που δεν έχει βιώσει ή υποπτευθεί παραβίαση της επικοινωνίας του/της είναι σχεδόν όμοιο σε άντρες και

γυναίκες και κυμαίνεται κοντά στο 30%. Ωστόσο, πολλοί από αυτούς σε ποσοστό 41% δεν χρησιμοποιεί ψηφιακά εργαλεία επομένως αυτό είναι ενδεικτικό καθώς ασκούν το επάγγελμά τους με πιο παραδοσιακά μέσα. Αναλογιζόμενοι αυτό, είναι ασφαλές να θεωρήσουμε ότι το ποσοστό αυτών που χρησιμοποιεί ψηφιακά εργαλεία και έχει βιώσει ή υποπτευθεί παραβίαση της επικοινωνίας του είναι αρκετά μεγαλύτερο. Οι περισσότεροι θεωρούν ότι αυτή η παραβίαση αφορά την επικοινωνία με πηγές ή συναδέλφους ενώ μεγάλη μερίδα πιστεύει ότι και με απλή χρήση του Διαδικτύου για συλλογή πληροφοριών είναι εκτεθειμένοι. Ενθαρρυντικό βεβαία είναι το γεγονός ότι παρά τις ανησυχίες τους, η πλειοψηφία των συμμετεχόντων δεν έχει πρόθεση είτε να παρατήσει τη Δημοσιογραφία ή την ενασχόλησή του με κάποιο θέμα υπό τον φόβο της παραβίασης των επικοινωνιών τους.

Στον αντίποδα, παρόλο που οι περισσότεροι από τους ερωτηθέντες και τις ερωτηθείσες δεν έχουν πρόθεση να παρατήσουν οποιοδήποτε θέμα, η επικοινωνία με πηγές ή τη Δημοσιογραφία γενικότερα, η πλειοψηφία αυτών ανέφερε ότι έχει αλλάξει έστω και λίγο τον τρόπο με τον όποιο χρησιμοποιεί το Διαδίκτυο, τον τρόπο με τον οποίο αποθηκεύει ή διαμοιράζεται πληροφορίες, τον τρόπο επικοινωνίας με συναδέλφους αλλά και με πηγές. Αυτό φανερώνει μια ενδιαφέρουσα τάση καταδεικνύοντας τη διάθεση των δημοσιογράφων να ενημερώνονται και να προσαρμόζονται παρά τους κινδύνους και τις προκλήσεις που επιφέρει η ψηφιακή εποχή. Τα σχόλια που ελήφθησαν σχετικά με τις εμπειρίες τους σχετικά με την ασφαλή επικοινωνία και τα εργαλεία που χρησιμοποιούνται από τους δημοσιογράφους, αφορούσαν από τη μία την αναγκαιότητα για χρήση τους καθώς αυτό σχεδόν επιτάσσεται από τις προσταγές της σύγχρονης εποχής και από την άλλη την ανάγκη για ενημέρωση και εκπαίδευση του δημοσιογραφικού συνόλου για τη διαθεσιμότητα και τις λειτουργίες αυτών. Σε κάθε περίπτωση, όπως αναφέρθηκε πολύ εύστοχα από κάποιους συμμετέχοντες, η ερευνητική Δημοσιογραφία και η Δημοσιογραφία γενικότερα αποτελεί πυλώνα για την κοινωνία και πρέπει να διαφυλάσσεται με κάθε μέσο.

Καταληκτικά, η πλειοψηφία των συμμετεχόντων ανέφερε ότι έχει γνώσεις τόσο για πρακτικές ασφαλούς επικοινωνίας όσο και γενικότερα για την ασφαλή επικοινωνία και την ασφαλή περιήγηση στο Διαδίκτυο (κοινή χρήση αρχείων, επικοινωνία, αναζήτηση πληροφοριών, κ.λπ.). Σχετικά με τις πρακτικές ασφαλούς επικοινωνίας, οι

χρήστες βασίζονται περισσότερο σε τεχνικά μέσα όπως χρήση ισχυρών κωδικών, χρήση antivirus, κ.α. πάρα στην εκπαίδευση και την ενημέρωσή τους. Όσον αφορά τις μεθόδους που χρησιμοποιούν ή θα ήθελαν να χρησιμοποιήσουν για να εμπλουτίσουν τις γνώσεις τους σχετικά με την ασφάλεια στο Διαδίκτυο, η δημοφιλέστερη είναι οι συζητήσεις και η ανταλλαγή γνώσεων με συναδέλφους με την ενημέρωση από εξειδικευμένο προσωπικό και τη συμμετοχή σε σεμινάρια να ακολουθούν. Έτσι, παρατηρείται μια τάση οι δημοσιογράφοι να βασίζονται αρκετά στις εμπειρίες και τις γνώσεις των συναδέλφων τους καθώς αισθάνονται πιο ασφαλείς, όταν κάτι έχει χρησιμοποιηθεί στην πράξη από άτομα που γνωρίζουν και εμπιστεύονται. Συμπληρωματικά, αρκετοί είχαν θετική στάση απέναντι στην ενημέρωση από εξειδικευμένο προσωπικό και τη συμμετοχή σε σχετικά σεμινάρια. Πολύ λίγοι ωστόσο έδειξαν ενδιαφέρον για προσωπική μελέτη και διερεύνηση χωρίς καθοδήγηση από ειδικούς ή για την πραγματοποίηση ενός σχετικού μεταπτυχιακού προγράμματός καθώς και την παρακολούθηση διαδικτυακών μαθημάτων και εκπαιδεύσεων, μιας και προτιμούν την πιο πρακτική στοχευμένη γνώση.

5.3 Αντίστοιχες έρευνες στη βιβλιογραφία

Το θέμα της ασφάλειας των επικοινωνιών στη Δημοσιογραφία αλλά και της ψηφιακής ασφάλειας των δημοσιογράφων γενικότερα, έχει απασχολήσει αρκετούς ερευνητές και φορείς ανά τον κόσμο. Μία ενδιαφέρουσα έρευνα που αφορά τον τομέα της ψηφιακής ασφάλειας στη Δημοσιογραφία πραγματοποιήθηκε από τους Holcomb and Mitchell υπό την αιγίδα του Pew Research Center (Holcomb & Mitchell, 2015). Στην εν λόγω έρευνα έλαβαν μέρος 671 επαγγελματίες από τον χώρο της Δημοσιογραφίας στις ΗΠΑ. Η κατανομή τους, όσον αφορά την επαγγελματική τους δραστηριότητα, παρουσίαζε όμοια χαρακτηριστικά με τις απαντήσεις στο ερευνητικό ερωτηματολόγιο που διαμοιράστηκε για τις ανάγκες της παρούσας εργασίας. Έτσι, ένα 88% απάντησε ότι δουλεύει για δημοσιογραφικό οργανισμό με το 63% αυτών να καλύπτουν κυρίως τοπικά θέματα. Τα αντίστοιχα ποσοστά στην έρευνα της παρούσας εργασίας είναι 72,5% και 56,9%. Ένα ακόμα ενδιαφέρον στατιστικό της έρευνας των Holcomb και Mitchell είναι ότι το 50% των συμμετεχόντων δήλωσαν ότι δεν χρησιμοποιούν κάποιο εργαλείο ψηφιακής ασφάλειας. Παρατηρείται λοιπόν ότι το ποσοστό αυτό είναι μειωμένο στην έρευνα της παρούσας εργασίας όπου το 37,3% δήλωσε ότι δεν χρησιμοποιεί κάποια

πλατφόρμα ασφαλούς επικοινωνίας. Αυτό μπορεί να οφείλεται κυρίως στο γεγονός ότι η έρευνα των Holcomb και Mitchell διεξήχθη τον Δεκέμβριο του 2014 και έκτοτε έχει αλλάξει ραγδαία η τεχνολογική ανάπτυξη και το δημοσιογραφικό τοπίο. Ένα ακόμη κοινό στοιχείο της έρευνας των Holcomb και Mitchell με την έρευνα της παρούσας εργασίας είναι ότι το 64% των ερωτηθέντων πιστεύει ότι η κυβέρνηση συγκεντρώνει δεδομένα από τις επικοινωνίες τους με το αντίστοιχο ποσοστό όπως φαίνεται στην Εικόνα 57 να είναι 60,8%. Στην ερώτηση κατά πόσον έχουν αλλάξει έστω και λίγο τον τρόπο με τον οποίο αποθηκεύουν ή μοιράζονται ευαίσθητα αρχεία, απάντησε θετικά το 49% με το αντίστοιχο ποσοστό της παρούσας έρευνας να είναι 82,4% όπως φαίνεται στην Εικόνα 66. Ομοίως, στην ερώτηση για το εάν έχουν αλλάξει έστω και λίγο τον τρόπο που επικοινωνούν με άλλους συναδέλφους τους, το 29% απάντησε θετικά με το αντίστοιχο ποσοστό στην έρευνα της παρούσας εργασίας να είναι εμφανώς υψηλότερο στο 78,4% (Holcomb & Mitchell, 2015).

Σε έρευνα που πραγματοποίησε ο Javier Garza Ramos (Ramos, 2016) τον Μάρτιο του 2016 για λογαριασμό του Center for International Media Assistance (CIMA) εξετάσθηκε η χρήση και η υιοθέτηση ψηφιακών εργαλείων ασφαλούς επικοινωνίας. Η συγκεκριμένη έρευνα διαμοιράστηκε σε όλο τον κόσμο και συγκέντρωσε 154 απαντήσεις από διαφορετικά μέρη της υφηλίου. Παρατηρούμε λοιπόν ότι το 60% αυτών, όπως διατυπώθηκε στην έρευνα του Ramos, απάντησαν ότι δεν χρησιμοποιούν ψηφιακά εργαλεία ενώ στην έρευνα που πραγματοποιήθηκε στο πλαίσιο της συγκεκριμένης εργασίας το 62,7% απάντησε ότι χρησιμοποιεί πλατφόρμες ασφαλούς επικοινωνίας. Η διαφοροποίηση αυτή μπορεί να οφείλεται και στο ότι η ερεύνα του Ramos έγινε το 2015-2016 αλλά και λόγω της γεωγραφικής κάλυψης που εμπεριείχε απαντήσεις από όλο τον κόσμο. Χαρακτηριστικό μάλιστα είναι ότι στην Ευρώπη και στην Αμερική τα ποσοστά χρήσης είναι υψηλότερα συγκριτικά με την Ασία, την Αφρική και τη Λατινική Αμερική.

Επιπλέον, σε ερωτήματα που αφορούσαν συγκεκριμένα τη χρήση εργαλείων ασφαλούς επικοινωνίας και κοινής χρήσης αρχείων, το ποσοστό θετικών απαντήσεων περιοριζόταν στο 30% και πάλι το μεγαλύτερο μέρος των θετικών απαντήσεων ήταν από την Ευρώπη και τη Βόρεια Αμερική. Ενδιαφέρον παρουσιάζει ότι σε αυτές τις απαντήσεις και συγκεκριμένα για τις πλατφόρμες ασφαλούς κοινής χρήσης αρχείων από τις πιο δημοφιλείς εφαρμογές ήταν το Tresorit και το OnionShare, τα οποία

συμπεριελήφθησαν στην παρούσα εργασία αλλά παραμένουν σχετικά άγνωστα ακόμα στην Ελλάδα, παρά την παρουσία τους αρκετά χρόνια στον δημοσιογραφικό κόσμο. Στο κομμάτι της κρυπτογράφησης παρατηρούμε ότι, παρόλο που η πλειοψηφία όπως απάντησε στο ερευνητικό ερωτηματολόγιο της παρούσας εργασίας ανέφερε ότι γνωρίζει για το συγκεκριμένο μέτρο ασφαλείας, το 78,4% δεν τη χρησιμοποιεί, ποσοστό πολύ κοντά σε αυτό που κατέγραψε η έρευνα του Ramos που είναι στο 83%. Καταληκτικά, και στην έρευνα του Ramos αλλά και σε αυτή που διενεργήθηκε για τις ανάγκες της παρούσας εργασίας, σε ποσοστό πάνω από το 45% οι ερωτηθέντες απάντησαν ότι έχουν βιώσει ή υποψιαστεί κάποιο ζήτημα ασφάλειας ή παραβίασης των επικοινωνιών, καταδεικνύοντας έτσι την ανάγκη για την ύπαρξη ισχυρών εργαλείων προστασίας της ψηφιακής ασφάλειας (Ramos, 2016).

Το 2017 οι Nasrullah Al-Ameen, Lowens, Mcgrecor και Caine (Nasrullah Al-Ameen, Lowens, Mcgrecor, & Caine, 2017) πραγματοποίησαν έρευνα για να διερευνήσουν την αντίληψη για την ασφάλεια πληροφοριοδοτών που συζήτησαν ευαίσθητα θέματα με δημοσιογράφους, όσον αφορά τις γνώσεις και την ενημέρωση που έχουν σχετικά με την ψηφιακή ασφάλεια και σχετικά ζητήματα ιδιωτικότητας. Τα αποτελέσματα έδειξαν ότι λίγοι πληροφοριοδότες χρησιμοποιούν ασφαλή εργαλεία κατά την επικοινωνία τους με δημοσιογράφους, με αποτέλεσμα να υπάρχουν κενά μεταξύ της γνώσης σχετικά με την ψηφιακή ασφάλεια και των πρακτικών που χρησιμοποιούνται προκειμένου να τη διασφαλίσουν. Επιπλέον, υπάρχει μια εμφανής έλλειψη σιγουριάς που αφορά την ύπαρξη εργαλείων που όντως προσφέρουν ουσιαστική προστασία και ασφάλεια απέναντι σε διαρροές και παραβιάσεις (Nasrullah Al-Ameen, Lowens, Mcgrecor, & Caine, 2017).

Πιο συγκεκριμένα, από το σύνολο των 76 ερωτηθέντων μόλις ένα 33% χρησιμοποιεί κρυπτογράφηση σε email, chat, μηνύματα ή σε άλλες μορφές. Επιπλέον, σχετικά με την ανησυχία τους στο ζήτημα εάν η κυβέρνηση τους παρακολουθεί, μόλις το 36% απάντησε ότι ανησυχεί. Αυτό έρχεται σε αντίθεση με τα αποτελέσματα της έρευνας που παρουσιάσθηκε στο Κεφάλαιο 5.1.4 που το 60,8% δήλωσε σίγουρο ότι υπάρχει ηλεκτρονική παρακολούθηση. Η αντίθεση αυτή ίσως οφείλεται στη γεωγραφική κατανομή των ερωτηθέντων καθώς η έρευνα των Nasrullah Al-Ameen, Lowens, Mcgrecor και Caine διενεργήθηκε στις ΗΠΑ, οι οποίες κατατάσσονται στη θέση 55 της ελευθερίας του λόγου, όπως φαίνεται στο Παράρτημα 1: Ελευθερία του Τύπου –

Κατάταξη χωρών, ενώ η Ελλάδα στη θέση 88. Η συγκεκριμένη έρευνα κατέδειξε την ανάγκη για τη γεφύρωση του χάσματος ανάμεσα στην απλή γνώση για θέματα ασφάλειας με την ουσιαστική εφαρμογή πρακτικών για την επίτευξη αυτής. Ενδεικτικό είναι ότι μόλις ένα 12% γνωρίζει/χρησιμοποιεί εργαλεία που προσφέρουν ασφάλεια και ανωνυμία όπως το Tor και το SecureDrop (Nasrullah Al-Ameen, Lowens, Mcgrecor, & Caine, 2017) ποσοστό ανάλογο με αυτό που εμφανίζεται και στην έρευνα της παρούσας εργασίας (11,8% γνωρίζουν τις εφαρμογές SecureDrop, OnionShare, GlobaLeaks).

Συμπερασματικά, λοιπόν, παρατηρείται ότι η καταγραφή των απόψεων του δημοσιογραφικού κόσμου σχετικά με την ψηφιακή ασφάλεια είναι ένα ενεργό πεδίο για τουλάχιστον μία δεκαετία. Γενικά, υπάρχουν συγκλίνουσες απόψεις στις διάφορες έρευνες σχετικά με την παραβίαση της ιδιωτικότητας και την ύπαρξη κινδύνων στον ψηφιακό κόσμο γεγονός που επαληθεύτηκε και στην έρευνα της παρούσας εργασίας. Ωστόσο, παρατηρήθηκαν και διαφοροποιήσεις τόσο στο κομμάτι της υιοθέτησης όσο και της γνώσης γύρω από τα ψηφιακά εργαλεία. Αυτό ίσως οφείλεται στη γεωγραφική κάλυψη της εκάστοτε έρευνας, στο πλήθος του δείγματος αλλά ακόμα και στη χρονολογία που πραγματοποιήθηκε η έρευνα. Χαρακτηριστικό αποτελεί ότι όσο πιο πρόσφατη είναι η έρευνα τόσο πιο ενημερωμένο είναι το κοινό για την ύπαρξη, τουλάχιστον, τέτοιων εργαλείων ψηφιακής ασφάλειας και ασφαλούς επικοινωνίας.

6 Συμπεράσματα και μελλοντικές επεκτάσεις

6.1 Συμπεράσματα

Η ασφαλής επικοινωνία ήταν πάντα ο ακρογωνιαίος λίθος της αποτελεσματικής Δημοσιογραφίας. Καθώς το ψηφιακό τοπίο εξελίσσεται, η ανάγκη για ισχυρές, αξιόπιστες και ασφαλείς πλατφόρμες επικοινωνίας γίνεται ακόμη πιο κρίσιμη. Στο σημερινό περιβάλλον των μέσων ενημέρωσης, η ασφαλής επικοινωνία είναι πρωταρχικής σημασίας για την προστασία των πηγών, τη διασφάλιση της ακεραιότητας των πληροφοριών και τη διασφάλιση της δημοσιογραφικής ανεξαρτησίας. Οι δημοσιογράφοι βασίζονται σε μια ποικιλία εργαλείων για να επιτύχουν αυτούς τους στόχους, συμπεριλαμβανομένων των κρυπτογραφημένων εφαρμογών ανταλλαγής μηνυμάτων όπως αυτές που παρουσιάστηκαν στο Κεφάλαιο 3 αλλά και σε άλλα εργαλεία και λύσεις, όπως αυτές που καταγράφηκαν στη βιβλιογραφική έρευνα που παρουσιάστηκε στο Κεφάλαιο 2.

Ωστόσο, παρά αυτές τις εξελίξεις, οι προκλήσεις παραμένουν. Οι κυβερνοεπιθέσεις γίνονται πιο εξελιγμένες και το ψηφιακό αποτύπωμα των δημοσιογράφων αυξάνεται, καθιστώντας τους ίδιους πρωταρχικούς στόχους παρακολούθησης και πειρατείας. Ως εκ τούτου, ο κλάδος πρέπει να προσαρμόζεται συνεχώς σε νέες απειλές και να αναπτύσσει πιο προηγμένα μέτρα ασφαλείας.

Το βασικό ερώτημα που τέθηκε στο Κεφάλαιο 1 του παρόντος και δεν είναι άλλο από τη χρήση των πλατφορμών ασφαλούς επικοινωνίας στη Δημοσιογραφία. Μέσα από τη βιβλιογραφική έρευνα του Κεφαλαίου 2 αλλά και από το ερευνητικό ερωτηματολόγιο που διαμοιράσθηκε, η απάντηση σε αυτό το ερώτημα εναποτίθεται σε πολλούς παράγοντες. Από τη μία, οι προκλήσεις είναι αρκετές στην ψηφιακή εποχή και απαιτούν την ύπαρξη και τη χρήση τέτοιων εργαλείων και πλατφορμών για τις οποίες το μεγαλύτερο ποσοστό των συμμετεχόντων είναι ενήμεροι και τις χρησιμοποιούν. Από την άλλη, παρά την αναγκαιότητα χρήσης τέτοιων εργαλείων, οι περισσότεροι από τους συμμετέχοντες δεν δηλώσαν πεπεισμένοι για την ασφάλεια που παρέχουν, όπως αποτυπώθηκε στα αποτελέσματα του Κεφαλαίου 5.

Παράλληλα, όπως αποτυπώθηκε και στη βιβλιογραφική έρευνα αλλά και στο ερωτηματολόγιο, οι προκλήσεις και οι κίνδυνοι είναι πολυάριθμοι στο ψηφιακό τοπίο της σύγχρονης Δημοσιογραφίας και αναγνωρίζονται από όλο το σύνολο που πήρε

μέρος στο ερωτηματολόγιο. Με γνώμονα αυτό, οι δημοσιογράφοι καταφεύγουν σε τέτοιες λύσεις και εργαλεία παρά την όποια αβεβαιότητα έχουν σχετικά με την παραβίαση των επικοινωνιών τους. Με δεδομένο αυτό και κοιτάζοντας προς το μέλλον, που οι κίνδυνοι και οι προκλήσεις θα εξελιχθούν, το ζητούμενο από τη δημοσιογραφική κοινότητα είναι περισσότερη ασφάλεια και διασφάλιση της ιδιωτικότητας από τέτοιου είδους εργαλεία και λύσεις σε συνδυασμό με την παροχή σωστής εκπαίδευσης και ενημέρωσης.

6.2 Οι τάσεις και το μέλλον της ασφαλούς επικοινωνίας

Όπως αναφέρθηκε και προηγουμένως, παρά τη μεγάλη τεχνολογική εξέλιξη, οι προκλήσεις είναι παρούσες και ποικίλες. Συνεπώς, ο κλάδος της Δημοσιογραφίας οφείλει να διαθέτει προσαρμοστικό χαρακτήρα σε συνεχή βάση απέναντι σε νέες απειλές και να στρέφεται σε πιο καινοτόμα μέτρα προστασίας.

Ο γρήγορος ρυθμός της τεχνολογικής καινοτομίας φέρνει νέα εργαλεία και μεθόδους στο προσκήνιο της ασφαλούς επικοινωνίας. Μεταξύ των πιο πολλά υποσχόμενων είναι η τεχνολογία Blockchain, η κβαντική κρυπτογράφηση και οι λύσεις ασφαλείας που βασίζονται σε τεχνητή νοημοσύνη.

Η τεχνολογία Blockchain, γνωστή για την αποκεντρωμένη και αδιάβλητη φύση της, προσφέρει σημαντικές δυνατότητες για ασφαλή επικοινωνία. Μπορεί να χρησιμοποιηθεί για τη δημιουργία μη-επεξεργάσιμων αρχείων, συναλλαγών και επικοινωνιών, διασφαλίζοντας τη διατήρηση της ακεραιότητας των δεδομένων. Αυτό θα μπορούσε να είναι ιδιαίτερα χρήσιμο για την προστασία ευαίσθητου δημοσιογραφικού υλικού από παραποίηση ή μη εξουσιοδοτημένη πρόσβαση.

Η κβαντική κρυπτογράφηση αντιπροσωπεύει ένα βήμα προς την αυξημένη ασφάλεια στην επικοινωνία. Αξιοποιώντας τις αρχές της κβαντικής μηχανικής, υπόσχεται ουσιαστικά άθραυστη κρυπτογράφηση. Ενώ είναι ακόμη στα αρχικά της στάδια, οι πιθανές εφαρμογές για τη Δημοσιογραφία είναι τεράστιες, από την ασφάλεια των επικοινωνιών έως την προστασία της αποθήκευσης δεδομένων.

Οι λύσεις ασφαλείας που βασίζονται στην τεχνητή νοημοσύνη αποτελούν πλέον πραγματικότητα, προσφέροντας πιο εξελιγμένους τρόπους για τον εντοπισμό και την αντιμετώπιση των απειλών. Η ΤΝ μπορεί να αναλύσει μοτίβα και να ανιχνεύσει ανωμαλίες στα δίκτυα επικοινωνίας, παρέχοντας προστασία σε πραγματικό χρόνο

από απειλές στον κυβερνοχώρο. Αυτές οι τεχνολογίες, ενώ εξακολουθούν να αναπτύσσονται, υποδεικνύουν ένα μέλλον όπου η ασφαλής επικοινωνία είναι πιο ισχυρή και προσαρμόσιμη στις αναδυόμενες απειλές. Παράλληλα, με την εγκαθίδρυση της TN, η χρήση και η λειτουργία της κάτω από ένα αυστηρό νομικά κανονιστικό πλαίσιο αποτελεί πλέον πραγματικότητα στην Ευρωπαϊκή Ένωση (ΕΕ) μέσω του κανονισμού AI Act όπως ονομάζεται. Βασικό σκοπός του AI Act είναι να εξασφαλίσει τη διαφανή, ιχνηλάσιμη και συμπεριληπτική λειτουργία των λύσεων TN με σκοπό να περιορίσει επιζήμιες επιπτώσεις σε άτομα και κοινωνίες (European Parliament, 2023).

Ατενίζοντας λοιπόν το μέλλον της ασφαλούς επικοινωνίας στη Δημοσιογραφία, διαφαίνεται πολλά υποσχόμενο αλλά και πολύπλοκο. Καθώς τεχνολογίες όπως το Blockchain, η κβαντική κρυπτογράφηση και η τεχνητή νοημοσύνη συνεχίζουν να αναπτύσσονται, πιθανότατα θα γίνουν αναπόσπαστο μέρος των δημοσιογραφικών πρακτικών. Αυτές οι εξελίξεις θα βοηθήσουν τους δημοσιογράφους να προστατεύσουν τις πηγές τους, να εξασφαλίσουν τις επικοινωνίες τους και να διατηρήσουν την ακεραιότητα της δουλειάς τους.

Ωστόσο, ο κλάδος πρέπει να παραμείνει σε εγρήγορση. Η εξελισσόμενη φύση των απειλών στον κυβερνοχώρο σημαίνει ότι είναι απαραίτητη και επιτακτική η συνεχής καινοτομία και προσαρμογή. Η συνεργασία μεταξύ τεχνολόγων, δημοσιογράφων και υπευθύνων χάραξης πολιτικής θα είναι ζωτικής σημασίας για την ανάπτυξη και την εφαρμογή αποτελεσματικών στρατηγικών ασφαλούς επικοινωνίας.

Βιβλιογραφικές Αναφορές

Abosede Olubunmi, B. (2022, 10). Impact of ICT in Journalism in 21st Century. *International Journal of Academic Information Systems Research (IJAISR), 6*(10), pp. 6-13. Retrieved from https://eprints.federalpolyilaro.edu.ng/2229/1/JOURNAL%20AUG.%202022.pdf

Abellán, A. (2021, 01 28). *Privacy Day 2021: what journalists need to know*. Retrieved 05 31, 2024, from DataJournalism.com: https://datajournalism.com/read/longreads/privacy-day-security-guide

Acton, B. (2018, 02 21). *Signal Foundation*. Retrieved 06 02, 2024, from Signal: https://signal.org/blog/signal-foundation/

Anvari, F., Wenzel, M., Woodyatt, L., & Haslam, S. (2019). The social psychology of whistleblowing: An integrated model. *Organizational Psychology Review, 9*(1), 41-67. doi:https://doi.org/10.1177/2041386619849085

Ausserhofer, J., Gutounig, R., Oppermann, M., Matiasek, S., & Goldgruber, E. (2017). The datafication of data journalism scholarship: Focal points, methods, and research propositions for the investigation of data-intensive newswork. *Journalism, 21*(7), 950-973. doi:https://doi.org/10.1177/1464884917700667

AWS Wickr. (2022). *AWS Wickr Overview.* Retrieved 06 01, 2024, from aws wickr: https://wickr.com/wp-content/uploads/2022/12/AWS-Wickr-Overview.pdf

BBC. (2017, 05 16). *Chelsea Manning: Wikileaks source and her turbulent life*. Retrieved 05 31, 2024, from BBC: https://www.bbc.com/news/world-us-canada-11874276

Bélair-Gagnon, V., Nelson, J., & Lewis, S. (2018, 11). Audience Engagement, Reciprocity, and the Pursuit of Community Connectedness in Public Media Journalism. *Journalism Practice, 13*(1), pp. 1-18. doi:http://dx.doi.org/10.1080/17512786.2018.1542975

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* Yale University Press. Retrieved from http://www.jstor.org/stable/j.ctt1njknw

Bounegru, L., & Gray, J. (2021). *The Data Journalism Handbook: Towards a Critical Data Practice.* Amsterdam: Amsterdam University Press. doi:10.5117/9789462989511

Briggs, A., & Burke, P. (2009). *A Social History of the Media: From Gutenberg to the Internet* (3rd ed.). Cambridge, CB2 1UR, UK: Polity.

Cadet, L. (2023, 07 11). *Nextcloud Delivers Full-Fledged Collaboration Platform With a Promise of Zero Data Leaks*. Retrieved 06 02, 2024, from HostingAdvice.com: https://www.hostingadvice.com/blog/nextcloud-offers-a-privacy-first-collaboration-suite/

Caled, D., & Silva , M. (2021, 05 27). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science, 5*, pp. 123-159. doi:https://doi.org/10.1007/s42001-021-00118-8

Castells, M. (2009). *The Rise of the Network Society.* Wiley. doi:10.1002/9781444319514

Chaffey, D. (2024, 05 01). *Global social media statistics research summary May 2024*. Retrieved 05 18, 2024, from Smart insights: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Council of the EU. (2024, 03 26). European Media Freedom Act: Council adopts new rules to protect journalists and media providers. Brussels, Belgium.

Craft, S., & Davis, C. (2021). *Principles of American Journalism: An Introduction* (3rd ed.). Routledge.

Deibert, R. (2017). Digital Threats Against Journalists". In E. Bell, & T. Owen, *Journalism After Snowden: The Future of the Free Press in the Surveillance State* (pp. 240-257). New York Chichester: West Sussex: Columbia University Press. doi:https://doi.org/10.7312/bell17612-020

Di Salvo, P. (2022). Information security and journalism: Mapping a nascent research field. *Sociology Compass, 16*(3). doi:https://doi.org/10.1111/soc4.12961

Donsbach, W., & Klett, B. (1993). Subjective objectivity. How journalists in four countries define a key term of their profession. *International Communication Gazette, 51*(1), pp. 53-83. doi:https://doi.org/10.1177/001654929305100104

Eberwein, T., Fengler, S., & Karmasin, M. (2017). *The European Handbook of Media Accountability.* London, UK: Routledge. doi:https://doi.org/10.4324/9781315616353

European Parliament. (2023, 12 19). *EU AI Act: first regulation on artificial intelligence*. Retrieved 06 13, 2024, from European Parliament: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Eurostat. (2023, 08 28). *Eurostat Statistics Explained*. Retrieved 05 20, 2024, from Glossary:Information and communication technology (ICT): https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)

Fitzgibbon, W., & Hudson, M. (2021, 04 03). *Five years later, Panama Papers still having a big impact*. Retrieved 05 31, 2024, from International Consortium of Investigative Journalists: https://www.icij.org/investigations/panama-papers/five-years-later-panama-papers-still-having-a-big-impact/

Fleck, A. (2024, 02 22). *Cybercrime Expected To Skyrocket in Coming Years*. Retrieved 05 30, 2024, from statista: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Freedom of Information Act. (2024). *FOIA*. Retrieved 04 22, 2024, from FOIA: https://www.foia.gov/

Freedom of the Press Foundation. (2024). *SecureDrop*. Retrieved 06 03, 2024, from Freedom of the Press Foundation: https://freedom.press/organizations/securedrop/

Gierow, H. (2024, 02 01). *'The highest priority is the security of our messenger'*. Retrieved 06 03, 2024, from Wire: https://wire.com/blog/interview-robert-kallwies

GlobaLeaks (a). (2024). *Our vision*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org/about/

GlobaLeaks (b). (2024). *Features*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org/features/

GlobaLeaks (c). (2024). *GlobaLeaks*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org

GlobaLeaks (d). (2024). *Use Cases: Anti-Corruption*. Retrieved 06 04, 2024, from GLobaLeaks: https://www.globaleaks.org/usecases/anti-corruption/

GlobaLeaks (e). (2024). *Use Cases: Corporate Compliance*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org/usecases/corporate-compliance/

GlobaLeaks (f). (2024). *Use Cases: Human Rights Protection*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org/usecases/human-rights-protection/

GlobaLeaks (g). (2024). *Use Cases: Investigative Journalism*. Retrieved 06 04, 2024, from GlobaLeaks: https://www.globaleaks.org/usecases/investigative-journalism/

Goodwin, A., Woolbright, J., & Tomé, J. (2022, 05 03). *The deluge of digital attacks against journalists*. Retrieved 05 22, 2024, from CLoudfare: https://blog.cloudflare.com/the-deluge-of-digital-attacks-against-journalists/

Graves, L. (2016). *Deciding What's True: The Rise of Political Fact-Checking in American Journalism.* Columbia University Press.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state.* New York, USA: Metropolitan Books/Henry Holt.

Harding, L. (2016, 04 05). *What are the Panama Papers? A guide to history's biggest data leak.* Retrieved 05 31, 2024, from The Guardian: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

Higgins, P. (2014, 06 27). *The Troubling Truth of Why It's Still So Hard to Share Files Directly*. Retrieved 06 04, 2024, from Wired:

https://www.wired.com/2014/06/the-troubling-truth-of-why-its-still-so-hard-to-share-files-directly/

Holcomb, J., & Mitchell, A. (2015). *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior.* Washington, DC: Pew Research Center. Retrieved from https://www.pewresearch.org/journalism/2015/02/05/investigative-journalists-and-digital-security/

HR future. (2024). *8 Challenges Whistleblowers Face in and out of the Workplace*. Retrieved 05 27, 2024, from HR future: https://www.hrfuture.net/future-of-work/trending/8-challenges-whistleblowers-face-in-and-out-the-workplace/

Humayun, M., & Ferrucci, P. (2022). Understanding Social Media in Journalism Practice: A Typology. *Digital Journalism, 10*(9), 1502-1525. doi:https://doi.org/10.1080/21670811.2022.2086594

International Telecommunication Union (ITU). (2024). *Internet use*. Retrieved 05 18, 2024, from International Telecommunication Union: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

Internet Society. (2022, 09 07). *Fact Sheet: How Encryption Can Protect Journalists and the Free Press*. Retrieved 05 31, 2024, from Internet Society: https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/

Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59-68. doi:https://doi.org/10.1016/j.bushor.2009.09.003

Kaspersky. (2024). *Tor Browser: What is it and is it safe?* Retrieved 05 22, 2024, from Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser

Kaul, V. (2013, 01 24). Journalism in the Age of Digital Technology. *Computer Science, 3*(1), pp. 125-143. doi:https://doi.org/10.29333/ojcmt/2414

Kietzmann, J., Hernmkens, K., McCarthy, I., & Silvestre, B. (2011). Social media? Get serious! Understanding the functional building blocks of social media.

Business Horizons, 54(3), 241-251. doi:https://doi.org/10.1016/j.bushor.2011.01.005

Kleinig, J. (2024, 05 04). *whistleblower*. Retrieved 05 28, 2024, from Britannica: https://www.britannica.com/topic/whistleblower

Kovach, B., & Rosenstiel, T. (2021). *The elements of journalism* (4th ed.). New York, USA: Crown.

Lám, I. (2023, 05 16). *Never trust, always verify: your 2023 guide to zero-knowledge encryption*. Retrieved 06 05, 2024, from Tresorit: https://tresorit.com/blog/zero-knowledge-encryption/

Lee, M. (2024). *How OnionShare Works*. Retrieved 06 04, 2024, from OnionShare: https://docs.onionshare.org/2.3.1/en/features.html#

Lusher, A. (2016, 04 05). *Panama Papers: 12 world leaders linked to offshore dealings - and the full allegations against them*. Retrieved 05 31, 2024, from Independent: https://www.independent.co.uk/news/world/politics/panama-papers-assad-putin-poroshenko-mubarak-al-saud-pm-iceland-sigmundur-davio-gunnlaugsson-a6967411.html

Lutkevich, B., & Gillis, A. (2022, 03). *Definition Bot*. Retrieved 06 05, 2024, from TechTarget WhatIs?: https://www.techtarget.com/whatis/definition/bot-robot

Marlinspike, M. (2013, 11 26). *Advanced cryptographic ratcheting*. Retrieved 06 02, 2024, from Signal: https://signal.org/blog/advanced-ratcheting/

Marlinspike, M. (2015, 03 02). *Signal 2.0: Private messaging comes to the iPhone*. Retrieved 06 02, 2024, from Signal: https://signal.org/blog/the-new-signal/

Matthias, M. (2024, 06 07). *Telegram cloub-based messaging app*. Retrieved 06 07, 2024, from Britannica: https://www.britannica.com/topic/Telegram-software

Media Defence. (2022, 11). *Module 4: Privacy and Security Online.* Retrieved 05 31, 2024, from Media Defence: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2022/12/Module-4-Privacy-and-security-online-Dec-2022.pdf

Mihajlov Prokopovic, A. (2021). Podcasts and Journalism. *Media Studies and Applied Ethics, 2*, 19-31. doi:10.46630/msae.2.2021.02

Munro, I. (2018). An interview with Chelsea Manning's lawyer: Nancy Hollander on human rights and the protection of whistleblowers. *Organization, 26*(2), 267-290. doi:https://doi.org/10.1177/1350508418779648

Nasrullah Al-Ameen, M., Lowens, B., Mcgrecor, S., & Caine, K. (2017). Security and Privacy Perception of Sources Who Discussed Sensitive Topics with Journalists. *Race/Ethnicity, 65*(4). Retrieved from https://cj2017.northwestern.edu/documents/security-cj2017-paper-3.pdf

Newman, N. (2024). *Overview and key findings of the 2023 Digital News Report.* Oxford: Reuters Institute, Oxford University. Retrieved from https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023/dnr-executive-summary

Nextcloud. (2024). *About us: You should control your data*. Retrieved 06 02, 2024, from Nextcloud: https://nextcloud.com/about/

O'Driscoll, A. (2023, 11 17). *16 privacy steps every journalist should take to protect themselves and their sources*. Retrieved 05 31, 2024, from comparitech: https://www.comparitech.com/blog/vpn-privacy/protection-of-journalistic-sources/

Oluwafemi Olaoye, G., & Adedokun, D. (2023, 11). *Digital Privacy and Security in the Age of Information and Communication Technology (Preprint).* Retrieved 5 23, 2024, from ResearchGate: https://www.researchgate.net/publication/375289237_Digital_Privacy_and_Security_in_the_Age_of_Information_and_Communication_Technology

Pang, L. (2022, 11 08). *Why open-source encryption is better for your privacy*. Retrieved 06 02, 2024, from Proton: https://proton.me/blog/open-source-encryption-privacy

Pavlik, J. (2008). *Media in the Digital Age.* Columbia University Press.

Precedence Research. (2023). *Cyber Security Market.* Precedence Research. Retrieved from https://www.precedenceresearch.com/cyber-security-market

Proton. (2024). *Proton: About Us*. Retrieved 06 02, 2024, from Proton: https://proton.me/about

Proton Team. (2024, 02 14). *Why Switzerland? An analysis of Swiss privacy laws*. Retrieved 06 02, 2024, from Proton: https://proton.me/blog/switzerland

Raina, K. (2023, 04 17). *Zero Trust Security Explained: Principles of the Zero Trust model*. Retrieved from Crowdstrike: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

Ramos, J. (2016). *Journalist Security in the Digital World: A Survey.* Washinghton, DC: Center for International Media Assistance (CIMA). Retrieved from https://www.cima.ned.org/wp-content/uploads/2016/03/CIMA-Journalist-Digital-Tools-03-01-15.pdf

Ray, M. (2024, 05 06). *Chelsea Manning: United States Army intelligence analyst*. Retrieved 05 31, 2024, from Britannica: https://www.britannica.com/biography/Chelsea-Manning

Ray, M. (2024, 05 07). *Edward Snowden*. Retrieved 05 22, 2024, from Encyclopedia Britannica: https://www.britannica.com/biography/Edward-Snowden

Reporters without borders. (2024). *2024 World Press Freedom Index – journalism under political pressure*. Retrieved 06 01, 2024, from Reporters without borders: https://rsf.org/en/2024-world-press-freedom-index-journalism-under-political-pressure?data_type=general&year=2024

Robinson, J. (2014). Likert Scale. In A. Michalos, *Encyclopedia of Quality of Life and Well-Being Research* (pp. 3620-3621). Dordrecht: Springer Netherlands. doi:https://doi.org/10.1007/978-94-007-0753-5_1654

Roytburg, E. (2024, 06 14). *Edward Snowden eviscerates OpenAI's decision to put a former NSA director on its board: 'This is a willful, calculated betrayal of the rights of every person on earth'*. Retrieved 06 22, 2024, from Fortune: https://fortune.com/2024/06/14/edward-snowden-eviscerates-openai-paul-nakasone-board-directors-decision/

Ryle, G. (2018, 07 31). *'What information should I include?' and other frequently asked questions about becoming a whistleblower*. Retrieved 05 28, 2024, from

International Consortium of Investigative Journalists: https://www.icij.org/inside-icij/2018/07/what-is-a-whistleblower-and-other-faqs-about-whistleblowers/

Schalk, C. (2021, 10 12). *Announcing the Google Forms API*. Retrieved 06 08, 2024, from Google for Developers: https://developers.googleblog.com/en/announcing-the-google-forms-api/

Schiffrin, A. (2017). *In the Service of Power: Media Capture and the Threat to Democracy.* Washinghton, DC, USA: The Center for International Media Assistance National Endowment for Democracy.

SecureDrop (a). (2024). *Welcome to SecureDrop's documentation!* Retrieved 06 03, 2024, from SecureDrop: https://docs.securedrop.org/en/stable/index.html

SecureDrop (b). (2024). *Directory*. Retrieved 06 03, 2024, from SecureDrop: https://securedrop.org/directory/

Shirky, C. (2008). *Here Comes Everybody.* Penguin Books.

Silverman, C., Buttry, S., Wardle, C., Barot, T., Browne, M., Ingram, M., . . . SH, M. (2016). *Verification Handbook: A definitive guide to verifying digital content for emergency coverage.* European Journalism Centre. Retrieved from https://verificationhandbook.com/

Stroud, N. (2011). *Niche News: The Politics of News Choice.* doi:https://doi.org/10.1093/acprof:oso/9780199755509.001.0001

Telegram. (2024). *Telegram FAQ*. Retrieved 06 05, 2024, from Telegram: https://telegram.org/faq#groups-and-channels

Threema (a). (2024). *Threema's Success Story: From the Company's Founding to Today.* Retrieved 06 02, 2024, from Threema: https://threema.ch/press-files/1_press_info/press_threema_story_en.pdf

Threema (b). (2024). *FAQ: Why isn't Threema free of charge?* Retrieved 06 02, 2024, from Threema: https://threema.ch/en/faq/why_not_free_of_charge

Threema (c). (2024). *Threema Focuses on Security and Comprehensive Privacy Protection*. Retrieved 06 02, 2024, from Threema: https://threema.ch/en/security

Thurman, N., & Walters, A. (2013). Live Blogging-Digital Journalism's Pivotal Platorfm? *Digital Journalism*, 82-101. doi:https://doi.org/10.1080/21670811.2012.714935

Tor. (2024). *History*. Retrieved 06 22, 2024, from Tor: https://www.torproject.org/about/history/

Tor project (a). (2024). *Browse Privately. Explore Freely.* Retrieved 06 22, 2024, from Tor: https://www.torproject.org/

Tor project (b). (2024). *ANTI-FINGERPRINTING*. Retrieved 06 22, 2024, from Tor: https://tb-manual.torproject.org/anti-fingerprinting/

Townend, J., & Danbury, R. (2017). *Protecting Sources and Whistleblowers in a Digital Age.* London: Information Law and Policy Centre, Institute of Advanced Legal Studies. Retrieved from https://infolawcentre.blogs.sas.ac.uk/files/2017/02/Sources-Report_webversion_22_2_17.pdf

Tresorit. (2024). *Why Tresorit?* Retrieved 06 05, 2024, from Tresorit: https://tresorit.com/why-tresorit

Tresorit Team. (2023, 07 03). *Secure file sharing 101: the essential guide to secure document sharing online*. Retrieved 06 05, 2024, from Tresorit: https://tresorit.com/blog/secure-file-sharing-101-the-essential-guide-to-secure-document-sharing-online/

Tsui, L. (2018). The importance of digital security to securing press freedom. *Journalism, 20*(1), 80-82. doi:https://doi.org/10.1177/1464884918809276

Tsui, L., & Lee, F. (2019). How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. *Journalism, 22*(6), 1317-1339. doi:https://doi.org/10.1177/1464884919849418

US Congress. (2015, 06 02). Public Law 114-23. *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015*. USA: US Congress. Retrieved 05 30, 2024, from https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

van der Nat, R., Müller, E., & Bakker, P. (2021). Navigating Interactive Story Spaces. The Architecture of Interactive Narratives in Online Journalism. *Digital Journalism, 11*(6), 1104-1129. doi:https://doi.org/10.1080/21670811.2021.1960178

van der Velden, P., Pecoraro, M., Houwerzijl, M., & van der Meulen, E. (2019). Mental Health Problems Among Whistleblowers: A Comparative Study. *Psychological Reports, 122*(2), 632-644. doi:https://doi.org/10.1177%2F0033294118757681

Veglis, A. (2023, 05). Presentation: Techniques and Tools for Secure Online Communication. Greece.

Višňovský, J., & Radošinská, J. (2016). Online Journalism: Current Trends and Challenges. In B. Peña Acuña, *The Evolution of Media Communication.* InTech. doi:http://dx.doi.org/10.5772/68086

Vosoughi, S., Roy, D., & Aral, S. (2018, 03 18). The spread of true and false news online. *Science, 359*(6380), pp. 1146-1151. doi:https://doi.org/10.1126/science.aap9559

WhatsApp (a). (2024). *About WhatsApp*. Retrieved 06 03, 2024, from WhatsApp: https://www.whatsapp.com/about

WhatsApp (b). (2024). *WhatsApp Home Page*. Retrieved 06 03, 2024, from WhatsApp: https://www.whatsapp.com

WhatsApp (c). (2024). *How to create and invite into a group*. Retrieved 06 03, 2024, from WhatsApp Help Center: https://faq.whatsapp.com/3242937609289432/?helpref=uf_share

WhatsApp (d). (2024). *How to use broadcast lists*. Retrieved 06 03, 2024, from WhatsApp Help Center: https://faq.whatsapp.com/861663048350950/?helpref=uf_share

WhatsApp. (2021). *End-to-End Encrypted Backups on WhatsApp*. Retrieved 06 03, 2024, from WhatsApp: https://blog.whatsapp.com/end-to-end-encrypted-backups-on-whatsapp

WhatsApp. (2023, 02 07). *New Ways to Enjoy WhatsApp Status*. Retrieved 06 03, 2024, from WhatsApp: https://blog.whatsapp.com/new-ways-to-enjoy-whatsapp-status

WhatsApp Business. (2024). *Engage your customers anywhere*. Retrieved 06 03, 2024, from Meta: https://business.whatsapp.com/products/business-app-features

Wire (a). (2024). *About us*. Retrieved 06 03, 2024, from Wire: https://wire.com/en/about-us

Wire (b). (2024). *The platform for confidential communication*. Retrieved 06 03, 2024, from Wire: https://wire.com/en/product

Wire (c). (2024). *Privacy Policy*. Retrieved 06 03, 2024, from Wire: https://wire.com/privacy-policy

Wire (d). (2024). *Confidential Communications for the Public Sector*. Retrieved 06 03, 2024, from Wire: https://wire.com/en/solution-public-sector

Wolford, B. (2023, 03 09). *Using Proton Mail for Journalism*. Retrieved 06 02, 2024, from Proton: https://proton.me/blog/journalism

Younger, N. (2020, 11 19). *The case of Edward Snowden*. Retrieved 05 30, 2024, from National Whistleblower Center: https://www.whistleblowers.org/news/the-case-of-edward-snowden/

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2019, 08 29). Νόμος 4624/2019. Αθήνα: Εφημερίδα της Κυβερνήσεως. Ανάκτηση από http://elib.aade.gr/elib/view?d=/gr/act/2019/4624/

Βουλή των Ελλήνων. (2019, 11 24). Σύνταγμα της Ελλάδας - Άρθρο 14: Ελευθερία του Τύπου. Αθήνα, Ελλάδα.

Ελληνική Δημοκρατία (α). (2022, 11 24). Νόμος 4996/2022. Αθήνα: Εφημερίδα της Κυβερνήσεως. Ανάκτηση από https://www.et.gr/api/Download_Small/?fek_pdf=20220100218

Ελληνική Δημοκρατία (β). (2022, 11 11). Νόμος 4990/2022. Αθήννα: Εφημερίδα της Κυβερνήσεως. Ανάκτηση από http://elib.aade.gr/elib/view?d=/gr/act/2022/4990/

ΕΝΩΣΗ ΣΥΝΤΑΚΤΩΝ ΗΜΕΡΗΣΙΩΝ ΕΦΗΜΕΡΙΔΩΝ ΘΕΣΣΑΛΙΑΣ - ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ - ΕΥΒΟΙΑΣ. (2024). *Ιστορικό ΕΣΗΕΘΣΤΕ-Ε*. Ανάκτηση 06 12, 2024, από ΕΝΩΣΗ ΣΥΝΤΑΚΤΩΝ ΗΜΕΡΗΣΙΩΝ ΕΦΗΜΕΡΙΔΩΝ ΘΕΣΣΑΛΙΑΣ - ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ - ΕΥΒΟΙΑΣ: https://www.pressunion.gr/10-Istoriko-ESHETHSTE-E.html

Ένωση Συντακτών Ημερησίων Εφημερίδων Μακεδονίας-Θράκης. (2024). *ΤΟ ΧΡΟΝΙΚΟ ΤΗΣ ΕΝΩΣΗΣ*. Ανάκτηση 06 12, 2024, από ΕΣΗΕΜ-Θ: https://esiemth.gr/chroniko/

ΕΣΗΕΑ. (1998, 05 20). *Αρχές δεοντολογίας δημοσιογραφικού επαγγέλματος*. Ανάκτηση 05 20, 2024, από ΕΝΩΣΙΣ ΣΥΝΤΑΚΤΩΝ ΗΜΕΡΗΣΙΩΝ ΕΦΗΜΕΡΙΔΩΝ ΑΘΗΝΩΝ: https://www.esiea.gr/kodikas-deontologias/arxes-deontologias-dimosiografikoy/

Ευρωπαΐκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης. (2016, 04 27). Γενικός Κανονισμός για την Προστασία Δεδομένων. *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, 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*. Ευρωπαϊκή Ένωση. Ανάκτηση από https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A02016R0679-20160504

Λάζαρης, Β. (2024). *ΙΣΤΟΡΙΚΟ*. Ανάκτηση 06 12, 2024, από ΕΝΩΣΗ ΣΥΝΤΑΚΤΩΝ ΗΜΕΡΗΣΙΩΝ ΕΦΗΜΕΡΙΔΩΝ ΠΕΛΟΠΟΝΝΗΣΟΥ-ΗΠΕΙΡΟΥ-ΝΗΣΩΝ: https://www.esiepin.gr/ενωση/ιστορικο/

ΟΟΣΑ. (2020). *Τεχνική Έκθεση για την Προστασία των Πληροφοριοδοτών που ενεργούν προς το Δημόσιο Συμφέρον.* Ανάκτηση 05 29, 2024, από

https://aead.gr/images/manuals/5.1.1-technical-report-whistleblower-protection-public-sector-greece-el.pdf

Παράρτημα 1: Ελευθερία του Τύπου – Κατάταξη χωρών

Η παρακάτω λίστα είναι με βάση την κατάταξη από τον ιστότοπο Reporters without borders την 1/6/2024 (Reporters without borders, 2024).

Χώρα	Κατάταξη	Βαθμολογία
Νορβηγία	1	91,89
Δανία	2	89,6
Σουηδία	3	88,32
Ολλανδία	4	87,73
Φινλανδία	5	86,55
Εσθονία	6	86,44
Πορτογαλία	7	85,9
Ιρλανδία	8	85,59
Ελβετία	9	84,01
Γερμανία	10	83,84
Λουξεμβούργο	11	83,8
Λετονία	12	82,9
Λιθουανία	13	81,73
Καναδάς	14	81,7
Λιχτενστάιν	15	81,52
Βέλγιο	16	81,49
Τσεχία	17	80,14
Ισλανδία	18	80,13
Νέα Ζηλανδία	19	79,72
Τιμόρ-Λέστε	20	78,92
Γαλλία	21	78,65
Σαμόα	22	78,41
Ηνωμένο Βασίλειο	23	77,51

Τζαμάικα	24	77,3
Τρινιντάντ και Τομπάγκο	25	76,69
Κόστα Ρίκα	26	76,13
Ταιβάν	27	76,13
Σουρινάμ	28	76,11
Σλοβακία	29	76,03
Ισπανία	30	76,01
Μολδαβία	31	74,86
Αυστρία	32	74,69
Μαυριτανία	33	74,2
Ναμίμπια	34	74,16
Δομινικανή Δημοκρατία	35	73,89
ΠΓΔΜ	36	73,78
Σεϋχέλλες	37	73,75
Νότια Αφρική	38	73,73
Αυστραλία	39	73,42
Μαυροβούνιο	40	73,21
Κάπο Βέρντε	41	72,77
Σλοβενία	42	72,6
Αρμενία	43	71,6
Φίτζι	44	71,23
Τόγκα	45	70,11
Ιταλία	46	69,8
Πολωνία	47	69,17
Κροατία	48	68,79
Ρουμανία	49	68,45
Γκάνα	50	67,71
Ουρουγουάη	51	67,7

Χιλή	52	67,32
Ακτή Ελεφαντοστού	53	66,89
Μπελίζ	54	66,85
ΗΠΑ	55	66,59
Γκαμπόν	56	65,83
Μαυρίκιος	57	65,55
Γκάμπια	58	65,53
Βουλγαρία	59	65,32
Λιβερία	60	65,13
Ουκρανία	61	65
Νότια Κορέα	62	64,87
Μαλάουι	63	64,46
Σιέρρα Λεόνε	64	64,27
Κύπρος	65	63,14
Αργεντινή	66	63,13
Ουγγαρία	67	62,98
ΟΑΚΠ	68	62,83
Κονγκό	69	62,57
Ιαπωνία	70	62,12
Κομόρες	71	61,47
Ανδόρρα	72	61,44
Μάλτα	73	60,96
Νεπάλ	74	60,52
Κόσοβο	75	60,19
Κεντροαφρικανική Δημοκρατία	76	60,12
Γουιάνα	77	60,1
Γουινέα	78	59,97

Μποτσουάνα	79	59,78
Νίγηρας	80	59,71
Βοσνία-Ερζεγοβίνη	81	58,85
Βραζιλία	82	58,59
Παναμάς	83	58,55
Κατάρ	84	58,48
Σουαζιλάνδη	85	58,31
Μπουρκίνα Φάσο	86	58,24
Ταϊλάνδη	87	58,12
Ελλάδα	88	57,15
Μπενίν	89	56,73
Ψευδοκράτος Κύπρου	90	56,72
Παπούα Νέα Γουινέα	91	56,02
Γουινέα Μπισάου	92	55,95
Αϊτή	93	55,92
Σενεγάλη	94	55,44
Ζάμπια	95	55,38
Τσαντ	96	54,81
Τανζανία	97	54,8
Σερβία	98	54,48
Αλβανία	99	54,1
Μαδαγασκάρη	100	54,07
Ισραήλ	101	53,23
Κένυα	102	53,22
Γεωργία	103	53,05
Αγκόλα	104	52,44
Μοζαμβίκη	105	52,42
Μαλδίβες	106	52,36

Μαλαισία	107	52,07
Μπουρούντι	108	51,78
Μογγολία	109	51,34
Εκουαδόρ	110	51,3
Ινδονησία	111	51,15
Νιγηρία	112	51,03
Τόγκο	113	50,89
Μάλι	114	50,56
Παραγουάη	115	50,48
Ζιμπάμπουε	116	50,31
Μπρουνέι	117	50,09
Τυνησία	118	49,97
Κολομβία	119	49,63
Κιργιζία	120	49,11
Μεξικό	121	49,01
Λεσότο	122	48,92
Λαϊκή Δημοκρατία του Κονγκό	123	48,91
Βολιβία	124	48,88
Περού	125	47,76
Σιγκαπούρη	126	47,19
Ισημερινή Γουινέα	127	46,49
Ουγκάντα	128	46
Μαρόκο	129	45,97
Καμερούν	130	44,95
Κουβέιτ	131	44,66
Ιορδανία	132	44,3
Ελ Σαλβαδόρ	133	44,01

Φιλιππίνες	134	43,36
Χονγκ Κόνγκ	135	43,06
Νότιο Σουδάν	136	42,57
Ομάν	137	42,52
Γουατεμάλα	138	42,28
Αλγερία	139	41,98
Λίβανος	140	41,91
Αιθιοπία	141	41,37
Καζακστάν	142	41,11
Λιβύη	143	40,59
Ρουάντα	144	40,54
Σομαλία	145	39,4
Ονδούρα	146	38,18
Μπουτάν	147	37,29
Ουζμπεκιστάν	148	37,27
Σουδάν	149	35,73
Σρι Λάνκα	150	35,21
Καμπότζη	151	34,28
Πακιστάν	152	33,9
Λάος	153	33,76
Υεμένη	154	33,67
Τατζικιστάν	155	33,31
Βενεζουέλα	156	33,06
Παλαιστίνη	157	31,92
Τουρκία	158	31,6
Ινδία	159	31,28
Ενωμένα Αραβικά Εμιράτα	160	30,62
Τζιμπουτί	161	30,14

Ρωσία	162	29,86
Νικαράγουα	163	29,2
Αζερμπαϊτζάν	164	27,99
Μπαγκλαντές	165	27,64
Σαουδική Αραβία	166	27,14
Λευκορωσία	167	26,8
Κούβα	168	25,63
Ιράκ	169	25,48
Αίγυπτος	170	25,1
Μυανμάρ	171	24,41
Κίνα	172	23,36
Μπαχρέιν	173	23,21
Βιετνάμ	174	22,31
Τουρκμενιστάν	175	22,01
Ιράν	176	21,3
Βόρεια Κορέα	177	20,66
Αφγανιστάν	178	19,09
Συρία	179	17,41
Ερυθραία	180	16,64

Παράρτημα 2: Ερωτηματολόγιο

Αγαπητή/έ συμμετέχουσα/οντα

Ευχαριστούμε προκαταβολικά για τον χρόνο που διαθέσατε για να συμμετάσχετε σε αυτήν την έρευνα. Οι απόψεις σας είναι πολύτιμες για την κατανόηση της χρήσης και της αντίληψης για τις πλατφόρμες ασφαλούς επικοινωνίας στη Δημοσιογραφία. Οι απαντήσεις σας θα παραμείνουν εμπιστευτικές.

ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

1. Ποιο είναι το φύλο σας;

- Άνδρας
- Γυναίκα
- Προτιμώ να μην απαντήσω

2. Σε ποια ηλικιακή ομάδα ανήκετε;

- 18-24
- 25-34
- 35-44
- 45-54
- >54

3. Ποιο είναι το επίπεδο της εκπαίδευσής σας;

- Απόφοιτος λυκείου
- Κάτοχος πτυχίου πανεπιστημίου
- Κάτοχος μεταπτυχιακού τίτλου
- Κάτοχος διδακτορικού
- Άλλο [προσδιορίστε]

ΠΛΗΡΟΦΟΡΙΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΤΟΜΕΑ ΑΠΑΣΧΟΛΗΣΗΣ ΣΑΣ

4. Εργάζεσθε ως... [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Δημοσιογράφος
- Συντάκτης
- Ειδικός δεδομένων

- Παραγωγός
- Φωτογράφος
- Γραφίστας
- Βιντεογράφος
- Άλλο [προσδιορίστε]

5. Εργάζεσθε σε ειδησεογραφικό οργανισμό ή εργάζεσθε ανεξάρτητα;

- Εργάζομαι σε ειδησεογραφικό οργανισμό
- Εργάζομαι ως ανεξάρτητος δημοσιογράφος
- Και τα δύο
- Ούτε το ένα ούτε το άλλο

6. Ποια από τα παρακάτω θέματα καλύπτετε τακτικά; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Κυβέρνηση και Πολιτική
- Έγκλημα και επιβολή του νόμου
- Επιχειρήσεις και Οικονομία
- Εκπαίδευση
- Περιβάλλον
- Υγεία και Ιατρική
- Επιστήμη και Τεχνολογία
- Εθνική ασφάλεια
- Εξωτερικές υποθέσεις
- Άλλο [προσδιορίστε]

7. Καλύπτετε κυρίως

- Τοπικές ειδήσεις
- Εθνικές ειδήσεις
- Διεθνείς ειδήσεις
- Δεν υπάρχει γεωγραφική εστίαση στο έργο μου

ΧΡΗΣΗ ΠΛΑΤΦΟΡΜΩΝ ΑΣΦΑΛΟΥΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΟΝ ΧΩΡΟ ΕΡΓΑΣΙΑΣ ΣΑΣ

8. Χρησιμοποιείτε αυτή τη στιγμή κάποια πλατφόρμα ασφαλούς επικοινωνίας για τη δημοσιογραφική σας εργασία;

- Ναι
- Όχι

9. Γνωρίζετε τα παρακάτω εργαλεία/εφαρμογές ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Nextcloud
- Wickr
- Proton Mail
- Signal
- Threema
- Wire
- WhatsApp
- Securedrop
- GlobaLeaks
- OnionShare
- Tresorit
- Telegram

10. Χρησιμοποιείτε κάποιο/κάποια από τα παρακάτω εργαλεία ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Nextcloud
- Wickr
- Proton Mail
- Signal
- Threema
- Wire
- WhatsApp
- Securedrop
- GlobaLeaks
- OnionShare

- Tresorit
- Telegram
- Άλλο [προσδιορίστε]

11. Αναφέρετε τη συχνότητα χρήσης

- Καθημερινά
- Εβδομαδιαία
- Περιστασιακά

12. Γνωρίζετε για τη δυνατότητα αποστολής και λήψης κρυπτογραφημένων emails;

- Ναι
- Όχι

13. Χρησιμοποιείτε κρυπτογράφηση στην αποστολή και λήψη emails;

- Ναι
- Όχι

14. Ποιες συγκεκριμένες λειτουργίες των πλατφορμών ασφαλούς επικοινωνίας βρίσκετε πιο επωφελείς στη δημοσιογραφική σας εργασία;

- Κρυπτογράφηση από άκρο σε άκρο
- Ασφαλής διαμοιρασμός αρχείων
- Πραγματοποίηση κρυπτογραφημένων κλήσεων (ήχος και βίντεο)
- Δυνατότητα χρήσης από διαφορετικές συσκευές (cross platform compatibility)
- Πιστοποίηση χρήστη
- Πολιτική διατήρησης μηνυμάτων
- Άλλο [προσδιορίστε]

15. Ποιες είναι οι τρεις κύριες χρήσεις για τις οποίες χρησιμοποιείτε τις πλατφόρμες ασφαλούς επικοινωνίας στη δημοσιογραφική σας εργασία;

16. Ποιοι παράγοντες επηρέασαν την επιλογή σας για τη χρήση των πλατφορμών ασφαλούς επικοινωνίας; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Κρυπτογράφηση από άκρο σε άκρο (end to end encryption)
- Διεπαφή Χρήστη/Ευχρηστία (User Interface)
- Αξιοπιστία/Απόδοση
- Συμβατότητα με άλλες πλατφόρμες
- Λειτουργίες Συνεργασίας
- Ασφάλεια
- Συστάσεις από Συναδέλφους/Συναδέλφους
- Άλλο [προσδιορίστε]

17. Ποιες βελτιώσεις θα θέλατε να δείτε στις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιείτε;

18. Θα συνιστούσατε τις πλατφόρμες ασφαλούς επικοινωνίας που χρησιμοποιείτε στους συναδέλφους σας στη δημοσιογραφική κοινότητα;

- Ναι
- Όχι

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΣΤΗΝ ΕΡΓΑΣΙΑ ΣΑΣ

19. Πιστεύετε ότι υπάρχει θέμα ασφαλείας επικοινωνιών στην άσκηση της Δημοσιογραφίας;

- Ναι σίγουρα υπάρχει
- Ενδεχομένως να υπάρχει
- Δεν γνωρίζω/δεν έχω γνώμη
- Ενδεχομένως να μην υπάρχει
- Σίγουρα δεν υπάρχει

20. Πόσο βέβαιη/ος είστε για την ασφάλεια και την ιδιωτικότητα των πλατφορμών ασφαλούς επικοινωνίας που χρησιμοποιείτε;

- • Πολύ Βέβαιη/Βέβαιος
- • Βέβαιη/Βέβαιος
- • Ουδέτερη/Ουδέτερος
- • Όχι Πολύ Βέβαιη/Βέβαιος

- Καθόλου Βέβαιη/Βέβαιος

21. Οι δημοσιογράφοι αντιμετωπίζουν σήμερα σημαντικές προσκλήσεις. Πιστεύετε ότι υπάρχουν οι παρακάτω προκλήσεις;

Ηλεκτρονική παρακολούθηση από κυβερνήσεις, εταιρείες και άλλες οντότητες

- Ναι σίγουρα υπάρχει
- Ενδεχομένως να υπάρχει
- Δεν γνωρίζω/δεν έχω γνώμη
- Ενδεχομένως να μην υπάρχει
- Σίγουρα δεν υπάρχει

Hackers που στοχεύουν δημοσιογράφους ή ειδησεογραφικούς οργανισμούς

- Ναι σίγουρα υπάρχει
- Ενδεχομένως να υπάρχει
- Δεν γνωρίζω/δεν έχω γνώμη
- Ενδεχομένως να μην υπάρχει
- Σίγουρα δεν υπάρχει

Αλλοίωση/επεξεργασία περιεχομένου και διαστρέβλωση της πραγματικότητας με χρήση μεθόδων τεχνητής νοημοσύνης (π.χ. deepfakes, AI-generated περιεχόμενο, κ.α.)

- Ναι σίγουρα υπάρχει
- Ενδεχομένως να υπάρχει
- Δεν γνωρίζω/δεν έχω γνώμη
- Ενδεχομένως να μην υπάρχει
- Σίγουρα δεν υπάρχει

22. Ποια από τις ακόλουθες δηλώσεις έρχεται πιο κοντά στη δική σας άποψη, ακόμη και αν καμία από τις δύο δεν είναι ακριβώς σωστή;

- Για τους σημερινούς δημοσιογράφους, τα οφέλη της ψηφιακής επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα, υπερτερούν των κινδύνων
- Για τους σημερινούς δημοσιογράφους, οι κίνδυνοι της ψηφιακής επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα υπερτερούν των πλεονεκτημάτων

ΕΜΠΕΙΡΙΑ ΑΠΟ ΠΑΡΑΒΙΑΣΗ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΡΓΑΣΙΑ ΣΑΣ

23. Έχετε βιώσει ή υποψιαστεί ότι έχετε υποστεί παραβίαση επικοινωνίας στην εργασία σας;

- Ναι
- Όχι
- Δεν γνωρίζω

24. Αν απαντήσατε ναι στην προηγούμενη ερώτηση, ποιες από τις παρακάτω διαδικασίες αφορά; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Χρήση του διαδικτύου για συλλογή πληροφοριών
- Αποθήκευση ή κοινή χρήση δυνητικά ευαίσθητων εγγράφων
- Επικοινωνία με άλλους δημοσιογράφους, συντάκτες ή παραγωγούς
- Επικοινωνία με πηγές

25. Τους τελευταίους 12 μήνες, υπήρξε περίπτωση κατά την οποία οι ανησυχίες για παρακολούθηση ή παραβίαση σας οδήγησαν στο να μην καλύψετε ή να μην ασχοληθείτε με ένα συγκεκριμένο θέμα;

- Ναι
- Όχι

26. Τους τελευταίους 12 μήνες, υπήρξε περίπτωση που οι ανησυχίες για παρακολούθηση ή παραβίαση σας οδήγησαν στο να μην απευθυνθείτε σε μια συγκεκριμένη πηγή;

- Ναι

- Όχι

27. Και κατά τους τελευταίους 12 μήνες, υπήρξε περίπτωση που οι ανησυχίες για παρακολούθηση ή hacking σας οδήγησαν να σκεφτείτε να εγκαταλείψετε την ερευνητική Δημοσιογραφία;

- Ναι
- Όχι

28. Τους τελευταίους 12 μήνες, πόσο, αν όχι καθόλου, έχετε αλλάξει τον τρόπο με τον οποίο...

Χρησιμοποιείτε το διαδίκτυο για να ερευνήσετε ιστορίες

- Πάρα πολύ
- Πολύ
- Λίγο
- Πολύ λίγο
- Καθόλου

Αποθήκευση ή κοινή χρήση δυνητικά ευαίσθητων εγγράφων

- Πάρα πολύ
- Πολύ
- Λίγο
- Πολύ λίγο
- Καθόλου

Επικοινωνία με άλλους δημοσιογράφους, συντάκτες ή παραγωγούς

- Πάρα πολύ
- Πολύ
- Λίγο
- Πολύ λίγο
- Καθόλου

Επικοινωνία με τις πηγές

- Πάρα πολύ
- Πολύ
- Λίγο
- Πολύ λίγο

- Καθόλου

29. Υπάρχει κάτι άλλο που θα θέλατε να μοιραστείτε σχετικά με τις εμπειρίες σας με τις πλατφόρμες ασφαλούς επικοινωνίας στη Δημοσιογραφία;

ΕΦΑΡΜΟΓΗ ΠΡΑΚΤΙΚΩΝ ΠΟΥ ΔΙΑΣΦΑΛΙΖΟΥΝ ΤΗΝ ΑΣΦΑΛΗ ΕΠΙΚΟΙΝΩΝΙΑ

30. Έχετε γνώση από πρακτικές που διασφαλίζουν την ασφαλή επικοινωνία;

- Ναι
- Όχι

31. Χρησιμοποιείτε κάποια από τα παρακάτω πρακτικές για ασφαλή επικοινωνία; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Χρήση κρυπτογράφησης σε emails, μηνύματα, κ.λπ.
- Χρήση ισχυρών κωδικών
- Χρήση ταυτοποίησης δύο παραγόντων (2 Factor Authentication – 2FA)
- Χρήση συσκευών με ισχυρή ασφάλεια
- Αποφυγή χρήσης επισφαλών δημόσιων δικτύων (Wi-Fi σε καφέ, εστιατόρια, δημόσιους χώρους)
- Συνεχής πραγματοποίηση ενημερώσεων ασφαλείας των εφαρμογών
- Χρήση antivirus
- Εκπαίδευση και ενημέρωση σχετικά με τις κυβερνοαπειλές

ΚΑΤΟΧΗ ΓΝΩΣΕΩΣ ΑΣΦΑΛΟΥΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΤΡΟΠΟΣ ΑΠΟΚΤΗΣΗΣ ΤΟΥΣ

32. Έχετε γνώσεις σχετικά με την ασφαλή επικοινωνία και διαμοίραση πληροφοριών μέσω διαδικτύου;

- Ναι
- Όχι

33. Ποια από τα παρακάτω έχετε εφαρμόσει, εφαρμόζετε ή θα εφαρμόζατε προκείμενου να αποκτήσετε ή να εμπλουτίσετε τις γνώσεις σας σχετικά με την ασφαλή επικοινωνία και διαμοίραση πληροφοριών μέσω διαδικτύου; [μπορείτε να επιλέξετε παραπάνω από μία απάντηση]

- Συμμετοχή σε σεμινάρια
- Πρακτική εκπαίδευση πάνω σε πρακτικές ασφαλούς επικοινωνίας
- Ενημέρωση από εξειδικευμένους ιστότοπους
- Παρακολούθηση διαδικτυακών σειρών μαθημάτων και εκπαιδεύσεων
- Πραγματοποίηση μεταπτυχιακών σπουδών στο συγκεκριμένο αντικείμενο
- Μελέτη και διερεύνηση σχετικής βιβλιογραφίας
- Συζητήσεις και ανταλλαγή γνώσεων και εμπειριών με συναδέλφους σας
- Άλλο [προσδιορίστε]

Σας ευχαριστούμε για τον χρόνο που διαθέσατε να συμπληρώσετε αυτό το ερωτηματολόγιο! Οι απόψεις και οι εμπειρίες σας είναι πολύτιμες για την κατανόηση της χρήσης ασφαλών πρακτικών επικοινωνίας στη Δημοσιογραφία.

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης.