

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΣΥΓΧΡΟΝΕΣ ΔΗΜΟΣΙΟΓΡΑΦΙΚΕΣ ΣΠΟΥΔΕΣ

Πτυχιακή Εργασία

Πλατφόρμες Ασφαλούς Επικοινωνίας Μεταξύ Δημοσιογράφων και
Whistleblowers

Η Ερευνητική Δημοσιογραφία στην Εποχή της Κρυπτογράφησης

Βασιλική Διονυσοπούλου

Επιβλέπων καθηγητής: κ. Ανδρέας Βέγλης

Πάτρα, Φεβρουάριος 2021

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή («συγγραφέας/δημιουργός») που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο ΕΑΠ, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε

τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

Πλατφόρμες Ασφαλούς Επικοινωνίας Μεταξύ Δημοσιογράφων και
Whistleblowers

Η Ερευνητική Δημοσιογραφία στην Εποχή της Κρυπτογράφησης

Βασιλική Διονυσοπούλου

Επιβλέπον καθηγητής

κ. Ανδρέας Βέγλης

Καθηγητής Εφαρμογών Τεχνολογιών Πληροφορίας και Επικοινωνιών στα ΜΜΕ

Ελληνικό Ανοικτό Πανεπιστήμιο

Πάτρα, Φεβρουάριος 2021

Ευχαριστώ τον επιβλέποντα καθηγητή κ. Ανδρέα Βέγλη για την πολύτιμη βοήθεια

και

Το Ελληνικό Ανοικτό Πανεπιστήμιο για τη δυνατότητα εκπόνησης της συγκεκριμένης εργασίας

Περίληψη

Οι πλατφόρμες ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers αποτελούν απαραίτητα εργαλεία του σύγχρονου δημοσιογράφου. Η δυνατότητα παρακολούθησης κάθε ψηφιακής δραστηριότητας καθιστά αναγκαία τη διασφάλιση του απορρήτου της επικοινωνίας μεταξύ του δημοσιογράφου και του πληροφοριοδότη. Η ψηφιακή τεχνολογία δίνει τη λύση με εργαλεία που βασίζονται στην κρυπτογράφηση και τον περιορισμό των μεταδεδομένων της διαδικτυακής επικοινωνίας. Εργαλεία όπως ο πλοηγητής Tor, το Tails, το Signal και ο κώδικας PGP διευκολύνουν την ασφαλή ψηφιακή επικοινωνία και ανταλλαγή περιεχομένου. Πολλές από τις τεχνολογίες αυτές χρησιμοποιήθηκαν από καινοτόμους μηχανικούς πληροφορικής για τη δημιουργία ασφαλέστερων εργαλείων επικοινωνίας της αίθουσας σύνταξης με τον έξω κόσμο. Η αρχή έγινε το 2006, με την εμφάνιση των WikiLeaks, τα οποία καθιέρωσαν νέες πρακτικές στον τρόπο άντλησης και παρουσίασης των ειδήσεων. Η ερευνητική δημοσιογραφία έψαχνε το βηματισμό της στο νέο περιβάλλον. Οι αποκαλύψεις, το 2013, του πρώην πράκτορα του National Security Agency, Edward Snowden, κατέστησαν απολύτως αναγκαία την προσπάθεια της διαδικασίας της επικοινωνία του δημοσιογράφου με τους whistleblowers. Τη λύση την έδωσαν δυο λογισμικά που βασίζονται σε ανοιχτό κώδικα και που παρέχονται από Μη Κυβερνητικές Οργανώσεις, δωρεάν σε όλα τα μέσα. Πρόκειται για τις πλατφόρμες ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers. Το SecureDrop και το GlobaLeaks είναι τα δυο βασικότερα εργαλεία που χρησιμοποιούνται από τα περισσότερα μέσα παγκοσμίως, με το πρώτο να αποτελεί τον αδιαμφισβήτητο ηγέτη στο χώρο. Το μέλλον της ερευνητικής δημοσιογραφίας, που συνδέεται άμεσα με την προστασία των πληροφοριοδοτών, έγκειται στη χρήση των εργαλείων αυτών. Οι δυνατότητες είναι τεράστιες και ο βαθμός της χρήσης τους θα κρίνει την πορεία του επαγγέλματος, σε μια εποχή που η αξιοπιστία του βάλλεται διεθνώς.

Λέξεις – Κλειδιά

Πλατφόρμες ασφαλούς επικοινωνίας, ερευνητική δημοσιογραφία, πληροφοριοδότης, κρυπτογράφηση, Tor, SecureDrop, GlobaLeaks, WikiLeaks.

Digital Whistleblowing Platforms Between Journalists and Whistleblowers

Investigative Journalism at the Cryptography Age

Vassiliki Dionyssopoulou

Abstract

Digital whistleblowing platforms are some essential tools for modern journalism. The possibility of any digital activity to be monitored makes it necessary to ensure the confidentiality of communication between journalist and whistleblower. Digital technology provides tools based on encryption and reduction of metadata. Tor Browser, Tails, Signal and the encryption code PGP are some of them. Many IT experts tried to make tools especially for the safe communication between press rooms and whistleblowers. WikiLeaks, in 2006, was the first big step. The disclosures of NSA's agent Edward Snowden were the turning point to this procedure. It was clear that journalists should find ways for safe communication. SecureDrop and GlobaLeaks was the solution. These two digital whistleblowing platforms are the main tools most of the media outlets use worldwide. They expand the way of journalistic investigation and it depends on the journalists to use them properly in order to regain their lost reliability.

Keywords

Digital whistleblowing platforms, investigative journalism, whistleblower, cryptography, Tor, SecureDrop, GlobaLeaks, WikiLeaks.

Περιεχόμενα

Πρόλογος	1
1. Διαρροή Πληροφοριών και Δημοσιογραφία.....	5
1.1 Η εξέλιξη του whistleblower.....	5
1.2 Wikileaks	6
1.2.1 Ο ρόλος των WikiLeaks.....	7
1.2.2 Η περίπτωση του Collateral Murder.....	9
1.2.3 Η περίπτωση των MegaLeaks.....	10
1.2.4 Νέες τάσεις.....	10
1.3 Η ιστορική πράξη του Edward Snowden.....	12
2. Ψηφιακή Τεχνολογία και Δημοσιογραφία.....	14
2.1 Κρυπτογράφηση.....	14
2.2 Εργαλεία Ασφαλούς Επικοινωνίας.....	16
2.2.1 Tor	17
2.2.2 Pretty Good Privacy.....	18
2.2.3 Off the Record	18
2.2.4 Signal.....	19
2.2.5 Tails.....	19
3. Πλατφόρμες ασφαλούς επικοινωνίας δημοσιογράφων με Whistleblowers.....	21

3.1 Η πρώτη επαφή.....	23
3.2 Η προϊστορία, Cryptome και BlackNet.....	24
3.3 Τα πρώτα βήματα, οι αντιγραφείς.....	25
3.4 Οι πρώτες προσπάθειες από τα κυρίαρχα μέσα.....	26
3.5 Οι πλατφόρμες ξεκινούν.....	28
3.5.1 GlobaLeaks, Η Πρώτη Πλατφόρμα.....	29
3.5.2 SecureDrop, Ο Ηγέτης.....	31
3.5.3 Το SecureDrop στο Harvard.....	34
4. Η σημασία της ασφαλούς επικοινωνίας.....	36
4.1 Οι ερευνητική δημοσιογραφία σε κίνδυνο.....	36
4.2 Ο στιγματισμός του whistleblower	37
4.3 Ο whistleblower ως κίνδυνος.	40
Επίλογος.....	42
Βιβλιογραφία	45
Παραπομπές	54
Σημειώσεις	57

Πρόλογος

Η ερευνητική δημοσιογραφία αποτελεί μια από τις δυσκολότερες προκλήσεις των ανθρώπων της ενημέρωσης, διαχρονικά. Η αναγκαιότητά της για την ομαλή λειτουργία των δημοκρατικών θεσμών είναι κεφαλαιώδους σημασίας. Το Reuters Institute for the Study of Journalism, στη φετινή ετήσια έκθεσή του, δίνει ιδιαίτερη βαρύτητα στην ανάγκη ελέγχου των κέντρων εξουσίας από τους δημοσιογράφους. “Η δημοσιογραφία, ως μέσο ελέγχου της εξουσίας συνεχίζει να αποκτά όλο και περισσότερη σημασία, καθώς οι πολιτικοί δείχνουν να εκμεταλλεύονται την ανησυχία σχετικά με την παραπληροφόρηση και να ενισχύουν τους περιορισμούς της ελευθερίας του λόγου. Αυτές οι τάσεις είναι επίσης προφανείς σε κάποιες φιλελεύθερες δημοκρατίες, όπως αποτυπώνονται στην διαμάχη γύρω από το νέο γαλλικό νόμο”, Newman. (2021).

Ο ρόλος της διαρροής πληροφοριών (whistleblowing) στην επιτέλεση του παραπάνω σκοπού από τους δημοσιογράφους είναι ιδιαίτερα σημαντικός. Ως διαρροή πληροφοριών ορίζεται η αποκάλυψη από, εν ενεργεία ή πρώην, μέλη οργανισμών, των παράνομων, ανήθικων ή παράτυπων πράξεων από τους προϊσταμένους τους, σε άτομα ή οργανισμούς που μπορούν να συμβάλλουν στην κινητοποίηση των αρμόδιων μηχανισμών προστασίας του δημοσίου συμφέροντος (Miceli and Near, 1992).

Η διαρροή των πληροφοριών μπορεί να είναι εσωτερική, δηλαδή εντός του οργανισμού, ή εξωτερική, κυρίως στη δικαιοσύνη ή στα ΜΜΕ. Πολλοί είναι οι οργανισμοί που ωθούνται στην υιοθέτηση πρακτικών ενίσχυσης της εσωτερικής διαρροής προκειμένου να ανιχνεύουν καταστάσεις και να τις λύνουν πριν αυτές καταστρέψουν τη φήμη τους (ACC, 2016; Kenny et al, 2019; Transparency International, 2019).

Η διαρροή πληροφοριών έχει αναγνωριστεί ως ένας αποτελεσματικός τρόπος αποκάλυψης και περιορισμού της διαφθοράς (ACFE, 2018; Devine, 2012). Στην έκθεσή της το 2014 η Διεθνής Ένωση Ελέγχου της Διαφθοράς (ACFE), υποστηρίζει ότι οι μάρτυρες δημοσίου συμφέροντος είναι η πιο αποτελεσματική πηγή εντοπισμού εγκληματικής συμπεριφοράς στους χώρους εργασίας².

Η αποκάλυψη παράνομων, ανήθικων ή παράτυπων πράξεων από τους ανθρώπους που λόγω της θέσης τους έχουν τη δυνατότητα να τις γνωρίζουν είναι μια από τις πιο σημαντικές, αν όχι

η σημαντικότερη, διαδικασία μέσω της οποίας οι κυβερνήσεις και οι επιχειρήσεις λογοδοτούν για τις πράξεις τους στους πολίτες. (Lewis et al, 2014) Μία έρευνα στη Μεγάλη Βρετανία η οποία εξέτασε τις περιπτώσεις 1000 whistleblowers, διαπίστωσε ότι η διαδικασία της παροχής πληροφοριών που σχετίζονται με φαινόμενα διαφθορά και ανηθικότητας αποτέλεσε βασικό παράγοντα βελτίωσης της κοινωνικής ζωής της χώρας (Vandekerckhove et al, 2013).

Η αποκάλυψη παράνομων πράξεων έχει μεγαλύτερη αποτελεσματικότητα όταν γίνεται εκτός του οργανισμού, αλλά ενέχει και μεγαλύτερο κίνδυνο αντιποίνων (Dworkin and Baucus, 1998). Έρευνα που πραγματοποιήθηκε στην Αυστραλία έδειξε ότι το μεγαλύτερο μέρος των αποκαλύψεων πραγματοποιήθηκε εντός των οργανισμών και μόνο το 1% των περιπτώσεων έγιναν με την εμπλοκή του τύπου (Brown et al, 2014). Η αποκάλυψη παράνομων ενεργειών μέσω των MME μπορεί να μεγιστοποιεί τις πιθανότητες διακοπής τους, αλλά εκθέτει σε κίνδυνο τους μάρτυρες δημοσίου συμφέροντος, κυρίως λόγω της έλλειψης ισχυρού και ξεκάθਾਰου νομικού πλαισίου για την προστασία των whistleblowers σε πολλές χώρες (Wolfe et al, 2014).

Η τεχνολογία παρουσιάζεται ως καταλύτης στη πραγματοποίηση της επικοινωνίας μεταξύ του επίδοξου πληροφοριοδότη και του δημοσιογράφου. Στο ψηφιακό περιβάλλον οι δυνατότητες ασφαλούς προσέγγισης των δημοσιογράφων από τους whistleblowers πολλαπλασιάζονται. Οι κίνδυνοι που μπορεί να συνοδεύουν οποιαδήποτε διαρροή καθιστούν αναγκαία την πραγματοποίηση της επικοινωνίας μεταξύ δημοσιογράφου και πηγών με απόλυτη μυστικότητα. Η ψηφιακή τεχνολογία, τα τελευταία χρόνια, έχει δημιουργήσει εργαλεία που μπορούν να εγγυηθούν σε μεγάλο βαθμό την αποκάλυψη φαινομένων διαφθοράς και ανηθικότητας, με ταυτόχρονη προστασία της ανωνυμίας της πηγής. Πρόκειται για της πλατφόρμες ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers.

Η παρούσα εργασία εξετάζει το καίριο για τη δημοσιογραφία θέμα της διαρροής πληροφοριών και τις δυνατότητες που δίνει η ψηφιακή τεχνολογία και χωρίζεται σε τέσσερα βασικά κεφάλαια. Στο πρώτο επιχειρείται μια γενική προσέγγιση της έννοιας της διαρροής πληροφοριών και της σημασίας της για το δημοσιογραφικό επάγγελμα. Ιδιαίτερη αναφορά γίνεται στα WikiLeaks, το πρώτο, παγκοσμίου εμβέλειας, εγχείρημα, το οποίο φιλοξένησε πολύ σημαντικές αποκαλύψεις και απέκτησε διεθνές κύρος και αναγνώριση. Η μελέτη της πορείας και του τρόπου που εξελίχθηκε το μέσο και που αντιμετώπισε τη διαρροή

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

πληροφοριών έχει πολύ μεγάλη σημασία για την ιστορική εξέλιξη των πλατφόρμων ασφαλούς επικοινωνίας και οποιαδήποτε προσέγγιση των τελευταίων, χωρίς προηγούμενη μελέτη των WikiLeaks, θα ήταν ελλιπής. Το κεφάλαιο αυτό κλείνει με την παρουσίαση της επίδρασης που είχαν οι αποκαλύψεις του πρώην πράκτορα του National Security Agency των ΗΠΑ Edward Snowden για τη δημιουργία λογισμικού ασφαλούς επικοινωνίας. Ο Edward Snowden δεν ήταν απλώς ένας ακόμη πληροφοριοδότης. Τα γεγονότα που αποκάλυψε δεν αφορούσαν κάποιο ζήτημα εξωτερικής πολιτικής, αλλά προσέβαλαν το κύρος και την αξιοπιστία συνολικά του οικοδομήματος της ψηφιακής επικοινωνίας. Όλα τα συστήματα ψηφιακής επικοινωνίας των πολιτών παγκοσμίως αποδείχτηκαν διάτρητα. Ο κόσμος γενικότερα, αλλά και ο δημοσιογραφικός κόσμος ειδικότερα, μετά το καλοκαίρι του 2013, δεν θα ήταν ποτέ ίδιος. Το κομβικό αυτό γεγονός, ο πιο απρόβλεπτος παράγοντας της σύγχρονης ψηφιακής ιστορίας, έδωσε πολύ μεγάλη δυναμική στην ανάπτυξη των πλατφόρμων ασφαλούς επικοινωνίας.

Το δεύτερο κεφάλαιο επιχειρεί μια παρουσίαση του τεχνικού σκέλους των εργαλείων ασφαλούς επικοινωνίας. Ιδιαίτερη αναφορά γίνεται στην κρυπτογράφηση των δεδομένων, η οποία αποτελεί ακρογωνιαίο λίθο του λογισμικού ασφαλούς επικοινωνίας. Αποφεύγονται τεχνικές λεπτομέρειες, που βρίσκονται εκτός του σκοπού αυτής της εργασίας, αλλά εξηγείται ο τρόπος λειτουργίας των συγκεκριμένων εργαλείων και η σημασία τους για την ασφαλή επικοινωνία. Πρόκειται για τεχνολογίες που προϋπήρχαν των πλατφόρμων και που χρησιμοποιήθηκαν από αυτές για να μπορέσουν να λειτουργήσουν ως εργαλεία ασφαλούς επικοινωνίας.

Στο τρίτο κεφάλαιο, παρουσιάζεται η ιστορική εξέλιξη των πλατφόρμων ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers. Το κεφάλαιο ξεκινά με την παρουσίαση του ιστορικού πλαισίου και συνεχίζει με την παράθεση όλων των, ελάχιστα σημαντικών στην πλειονότητά τους, προσπαθειών πριν και αμέσως μετά την εμφάνιση των WikiLeaks. Το κεφάλαιο ολοκληρώνεται με τις δυο πιο σημαντικές πλατφόρμες, το GlobaLeaks και το θρυλικό SecureDrop, οι οποίες έχουν υιοθετηθεί από δεκάδες μέσα σε ολόκληρο τον κόσμο και έχουν αλλάξει τον τρόπο που πραγματοποιείται η ερευνητική δημοσιογραφία.

Το τέταρτο κεφάλαιο προβάλλει τους κινδύνους που συνήθως έχει η διαρροή πληροφοριών για τον πληροφοριοδότη και όχι μόνο. Ο συστηματικός στιγματισμός του τελευταίου από τον

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

οργανισμό που κατηγορείται για διαφθορά και η άσκηση φυσικής και ψυχολογικής βίας καθιστούν περισσότερο από επιβεβλημένη τη δυνατότητα ασφαλούς επικοινωνίας. Η ζωή δεν είναι η ίδια μετά τη διαρροή για τον whistleblower. Οι πλατφόρμες επιδιώκουν ακριβώς την ολοκλήρωση της διαρροής με επιτυχία, αλλά και τη δυνατότητα του πληροφοριοδότη να διατηρήσει την ανωνυμία του εφ' όσον το επιθυμεί. Οι κίνδυνοι που συνεπάγεται για τον πληροφοριοδότη η αποκάλυψη απόρρητων πληροφοριών καθιστούν τις πλατφόρμες αυτές απαραίτητες.

Η συγκεκριμένη εργασία αποτελεί προσωπική μου επιλογή, η οποία, τολμώ να πω, ότι είχε ήδη γίνει από το πρώτο εξάμηνο του συγκεκριμένου μεταπτυχιακού, όταν πρωτοήρθα σε επαφή με τις πλατφόρμες αυτές. Οι δυσκολίες που αντιμετώπισα οφείλονται κυρίως στην αδυναμία προσέγγισης πανεπιστημιακών βιβλιοθηκών, όπου οι βιβλιογραφικές πηγές είναι πιο προσβάσιμες. Παρόλα αυτά, κατάφερα να αποκτήσω το μοναδικό αγγλόφωνο βιβλίο για το συγκεκριμένο θέμα, το Digital Whistleblowing Platforms for Journalist, του Ιταλού καθηγητή Philip Di Salvo, το οποίο με βοήθησε να καταλάβω πολλά. Οποσδήποτε όποιος επιθυμεί σφαιρική προσέγγιση των εργαλείων ασφαλούς επικοινωνίας για δημοσιογράφους θα το βρει ιδιαίτερα χρήσιμο. Παράλληλα, οι προσπάθειες που έκανα για τοποθέτηση εκπροσώπων των ελληνικών μέσων απέναντι στο ζήτημα της χρήσης των συγκεκριμένων εργαλείων, δεν απέδωσαν καρπούς. Ίσως να ευθύνονται οι ιδιαίτερες συνθήκες που βιώνουμε. Ίσως το θέμα να φαντάζει ουτοπικό για το ισχύον μεντιακό σύστημα, με τα πολλά προβλήματά του. Παρόλα αυτά, οφείλω να ομολογήσω ότι η παρούσα προσπάθεια, που αποτελεί την πιο ολοκληρωμένη δουλειά μου στα πλαίσια του μεταπτυχιακού, ήταν ένα ιδιαίτερα ευχάριστο ταξίδι, που ήθελα πάντα να κάνω. Εύχομαι να αφήσει κάποια γνώση σε αυτούς που θα τη διαβάσουν, από τη συσσωρευμένη γνώση που επέλεξα να παρουσιάσω στις λίγες σελίδες της. Προσδοκία μου είναι να ξεκινήσουν να διδάσκονται οι νέοι δημοσιογράφοι τις τεχνικές ασφαλούς επικοινωνίας στα πανεπιστήμια που φοιτούν.

1. Διαρροή Πληροφοριών και Δημοσιογραφία

Η σχέση μεταξύ whistleblowers και δημοσιογράφων είναι περίπλοκη. Οι μάρτυρες δημοσίου συμφέροντος χρειάζονται τους δημοσιογράφους για να δώσουν δημοσιότητα σε όσα γνωρίζουν και οι δημοσιογράφοι τους μάρτυρες για να τους παρέχουν πληροφορίες που διαφορετικά θα ήταν αδύνατο να έχουν. Παρά την τεράστια επίδραση που μπορεί να έχουν αυτές οι μαρτυρίες στην παραγωγή ειδήσεων, η έρευνα σχετικά με την αξιοποίηση των whistleblowers στη διαδικασία συγκέντρωσης πληροφοριών δεν έχει λάβει ανάλογης προσοχής από τις δημοσιογραφικές σπουδές (Brown et al, 2014).

1.1 Η εξέλιξη του whistleblower

Η εμφάνιση της ψηφιακής τεχνολογίας έχει ένα προφανή αντίκτυπο στη διαδικασία της διαρροής πληροφοριών, διαμορφώνοντας ένα νέο πλαίσιο και αλλάζοντας ουσιαστικά τον τρόπο που αυτή μπορεί να πραγματοποιηθεί. Ο Philip Di Salvo (2020) φέρει ένα ιδιαίτερα εύγλωττο παράδειγμα, συγκρίνοντας δύο εμβληματικούς whistleblowers του 20ου και του 21 πρώτου αιώνα. Ο πρώτος είναι ο Daniel Ellsberg, ο άνθρωπος που, το 1971, έδωσε στη δημοσιότητα την αναφορά έκτασης 7.000 σελίδων, η οποία περιέχει λεπτομερή στοιχεία της αμερικανικής εξωτερικής πολιτικής από το 1945 μέχρι το 1968 και αποδεικνύει την άσκοπη και καταστροφική εμπλοκή των ΗΠΑ στον πόλεμο του Βιετνάμ³. Ο δεύτερος είναι η Chelsea Manning, ο άνθρωπος που, 39 χρόνια αργότερα, έδωσε στα WikiLeaks χιλιάδες αρχεία που αποδεικνύουν, μεταξύ άλλων, τις απάνθρωπες πρακτικές του αμερικανικού στρατού, όπως εν ψυχρώ δολοφονίες αμάχων, στον πόλεμο του Ιράκ το 2007 και του Αφγανιστάν το 2009⁴.

Η αλματώδης εξέλιξη της τεχνολογίας έδωσε δυνατότητες συγκέντρωσης και διάδοσης της πληροφορίας σε ανθρώπους που ως τότε δεν τις είχαν (Benkler, 2011). Ουσιαστικά άλλαξε τα τυπικά χαρακτηριστικά του ανθρώπου που μπορεί να εξελιχθεί σε πληροφοριοδότη.

Ο Daniel Ellsberg ήταν απόφοιτος του Harvard, κάτοχος διδακτορικού διπλώματος στις οικονομικές επιστήμες, σύμβουλος του αμερικανικού Υπουργείου Άμυνας και υψηλόβαθμο στέλεχος του RAND Corporation⁵, του ινστιτούτου που μελετούσε για λογαριασμό της κυβέρνησης των ΗΠΑ την αμερικανική εξωτερική πολιτική από το Δεύτερο Παγκόσμιο Πόλεμο και μετά. Η θέση του αυτή τον έφερε αντιμέτωπο με την αλήθεια που τελικά διέρρευσε

στον τύπο με τα περίφημα Pentagon Papers, αφού πρώτα επί μήνες προσέγγιζε και ενημέρωνε κρατικούς αξιωματούχους της χώρας του, χωρίς ανταπόκριση.

Στον αντίποδα η Chelsea Manning υπήρξε χαμηλόβαθμο στέλεχος του αμερικανικού στρατού, που το 2010 παρέδωσε στα WikiLeaks περισσότερα από 700.000 έγγραφα και αρχεία τα οποία περιείχαν τις ανίερές πρακτικές του αμερικανικού στρατού σε Ιράκ και Αφγανιστάν. Πρόκειται για στοιχεία που αντλήθηκαν από τη βάση δεδομένων SIPRNet του Υπουργείου Άμυνας, στην οποία, σύμφωνα με το BBC (2010), είχαν πρόσβαση περίπου 2,5 εκατομμύρια άνθρωποι.

Η δημιουργία ψηφιακών βάσεων δεδομένων στις οποίες έχουν πρόσβαση χιλιάδες εργαζόμενοι, αλλά κυρίως η ύπαρξη διαύλων όπως τα WikiLeaks έδωσαν και δίνουν τη δυνατότητα σε χαμηλόβαθμα στελέχη του στρατού, των μυστικών υπηρεσιών, του κρατικού μηχανισμού αλλά και των ιδιωτικών επιχειρήσεων να έρχονται αντιμέτωποι με πληροφορίες που χρήζουν, για λόγους δημοσίου συμφέροντος, δημοσιοποίησης και να τις δημοσιοποιούν. Αυτή είναι η ουσιαστικότερη συμβολή των νέων τεχνολογιών στη διαδικασία της διάδοσης της απόρρητης πληροφορίας. Η τεχνολογία πλέον δίνει σε οποιονδήποτε το δικαίωμα να διαρρεύσει στον τύπο, και όχι μόνο, μυστικές πληροφορίες. Ουσιαστικά πολλαπλασιάζει τις πιθανότητες ύπαρξης διαρροών και τις αφαιρεί από μια εργασιακή elite που λόγω θέσης και μόνο, είχε μέχρι πρότινος πρόσβαση σε ευαίσθητες πληροφορίες. Λαμβάνοντας υπ' όψιν ότι τα χαμηλόβαθμα στελέχη, σε οποιοδήποτε χώρο, έχουν πολύ λιγότερα να χάσουν από τα υψηλόβαθμα τα οποία βρίσκονται πιο κοντά στις οικονομικές elite, αντιλαμβανόμαστε ότι οι πιθανότητες διαρροών αυξάνονται με γεωμετρική πρόοδο.

1.2 Wikileaks

Όταν τίθεται το θέμα της διαρροής μυστικών πληροφοριών ως πρακτική, δεν υπάρχει αμφιβολία ότι η νέα ψηφιακή τεχνολογία έχει εφοδιάσει whistleblowers και δημοσιογράφους με νέες στρατηγικές και δυνατότητες. Παράλληλα, δεδομένης της γενικευμένης διαδικτυακής παρακολούθησης, τόσο σε επίπεδο κυβερνήσεων όσο και στο εμπόριο (Snowden, 2019), οι κίνδυνοι έχουν πολλαπλασιαστεί. Η προσέγγιση των νέων δεδομένων που επέφερε η ψηφιοποίηση στη διαρροή μυστικών πληροφοριών, δε μπορεί να ξεκινήσει χωρίς να μελετηθεί ένα μεγάλο μέσο που υπήρξε πρωτοπόρο στο συγκεκριμένο πεδίο και δεν είναι άλλο από τα WikiLeaks. Η εμφάνιση των WikiLeaks, ενός κεφαλαιώδους σημασίας για την ψηφιακή

δημοσιογραφία φαινομένου, από την δημιουργία του παγκόσμιου ιστού (Beckett and Ball, 2012), βρίσκεται στο επίκεντρο πολλών θεμελιωδών ζητημάτων που είναι απολύτως συνυφασμένα με την κατανόηση του τρόπου λειτουργίας των ψηφιακών πλατφόρμων επικοινωνίας των δημοσιογράφων με τους whistleblowers. Ο ρόλος της κρυπτογράφησης, η σχέση μεταξύ δημοσιογραφίας και hacking και η εφαρμογή μεθόδων υποκλοπής ψηφιακών πληροφοριών από δημοσιογράφους βρίσκονται στον πυρήνα αυτής της προσέγγισης (Di Salvo, 2020).

Από την εμφάνισή τους, το 2006, τα WikiLeaks καθιερώθηκαν ως ένας από τους πιο δυναμικούς και ανατρεπτικούς μεντιακούς οργανισμούς που δημιουργήθηκαν στην ψηφιακή εποχή, των οποίων η επιρροή ξεπερνάει τα μέσα ενημέρωσης και τη δημοσιογραφία και αγγίζει περιοχές όπως η διπλωματία, η ασφάλεια, οι διεθνείς σχέσεις και ο νόμος. Στον τομέα της ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers, τα WikiLeaks αντιπροσωπεύουν ένα μοναδικό και πρωτοπόρο παράδειγμα πλατφόρμας ασφαλούς διαρροής πληροφοριών, καθώς είναι το πρώτο μέσο που αξιοποίησε την τεχνολογία για το συγκεκριμένο σκοπό. Για το λόγο αυτό, η όποια προσέγγιση του ζητήματος της ασφαλούς επικοινωνίας στο χώρο της δημοσιογραφίας, θα ήταν ατελής αν δεν λάμβανε υπόψη την παρακαταθήκη που έχουν αφήσει τα WikiLeaks, ήδη από την πρώτη δεκαετία του αιώνα μας, αλλά και στις αρχές της δεύτερης, όταν οι πλατφόρμες ασφαλούς επικοινωνίας δεν είχαν ακόμη διαμορφωθεί και χρησιμοποιηθεί από μέσα ενημέρωσης.

1.2.1 Ο ρόλος των WikiLeaks

Όπως επισημαίνει ο Micah L. Sifry (2011) τα WikiLeaks συνέβαλαν με ποικίλους τρόπους στη διαρροή μυστικών πληροφοριών στον τύπο. Αρχικά, λειτουργούν ως πηγή πληροφοριών για μέσα ενημέρωσης, δημοσιεύοντας πλήθος ανεπεξέργαστων αρχείων. Παράλληλα, παράγουν το δικό τους περιεχόμενο βασιζόμενα στις πηγές και τα στοιχεία που συλλέγουν. Τέλος, η δραστηριότητα ίσως που τα έκανε περισσότερο γνωστά είναι η συνεργασία με μεγάλους διεθνείς δημοσιογραφικούς οργανισμούς, κυρίως έντυπες εφημερίδες της Ευρώπης και των ΗΠΑ, πάνω σε συγκεκριμένα θέματα για τα οποία τα WikiLeaks συγκεντρώνουν το επίμαχο υλικό.

Μετά το 2011, ο Philip Di Salvo προσθέτει άλλες δύο διακριτές λειτουργίες τους. Η μία είναι η συστηματική συνεργασία με τοπικά ΜΜΕ σε ολόκληρο τον κόσμο και η δεύτερη, η αναδημοσίευση σημαντικών πληροφοριών που έχουν ήδη δει το φως της δημοσιότητας σε πιο αδύναμα μέσα και που με την εμφάνισή τους στα WikiLeaks επιδιώκεται η αύξηση της επιρροής που θα επιφέρει η ευρεία διάδοσή τους. Εκείνο που πρέπει να επισημάνουμε είναι ότι οι παραπάνω πρακτικές δεν ακολούθησαν μια χρονολογική σειρά εξέλιξης, αλλά εφαρμόζονται σε όλη τη διάρκεια της πορείας τους κατά περίπτωση. Για παράδειγμα στην εμπλοκή τους στις εκλογές των ΗΠΑ, το 2016, με τη δημοσιοποίηση χιλιάδων emails από τους προσωπικού λογαριασμούς της υποψήφιας προέδρου με την παράταξη των Δημοκρατικών, Hillary Clinton, δεν συνεργάστηκαν με κανένα μεγάλο μέσο, αλλά παρέδωσαν στη δημοσιότητα το υποκλαπέν υλικό από τη σελίδα τους (Di Salvo, 2020).

Με τον ίδιο τρόπο γίνονταν και οι αρχικές δημοσιεύσεις τους, τότε που, άγνωστα ακόμη στο ευρύ κοινό, αποτελούσαν μια πολύτιμη και ανέλπιστη μέχρι τότε δημοσιογραφική πηγή. Ήταν η εποχή που τα wikileaks έδιναν στη δημοσιότητα το υλικό που συγκέντρωναν, χωρίς ιδιαίτερη δημοσιογραφική επεξεργασία και ανάλυση. Η εμπλοκή τους περιοριζόταν κυρίως στην επιβεβαίωση της ορθότητας των πληροφοριών και η πρόθεσή τους ήταν η προσέγγιση των κυρίαρχων μέσων, τα οποία θα έδιναν στο υλικό ευρεία δημοσιότητα (Lynch, 2010). Η πραγματοποίηση του στόχου τους ήταν δεδομένη, ως συνάρτηση της παγκόσμιας σημασίας των πληροφοριών που συνήθως διέρρεαν.

Δύο είναι τα πιο χαρακτηριστικά παραδείγματα εκείνης της εποχής. Η δημοσίευση, το 2007, του απόρρητου στρατιωτικού εγχειριδίου με τίτλο “Camp Delta Standard Operating Procedure”, το οποίο κατέγραφε τις καθημερινές επιχειρήσεις στη στρατιωτική βάση και τις φυλακές του Guantanamo (Singel, 2007). Το δεύτερο παράδειγμα αφορά τα αποκαλυπτικά στοιχεία που έδωσε, το 2008, στη δημοσιότητα η ιστοσελίδα και αποδείκνυαν τη διαφθορά σε υψηλά κλιμάκια του πολιτικού συστήματος στην Κένυα. Τα WikiLeaks κατόρθωσαν να βρουν και να δημοσιεύσουν την έκθεση της Εθνικής Επιτροπής για τα Ανθρώπινα Δικαιώματα με τίτλο “The Cry of Blood - Report on ExtraJudicial Killings and Disappearances”. Τα έγγραφα δημοσιεύτηκαν ανεπεξέργαστα και χωρίς τη συνδρομή άλλων μέσων ενημέρωσης. Παρότι στο μεταξύ η ιστοσελίδα συνεργάστηκε με μεγάλα διεθνή μέσα για την αποκάλυψη σκανδάλων, η παραπάνω τακτική ακολουθήθηκε και στην περίπτωση της δημοσίευσης των emails που υποκλάπηκαν από την υποψήφια των Δημοκρατικών στις εκλογές του 2016, Hillary Clinton.

Η δημοσίευση αφορούσε 9.252 emails και 8.032 επισυναπτόμενων αρχείων, τα οποία παρουσιάστηκαν από τη σελίδα αυτούσια, χωρίς επεξεργασία.

1.2.2 Η περίπτωση του Collateral Murder

Το 2010, τα WikiLeaks δημοσιοποίησαν το πιο κραυγαλέο μέχρι τότε θέμα, το οποίο είχε να κάνει με τις εγκληματικές πρακτικές του αμερικανικού στρατού, εναντίων αμάχων, σε Ιράκ και Αφγανιστάν. Η δημοσιοποίηση περιλάμβανε και οπτικό υλικό, γεγονός που προσ αύξησε την αξία των αποκαλύψεων. Ήταν όμως και η χρονιά που έκαναν το μεγάλο βήμα προς μια πιο δημοσιογραφική προσέγγιση, καθώς η παγκόσμια σημασία των γεγονότων που αποκάλυπταν, ακύρωνε εκ των πραγμάτων την αποστασιοποιημένη δημοσιοποίηση των ανεπεξέργαστων δεδομένων. Αρχικά ήταν η ύπαρξη 700.000 απόρρητων εγγράφων του στρατού των ΗΠΑ, τα οποία η Chelsea Manning διοχέτευσε στα WikiLeaks. Παράλληλα, μεταξύ αυτών υπήρξε το αποκαλυπτικό βίντεο, που δείχνει την εν ψυχρώ δολοφονία δώδεκα αμάχων, συμπεριλαμβανομένων και των δημοσιογράφων του πρακτορείου Reuters, Namir Noor Eldeen και Saeed Chmagh, στις 12 Ιουλίου του 2007, από μέλη του αμερικανικού στρατού, στο πλαίσιο εναέριων επιθέσεων στα περίχωρα της Βαγδάτης. Τα WikiLeaks τιτλοφορούν τη δημοσίευση “Collateral Murder”, δηλαδή παράπλευρη δολοφονία.

Για πρώτη φορά παίρνουν σαφή θέση απέναντι στα γεγονότα, όχι μόνο μέσω του καυστικού τους τίτλου, αλλά και γιατί όπως σημειώνουν στη σελίδα τους, για τα δύο βίντεο 39 και 18 λεπτών που δημοσίευσαν εργάστηκε πλήθος εθελοντών, ορισμένοι εκ των οποίων ταξίδεψαν στην Βαγδάτη και συνομίλησαν με τους συγγενείς των δολοφονηθέντων. Τα WikiLeaks δεν περιμένουν τα κυρίαρχα media να τοποθετήσουν τα στοιχεία στο κατάλληλο πλαίσιο. Παίρνουν για πρώτη φορά θέση και κάνουν την πληροφορία είδηση. Η υπόθεση “Collateral Murder” αποτελεί σημείο αναφοράς στην πορεία των WikiLeaks, καθώς πρόκειται για μια κεφαλαιώδους σημασίας δημοσιογραφική επιτυχία η οποία έθεσε τα θεμέλια της διεθνούς αναγνώρισής τους (Beckett and Ball, 2012; Christensen, 2014; Dunn, 2013).

1.2.3 Η περίπτωση των MegaLeaks

Στο δεύτερο μισό του 2010 τα WikiLeaks άρχισαν την πιο ογκώδη διαρροή μεγαδεδομένων - MegaLeaks - στην ιστορία τους. Πρόκειται για το “Afghan War Diary”, που περιλαμβάνει 90.000 απόρρητα έγγραφα σχετικά με τον πόλεμο στο Αφγανιστάν, το “Iraqi War Logs” με 400.000 αρχεία που αφορούν τις συγκρούσεις στο Ιράκ και το “Cablegate”, το οποίο περιλαμβάνει 250.000 διπλωματικά τηλεγραφήματα των ΗΠΑ (Madar 2013). Το παραπάνω εγχείρημα όμως δεν χαρακτηρίζεται μόνο από την ποσότητα των δεδομένων που διέρρευσε η ιστοσελίδα, αλλά και από τη συνεργασία της με μεγάλους δημοσιογραφικούς οργανισμούς σε Ευρώπη και ΗΠΑ. Η σύμπραξη των WikiLeaks με τον Guardian, τους New York Times, την Der Spiegel και την El Pais αποτελεί ένα από τα πρωτοπόρα project συνεταιρικής, ψηφιακής, ερευνητικής δημοσιογραφίας και ένα από τα πιο αντιπροσωπευτικά και πρώιμα παραδείγματα δημοσιογραφίας δεδομένων (Baack, 2013; Splendore et al, 2015).

1.2.4 Νέες τάσεις

Η πρώτη αυτή συνεργασία των WikiLeaks με ορισμένες από τις μεγαλύτερες εφημερίδες του δυτικού κόσμου διαμόρφωσε νέα δεδομένα, που διαποτίζουν έκτοτε τη σύγχρονη ερευνητική δημοσιογραφία. Η συνεργασία μέσω ενημέρωσης από διαφορετικές γωνίες του πλανήτη στη βάση του διαδικτυακού διαμοιρασμού ψηφιακού υλικού, όπως στην περίπτωση των Panama Papers και των Paradise Papers, συμβαίνει για πρώτη φορά (Di Salvo, 2020).

Παράλληλα, η σύμπραξη δεν αφορούσε μόνο τη συνεργασία μέσω ενημέρωσης από διαφορετικές χώρες, αλλά την προσέγγιση διαφορετικών, εκ φύσεως, μεντιακών οργανισμών. Από τη μια είναι ένα καινοτόμο, αντισυμβατικό μέσο και από την άλλη ορισμένα από τα πλέον παραδοσιακά και κυρίαρχα ΜΜΕ. Επιπροσθέτως, η συγκεκριμένη συνεργασία έδωσε σαφή ώθηση στη διαδικτυακή δημοσιογραφία καθώς το υλικό είναι μόνο σε ψηφιακή μορφή και διακινείται αποκλειστικά μέσω του διαδικτύου.

Μια ακόμη αναμφισβήτητη καινοτομία που εισήγαγαν τα WikiLeaks είναι η εμφάνιση αυτού που συνηθίσαμε να αποκαλούμε δημοσιογραφία δεδομένων, καθώς, ο μεγάλος όγκος του υλικού προς μελέτη απέδειξε την αναγκαιότητα διερεύνησης μεγάλων βάσεων δεδομένων και δημιούργησε την ανάγκη διαμόρφωσης νέων εργαλείων δημοσιογραφικής έρευνας. Οι μεγάλοι

δημοσιογραφικοί οργανισμοί έχουν ήδη αντιληφθεί τη σπουδαιότητα του συγκεκριμένου εργαλείου και έχουν δημιουργήσει τμήματα επεξεργασίας δεδομένων. Σε αυτό το πλαίσιο τα WikiLeaks προχώρησαν και σε μια ακόμη καινοτομία. Δημοσίευσαν έγγραφα και αρχεία, τα οποία είχαν μεν δημοσιοποιηθεί, αλλά χωρίς να είναι ιδιαίτερα χρηστικά για το κοινό. Χαρακτηριστικό παράδειγμα είναι τα “Kissinger Cables”, τα οποία περιλάμβαναν περίπου 1,7 εκατομμύρια έγγραφα από το 1973 έως το 1976, τα οποία ψηφιοποιήθηκαν από τα WikiLeaks, το 2013, και έγιναν προσβάσιμα για ηλεκτρονική αναζήτηση με λέξεις κλειδιά.

Η χρήση μεθόδων ηλεκτρονικής υποκλοπής, κατευθείαν από το μέσο ενημέρωσης, είναι μια ακόμη κατάκτηση των WikiLeaks. Το χακάρισμα, το 2012, πέντε εκατομμυρίων emails από την αμερικανικό όμιλο μυστικών υπηρεσιών Stratfor, ο οποίος δραστηριοποιείται στον τομέα της εξωτερικής πολιτικής, γνωστό ως “The Global Intelligence Files”, είναι η πρώτη μεγάλη δημοσιογραφική επιτυχία που βασίζεται σε μεθόδους ηλεκτρονικής υποκλοπής μυστικών πληροφοριών από μέσο ενημέρωσης.

Η μεγαλύτερη όμως, ίσως, παρακαταθήκη στη σύγχρονη ερευνητική δημοσιογραφία, αλλά και στις σύγχρονες δημοκρατίες γενικότερα, είναι η απόδειξη της δυνατότητας ενός μικρού μέσου να αλλάζει την ημερήσια ειδησεογραφία και να ορίζει εκείνο την πρώτη είδηση, με μοναδικό εργαλείο την τεχνολογία και ιδιαίτερα την τεχνολογικά υποβοηθούμενη προσέγγιση whistleblowers. Αυτές οι τεχνολογικές δυνατότητες αξιοποιήθηκαν κατάλληλα από τα WikiLeaks διαμορφώνοντας, για πρώτη φορά, μια πλατφόρμα ασφαλούς επικοινωνίας μεταξύ του πομπού και του δέκτη. Η ασφάλεια έγκειται σε δύο πυλώνες. Ο πρώτος έχει να κάνει με τη χρήση της τεχνολογίας περιήγησης στο διαδίκτυο Tor, η οποία δεν αφήνει ψηφιακά ίχνη και έτσι δεν είναι δυνατό να εντοπιστεί ο whistleblower. Ο δεύτερος πυλώνας έχει να κάνει με την περίφημη κρυπτογράφηση, το πολύτιμο αυτό εργαλείο που παρέχει η ψηφιοποίηση των δεδομένων (Lynch, 2010; Bosua et al, 2014). Η κρυπτογράφηση των πληροφοριών αποτρέπει την πιθανή παρακολούθηση, κατά τη διαδικασία διακίνησής τους μέσω διαδικτύου. Δεν αρκεί να μένουν κρυφά τα υποκείμενα της επικοινωνίας, δηλαδή ο δημοσιογράφος και ο whistleblower, αλλά και να μη μπορεί να εντοπιστεί η διαδρομή κατά τη μετάδοσή της μέσω του διαδικτύου. Οι επικών διαστάσεων αποκαλύψεις που έκανε ο πρώην μυστικός πράκτορας του NSA Edward Snowden, το 2013, προσαύξησαν τη σημασία της κρυπτογράφησης και απέδειξαν την αναγκαιότητά της όχι μόνο στη δημοσιογραφική πρακτική, αλλά σε όλες τις

εκφάνσεις της χρήσης του διαδικτύου στο πλαίσιο της προσωπικής και επαγγελματικής δραστηριότητας των πολιτών (Hellegren, 2017).

1.3 Η ιστορική πράξη του Edward Snowden

Οι αποκαλύψεις, το 2013, του μέχρι τότε υπαλλήλου των μυστικών υπηρεσιών του National Security Agency (NSA) των ΗΠΑ, Edward Snowden, σχετικά με τις εκτεταμένες παρακολουθήσεις εκατομμυρίων πολιτών σε Αμερική και Ευρώπη από την κυβέρνηση των Ηνωμένων Πολιτειών, αποτέλεσαν το σημείο τομής της σύγχρονης ερευνητικής δημοσιογραφίας. Η τοποθέτηση του Edward Snowden στο τιμόνι του ιδρύματος Freedom of the Press Foundation, λίγα χρόνια αργότερα, αποτελεί την ηθική δικαίωση του πρώην πράκτορα, αλλά και την αναγνώριση της σημασίας της σπουδαίας και εξόχως επικίνδυνης πράξης του για την άσκηση του δημοσιογραφικού λειτουργήματος. Όπως χαρακτηριστικά επισημαίνει ο Philip Di Salvo, η υπόθεση Σνόουντεν έχει εμπνεύσει έναν εκ βάθρων επαναπροσδιορισμό της ισορροπίας μεταξύ κρατικής εξουσίας, τεχνολογίας και πολιτικής. Στον πυρήνα αυτής της συζήτησης βρίσκεται η ρόλος της παρακολούθησης που πραγματοποιούν τα κράτη, οι κίνδυνοι που ενέχει, οι καταχρήσεις και οι κοινωνικές προεκτάσεις για τη δημοσιογραφική δουλειά και τις δημοκρατικές διαδικασίες (Di Salvo 2020).

Η μελέτη των επιδράσεων της υπόθεσης Snowden στη δημοσιογραφία λαμβάνει ποικίλες διαστάσεις. Η πρώτη έχει να κάνει με τις πιθανές τρομακτικές επιδράσεις της στην άσκηση του δημοσιογραφικού επαγγέλματος. Η δεύτερη αφορά την αναγκαιότητα χρήσης ισχυρότερων και ασφαλέστερων επικοινωνιακών εργαλείων για δημοσιογράφους και whistleblowers. Η τρίτη περιλαμβάνει τις συνέπειες που μπορεί να έχει η, δια του τύπου και με τη συμμετοχή των whistleblowers, διαρροή μυστικών πληροφοριών (Di Salvo, 2020).

Η διαδικτυακή παρακολούθηση έχει καταγραφεί ως μια από τις πιο σοβαρές σύγχρονες απειλές για το δημοσιογραφικό επάγγελμα (Lyon, 2015; Simon, 2015), παράλληλα με άλλους ψηφιακούς κινδύνους όπως το hacking και η υποκλοπή δεδομένων, το κλείδωμα λογαριασμών, η καταστροφή προγραμμάτων και πολλές άλλες μορφές διαδικτυακών απειλών (Thorsen, 2019). Οι τρομακτικές επιδράσεις που επέφερε η αποκάλυψη των μαζικών παρακολουθήσεων από την αμερικανική κυβέρνηση, συνοψίζονται, το 2014, στην έκθεση των μη κερδοσκοπικών

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

οργανώσεων American Civil Liberty Union και Human Rights Watch, η οποία μέσα από πλήθος συνεντεύξεων σε Αμερικανούς δημοσιογράφους, αποκαλύπτει πως η υπόθεση Snowden άλλαξε τον τρόπο παραγωγής των ειδήσεων (ACLU and HRW, 2014). Σύμφωνα με τις παραπάνω τοποθετήσεις, καθίσταται πλέον εξαιρετικά επισφαλής η προσέγγιση κρατικών αξιωματούχων ή απλών υπαλλήλων, οι οποίοι έχουν και θέλουν να διαρρεύσουν σημαντικές πληροφορίες. Η καθολική παρακολούθηση από τις μυστικές υπηρεσίες δεν είναι απλά ένας αποτρεπτικός παράγοντας, αλλά η ακύρωση οποιασδήποτε τέτοιας πρόθεσης.

2. Ψηφιακή Τεχνολογία και Δημοσιογραφία

Οι αποκαλύψεις Snowden έδειξαν ότι τα κοινά μέσα διαδικτυακής επικοινωνίας δεν μπορούν να εγγυηθούν επαρκή επίπεδα εμπιστευτικότητας στην εποχή των μαζικών ψηφιακών παρακολουθήσεων (O'Brien, 2015; Simon, 2015). Οι δημοσιογράφοι θα πρέπει να επαναπροσδιορίσουν τους τρόπους που χρησιμοποιούν το διαδίκτυο και προσεγγίζουν τις πηγές τους. Ο παγκόσμιος ιστός, στη μετά Snowden εποχή, δεν είναι ένας χώρος ελευθερίας, αλλά παγκόσμιας παρακολούθησης (Beaude, 2016). Η λύση μπορεί να δοθεί από το ίδιο μέσο που επέτρεψε τη μαζική παρακολούθηση, την τεχνολογία. Τα εργαλεία κρυπτογράφησης της πληροφορίας και οι πρακτικές ασφαλούς διακίνησής της μπορούν να δώσουν στους δημοσιογράφους τη δυνατότητα ασφαλούς διαδικτυακής επικοινωνίας με τις πηγές τους.

2.1 Κρυπτογράφηση

Ο Geert Lovink δίνει έναν, ιδιαίτερα εύστοχο, θεωρητικό ορισμό της κρυπτογράφησης των διαδικτυακών πληροφοριών. “Όπως ο Jean Francois Blanchette έχει πρόσφατα επισημάνει, η κρυπτογράφηση είναι μια μορφή επικοινωνίας που συμβαίνει παρουσία των αντιπάλων. Αλλά είναι και κάτι παραπάνω από τη διαρροή μυστικών. Δεν είναι απλά ένας ψίθυρος. Είναι περισσότερο η ιδιωτικότητα σε συνθήκες συνωστισμού, παρουσία των άλλων. Μπορούμε να μιλάμε για μια ιδιωτικότητα σε έναν κόσμο που χαρακτηρίζεται από ανοιχτή επικοινωνία.” (2016).

Σε έναν πιο τεχνικό ορισμό, ο δημοσιογράφος και χάκερ Micah Lee ορίζει την κρυπτογράφηση ως τη διαδικασία όπου ένα κείμενο και ένα τυχαία επιλεγμένο κλειδί συνδυάζονται με μαθηματικούς υπολογισμούς και δίνουν μια κωδικοποιημένη μορφή του κειμένου. Η αποκρυπτογράφηση είναι η διαδικασία κατά την οποία το κωδικοποιημένο κείμενο και το κλειδί υπόκεινται στους αντίστροφους μαθηματικούς υπολογισμούς μέχρι το κείμενο να επανέλθει στην αρχική του μορφή (2013).

Το πρόβλημα το παρουσιάζει ιδιαίτερα εύγλωττα η ερευνήτρια δημοσιογράφος Julia Angwin, πρώην συντάκτης στο ProPublica και νυν αρχισυντάκτρια και ιδρυτικό μέλος του Markup. “Το να κρατάς μυστικά είναι πολύ πιο δύσκολο σήμερα, που σχεδόν κάθε μορφή επικοινωνίας, από τα emails, τις τηλεφωνικές κλήσεις και τα γραπτά μηνύματα, μέχρι την εκ του σύνεγγυς

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

επικοινωνία, μπορούν να αφήσουν ένα ψηφιακό αποτύπωμα, το οποίο δύναται να δώσει στοιχεία σε μια πιθανή έρευνα. Πιστεύω ότι οι δημοσιογράφοι πρέπει να συνεχίζουν να κρατούν μυστικά, παρά τις προκλήσεις. Παραδέχομαι ότι μοιάζει οξύμωρο να μιλάμε για διαφύλαξη μυστικότητας στο δημοσιογραφικό επάγγελμα όταν η δουλειά μας είναι να αποκαλύπτουμε μυστικά. Όμως, παραδόξως, συχνά οι δημοσιογράφοι χρειάζονται μυστικότητα για να μπορέσουν να διαφυλάξουν την διαφάνεια” (2017).

Αναλύοντας την επίδραση των παρακολούθησεων στη δημοσιογραφία, μέσα από το πρίσμα της υπόθεσης Snowden, διαπιστώνουμε ότι η χρήση των εργαλείων κρυπτογράφησης αποτελεί μονόδρομο για την επιβίωση της λεγόμενης τέταρτης εξουσίας (Ruby et al, 2017). Η χρήση μεθόδων προστασίας της διακινούμενης πληροφορίας συνδέεται άρρηκτα με την ελευθερία του τύπου, την εποχή της εκτεταμένης διαδικτυακής παρακολούθησης (Tsui and Lee, 2019). Καθώς τα δεδομένα γίνονται ευάλωτα σε αυθαίρετη πρόσβαση είτε κατά τη διαβίbasή τους μέσω του διαδικτύου (μεταξύ δημοσιογράφου και πληροφοριοδότη) ή κατά την αποθήκευσή τους σε μια συσκευή που συνδέεται με τον παγκόσμιο ιστό (Phillips, 2001) και με δεδομένο τον προφανή κίνδυνο που θέτει η ψηφιακή παρακολούθηση στη δημοσιογραφική πρακτική, τα εργαλεία κρυπτογράφησης έχουν καταστεί απαραίτητα για τους δημοσιογράφους που θέλουν να προστατεύσουν τις πηγές και τη δουλειά τους (Di Salvo, 2020).

Στον απόηχο των αποκαλύψεων Snowden, η συζήτηση για τη χρήση των δυνατοτήτων που παρέχει η τεχνολογία κρυπτογράφησης στη δημοσιογραφική πρακτική κορυφώνεται, καθώς αυτά τα εργαλεία είναι, στην πραγματικότητα, οι λύσεις για “να αποφύγουμε, να μπλοκάρουμε, να αλλοιώσουμε και να σπάσουμε την παρακολούθηση” (Schneier, 2015). Στην εποχή μας, πολλοί δημοσιογραφικοί οργανισμοί ή Μη Κερδοσκοπικές Οργανώσεις που δραστηριοποιούνται στο πεδίο της πληροφορίας και των ψηφιακών δικαιωμάτων έχουν εκδώσει κατευθυντήριες γραμμές και οδηγίες σχετικά με το πώς οι δημοσιογράφοι μπορούν να αξιοποιήσουν την κρυπτογράφηση. Από τα πιο ολοκληρωμένα εγχειρίδια είναι αυτό του αμερικάνικου ιδρύματος Freedom of the Press Foundation, το οποίο έχει συνταχθεί από το δημοσιογράφο και hacker Mical Lee (2013). Ιδιαίτερα χρήσιμες πληροφορίες παρέχει και το εγχειρίδιο του βρετανικού ιδρύματος Centre for Investigative Journalism, το οποίο καταρτίστηκε από τους δημοσιογράφους και hackers Silkie Carlo και Arjen Kamphuis (2014). Παράλληλα, η UNESCO έχει εκδώσει μια Λευκή Βίβλο σχετικά με τις ψηφιακές απειλές που οι δημοσιογράφοι αντιμετωπίζουν, η οποία βασίζεται σε διεθνή έρευνα (Henrichsen et al,

2015). Αντίστοιχα εγχειρίδια έχουν εκδώσει και ορισμένα πανεπιστημιακά ιδρύματα, όπως το Tow Center for Digital Journalism του πανεπιστημίου της Κολούμπια (McGregor, 2014). Όλα τα παραπάνω διατίθενται στο διαδίκτυο δωρεάν.

Λίγη έκπληξη προκαλεί το γεγονός ότι αυτές οι εκδόσεις ξεκίνησαν αμέσως μετά τις αποκαλύψεις Snowden, που έδωσαν την αφορμή για μια παγκόσμια συζήτηση σχετικά με την ιδιωτικότητα, την ασφάλεια και την ανωνυμία, η οποία έχει επίδραση σε πολίτες, κυβερνήσεις και δημοσιογράφους (Thorsen, 2019). Τα παραπάνω εγχειρίδια προσφέρουν μια εισαγωγή στις μεθόδους ασφαλούς επικοινωνίας και προστασίας των πηγών, σε δημοσιογράφους που δεν έχουν ιδιαίτερη εκπαίδευση στον τομέα. Η εξατομικευμένη εκπαίδευση σε θέματα ψηφιακής ασφάλειας είναι επιβεβλημένη, καθώς πάρα πολύ λίγα εκπαιδευτικά ιδρύματα περιλαμβάνουν στο πρόγραμμά τους μαθήματα σχετικά με τις τεχνολογίες και τις δυνατότητες κρυπτογράφησης, ακόμη και στις ΗΠΑ (Kirchner, 2013; Henrichsen et al, 2015).

2.2 Εργαλεία Ασφαλούς Επικοινωνίας

Οι αποκαλύψεις του Edward Snowden έδωσαν το έναυσμα για τη μετάβαση της ερευνητικής δημοσιογραφίας σε μια νέα εποχή. Μπορεί τα WikiLeaks να είχαν είδη προετοιμάσει το έδαφος για την τεχνολογικά υποβοηθούμενη διαρροή πληροφοριών, αλλά η συνειδητοποίηση της σκόπιμης, μαζικής παρακολούθησης από τις κυβερνήσεις, όλων των μέσων διαπροσωπικής επικοινωνίας προκάλεσε ιδιαίτερο προβληματισμό στο δημοσιογραφικό κόσμο και την ανάγκη διασφάλισης του απορρήτου της επικοινωνίας τους, τουλάχιστον σε επίπεδο πηγών. Πολλά εργαλεία κρυπτογράφησης υπήρχαν ήδη από τον περασμένο αιώνα, αλλά η υπόθεση Snowden αποτέλεσε κομβικό σημείο στην αξιοποίηση από τους. Παρακάτω παρατίθενται τα πιο γνωστά και χρηστικά εργαλεία ασφαλούς χρήσης των μεθόδων ψηφιακής επικοινωνίας, έτσι όπως έχουν διαμορφωθεί τα τελευταία χρόνια. Πρόκειται για τεχνολογίες που διαρκώς εξελίσσονται, ανάλογα με τις νέες δυνατότητες της ψηφιακής σφαίρας και σε συνάρτηση με τις καινούριες απαιτήσεις που προκύπτουν στη σύγχρονη δημοσιογραφική πρακτική.

2.2.1 Tor



Ο πλοηγτής Tor είναι ένα λογισμικό που επιτρέπει στους χρήστες να σερφάρουν στο διαδίκτυο χωρίς να αφήνουν ίχνη, με βασικότερο εκείνο της IP τους, η οποία μαρτυρά την τοποθεσία του χρήστη. Το δίκτυο Tor αποτελείται από 3.600 servers εθελοντών οι οποίοι αποκαλούνται κόμβοι.

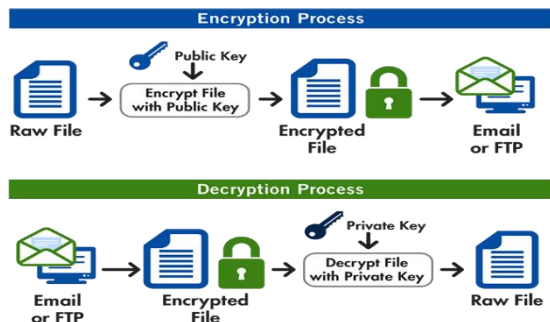
Όταν κάποιος πλοηγείται στο internet δια μέσου του Tor, η σύνδεση αναπηδά μεταξύ ορισμένων από αυτούς τους κόμβους μέχρι να καταλήξει στον προορισμό της. Οποιαδήποτε παρακολούθηση έχει ως αποτέλεσμα να λαμβάνεται ως αφετηρία ο τελευταίος κόμβος. Με αυτό τον τρόπο η παρακολούθηση της πλοήγησης μέσω του Tor καθίσταται άχρηστη (Lee, 2013).

Ο Tor λειτουργεί σαν ένας εμπορικός πλοηγτής όπως ο Chrome, αλλά βασίζεται στο δικό του δίκτυο για να αποπροσανατολίσει τα μεταδεδομένα που αφορούν την IP του χρήστη και έτσι να είναι ιδιαίτερα δύσκολο αυτός να εντοπιστεί. Χρησιμοποιείται από δημοσιογράφους, ακτιβιστές και πολίτες, σε όλο τον κόσμο, προκειμένου να παρακάμπτουν τη λογοκρισία και το διαδικτυακό φιλτράρισμα και να φτάνουν σε λογοκριθέν διαδικτυακό περιεχόμενο. Η χρήση του σε περιοχές όπου μαστίζονται από απολυταρχικά καθεστώτα αποδεικνύει τη σημασία του για τη λειτουργία της δημοκρατίας.

Το πρόγραμμα Tor παρόλα αυτά δεν είναι μόνο ένας πλοηγτής. Είναι παράλληλα ένα λογισμικό για ανώνυμη φιλοξενία ιστοσελίδων. Για παράδειγμα, το δίκτυό του διαθέτει κρυμμένες υπηρεσίες από servers που δεν είναι ορατοί στο λοιπό διαδίκτυο και δεν μπορούν να ανιχνευτούν. Είναι το γνωστό Darknet (Hellegren, 2017). Οι κρυμμένες υπηρεσίες είναι μέρος αυτού που αποκαλούμε βαθύ διαδίκτυο και παίζουν σημαντικό ρόλο στη λειτουργία των ψηφιακών πλατφόρμων ασφαλούς επικοινωνίας. Παράλληλα, το σκοτεινό διαδίκτυο αποτελεί βασικό εργαλείο παροχής δημοσιογραφικών υπηρεσιών, καθώς κορυφαίοι δημοσιογραφικοί οργανισμοί, όπως το ProPublica και οι New York Times παρέχουν τις ψηφιακές τους υπηρεσίες και μέσω ξεχωριστής σελίδας τους στο δίκτυο Tor, για εκείνους τους χρήστες που δίνουν ιδιαίτερη βαρύτητα στη διατήρηση της ανωνυμίας τους κατά την διαδικτυακή τους ενημέρωση. Ο προγραμματιστής του ProPublica, Mike Tigas, εξηγεί ότι: “Οι αναγνώστες μας δεν θα έπρεπε ποτέ να ανησυχούν ότι κάποιος τους παρακολουθεί κατά το ξεφύλλισμα του

διαδικτυακού τόπου μας. Για αυτό είμαστε διαθέσιμοι μέσω των κρυμμένων υπηρεσιών του Tor (2016).

2.2.2 Pretty Good Privacy

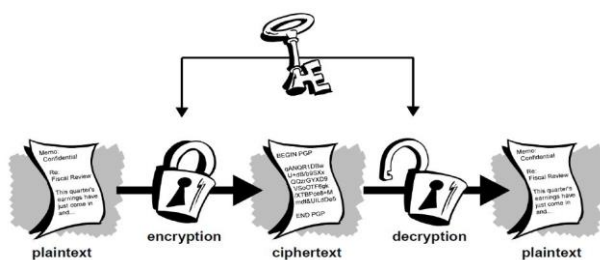


Εικόνα 2 <https://www.freecodecamp.org/news/how-does-pretty-good-privacy-work-3f5f75ecae97/>

Το πρόγραμμα Pretty Good Privacy (PGP) επιτρέπει την αποστολή και λήψη κρυπτογραφημένων emails μεταξύ πομπού και δέκτη, βασιζόμενο στην κρυπτογράφηση με συνδυασμό ενός συμμετρικού μυστικού κλειδιού και ενός ασύμμετρου δημόσιου (Rhee,

2003). Η αρχή της απ' άκρου εις άκρον κρυπτογράφησης κάνει τα μηνύματα που στέλνονται με PGP αδύνατον να διαβαστούν από οποιονδήποτε άλλο εκτός από τον αποστολέα και τον αποδέκτη, οι οποίοι διαθέτουν το αντίστοιχο κλειδί. Κατά την μεταβίβασή τους τα κρυπτογραφημένα emails εμφανίζονται με τη μορφή αλληλουχίας γραμμάτων ή αριθμών η οποία δεν έχει νόημα. Η μέθοδος PGP δημιουργήθηκε το 1991, από τον κρυπτογράφο Phil Zimmerman, και διατίθεται δωρεάν στο <https://gnupg.org>. Σήμερα, παρότι για κάποιους μελετητές είναι ξεπερασμένο (Franceschi – Bicchierai, 2015), το PGP είναι το βασικό λογισμικό κρυπτογράφησης email και χρησιμοποιείται από δημοσιογράφους, για την ασφαλή επικοινωνία τους με πηγές και επαφές μέσω του ηλεκτρονικού ταχυδρομείου. Η κρυπτογράφηση ωστόσο αφορά μόνο το περιεχόμενο της αλληλογραφίας, αφήνοντας ανεπηρέαστα τα μεταδεδομένα της επικοινωνίας, όπως η ταυτότητα του αποστολέα και του παραλήπτη.

2.2.3 Off the Record

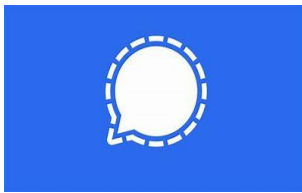


Εικόνα 3 <https://blog.securegroup.com/otr-encryption-for-chat-explained>

Το Off the Record (OTR) είναι ένα πλαίσιο κρυπτογράφησης που μπορεί να τοποθετηθεί σε οποιοδήποτε πρόγραμμα ανταλλαγής στιγμιαίων μηνυμάτων (Lee, 2013). Όπως το PGP, το OTR βασίζεται σε

ένα δημόσιο κλειδί και μπορεί να χρησιμοποιηθεί μέσω ενός software όπως το Adium ή το Pidgin. Το OTR επιτρέπει την ανταλλαγή άμεσων μηνυμάτων υπό την προστασία της κρυπτογράφησης που προστατεύει το περιεχόμενο της επικοινωνίας. Είναι ιδιαίτερα χρήσιμο εργαλείο για τους δημοσιογράφους που συχνά, στη διάρκεια μιας έρευνας χρειάζεται να επικοινωνούν άμεσα με τις πηγές τους ή με άλλους ανθρώπους, χωρίς να ανησυχούν για την παρακολούθηση των συνομιλιών τους. Δημιουργήθηκε το 2004 από τους Nikita Borisov, Avrum Goldberg και Eric A. Brewer, σε μια προσπάθεια βελτίωσης του PGP το οποίο αφορά μόνο την επικοινωνία μέσω emails. Το OTR παρότι είναι ιδανικό για άμεση επικοινωνία μεταξύ δύο μερών, δεν επιτρέπει τη συμμετοχή περισσότερων χρηστών ταυτόχρονα και δεν είναι κατάλληλο για τη μεταφορά δεδομένων video και ήχου.

2.2.4 Signal



Εικόνα 4 <https://signal.org/el/#signal>

Το Signal είναι ίσως η πλέον διαδεδομένη εφαρμογή ασφαλούς επικοινωνίας για κινητά τηλέφωνα, η οποία είναι κατάλληλη για Android και iOS. Επιτρέπει την πραγματοποίηση τηλεφωνικών κλήσεων και ανταλλαγής μηνυμάτων, μέσα από ένα πλαίσιο αυστηρούς κρυπτογράφησης. Είναι η εφαρμογή που χρησιμοποιεί, σύμφωνα με τα λεγόμενά του, ο Edward Snowden⁶. Το Signal δημιουργήθηκε από το Open Whisper System, ένα μη κερδοσκοπικού χαρακτήρα οργανισμό παραγωγής λογισμικού, ο οποίος διευθύνεται από τον Moxie Marlinspike (Rosenblum, 2016). Το Signal διακρίνεται για τον εξαιρετικά μικρό όγκο μεταδεδομένων και πληροφοριών που συγκεντρώνει από τους χρήστες (Farivar, 2016).

2.2.5 Tails



Εικόνα 5 <https://9to5linux.com/tails-4-6-anonymous-linux-os-adds-support-for-u2f-usb-security-keys>

Το Tails είναι ένα φορητό πλήρες λειτουργικό σύστημα που έχει σχεδιαστεί με γνώμονα την αυστηρή ιδιωτικότητα. Μπορεί να τρέξει σε οποιοδήποτε μηχάνημα, από ένα USB, ένα DVD ή μια κάρτα SD. Με αυτό τον τρόπο ο χρήστης μπορεί να κάνει χρήση οποιουδήποτε υπολογιστή χωρίς να αφήσει κανένα ίχνος στο συγκεκριμένο μηχάνημα και

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

αφαιρώντας τη φορητή συσκευή, ο υπολογιστής μοιάζει ανέγγιχτος. Το Tails ενεργοποιεί όλες τις δυνατότητες που δίνει η τεχνολογία της κρυπτογράφησης προκειμένου να ελαττώσει την πιθανότητα εναπόθεσης ψηφιακού ίχνους. Μπορεί να χρησιμοποιηθεί για τη διαχείριση ιδιαίτερα ευαίσθητων πληροφοριών που προέρχονται από whistleblowers, χωρίς να αφήνει οποιοδήποτε ψηφιακό αποτύπωμα στο computer. Το Tails είναι μέρος του Tor Project, το οποίο είναι υπεύθυνο για τον πλοηγτή Tor.

Το Tails μπορεί να εγκατασταθεί σε περιβάλλον windows, mac ή linux. Ανάλογα με το περιβάλλον του υπολογιστή στον οποίο θα γίνει χρήση του Tails, η εγκατάσταση έχει διαφορετικές απαιτήσεις. Αρχικά θα πρέπει ο χρήστης να κατεβάσει το πρόγραμμα από την ιστοσελίδα του Tails. Για το περιβάλλον windows απαιτείται ένα USB και 1,5 ώρες για να κατέβει το αρχείο και να εγκατασταθεί στη συσκευή αποθήκευσης. Μετά την αποθήκευση το USB μπορεί να συνδεθεί σε οποιοδήποτε υπολογιστή με windows και να παρέχει στο χρήστη τη δυνατότητα να κάνει χρήση του υπολογιστή χωρίς να αφήσει ψηφιακά ίχνη.

Ο πλοηγτής που χρησιμοποιεί είναι το Tor, αλλά δεν προσφέρει μόνο του κρυπτογράφηση στα έγγραφα. Ο χρήστης θα πρέπει να κρυπτογραφεί τα έγγραφά του για αποστολή για παράδειγμα με email, προκειμένου να μεγιστοποιήσει την ασφάλεια. Το Tails είναι ένα πρόγραμμα σχεδιασμένο για να δίνει τη δυνατότητα μυστικής χρήσης ενός υπολογιστή και προσφέρει ένα βασικό επίπεδο ασφάλειας χρησιμοποιώντας το Tor για πλοήγηση. Ο συνδυασμός του με άλλα λογισμικά που παρέχει η ψηφιακή τεχνολογία μπορεί να μεγιστοποιήσει την ασφάλεια. Όσον αφορά τους ιούς, καμία λειτουργία που πραγματοποιείται στο περιβάλλον του δεν σχετίζεται με το σκληρό δίσκο, οπότε ο υπολογιστής δεν κινδυνεύει. Παρόλα αυτά, κίνδυνοι μπορεί να προκύψουν αν ο υπολογιστής από τον οποίο έγινε η εγκατάσταση στο USB είχε ιό, ενώ προβλήματα μπορεί να δημιουργηθούν και σε περίπτωση που το Tails χρησιμοποιηθεί σε υπολογιστή με κακόβουλο λογισμικό¹².

3. Πλατφόρμες ασφαλούς επικοινωνίας δημοσιογράφων με Whistleblowers

Η δεύτερη δεκαετία του 21ου αιώνα υπήρξε ιδιαίτερα αποκαλυπτική όσον αφορά τη σημασία της πληροφορίας για την χάραξη της σύγχρονης πολιτικής ιστορίας, ακόμη και εκείνης της πληροφορίας που θεωρείται ασήμαντη ή απίθανο να ενδιαφέρει κάποιον. Τόσο η αποκάλυψη της μαζικής παρακολούθησης εκατομμυρίων πολιτών σε Ευρώπη και Αμερική από την κυβέρνηση των ΗΠΑ, όσο και το σκάνδαλο της Cambridge Analytica²¹, με την παραχώρηση τεράστιου όγκου δεδομένων των χρηστών του Facebook, από το τελευταίο στην εταιρεία, απέδειξαν ότι οι πολιτικοοικονομικές elite όχι μόνο μπορούν να παρακολουθούν άπαντες, αλλά και έχουν λόγο να το κάνουν. Οι δραματικές εξελίξεις, που ακολούθησαν το Brexit και την εκλογή του Donald Trump στις ΗΠΑ, δεν αφήνουν περιθώρια αμφισβήτησης. Η καμπάνια του Brexit, όσο και εκείνη του Ρεπουμπλικανικού κόμματος στις εκλογές του 2016, βασίστηκαν σε επεξεργασία των δεδομένων εκατομμυρίων χρηστών του Facebook, τα οποία παρανόμως παραχωρήθηκαν από τον κολοσσό του Mark Zuckerberg στη βρετανική εταιρία Cambridge Analytica. Ουδείς μπορεί να γνωρίζει ποιά θα ήταν η εξέλιξη στις δύο αυτές κομβικές ψηφοφορίες, αν έλειπε το παραπάνω δεδομένο. Είναι όμως προφανές ότι οι κοινωνικοπολιτικές elite δίνουν πολύ μεγάλη σημασία στα προσωπικά δεδομένα των πολιτών. Ως εκ τούτου, οι παρακολουθήσεις, και δη στον ψηφιακό κόσμο, καθίστανται στοιχείο της καθημερινότητάς του σύγχρονου πολίτη, η ιδιωτική ζωή του οποίου βάλλεται και η κοινωνικοπολιτική του συμπεριφορά πιθανώς χειραγωγείται.

Οι κίνδυνοι όμως που μπορεί να ελλοχεύουν πολλαπλασιάζονται όταν γίνεται λόγος για την άσκηση του δημοσιογραφικού επαγγέλματος. Ο δημοσιογράφος αντιλαμβάνεται ότι η βασική αρχή της προστασίας των πηγών του δεν μπορεί να υφίσταται σε ένα τέτοιο πλαίσιο. Οι δύο παραπάνω κομβικές αποκαλύψεις έγιναν χάρη σε δύο whistleblowers. Ο ένας κρατικός υπάλληλος, ο μηχανικός υπολογιστών Edward Snowden, και ο άλλος ιδιωτικός υπάλληλος, ο σύμβουλος δεδομένων Christopher Wylie. Πρόκειται για δύο ιστορικής σημασίας γεγονότα που έδειξαν τόσο τη σημασία της πληροφορίας, όσο την αναγκαιότητα διασφάλισης του απορρήτου των επικοινωνιών. Στο σημείο αυτό είναι που ιστορικά επιταχύνθηκε η διαμόρφωση βελτιωμένων εργαλείων, που θα μπορούσαν να παρέχουν ασφαλή επικοινωνία

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

μεταξύ δημοσιογράφων και whistleblowers. Οι διαδικασίες είχαν ξεκινήσει λίγα χρόνια νωρίτερα, με τα WikiLeaks να προετοιμάζουν το έδαφος για τις πλατφόρμες ασφαλούς επικοινωνίας. Η κρυπτογράφηση βρίσκεται στον πυρήνα του νέου αυτού εγχειρήματος.

Με δεδομένη την γενικευμένη ψηφιακή παρακολούθηση, τόσο για πολιτικούς όσο και για εμπορικούς σκοπούς, η πρακτική της κρυπτογράφησης είναι αναγκαία συνθήκη για τους δημοσιογράφους που διαχειρίζονται ιδιαίτερα ευαίσθητες πληροφορίες. Οι δημοσιογράφοι και οι whistleblowers πλέον μπορούν να χρησιμοποιήσουν την κρυπτογράφηση με πολλούς τρόπους, ανάλογα με τις ανάγκες τους και το λογισμικό που έχουν στη διάθεσή τους. Πρόκειται για τεχνολογίες που ωφελούν και τις δύο πλευρές, καθώς όχι μόνο προσφέρουν στους μάρτυρες δημοσίου συμφέροντος τη δυνατότητα της ανώνυμης μετάδοσης σημαντικών πληροφοριών, αλλά και πολλαπλασιάζουν τις πιθανές πηγές για τους ερευνητές δημοσιογράφους. Από αυτή την άποψη οι ψηφιακές πλατφόρμες ασφαλούς επικοινωνίας αντιπροσωπεύουν μια από τις πιο ενδιαφέρουσες πλευρές της σύγχρονης ψηφιακής δημοσιογραφίας. Οι πλατφόρμες αυτές συνδυάζουν τη φιλοσοφία της διαρροής πληροφοριών, την χρήση της κρυπτογράφησης στη δημοσιογραφική πρακτική και την ισχυροποίηση των δεσμών μεταξύ δημοσιογράφων και hackers, ενώ μπορούν ήδη να θεωρηθούν ένα νέο δημοσιογραφικό δεδομένο, στον τομέα της προστασίας των πηγών (Di Salvo, 2020). Παρόλα αυτά, κανένα λογισμικό κρυπτογράφησης και κανένα τεχνολογικό εργαλείο δεν μπορεί να εγγυηθεί 100% ασφαλή επικοινωνία σε όλα τα πιθανά σενάρια (Blake et al, 2013).

Οι μέθοδοι κρυπτογράφησης προϋπήρχαν πολύ πριν την δυναμική εμφάνιση των WikiLeaks, κυρίως με το λογισμικό PGP. Εκείνο που έκαναν τα WikiLeaks και που αποτέλεσε προπομπό των πλατφόρμων ασφαλούς επικοινωνίας είναι η σύνδεση αυτής της τεχνολογίας με τη δημοσιογραφία. Οι πλατφόρμες αυτές παρέχουν ασφάλεια και στις τρεις βασικές διαστάσεις της πρακτικής της διαρροής πληροφοριών. Η πρώτη αφορά τη δυνατότητα προσέγγισης των δύο πλευρών με όρους ανωνυμίας και μυστικότητας. Η δεύτερη αφορά την διοχέτευση μεγάλου όγκου δεδομένων μέσα από το διαδίκτυο, χωρίς να μπορούν να γίνουν αντιληπτά από αδιάκριτα βλέμματα. Η τρίτη έχει να κάνει με τη χρηστικότητά τους και τη δυνατότητα οποιουδήποτε θελήσει, να έχει πρόσβαση σε αυτά τα εργαλεία. Πρόκειται για τεχνολογία που όχι μόνο καθιστά εφικτή τη διαρροή πληροφοριών στον Τύπο, αλλά την κάνει και ιδιαίτερα προσιτή. Με αυτά τα εργαλεία, όποιος θέλει να διαρρεύσει πληροφορίες, μπορεί να το κάνει.

3.1 Η πρώτη επαφή

Οι ψηφιακές πλατφόρμες ασφαλούς επικοινωνίας έχουν ήδη γίνει, πριν ακόμη συμπληρώσουν την πρώτη δεκαετία λειτουργίας τους, θεσμός στην on line προσέγγιση whistleblowers. Μια βασική πρώτη διαφορά μεταξύ των εργαλείων αυτών και άλλων λογισμικών, βασισμένων στην κρυπτογράφηση, είναι ότι δίνουν τη δυνατότητα στο whistleblower να επικοινωνήσει κατευθείαν με το δημοσιογράφο, χωρίς προηγούμενη επικοινωνία με άλλη λιγότερο ασφαλή μέθοδο. Τόσο η αρχική προσέγγιση, όσο και η επικοινωνία που πραγματοποιείται στη συνέχεια και η τελική αποστολή του επίμαχου υλικού γίνονται μέσα από τις συγκεκριμένες πλατφόρμες. Παράλληλα, ο ταυτότητα του πληροφοριοδότη παραμένει μυστική και αποκαλύπτεται μόνο αν το θελήσουν και οι δύο πλευρές.

Οι πλατφόρμες ασφαλούς επικοινωνίας έχουν δώσει λύση στο κεφαλαιώδες πρόβλημα της πρώτης επαφής, καθώς είναι διαθέσιμες στις ιστοσελίδες πολλών μέσων ενημέρωσης. Ο επίδοξος πληροφοριοδότης δεν έχει μόνο να ξεπεράσει τους φόβους και τις ανασφάλειές του για το ρίσκο που αναλαμβάνει, αποφασίζοντας να μιλήσει, αλλά και το σε ποιον και με ποιον τρόπο θα μιλήσει. Τα συγκεκριμένα εργαλεία δίνουν λύση, καθώς ο whistleblower πρέπει μόνο να επιλέξει το μέσο στο οποίο θέλει να δώσει τις πληροφορίες του. Η επιλογή του δημοσιογράφου και ο τρόπος προσέγγισης γίνονται αυτόματα μέσα από την πλατφόρμα. Πολλές μελέτες έχουν δείξει πόσο αξεπέραστο πρόβλημα θεωρούν τόσο οι δημοσιογράφοι όσο και οι πληροφοριοδότες την πρώτη επαφή, την οποία ορίζουν ως μια από τις πλέον ευαίσθητες στιγμές της διαδικασίας διαρροής πληροφοριών (Bosua et al, 2014). Στην πραγματικότητα, οι δημοσιογράφοι δηλώνουν ότι προτιμούν να συναντιούνται με τις πηγές τους εκ του σύνεγγυς, προκειμένου να αποφύγουν τη χρήση οποιασδήποτε τεχνολογίας που θα μπορούσε να εκθέσει σε κίνδυνο τις πηγές τους (Bosua et al, 2014). Αυτό ακριβώς το πρόβλημα ήρθαν να λύσουν πρώτα τα WikiLeaks και έπειτα οι πλατφόρμες ασφαλούς επικοινωνίας, δημιουργώντας το κατάλληλο ασφαλές περιβάλλον για την προσέγγιση των δύο πλευρών.

3.2 Η προϊστορία, Cryptome και BlackNet

Παρότι τα WikiLeaks πρέπει να αναγνωριστούν ως το πιο καινοτόμο παράδειγμα ψηφιακής πλατφόρμας διαρροής πληροφοριών και ο πρώτος οργανισμός που οικειοποιήθηκε, διαμόρφωσε και χρησιμοποίησε το αντίστοιχο λογισμικό, η προϊστορία της χρήσης της ψηφιακής τεχνολογίας από τους whistleblowers ξεκίνησε με κάποιες προηγούμενες προσπάθειες που όμως δεν κατόρθωσαν να αποτελέσουν αξιόλογα εγχειρήματα. Πριν τα WikiLeaks, παρουσιάζονται πρωτοβουλίες οι οποίες προσπαθούν να συγκεράσουν τις διαρροές πληροφοριών με την κρυπτογράφηση, κυρίως για πολιτικούς και ακτιβιστικούς λόγους.

Το Cryptome δημιουργήθηκε το 1996 από τους John Young και Deborah Natsios και είναι ακόμη λειτουργικό. Πρόκειται για μια σελίδα η οποία στοχεύει στη δημοσίευση απόρρητων μυστικών εγγράφων διαφόρων ειδών, ανεξάρτητα από την προέλευση και τη θεματολογία τους. Επί του παρόντος, φιλοξενεί περίπου 90.000 έγγραφα, τα οποία έχει αποκτήσει από την ίδρυσή του. Παρότι θεωρείται, ακόμη και από τα WikiLeaks, ως ο πνευματικός πατέρας της online διαρροής πληροφοριών (Greenberg, 2012), το Cryptome δεν μπορεί να θεωρηθεί ως μια ψηφιακή πλατφόρμα επικοινωνίας έτσι όπως ορίζεται σήμερα. Όπως έχει ήδη επισημάνει ο Greenberg (2012), το Cryptome δεν χρησιμοποίησε ποτέ λογισμικό που να έχει σχεδιαστεί για τη χρήση του σε διαδικασίες διαρροής πληροφοριών. Βασίζεται σε μια διεύθυνση email σε συνδυασμό με την κρυπτογράφηση PGP και σε μια ταχυδρομική διεύθυνση. Η μοναδική, αλλά καίρια, ομοιότητά του με τις ιστοσελίδες και τις πλατφόρμες που καθιερώθηκαν τις επόμενες δεκαετίες είναι η βασική ιδέα, ο σκοπός της ύπαρξής του. Κατά κάποιο τρόπο τα WikiLeaks, δέκα χρόνια μετά, και οι πλατφόρμες επικοινωνίας δημοσιογράφων με whistleblowers, λίγο αργότερα, ουσιαστικά τελειοποίησαν τεχνικά αυτό που ευαγγελίστηκαν οι δημιουργοί του Cryptome.

Το Cryptome δεν είχε ποτέ ξεκάθαρη δημοσιογραφική προσέγγιση καθώς δημοσιεύει απόρρητα και μυστικά έγγραφα, τα οποία έχει λάβει από ανώνυμες πηγές, με πενιχρή ή καθόλου ανάλυση και ελάχιστη συμμετοχή στη διαμόρφωση του περιεχομένου που δημοσιεύει. Σε μια συνέντευξή του, το 2014, ο ιδρυτής του John Young εμβαθύνει και σε πιο ουσιαστικές διαφορές που ξεφεύγουν από την τεχνολογική διάσταση. “Η βασική καινοτομία που έφεραν τα WikiLeaks και που εμείς ποτέ δεν κάναμε είναι ότι επένδυσαν στη δημοσιότητα

και στην προσέγγιση του Τύπου. Παρουσίασαν μια πιο οργανωμένη δομή λειτουργίας” (Cox, 2014). Ο John Young, εν ενεργεία αρχιτέκτονας στη Νέα Υόρκη σήμερα, είχε εμπλακεί και με το εγχείρημα των WikiLeaks, στα πρώτα βήματά του οργανισμού, αλλά εγκατέλειψε σύντομα, καθώς διαφώνησε με τον ιδεολογικό προσανατολισμό και τους σκοπούς της σελίδας (McCullagh, 2010).

Το BlackNet είναι μία ιστοσελίδα που αγοράζει διαρρέοντα κρατικά μυστικά, σε συνθήκες απόλυτης ανωνυμίας πηγών, και τα πουλά χρησιμοποιώντας τη μέθοδο της κρυπτογράφησης (Myers West, 2017). Είναι περισσότερο μια ιδέα, που ποτέ δεν προχώρησε στην πράξη, η οποία διατυπώθηκε, το 1993, από τον συγγραφέα, κρυπτογράφο και μέλος της επιστημονικής ομάδας της Intel, Tim May. Παρόλα αυτά μπορεί να θεωρηθεί ως ένας προάγγελος των πλατφόρμων επικοινωνίας δημοσιογράφων με whistleblowers, καθώς εισήγαγε για πρώτη φορά την μέγιστη προστασία της ανωνυμίας των πηγών, από την πρώτη επαφή, με τη μέθοδο της κρυπτογράφησης (Bartlett, 2015). Παρότι το BlackNet παρέμεινε περισσότερο μια ιδέα παρά ένα project, μπορεί να θεωρηθεί ως ο αρχέγονος, καινοτόμος πρόγονος των WikiLeaks (Greenberg, 2012).

3.3 Τα πρώτα βήματα, οι αντιγραφείς

Το 2011 μπορεί να θεωρηθεί ως το έτος μηδέν για τις ψηφιακές πλατφόρμες επικοινωνίας δημοσιογράφων με whistleblowers. Έπειτα από τη μεγάλη δημοσιογραφική επιτυχία του Collateral Murder από τα WikiLeaks, το 2010, δεν χρειάστηκε πολύς χρόνος για να εμφανιστούν αντίστοιχες προσπάθειες στο διαδίκτυο. Όπως παρατηρεί ο Greenberg “Οι αντιγραφείς ξεκίνησαν να ξεπηδούν σε όλες τις γλώσσες, τις μορφές, τις τεχνολογικές και ιδεολογικές προσεγγίσεις: BaltiLeaks, BritiLeaks, BrusselsLeaks, Corporate Leaks, CrowdLeaks, EnviroLeaks, FrenchLeaks, GlobaLeaks, IndoLeaks, IrishLeaks, IsrealiLeaks, Jumbo Leaks, KHLeaks, LeakyMails, LocaLeaks, MarpleLeaks, MurdochLeaks, Office Leaks, Porn WikiLeaks, PinoyLeaks, PirateLeaks, QuebecLeaks, RuLeaks, ScienceLeaks, TradeLeaks, UniLeaks” (2012).

Όλα τα παραπάνω προσπάθησαν να αντιγράψουν τα WikiLeaks, χωρίς όμως να προσφέρουν αντίστοιχες τεχνολογικές λύσεις, με αποτέλεσμα να οδηγηθούν σε μια αποτυχημένη προσπάθεια προσέλκυσης διαρροών οποιουδήποτε είδους. Το γεγονός αυτό σε συνδυασμό με

τον εθελοντικό χαρακτήρα και τις οργανωτικές δυσλειτουργίες, οδήγησε σε παταγώδη αποτυχία το σύνολο αυτών των εγχειρημάτων, πολλά από τα οποία δεν παρουσιάζονται πλέον on line ή δεν κατάφεραν να αφήσουν το ίχνος τους στο διαδίκτυο. Η συγκεκριμένη δράση τους και η προσέγγιση που είχαν όλες αυτές οι σελίδες απέναντι στη διαδικασία της διαρροής πληροφοριών είναι δύσκολο να ανιχνευθεί καθώς οι περισσότερες έχουν πάψει προ πολλού να λειτουργούν.

Μια ιδιαίτερη περίπτωση ήταν τα TuniLeaks, μια ιστοσελίδα που εμφανίστηκε on line στις 28 Νοεμβρίου 2010, μια ώρα μετά τη δημοσίευση από τα WikiLeaks της έρευνα Cablegate, η οποία περιλάμβανε απόρρητα έγγραφα από 274 πρεσβείες και διπλωματικές αποστολές των ΗΠΑ σε ολόκληρο τον κόσμο από το 1966 έως το 2010. Η σελίδα αυτή παρουσίαζε σε μια οργανωμένη βάση δεδομένων όλα τα αρχεία που αφορούσαν την Τυνησία και είχαν ήδη δημοσιευθεί από τα WikiLeaks (Lengel, 2014). Ιδιαίτερα φιλόδοξο ήταν το σχέδιο και του πρώην μέλους των WikiLeaks, Daniel Domscheit Berg, ο οποίος αφού εγκατέλειψε το γνωστό οργανισμό, παρουσίασε το project OpenLeaks, το οποίο φιλοδοξούσε να γίνει ένα εργαλείο συλλογής διαρροών προκειμένου να τις διοχετεύει σε άλλα μέσα, χωρίς να τις δημοσιεύει το ίδιο στο διαδίκτυο. Παρά το φιλόδοξο σχέδιο, τα OpenLeaks δεν λειτούργησαν ποτέ, κυρίως γιατί δεν μπόρεσαν να ανταπεξέλθουν στις τεχνικές δυσκολίες του εγχειρήματος (Di Salvo and Porlezza, 2014; Greenberg, 2012).

3.4 Οι πρώτες προσπάθειες από τα κυρίαρχα μέσα.

Μερικά κυρίαρχα μέσα ενημέρωσης προσπάθησαν να ακολουθήσουν τα WikiLeaks, ενσωματώνοντας τεχνολογικές λύσεις αντίστοιχες με εκείνες που χρησιμοποιούσε η καινοτόμος ιστοσελίδα, προκειμένου να προσελκύσουν διαρροές και πληροφοριοδότες. Σε αυτή τη φάση, κορυφαίοι εκδοτικοί οίκοι προσπάθησαν να δραστηριοποιηθούν στον τομέα της κρυπτογράφησης και της ψηφιακής διαρροής πληροφοριών. Παρότι είχαν πολύ περισσότερους πόρους από τους προαναφερθέντες αντιγραφείς, οι προσπάθειες αυτές των κυρίαρχων μέσων κατέληξαν σε φιάσκο, αποδεικνύοντας ότι πολύ λίγη ουσία υπήρχε πίσω από τη διαφήμιση (Di Salvo, 2010).

Η Wall Street Journal, για παράδειγμα, ανακοίνωσε το SafeHouse project, το 2011, στοχεύοντας στην παροχή ενός ασφαλούς καναλιού επικοινωνίας των whistleblowers με την

αίθουσα σύνταξης. Λίγο μετά την έναρξή του, το SafeHouse υπέστη δριμεία κριτική για έλλειψη ακόμη και των βασικότερων τεχνικών προδιαγραφών ασφάλειας και για υποτυπώδη κρυπτογράφηση, σε σημείο που οι αντίστοιχες υπηρεσίες δεν ήταν προσβάσιμες από τον πλοηγό Tor (Greenberg, 2011, 2012). Η αποτυχία του SafeHouse όμως δεν οφείλεται μόνο στην προβληματική τεχνική του ασφάλεια, αλλά και στη μη κατοχύρωσή του ως προς το δικαίωμά του να μην αποκαλύπτει τις πηγές του. Ένα νομικό κενό στους όρους χρήσης της εφαρμογής είχε ως αποτέλεσμα το μέσο να μην είναι νομοθετικά κατοχυρωμένο στη διατήρηση της ανωνυμίας των πηγών του σε περίπτωση που οι τελευταίες δεν το είχαν δηλώσει ρητά κατά τη χρήση τους συγκεκριμένου λογισμικού (Greenberg, 2011). Προφανώς, όλα τα παραπάνω συνέβαλαν στη νομοτελειακή αποτυχία της προσπάθειας της μεγάλης νεοϋορκέζικης εφημερίδας.

Στο ίδιο μήκος κύματος το Al Jazeera παρουσίασε, την ίδια χρονιά το δικό του εργαλείο με τον τίτλο Transparency Unit (Bieber, 2013). Όπως και στην προηγούμενη προσπάθεια, οι ειδικοί στην ασφάλεια των επικοινωνιών εντόπισαν σοβαρές τεχνικές ελλείψεις, ενώ η Μη Κυβερνητική Οργάνωση Electronic Frontier Foundation (EFF), απέδωσε στην εφαρμογή σοβαρά νομικά κενά, κάνοντας λόγο για επίπλαστη ανωνυμία (Fakhouri, 2011). Αποτέλεσμα ήταν η διακοπή λειτουργίας του, λίγους μήνες μετά την πρώτη κυκλοφορία του, η οποία ξαναξεκίνησε στα τέλη τους 2011. Παρά τις δυσκολίες που αντιμετώπισε στα πρώτα βήματά του, κατόρθωσε να αποκαλύψει τα Palestine Papers, που έριξαν φως στις Ισραηλινοπαλαιστινιακές διαπραγματεύσεις, μέσα από 1.500 απόρρητα έγγραφα. Το transparency.aljazeera.net είναι ακόμη και σήμερα διαθέσιμο στην αγγλική και αραβική γλώσσα, παρέχοντας στους χρήστες του αναζήτηση των αρχείων που τους ενδιαφέρουν, ενώ παρά τις δυσκολίες που αρχικά αντιμετώπισε συνεχίζει να δέχεται διαρροές.

Όλες οι παραπάνω κινήσεις που πραγματοποιήθηκαν στον απόηχο της ηχηρής άφιξης των WikiLeaks στη σύγχρονη διαδικτυακή δημοσιογραφία, είτε πρόκειται για εγχειρήματα κυρίαρχων μέσων ή για απλές προσπάθειες αντιγραφής της καινοτόμου σελίδας, αξίζει να εξεταστούν συλλογικά, ως ενιαίο φαινόμενο, και όχι ως μεμονωμένες ιστορίες (Chen, 2011). Η παραπάνω εξέταση είναι σημαντική γιατί δείχνει την προσπάθεια δεκάδων πολιτών, ομάδων ή ακόμη και κυρίαρχων μέσων να αντιγράψουν τις ψηφιακές μεθόδους προσέγγισης πληροφοριοδοτών, αλλά κυρίως βεβαιώνει την σημασία της ύπαρξης ισχυρών τέτοιων εργαλείων προκειμένου να μπορέσει το μέσο να προσεγγίσει τον whistleblower. Από αυτή την

άποψη, η αποτυχία των πρώιμων, ερασιτεχνικών προσπαθειών μπορεί να αποδοθεί στην απουσία οράματος και ωριμότητας, ενώ στην περίπτωση των κυρίαρχων μέσων οφείλεται στην απουσία ισχυρής μεθόδου κρυπτογράφησης, διαδικτυακής ασφάλειας και τεχνικής κατάρτισης γενικότερα (Di Salvo, 2020).

Λίγο πριν τις αποκαλύψεις του Edward Snowden, οι κίνδυνοι της ψηφιακής διαρροής πληροφοριών δεν ήταν προφανώς αντιληπτοί από τους δημοσιογράφους και τους μεντιακούς οργανισμούς, καθώς υπήρχε πολύ μικρή γνώση γύρω από το ζήτημα της ψηφιακής παρακολούθησης και των κινδύνων που αυτή έχει για τους δημοσιογράφους και τις πηγές τους. Το επόμενο στάδιο των ψηφιακών πλατφόρμων ασφαλούς επικοινωνίας αλλάζει πορεία και κινείται προς ένα μοντέλο πιο στενής συνεργασίας μεταξύ δημοσιογράφων και hackers. Αυτή η προσέγγιση οφείλεται κυρίως στην εμφάνιση δύο τύπων λογισμικού, οι οποίοι έχουν πλέον επικρατήσει και είναι οι πλατφόρμες που πλέον χρησιμοποιούνται από την πλειονότητα των μέσων.

3.5 Οι πλατφόρμες ξεκινούν

Το GlobaLeaks και το SecureDrop παρουσιάστηκαν το 2011 και το 2013 αντίστοιχα, ενισχύοντας το χώρο των ψηφιακών πλατφόρμων ασφαλούς επικοινωνίας με εργαλεία πλήρη και έτοιμα προς χρήση. Και τα δύο μοιράζονται ένα κοινό σκοπό, την παροχή πιστοποιημένης και αξιόπιστης τεχνολογίας, προκειμένου να είναι δυνατή η ασφαλής διαρροή πληροφοριών. Η διαφορά που έφεραν στο χώρο έγκειται στην δημιουργία ενός περιβάλλοντος υψηλού επιπέδου ασφάλειας, το οποίο μπορεί να χρησιμοποιηθεί από οποιοδήποτε μέσο και οργανισμό, είτε χαμηλού είτε υψηλού προϋπολογισμού. Δεν είναι τυχαίο άλλωστε που τα δύο αυτά λογισμικά είναι εκείνα που χρησιμοποιούνται από την πλειονότητα των μέσων ενημέρωσης παγκοσμίως και από μεγάλα κυρίαρχα μέσα έως Μη Κυβερνητικές Οργανώσεις (ΜΚΟ) και μεμονωμένους δημοσιογράφους.

3.5.1 GlobaLeaks, Η Πρώτη Πλατφόρμα



Εικόνα 7
https://www.globaleaks.org/?gclid=CJ0KCQIAst2BBhDJARIsAGo2ldVatm7oBJW6VBsdbgO233nmmpUIBfdKTIZBgdkCOPayTcGfxqaM8waAlqmEALw_wcB

Το GlobaLeaks αυτοπροσδιορίζεται ως το πρώτο λογισμικό ανοιχτού κώδικα που απλοποιεί την ασφαλή, ανώνυμη και απρόσκοπτη διαρροή πληροφοριών.

Προσφέρεται από την Ιταλική ΜΚΟ

Hermes Center for Transparency and Digital Human Rights. Το Hermes Center αποτελείται από δικηγόρους, ακτιβιστές και προγραμματιστές/hackers οι οποίοι δουλεύουν στον τομέα της διαδικτυακής ασφάλειας, της διαδικτυακής ελευθερίας και των ψηφιακών δικαιωμάτων και το GlobaLeaks είναι μόνο ένα project από τα πολλά που πραγματοποιεί η οργάνωση. Το GlobaLeaks επιτρέπει τη διαρροή μυστικών πληροφοριών και είναι κατάλληλο για διαφορετικά είδη φορέων, όπως μέσα ενημέρωσης, ακτιβιστικές οργανώσεις, εμπορικές εταιρείες, ΜΚΟ κλπ, ενώ ο κώδικας στον οποίο βασίζεται πρωτοεμφανίστηκε το 2011. Σκοπός του συγκεκριμένου λογισμικού είναι να αποτελέσει τον τεχνολογικό σκελετό μιας πλατφόρμας ασφαλούς επικοινωνίας και να την κάνει ασφαλή και απροσπέλαστη από εξωγενείς παράγοντες. Ήδη, χρησιμοποιείται κυρίως στην Ευρώπη, από ακτιβιστές, ΜΚΟ που δραστηριοποιούνται στον τομέα της καταπολέμησης της διαφθοράς, κόμματα και μικρού ή μεσαίου μεγέθους δημοσιογραφικούς οργανισμούς.

Το GlobaLeaks χρησιμοποιεί μεθόδους κρυπτογράφησης τόσο για να προστατέψει την ανωνυμία του πληροφοριοδότη, όσο και για να μεταφέρει με ασφάλεια τα επίμαχα αρχεία μέσω του διαδικτύου. Χρησιμοποιεί δε, διαφορετικά εργαλεία προκειμένου να ολοκληρώσει την επικοινωνία με ασφάλεια. Για να κωδικοποιήσει τα έγγραφα που δίνει ο whistleblower χρησιμοποιεί τη μέθοδο PGP, ενώ η ασφαλής επικοινωνία πραγματοποιείται μέσω της τεχνολογίας Tor. Με αυτό τον τρόπο διασφαλίζει στο μέγιστο βαθμό την ασφαλή επικοινωνία μεταξύ δημοσιογράφων και whistleblowers, την απρόσκοπτη ανταλλαγή υλικού και την αποθήκευσή του για μικρό χρονικό διάστημα, πριν καταστραφεί από το ίδιο το πρόγραμμα. Ο whistleblower μπορεί να επιλέξει μεταξύ της αποκάλυψης της ταυτότητάς του στο δημοσιογράφο ή της διατήρησης της ανωνυμίας του, ενώ έχει τη δυνατότητα να επικοινωνήσει, σε πραγματικό χρόνο, μέσω chat, διατηρώντας την ανωνυμία του.

Η μεγάλη καινοτομία που έφερε το GlobaLeaks και που έμελλε να εδραιωθεί στο χώρο της ψηφιακής διαρροής πληροφοριών είναι η δημιουργία ενός λογισμικού το οποίο θα είναι διαθέσιμο προς χρήση από όλα τα μέσα ενημέρωσης και όχι μόνο. Δεν αποτελεί το ίδιο on line σελίδα, ούτε έχει σχεδιαστεί από ένα μέσο ενημέρωσης. Όπως εξηγεί ο μηχανικός υπολογιστών και δημοσιογράφος του WIRED, Andy Greenberg, οι δύο Ιταλοί δημιουργοί του προγράμματος, Fabio Pietrosanti και Arturo Filasto, ήθελαν να μεταφέρουν τη διαρροή των μυστικών πληροφοριών από τις μερικές δεκάδες αντιγραφείς των WikiLeaks σε ένα δίκτυο πολλών χιλιάδων μέσων ενημέρωσης που θα παρέχουν τις συγκεκριμένες υπηρεσίες στο κοινό τους. Με το προϊόν που παρουσίασαν το 2011 έδειξαν ότι δεν χρειάζονται τα WikiLeaks ή μια πανομοιότυπη σελίδα για να γίνει μια διαρροή με μυστικότητα και ασφάλεια, ούτε τα κυρίαρχα μέσα πρέπει να φτιάξουν το δικό τους λογισμικό. Αρκεί να κάνουν χρήση του GlobaLeaks.

Το σημαντικότερο όμως είναι ότι το συγκεκριμένο λογισμικό παρέχεται δωρεάν από τη σελίδα του Hermes Center και η εγκατάσταση και λειτουργία του μπορεί να υποβοηθηθεί από τους τεχνικούς της οργάνωσης. Με τον τρόπο αυτό το GlobaLeaks αντιπροσωπεύει την έναρξη της συνεργασίας μεταξύ δημοσιογράφων και hackers με σκοπό την προστασία των δημοσιογραφικών πηγών και την διασφάλιση των whistleblowers. Η ιδιότητα της διάθεσής του μέσω ανοιχτού κώδικα είναι ιδιαίτερα κρίσιμη για τη συνεισφορά της πλατφόρμας στην ευρεία χρήση του από τα μέσα και τον συνεπακόλουθο πολλαπλασιασμό των whistleblowers (Heemsbergen, 2016). Ως εκ τούτου, η συμβολή του GlobaLeaks υπήρξε ιδιαίτερα καθοριστική στην τόνωση της ερευνητικής δημοσιογραφίας. Εξηγώντας τη σημασία της ύπαρξης ελεύθερου λογισμικού ανοιχτού κώδικα ο καθηγητής ψηφιακού πολιτισμού στο Πανεπιστήμιο του Sussex, Tim Jordan, λέει: “Αυτό που οφείλουμε να κατανοήσουμε είναι ότι το ελεύθερο λογισμικό ανοιχτού κώδικα είναι διαθέσιμο δωρεάν, που σημαίνει όχι μόνο ότι οι προγραμματιστές δεν πληρώνονται, αλλά κυρίως ότι ο κώδικας του λογισμικού μπορεί να χρησιμοποιηθεί και να προσαρμοστεί από το χρήστη και αυτή η τροποποίηση μπορεί να φανεί χρήσιμη και σε άλλους χρήστες”, (2008).

3.5.2 SecureDrop, ο Ηγέτης



Εικόνα 6 <https://securedrop.org/>

Το SecureDrop είναι η πλατφόρμα που έχει κάνει τη διαφορά στον τομέα της ασφαλούς ψηφιακής επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers, καθώς είναι η μόνη που επικεντρώνεται στην διασφάλιση της επικοινωνίας στα πλαίσια άσκησης του δημοσιογραφικού επαγγέλματος. Πρωτοεμφανίστηκε το 2013 από την ηλεκτρονική έκδοση του ιστορικού περιοδικού The New

Yorker και σήμερα χρησιμοποιείται σε περισσότερα από 50 μέσα ενημέρωσης σε όλο τον κόσμο. Αξιοσημείωτο είναι ότι τη συγκεκριμένη πλατφόρμα τη χρησιμοποιούν και μεμονωμένοι ερευνητές δημοσιογράφοι, οι οποίοι ασχολούνται κυρίως με φαινόμενα διαφθοράς.

Το SecureDrop έχει άρρηκτα συνδεθεί με το έργο του Αμερικανού μηχανικού υπολογιστών και ακτιβιστή Aaron Swartz¹, ο οποίος μαζί με το δημοσιογράφο και hacker Kevin Poulsen και τον ειδικό σε θέματα ασφάλειας υπολογιστών James Dolan ξεκίνησαν, το 2012, να δουλεύουν πάνω στην ιδέα της δημιουργίας μιας ασφαλούς πλατφόρμας επικοινωνίας την οποία ονόμασαν DeadDrop και θα προοριζόταν αποκλειστικά για δημοσιογράφους. Η χαρισματική προσωπικότητα του Aaron Swartz αποτέλεσε καταλυτικό παράγοντα στη δημιουργία της πιο ασφαλούς και εύχρηστης πλατφόρμας επικοινωνίας που ακόμη και σήμερα δεν έχει αντικατασταθεί από κάποιο άλλο εργαλείο. Η τεχνολογικές γνώσεις του νεαρού ακτιβιστή, σε συνάρτηση με την ακλόνητη πίστη του στο ιδανικό της ελεύθερης διακίνησης της γνώσης, απαλλαγμένης από τους περιορισμούς που την καθιστούν προσβάσιμη σε μια περιορισμένη οικονομική elite, τον έστρεψαν προς τη διαμόρφωση του συγκεκριμένου εργαλείου. Η πληροφορία έπρεπε να διακινείται απρόσκοπτα και η συμμετοχή των δημοσιογράφων σε αυτή τη διακίνηση ήταν καίρια. Συνεπώς, η δημιουργία ενός εργαλείου που να επιτρέπει την επικοινωνία με το δημοσιογράφο, χωρίς φραγμούς, παρακολούθησεις και λογοκρισία ήταν η μόνη λύση.

Το project όμως σταμάτησε απότομα τον Ιανουάριο του 2013, με την ξαφνική απώλεια του Aaron Swartz. Η προσωρινή παύση του εγχειρήματος διακόπτεται, λίγους μήνες αργότερα, και το Μάιο της ίδιας χρονιάς το προϊόν χρησιμοποιείται, με την ονομασία StrongBox, στην

ηλεκτρονική έκδοση του ιστορικού περιοδικού The New Yorker του συγκροτήματος Conde Nast. Σύντομα όμως το λογισμικό παραδίδεται στο ίδρυμα Freedom of the Press Foundation, το οποίο του δίνει τη σημερινή του ονομασία και το παρέχει, από τον Οκτώβριο του 2013, δωρεάν στην ιστοσελίδα του.

Όπως εξηγεί ο ίδιος ο οργανισμός στη σελίδα του “η κυβέρνηση δεν χρειάζεται να ασκήσει διώξεις σε δημοσιογράφους για τη μη αποκάλυψη πηγών. Μπορεί απλά να λάβει από τους ψηφιακούς διαμεσολαβητές όπως είναι η αμερικάνικη εταιρία τηλεπικοινωνιών ATT, η Google και το Facebook το πολύτιμο ψηφιακό αποτύπωμα της επικοινωνίας των δημοσιογράφων με τις πηγές τους. Για παράδειγμα το Associated Press έχει αποκαλύψει την παρακολούθηση είκοσι τηλεφωνικών γραμμών του με στόχο την ανίχνευση των πηγών του, ενώ δημοσιογράφος του Fox News έχει δεχθεί αντίστοιχη επίθεση στο λογαριασμό του ηλεκτρονικού ταχυδρομείου του. Και στις δύο περιπτώσεις προσήχθησαν στη δικαιοσύνη οι πηγές, χωρίς να έχουν μιλήσει οι δημοσιογράφοι”⁷.

Βασική ασφαλιστική δικλείδα είναι και ο περιορισμός των μεταδεδομένων των συνομιλιών που πραγματοποιούνται μέσω της πλατφόρμας. Η αποκλειστική χρήση του πλοηγτή Tor δεν επιτρέπει την ανίχνευση της IP της πηγής, με αποτέλεσμα να μην μπορεί να εντοπιστεί ούτε η γεωγραφική προέλευση του πληροφοριοδότη. Η επιλογή τυχαίων κωδικών ονομάτων για τους χρήστες ελαχιστοποιεί επίσης τη δυνατότητα εντοπισμού μέσω του username. Παράλληλα δεν υπάρχει αποθήκευση του ιστορικού της συνομιλίας. Κάθε φορά που η πηγή στέλνει ένα μήνυμα, διαγράφεται αυτόματα και το ίχνος του προηγούμενου. Με αυτό τον τρόπο δεν μπορεί να ανιχνευθεί η ακριβής διάρκεια της επικοινωνίας δύο των μερών⁸.

Η κρυπτογράφηση του περιεχομένου της επικοινωνίας είναι βασική μέριμνα του συγκεκριμένου λογισμικού. Το μήνυμα μεταδίδεται κωδικοποιημένο δια μέσου του διαδικτύου, που σημαίνει ότι ακόμη και αν θα μπορούσε να γίνει αντιληπτό, δεν θα μπορούσε να γίνει κατανοητό. Παράλληλα, η αποθήκευσή τους στο server του μέσου γίνεται επίσης σε κρυπτογραφημένη μορφή, οπότε ακόμη και αν κάποιος καταφέρει να παραβιάσει τον κεντρικό υπολογιστή, τα δεδομένα που θα βρει θα του είναι άχρηστα. Για περισσότερη ασφάλεια το κλειδί αποκρυπτογράφησης βρίσκεται σε έναν υπολογιστή που δεν συνδέεται στο διαδίκτυο και η αποκωδικοποίηση και μελέτη των αρχείων πραγματοποιείται μόνο σε αυτόν. Με τον τρόπο αυτό οι πιθανότητες κυβερνοεπίθεσης περιορίζονται δραστικά⁹.

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

Σύμφωνα με την ομάδα του SecureDrop¹⁰, το 2014, σχετική έρευνα έδειξε, ότι από 25 οργανισμούς που ελέγχθηκαν, οι 20 είχαν δεχτεί επίθεση από κρατικά χρηματοδοτούμενους hackers. Για το λόγο αυτό το SecureDrop διαχωρίζει τη λειτουργία του από το δίκτυο των μέσων ενημέρωσης. Όλη η διαδικασία της επικοινωνίας μεταξύ δύο υπολογιστών, του μέσου ενημέρωσης και του whistleblower, γίνεται με τη χρήση του προγράμματος Tails μέσω ενός USB και στους δύο υπολογιστές, το οποίο δεν επιτρέπει την δημιουργία ψηφιακού αποτυπώματος. Παράλληλα, η διακίνηση του υλικού γίνεται μέσω του ασφαλούς περιβάλλοντος Tor. Η αποκρυπτογράφηση συμβαίνει επίσης σε υπολογιστή που όχι μόνο δεν είναι συνδεδεμένος στο διαδίκτυο, αλλά χρησιμοποιεί και το πρόγραμμα Tails το οποίο δεν αφήνει ίχνη. Με αυτό τον τρόπο προστατεύεται τόσο η πλατφόρμα από πιθανές επιθέσεις, όσο και τα ίδια τα ΜΜΕ.

Ιδιαίτερα σημαντική είναι η ελεύθερη πρόσβαση στην πλατφόρμα από όλους όσους θέλουν να εγκαταστήσουν το συγκεκριμένο λογισμικό, αλλά και η online διάθεση του κώδικα κρυπτογράφησης, προκειμένου όποιος επιθυμεί να μπορεί να ελέγξει το πόσο ευάλωτος μπορεί να είναι. Όπως αποκαλύπτει η ομάδα που το διαχειρίζεται, από την έναρξή του, το SecureDrop έχει ελεγχθεί τέσσερις φορές, ως προς την αποτελεσματικότητα του κώδικα που χρησιμοποιεί. Τα αποτελέσματα έχουν ήδη δημοσιοποιηθεί και οι έλεγχοι θα συνεχίζονται κάθε φορά που θα εξελίσσεται ο κώδικας κρυπτογράφησης, προκειμένου να διασφαλίζεται ο μεγαλύτερος δυνατός βαθμός αποτελεσματικότητας¹¹.

Το SecureDrop είναι ίσως το πιο εξελιγμένο λογισμικό ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers, ενώ είναι και εκείνο που χρησιμοποιείται από τα περισσότερα και τα πλέον ονομαστά για την ερευνητική δημοσιογραφία μέσα ενημέρωσης. Το ProPublica, ο Guardian, Οι New York Times, το Al Jazeera, οι Financial Times, το περιοδικό Forbes είναι μερικά από τα μεγάλα ΜΜΕ που παρέχουν ασφαλή επικοινωνία μέσω του SecureDrop. Ιδιαίτερο ενδιαφέρον προκαλεί το γεγονός ότι στη λίστα των οργανισμών που έχουν SecureDrop είναι και δύο μη δημοσιογραφικοί φορείς. Ο πρώτος είναι το Lucy Parsons Lab, που αποτελεί μια σύμπραξη μεταξύ μηχανικών υπολογιστών, ακτιβιστών και καλλιτεχνών και στοχεύει στη διασφάλιση των ψηφιακών ελευθεριών και στην προστασία των πολιτών έναντι στην αστυνομική βία. Η χρήση της πλατφόρμας για το σκοπό αυτό σε μια χώρα που μαστιάζεται από την απρόκλητη αστυνομική βία είναι απολύτως δικαιολογημένη.

3.5.3 Το SecureDrop στο Harvard

Η δεύτερη περίπτωση μη δημοσιογραφικού φορέα είναι ακόμη πιο ενδιαφέρουσα. Πρόκειται για το Institute for Quantitative Social Science του Πανεπιστημίου του Harvard, ο πρώτος και μοναδικός επί του παρόντος πανεπιστημιακός φορέας που παρέχει επικοινωνία μέσω του SecureDrop. Η χρήση της πλατφόρμας από το κορυφαίο αμερικανικό πανεπιστήμιο, δείχνει ακριβώς την τεράστια σημασία που έχει η ασφαλής διακίνηση των δεδομένων, σε μια εποχή που η ψηφιακή παρακολούθηση είναι δεδομένη.

Το Institute for Quantitative Social Science είναι το μεγαλύτερο ερευνητικό κέντρο κοινωνικών επιστημών του Πανεπιστημίου του Harvard. Αποστολή του είναι η ανάπτυξη της απαιτούμενης επιστημονικής γνώσης για την επίλυση των μεγαλύτερων προβλημάτων που επηρεάζουν τις ανθρώπινες κοινωνίες. Όπως εξηγεί στη σελίδα του “πιστοί στην αποστολή μας, συλλέγουμε στοιχεία τα οποία καλύπτουν όλες τις πλευρές της δράσης των ανθρώπων, των κοινωνιών, των κυβερνήσεων, των πολιτισμών και άλλων, αλλά δεν δίνουμε αμοιβή για τα στοιχεία αυτά και δεν θέλουμε να συλλέξετε παράνομα τα δεδομένα αυτά για εμάς”. Αφού μάλιστα δηλώνει απερίφραστα ότι θα παρέχει προστασία των δεδομένων και της ταυτότητας των χρηστών προσδιορίζει το συγκριτικό πλεονέκτημα σε σχέση με τα MME που μπορεί να έχει ως αποδέκτης μυστικών πληροφοριών. “Ως πανεπιστημιακοί ερευνητές, σε αντίθεση με τους μεντιακούς οργανισμούς, απαγορεύεται νομοθετικά να αποκαλύπτουμε τις ταυτότητες των όσων συμμετέχουν στην έρευνα”¹³.

Το ινστιτούτο δε, δεν διστάζει να δώσει σαφείς πληροφορίες στους επίδοξους whistleblowers για το πώς πρέπει να κάνουν χρήση της πλατφόρμας. Αυτό λοιπόν που πρέπει να κάνουν οι πληροφοριοδότες είναι να πάνε σε ένα internet spot όπου η σύνδεση είναι δημόσια, στο οποίο συνήθως δε συχνάζουν και, χρησιμοποιώντας το περιβάλλον Tails, να κατεβάσουν τον πλοηγτή Tor. Αφού τον εγκαταστήσουν, θα πρέπει να πληκτρολογήσουν τη διεύθυνση του ινστιτούτου στη γραμμή διευθύνσεων και μέσω της πλατφόρμας που ήδη θα έχουν μπροστά τους μπορούν να επικοινωνήσουν απρόσκοπτα και με ασφάλεια με το ινστιτούτο. Ο χρήστης λαμβάνει και έναν κωδικό, ο οποίος θα πρέπει να κρατηθεί μυστικός και απαιτείται σε κάθε επικοινωνία του χρήστη με το πανεπιστήμιο, μέσω της πλατφόρμας. Σε περίπτωση που ο χρήστης χάσει τον κωδικό, δεν θα είναι δυνατή η συνέχιση της επικοινωνίας με το ινστιτούτο. Ο σαφής και λεπτομερής τρόπος που περιγράφει τη διαδικασία της ορθής επικοινωνίας μέσω

του SecureDrop, δείχνει πόσο μεγάλη σημασία δίνει το κορυφαίο αμερικανικό πανεπιστήμιο στη διαδικασία της ασφαλούς διαρροής μυστικών πληροφοριών.

4. Η σημασία της ασφαλούς επικοινωνίας

Η σημασία που έχει το λογισμικό ασφαλούς ψηφιακής επικοινωνίας για τον πολλαπλασιασμό των whistleblowers ενισχύεται, όσο αυξάνονται οι απειλές που δυνητικά μπορεί να αντιμετωπίσει ένας πληροφοριοδότης. Πολλές μελέτες έχουν γίνει γύρω από το κόστος που μπορεί να έχει η διαρροή σκανδάλων για τους πληροφοριοδότες (Bjorkelo, 2013; Devine and Maassarani, 2011; MesmerMagnus and Viswesvaran, 2005; Paul and Townsend, 1996; Rehge et al. 2008). Οι κίνδυνοι οι οποίοι ελλοχεύουν για τους whistleblowers επιτάσσουν την πραγματοποίηση της διαρροής υπό συνθήκες μυστικότητας. Όσο πιο μεγάλοι είναι αυτοί οι κίνδυνοι, τόσο πιο επιτακτική είναι η ανάγκη διατήρησης της ανωνυμίας της πηγής.

4.1 Οι ερευνητική δημοσιογραφία σε κίνδυνο

Το 2017 και το 2018 ήταν δυο τραγικά έτη για την ευρωπαϊκή ερευνητική δημοσιογραφία. Στις 16 Οκτωβρίου 2017 δολοφονήθηκε, από εκρηκτικό μηχανισμό που είχε τοποθετηθεί στο αυτοκίνητό της, η Μαλτέζα δημοσιογράφος Daphne Caruana Galizia, η οποία ερευνούσε φαινόμενα κρατικής διαφθοράς και είχε, μεταξύ άλλων, αποκαλύψει την εμπλοκή της κυβέρνησης της χώρας της στα περίφημα Panama Papers¹⁴. Λίγους μήνες αργότερα, στις 21 Φεβρουαρίου του επομένου έτους, ο Σλοβάκος δημοσιογράφος Jan Kuciak, ο οποίος ερευνούσε την διαπλοκή της πολιτικής elite της χώρας του με το οργανωμένο οικονομικό έγκλημα, πυροβολήθηκε στο σπίτι του. Πρόκειται για απροκάλυπτες δολοφονίες Ευρωπαίων δημοσιογράφων σε ευρωπαϊκό έδαφος, που είχαν περισσότερη ή λιγότερη επίδραση στο πολιτικό σκηνικό των χωρών τους, καθώς η δεύτερη ξεσήκωσε τη λαϊκή οργή και οδήγησε στην παραίτηση της κυβέρνησης του Robert Fico, λίγες ημέρες αργότερα¹⁶, κάτι που, ελλείψει αντίστοιχων μαζικών αντιδράσεων, συνέβη για την κυβέρνηση του Joseph Muscat περισσότερα από δύο χρόνια μετά, στη Μάλτα¹⁷.

Οι παραπάνω τραγικές ιστορίες είναι επόμενο ότι αποτελούν καίριο πλήγμα για την ερευνητική δημοσιογραφία, καθώς αποθαρρύνουν αμφότερους, whistleblowers και δημοσιογράφους. Η πίεση που δέχεται, χρόνια μετά τη δολοφονία της δημοσιογράφου, η βασική πληροφοριοδότης της Daphne Caruana Galizia, πρώην τραπεζική υπάλληλος, Maria Efimova,

είναι ενδεικτική της δραματικής επίδρασης που μπορεί να έχει μια διαρροή για την υπόλοιπη ζωή του πληροφοριοδότη¹⁸.

4.2 Ο στιγματισμός του whistleblower

Πολλές μελέτες έχουν διαπιστώσει ότι η διαδικασία της διαρροής πληροφοριών δεν είναι ένα στιγμιαίο γεγονός το οποίο παύει, όταν σταματήσει ο θόρυβος γύρω από το αποκαλυφθέν σκάνδαλο (Weiskopf and Tobias-Miersch, 2016). Τα άτομα που αποφασίζουν να μιλήσουν, δεν κινδυνεύουν μόνο στιγμιαία από προσπάθεια φίμωσης, με διάφορους τρόπους, αλλά, εφόσον καταφέρουν να επιβιώσουν, φέρουν συχνά για πάντα το στίγμα του πληροφοριοδότη. Μπορεί για μερικούς βέβαια αυτό να μην έχει μόνο αρνητικό πρόσημο, όπως στην περίπτωση του Edward Snowden, αλλά στις περισσότερες περιπτώσεις η ηρωοποίηση ξεχνιέται γρήγορα και οι πληροφοριοδότες καλούνται τουλάχιστον να αλλάξουν επάγγελμα¹⁹. Ποιός θα ήθελε, για παράδειγμα, έναν τραπεζικό υπάλληλο που έχει δώσει στον τύπο στοιχεία που αποδείκνυν την εμπλοκή της τράπεζας όπου εργαζόταν σε οικονομικά σκάνδαλα.

Ο Clegg (2020) κάνει λόγο για κοινωνικό αποκλεισμό των whistleblowers που στιγματίζονται από τους εργοδότες, τους συναδέλφους και τα μέσα ενημέρωσης. Ο στιγματισμός χρησιμοποιείται σαν όπλο για τη μείωση της λαϊκής αποδοχής του ανθρώπου που αποφασίζει να μιλήσει, τον περιορισμό της δράσης του, τη συρρίκνωση του ενδιαφέροντος του κοινού για το θέμα και τελικά τον περιορισμό ανάλογων πράξεων (Ash, 2016; Foxley, 2019). Εταιρείες και οργανισμοί εμφανίζονται να επιδιώκουν συστηματική καταστροφή της φήμης των whistleblowers, προκειμένου στη μάχη μεταξύ της αξιοπιστίας του ατόμου και εκείνης του οργανισμού, να μπορέσει να επικρατήσει η δεύτερη (Alford, 2001; Devine and Maassarani, 2011).

Η αποτελεσματικότητα της διαρροής πληροφοριών βασίζεται στην αξιοπιστία, η οποία με τη σειρά της εδρεύει στην εγκυρότητα της μαρτυρίας και τη φερεγγυότητα εκείνου που κάνει τις αποκαλύψεις (Paul and Townsend, 1996). Ενώ οι οργανισμοί και τα καθεστώτα δεν μπορούν εύκολα να διαψεύσουν την μαρτυρία που είναι τεκμηριωμένη, μπορούν πολύ πιο εύκολα να βλάψουν ή να καταστρέψουν τη φήμη, και ως εκ τούτου την αξιοπιστία, του ατόμου (Foxley, 2019). Πράγματι, αν ο χαρακτήρας και η μαρτυρία του whistleblower ληφθούν σοβαρά υπ' όψιν, τότε οι δράστες και οι οργανισμοί τους βρίσκονται αντιμέτωποι με την προσωπική,

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

επαγγελματική και εταιρική σπίλωση, με πιθανές τεράστιες εμπορικές, πολιτικές και οικονομικές απώλειες (Dasgupta and Kesharwani, 2010). Για αυτό, το ζήτημα της αποκάλυψης των κακώς κειμένων σύντομα κλιμακώνεται σε μια μάχη φήμης μεταξύ της εταιρείας ή του οργανισμού και του whistleblower, με αποτέλεσμα η διαμάχη να μετατρέπεται σε μια πάλη ανάμεσα στο σφάλμα του οργανισμού και το σφάλμα του ατόμου (Alford, 2001). Ως εκ τούτου, ο στιγματισμός του πληροφοριοδότη γίνεται βασικό στοιχείο της αμυντικής στρατηγικής του οργανισμού.

Ιδιαίτερο ενδιαφέρον έχει η πεποίθηση που συχνά υπάρχει και που προέρχεται από την πλευρά του οργανισμού, ότι ο πληροφοριοδότης έχει συνήθως προσωπικά και οικονομικά κίνητρα και για αυτό προβαίνει στις συγκεκριμένες αποκαλύψεις (Armstrong et al., 2015; Oakley and Myers, 2004; Skivenes and Trygstad, 2010). Για αυτό το λόγο στα μάτια της κοινής γνώμης, αυτό το στερεότυπο εγείρει έναν παράδοξο σκεπτικισμό σχετικά με τα πραγματικά κίνητρα του whistleblower, παραγκωνίζοντας το πραγματικό γεγονός της αποκάλυψης παράνομων, ανήθικων ή ανάρμοστων πράξεων (Vinten, 1994).

Σύμφωνα με έρευνα μεταξύ 14 Βρετανών whistleblowers από διάφορους επαγγελματικούς χώρους, που πραγματοποίησε το 2017, το Centre for Applied Human Rights, του πανεπιστημίου του York, παρότι ποτέ δεν υπήρξε επίσημη blacklist στους συγκεκριμένους επαγγελματικούς χώρους, όλοι οι μετέχοντες στην έρευνα απάντησαν ότι πιστεύουν ότι ήταν, ανεπίσημα, επαγγελματικά στιγματισμένοι. Δήλωσαν ότι ως αποτέλεσμα της διαρροής τους, η επαγγελματική τους φήμη στιγματίστηκε και η παρούσα και μελλοντική τους σταδιοδρομία χειροτέρεψε. Παράλληλα, όλοι θεωρούν ότι αντιμετωπίζονται ως πιθανός κίνδυνος για τις δουλειές στις οποίες απευθύνονται (Foxley, 2019).

Η διαρροή της πληροφορίας όμως δεν επηρεάζει μόνο το μέλλον του whistleblower, αλλά κυρίως το παρόν του, με την επαγγελματική σχέση του με τον οργανισμό, στον οποίο εργάζεται, να κλονίζεται μετά από τις αποκαλύψεις. Η έντεκα από τους 14 πληροφοριοδότες που συμμετείχαν στην έρευνα είτε απολύθηκαν ή συνταξιοδοτήθηκαν ή δεν τους ανανεώθηκε το συμβόλαιο. Από τους υπόλοιπους τρεις, ο ένας είχε ήδη παραιτηθεί πριν τη διαρροή, ενώ οι άλλοι δύο συνέχισαν.

Είναι προφανές ότι η απώλεια της εργασίας είναι από τους βασικότερους κινδύνους που αντιμετωπίζει ένας whistleblower και ο πλέον δεδομένος, με τεράστιες ενδεχομένως

οικονομικές συνέπειες. Η δυσκολία στην εξεύρεση δουλειάς στο ίδιο επάγγελμα είναι δεδομένη και ακόμη και αν ξεπεραστεί, συνήθως αφορά πολύ πιο χαμηλόβαθμες θέσεις από αυτή που κατείχε (Floxley, 2019).

Πέρα όμως από τον επαγγελματικό στίβο, οι βολές από τον οργανισμό ρίπτονται και κατά της προσωπικής ζωής των whistleblowers, επιδιώκοντας πολλές φορές να τους παρουσιάσουν ψυχικά διαταραγμένους ή πνευματικά ανεπαρκείς (Moore, 2015). Η ψυχολογική πίεση που περιέγραψαν, σύμφωνα με τον Floxley (2019), ότι υπέστησαν οι πληροφοριοδότες, κατά το διάστημα των αποκαλύψεων στις οποίες προέβησαν, είναι πολύ μεγάλη. Η προσπάθεια της εταιρείας να διαστρεβλώσει στοιχεία του χαρακτήρα και της προσωπικότητάς τους είναι ιδιαίτερα οργανωμένη. “Οι άνθρωποι αυτοί χρειάζονται τεράστια ψυχολογική υποστήριξη σε συνδυασμό με την κατάλληλη εκπαίδευση και πρακτικές συμβουλές για το πώς να αντιμετωπίσουν καλύτερα την κατάσταση. Οι συμβουλές αυτές έχουν να κάνουν με τον τρόπο που θα επιλέξουν να διαρρεύσουν της πληροφορία και τα στοιχεία που θα παρουσιάσουν”, εξηγεί ο Floxley (2019). Πολλοί ήταν εκείνοι δε, που παραδέχτηκαν ότι η υποστήριξη της δράσης τους από τα μέσα, λειτούργησε θεραπευτικά στη ζημία που προκλήθηκε στην επαγγελματική και προσωπική τους ζωή ως συνέπεια της πράξης τους.

Τα μέσα ενημέρωσης μπορούν με πολλούς τρόπους να παρέχουν τη στήριξή τους στους μάρτυρες δημοσίου συμφέροντος. Η παροχή υπηρεσιών ασφαλούς επικοινωνίας μέσω των σχετικών πλατφόρμων έχει διπλό ρόλο στην παροχή στήριξης στους πληροφοριοδότες. Από τη μια οι πλατφόρμες παρέχουν ένα ασφαλές περιβάλλον, εντός του οποίου ο whistleblower έρχεται σε επαφή με το μέσο, δίνει τα στοιχεία που κατέχει και αποφασίζει ο ίδιος πότε θα αποκαλύψει την ταυτότητά του και μόνο σε περίπτωση που το επιθυμεί. Η συμβολή τους ως προς αυτό το σκέλος είναι τεράστια, καθώς η επικοινωνία του πληροφοριοδότη με το μέσο μπορεί να λάβει μεγάλο χρονικό διάστημα μέχρι οι δύο πλευρές να συμφωνήσουν στην προβολή του θέματος. Αν μέχρι τότε οι συνομιλίες τους γίνουν αντιληπτές από φορείς παρακολούθησης, μπορεί όχι μόνο η διαρροή να μην πραγματοποιηθεί ποτέ, αλλά μπορεί να κινδυνέψουν και οι εμπλεκόμενοι, ανάλογα με τη σοβαρότητα της καταγγελίας. Από την άλλη, η παροχή από τα μέσα εργαλείων που στοχεύουν αποκλειστικά στην προστασία των whistleblowers, δείχνει τη βαρύτητα που δίνουν οι δημοσιογραφικοί οργανισμοί στη διαδικασία της διαρροή και αποτελούν εγγύηση για τη στήριξη του πληροφοριοδότη. Ένα

μέσο ενημέρωσης που διαθέτει ειδική πλατφόρμα για επικοινωνία με whistleblowers δε μπορεί παρά να τους πιστεύει και να τους στηρίζει, σε κάθε περίπτωση.

4.3 Ο whistleblower ως κίνδυνος.

Μπορεί ο whistleblower να έχει πολλούς λόγους να φοβάται να μιλήσει, αλλά ο ίδιος από μόνος τους είναι μέγας κίνδυνος για τους φορείς της κατεστημένης διαφθοράς (Snowden 2020). Η ύπαρξη εργαλείων ασφαλούς επικοινωνίας στα μέσα ενημέρωσης, τα οποία οφείλουν να ελέγχουν τα κέντρα εξουσίας, είναι ο μόνος τρόπος για να μιλήσουν όσοι πρέπει να μιλήσουν, αλλά και για να προστατευτούν αυτοί που ξέρουν.

Ο Κώστας Τσαλικίδης¹⁹ θα μπορούσε να είναι ο εμβληματικότερος Έλληνας whistleblower, όλων των εποχών, αν δεν είχε δολοφονηθεί. Ουδείς γνωρίζει βέβαια αν είχε σκοπό να μιλήσει, αλλά όλοι πλέον γνωρίζουμε ότι ήξερε. Κάτι που γνώριζαν και οι δολοφόνοί του. Ο 39χρονος, τότε, μηχανικός δικτύου της Vodafone, βρέθηκε απαγχονισμένος στο σπίτι του στον Κολωνό, στις 9 Μαρτίου του 2005. Ήταν μια αυτοκτονία που δεν απασχόλησε τα φώτα της δημοσιότητας, αλλά ουδέποτε έγινε πιστευτή από τον αδερφό του, Παναγιώτη. Ο τελευταίος, αφού φωτογράφησε το θύμα και το χώρο με κάθε λεπτομέρεια και συνέλεξε οποιοδήποτε στοιχείο θα μπορούσε να φανεί χρήσιμο, ξεκίνησε ένα πολυετή δικαστικό αγώνα για να αποδείξει την αλήθεια.

Δύο δικαστικά πορίσματα αποφάνθηκαν ότι επρόκειτο για αυτοκτονία. Το πρώτο το 2006 και το δεύτερο το 2014. Όμως η οικογένεια Τσαλικίδη προσέφυγε, το Νοέμβριο του 2014, στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, το οποίο απεφάνθη ότι τα ελληνικά δικαστήρια δεν είχαν διεξάγει επαρκή έρευνα για τα αίτια του θανάτου του. Ως αποτέλεσμα, η Εισαγγελία Εφετών Αθηνών άνοιξε πάλι την υπόθεση και, τον Ιούνιο του 2018, το Πρωτοδικείο Αθηνών υποβάλλει μήνυση κατά αγνώστου για ανθρωποκτονία από πρόθεση, καθώς ο θάνατος του Κώστα Τσαλικίδη ήταν αποτέλεσμα οργανωμένου εγκλήματος.

Το ερώτημα που τίθεται είναι κατά πόσο θα μπορούσε η ύπαρξη λογισμικού ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblowers να έχει οδηγήσει όχι μόνο στην πρόωρη αποκάλυψη του μεγαλύτερου σκανδάλου κατασκοπείαςⁱⁱⁱ που έχει καταγραφεί στην χώρα μας, αλλά και στην αποτροπή του αποτρόπαιου εγκλήματος. Το σκάνδαλο αποκάλυψε η

ίδια η κυβέρνηση το Φεβρουάριο του 2006. Αν ο Τσαλικίδης είχε μιλήσει, θα είχε αποκαλυφθεί, ένα χρόνο νωρίτερα, η παρακολούθηση Ελλήνων πολιτών, στις αρχές του 2005. Πρωτίστως όμως θα είχε αποκαλυφθεί η παράνομη, καθώς έλειπε το αντίστοιχο νομοθετικό πλαίσιο, παρακολούθηση που διεξήγαγαν από κοινού οι ελληνικές και αμερικανικές μυστικές υπηρεσίες, κατά τη διάρκεια των Ολυμπιακών Αγώνων. Η ετεροχρονισμένη δημοσίευση του Προεδρικού Διατάγματος για τη νομιμοποίηση των παραπάνω παρακολουθήσεων, έγινε την επομένη της δολοφονίας Τσαλικίδη.

Οι ψηφιακές πλατφόρμες ασφαλούς επικοινωνίας πέρα από το προφανές όφελος που προσθέτουν στο συλλογικό συμφέρον, μπορεί να αποβούν σωτήριες και για μεμονωμένα άτομα που βρέθηκαν αντιμέτωποι με σκανδαλώδεις πληροφορίες. Δεν είναι η αποκάλυψη του μυστικού που θέτει σε κίνδυνο εκείνον που γνωρίζει, αλλά η γνώση του αυτή καθαυτή. Ο μόνος τρόπος για να μπορέσει να απαλλαγεί από το βάρος του μυστικού και τους κινδύνους που το συνοδεύουν, είναι να μιλήσει και οι ψηφιακές πλατφόρμες παρέχουν τον πιο άμεσο και ασφαλή τρόπο.

Επίλογος

Η ερευνητική δημοσιογραφία αποτελεί θεματοφύλακα της δημοκρατίας. Είναι το πιο ισχυρό και διαχρονικό εργαλείο μιας ελεύθερης κοινωνίας για τον έλεγχο των κέντρων εξουσίας. Είναι η δημοσιογραφία που παραδοσιακά διατηρεί τον πρωταρχικό αξιακό της κανόνα και στέκεται μακριά από την εξουσία. Τα εργαλεία και οι μέθοδοι άσκησής της ποικίλουν, αλλά εκείνο που δεν μπορεί να λείπει σχεδόν σε καμία έρευνα είναι οι πηγές του δημοσιογράφου. Όσα στοιχεία και αν μπορέσει να αντλήσει μόνος του, πάντα υπάρχουν άνθρωποι, ικανοί να ενδυναμώσουν την έρευνά του. Και εκτός από αυτούς που μπορεί να βρει μόνος του κατά τη διαδικασία του ρεπορτάζ, υπάρχουν και οι εθελοντές, οι περίφημοι whistleblowers.

Την ευαίσθητη αυτή ομάδα των ανθρώπων που κυρίως λόγω της επαγγελματικής τους θέσης, γνωρίζουν γεγονότα που δεν συνάδουν με τον ορισμό μιας ευνομούμενης πολιτείας, καλείται να προσελκύσει ο ερευνητής δημοσιογράφος. Οι πλατφόρμες ασφαλούς ψηφιακής επικοινωνίας είναι το χρησιμότερο εργαλείο για την επίτευξη του παραπάνω στόχου. Ιδιαίτερα το τελευταίο διάστημα η επικαιρότητα αποδεικνύει πόσο πολύτιμη είναι η χρήση των συγκεκριμένων δυνατοτήτων της ψηφιακής τεχνολογίας.

Πόσο διαφορετικός θα ήταν άραγε ο κόσμος της τέχνης, του αθλητισμού, αλλά και κάθε επαγγελματικός χώρος αν υπήρχε η δυνατότητα ανώνυμων αλλά εμπεριστατωμένων καταγγελιών στον τύπο, κάθε μορφής κακοποίησης και ανάρμοστης συμπεριφοράς. Η καταγγελίες εγκληματικών πράξεων, είκοσι χρόνια μετά την τέλεσή τους, πέρα από την αδυναμία δίωξης των δραστών, καθώς έχει επέλθει παραγραφή τους, δεν αποτελούν λύση του προβλήματος. Μπορεί να στοχεύουν στον κοινωνικό στιγματισμό του θύτη, στην επαγγελματική του περιθωριοποίηση και την εδραίωση μια νέας πιο ανθρωποκεντρικής κουλτούρας στους εργασιακούς χώρους, αλλά αποτελούν μερική λύση των προβλημάτων. Οι παθογένειες, οποιασδήποτε μορφής, πρέπει να επισημαίνονται κατά την τέλεσή τους. Ο άνθρωπος που κακοποίησε άνθρωπο πριν είκοσι χρόνια είναι πολύ πιθανό να το έκανε πολλές φορές και τα είκοσι χρόνια που μεσολάβησαν από τότε.

Πόσα εγκλήματα πραγματοποιούνται σήμερα που θα τα μάθουμε, πιθανώς μετά από 20 χρόνια; Πόσοι εργαζόμενοι δεν θα είχαν πολλά να πουν σχετικά με τη στάση που κρατά ο εργοδότης τους, κρατικός ή ιδιωτικός, απέναντι στην πανδημία και τα μέτρα υγειονομικής προστασίας και οικονομικής στήριξης; Ο φόβος όμως, της απόλυσης και της επαγγελματικής

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

περιθωριοποίησης είναι παρόν. Για αυτό ακριβώς τα εργαλεία που παρουσίασε η συγκεκριμένη εργασία είναι κεφαλαιώδους σημασίας όχι μόνο για την αξιοπρεπή άσκηση του δημοσιογραφικού επαγγέλματος, το κύρος του οποίου ιδιαίτερα στη χώρα μας φυλλοροεί, αλλά κυρίως για την προάσπιση του δημοσίου συμφέροντος.

Τα WikiLeaks έκαναν την αρχή. Έδωσαν βήμα να μιλήσουν και να δημοσιοποιήσουν τα στοιχεία που διαθέτουν πολλοί κρατικοί και ιδιωτικοί υπάλληλοι. Ο Edward Snowden αποτέλεσε το πρόσωπο κλειδί στην ιστορία της ασφαλούς επικοινωνίας μεταξύ δημοσιογράφων και whistleblower. Δεν έκανε απλώς μια ακόμη σημαντική αποκάλυψη. Χτύπησε στον πυρήνα της ερευνητικής δημοσιογραφίας, αποκαλύπτοντας τη διάτρητη ασφάλεια της ψηφιακής επικοινωνίας. Μπορεί η κρυπτογράφηση των ηλεκτρονικών μηνυμάτων να χρησιμοποιείται δειλά από τα τέλη του περασμένου αιώνα, αλλά η ώθηση στην ασφαλή επικοινωνία πραγματοποιήθηκε με τις πλατφόρμες ασφαλούς επικοινωνίας και κυρίως με το SecureDrop και το GlobalLeaks.

Η ελεύθερη διάθεσή τους από το διαδίκτυο αποτελεί βασικό στοιχείο της ύπαρξής τους, καθώς στοχεύουν στην απρόσκοπτη διακίνηση της γνώσης και της πληροφορίας και δεν θα μπορούσαν να είναι εμπορικά προϊόντα. Η χρήση τους από κορυφαία μέσα ενημέρωσης σε όλο τον κόσμο αποδεικνύει τη σπουδαιότητά τους. Η απουσία τους από τα ελληνικά ΜΜΕ, με μοναδική εξαίρεση την ελληνική έκδοση της huffington post, δεν μπορεί να εξεταστεί ξέχωρα από τη μειωμένη αξιοπιστία που απολαμβάνουν τα μέσα στη χώρα μας. Η ερευνητική δημοσιογραφία, μέσα από τα ψηφιακά εργαλεία που δίνει η νέα τεχνολογία, αποτελεί μονόδρομο τόσο για τη βελτίωση της εικόνας του επαγγέλματος, όσο και για την προστασία της δημοκρατίας.

Στο σημείο αυτό θα μπορούσε η ακαδημαϊκή έρευνα να δώσει ώθηση στην εισαγωγή των νέων αυτών εργαλείων στη δημοσιογραφική πρακτική. Ιδιαίτερα στη χώρα μας και με δεδομένη την ύπαρξη πανεπιστημιακών τμημάτων δημοσιογραφίας, θα πρέπει να ξεκινήσει η ακαδημαϊκή έρευνα στο πεδίο της ερευνητικής δημοσιογραφίας. Οι νέοι φοιτητές που γοητεύονται από το επάγγελμα του δημοσιογράφου πρέπει να γνωρίσουν τη δυσκολότερη αλλά πιο ενδιαφέρουσα και απαραίτητη πλευρά της. Εκείνη της ερευνητικής δημοσιογραφίας στη σύγχρονη ψηφιακή εποχή. Παράλληλα, η παραγωγή υλικού ακαδημαϊκής έρευνα γύρω από το θέμα της ερευνητικής δημοσιογραφίας και των εργαλείων που μπορεί να αξιοποιήσει θα ωθήσει και τους επαγγελματίες δημοσιογράφους να επαναπροσδιορίσουν τους στόχους και τις πρακτικές

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

τους και να αποδώσουν στην ερευνητική δημοσιογραφία το μερίδιο προσοχής που απαιτεί το δημόσιο συμφέρον και η δημοκρατία.

Βιβλιογραφία

ACCA. (2016). Effective whistleblowing arrangements. Retrieved January 29, 2019, from <https://www.accaglobal.com/uk/en/technical-activities/technical-resources-search/2016/may/effectivespeak-up-arrangements-for-whistle-blowers.html>.

ACFE. (2018). Report to the nations: 2018 global study on occupational fraud and abuse. Retrieved November 21, 2019, from <https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf>

ACLU and Human Rights Watch. (2014). With Liberty to Monitor All. How Large Scale US Surveillance Is Harming Journalism, Law and American Democracy¹.

Alford, F. (2001) Whistleblowers: Broken lives and organizational power. Ithaca: Cornell University Press.

Angwin, J. (2017). Digital Security for Journalists. In E. Bee and T. Owen (Eds.), Journalism After Snowden. The Future of the Free Press in the Surveillance State. New York: Columbia Journalism Review Books¹.

Armstrong, A.F., I. Foxley and R.D. Francis (2015) ‘Whistleblowing: a three-part view’, Journal of Financial Crime, 22(2): 208-218.

Ash, A. (2016) Whistleblowing and ethics in health and social care. London: Jessica Kingsley Publishers.

BBC News (2010, November 29) Siphnet: Where the Leaked Cables Came from. BBC News¹.

Baack, S. (2013). A New Style of News Reporting: WikiLeaks and Data-Driven Journalism. Scotts Valley: CreateSpace Independent Publishing Platform¹.

Beaude, B. (2016). The Ends of the Internet. Network Notebook. Institute of Network Cultures¹.

Beckett, C., and Ball, J. (2012) Wikileaks. News in the Networked Era. Cambridge: Polity Press¹.

Benkler, Y. (2011). Networks of Power, Degrees of Freedom. International Journal of Communication¹.

Bieber, C. (2013). Lessons of the Leaks. In J. Hartley, J. Burgess, and A. Bruns (Eds.), A Companion to New Media Dynamics¹.

Blake, M., Aronsen, G., and Liebelson, D. (2013). There Is no Such Thing as NSA Proof Email. Mother Jones¹.

Bjorkelo, B. (2013). Workplace bullying after whistleblowing: Future research and implications. Journal of Managerial Psychology, 28(3), 306–323.

Bosua, R., Milton, S., Dreyfus, S., και Lederman, R. (2014). Going Public: Researching External Whistleblowing in a New Media Age. International Handbook on Whistleblowing Research¹.

Brown, A. J., Bybee, C., Wearden, S., and Vandekerckove, W. (Eds.). (2014). International Handbook on Whistleblowing Research¹.

Carlo, S. and Kamphuis, A. (2014). Information Security for Journalists. Protecting Your Story, Your Source and Yourself Online. The Centre for Investigative Journalism¹.

Chen, N. (2011). WikiLeaks and Its Spinoffs: New Models of Journalism or the New Media Gatekeepers. Journal of Digital Research and Publishing¹.

Christensen, C. (2014). WikiLeaks and the Afterlife of Collateral Murder. International Journal of Communication¹.

Clegg, S. (2020). Organizing the Identity of the Whistleblower: Stigma, power and resistance. Journal of Political Power, 13(1), 161–163.

Cox, J. (2014). Why All the Snowden Docs Should Be Public: An Interview with Cryptome. Motherboard¹.

Devine, T. (2012). Corporate whistleblowers gain new rights and opportunities in the us. Space for transparency, transparency international. Retrieved January 28, 2019, from <https://blog.transparency.org/2012/10/01/corporate-whistleblowers-gain-new-rights-and-opportunities-in-the-us/>

Devine, T. and T.F. Maassarani (2011) The corporate whistleblower's survival guide, San Francisco: Berrett-Koehler Publishers Inc, in association with the Government Accountability Project.

Di Salvo, Ph., (2020). Digital Whistleblowing Platforms in Journalism. Encrypting Leaks. Palgrave Macmillan.

Dworkin, T. M., and Baucus, M. S. (1998). Internal vs. External Whistleblowing: A Comparison of Whistleblowing Processes¹.

Di Salvo, P. and Porlezza, C. (2014). OpenLeaks. In K. Harvey (Ed.), Encyclopedia of Social Media and Politics. Thousand Oaks: Sage Publications¹.

Fakhouri, H. (2011). WSJ and Al Jazeera Lure Whistleblowers with False Promises of Anonymity. Electronic Frontier Foundation¹.

Faviar, C. (2016). FBI Demands Signal User Data, But There's Not Much to Hand Over. Ars Technica¹.

Foxley, I. (2019). Overcoming stigma: Whistleblowers as 'supranormal' members of society? Ephemera Theory and politics in organization

Franceschi Bicchierai, L. (2015). Even the Inventor of PGP Doesn't Use PGP. Motherboard.vice.com¹.

Greenberg, A. (2011). Researchers Say WSJ's WikiLeaks Copycat Is Full of Holes. Forbes¹.

Greenberg, A. (2012). This Machine Kills Secrets. New York: Penguin¹.

Heemsbergen, L. J. (2016). From Radical Transparency to Radical Disclosure: Reconfiguring (in)Voluntary Transparency Through the Management of Visibilities. *International Journal of Communication*¹.

Hellegren, Z. I. (2017). A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom. *Internet Histories*¹.

Henrichsen, J. R., Betz, M., and Lisosky, J. M. (2015). Building Digital Safety for Journalism: A Survey of Selected Issues. UNESCO¹.

Hintz, A., Dencik, L., and Wahl - Jorgensen, K. (2016). Digital Citizenship in a Datafied Society. Hoboken: Wiley¹.

Jordan, T. (2008). Haching. Cambridge: Polity¹.

Kenny, K., & Fotaki, M. (2019). Post-disclosure survival strategies: Transforming whistleblower experiences. NUI Galway, Galway. Retrieved July 31, 2020, from <https://www.whistleblowingimpact.org/wp-content/uploads/2019/06/19-Costs-of-WhistleblowingESRC-report.pdf>

Kirchner, L. (2013). Teaching J-School Students Cyber-Security. *Columbia Journalism Review*¹.

Lee, M. (2013). Encryption Works: How to Protect Your Privacy in the Age of NSA SurveilLance. Freedom of the Press Foundation¹.

Lee, M. (2014). Ed. Snowden Taught Me to Smuggle Secrets Past Incredible Dangers. Now I Teach You¹.

Lengel, L. (2014). TuniLeaks. In K. Harvey (Ed.), Encyclopedia of Social Media and Politics. Thousand Oaks: Sage Publications¹.

Lewis, D., Brown, A. J., and Moberly, R. (2014). Whistleblowing, Its Importance and the state of the Research¹.

Lovink, G. (2016). Social Media Abyss: Critical Internet Cultures and the Force of Negation. Hoboken: Wiley¹.

Lynch, L. (2010). “We’ re Going to Crack the World Open”. WikiLeaks and the Future of Investigative Reporting. Journalism Practice¹.

Lyon D. (2015). Surveillance After Snowden, Cambridge: Polity¹.

Madar, C. (2013). The Passion of Bradley Manning: The Story Behind the WikiLeaks whistleblower. New York. Verso Books¹.

McCullagh, D. (2010). WikiLeaks’ Estranged Co Founder Becomes a Critic. CNET¹.

McGregor, S. (2014). Digital Security and Source Protection for Journalists. A Handbook. Tow Center for Digital Journalism¹.

Mesmer-Magnus, J., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics*, 62(3), 277–297.

Miceli M. P. and Near J. P., *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*, New York: Lexington Books¹.

Moore, P. (2015) *Crash Bank Wallop*. York: New Wilberforce Media.

Myers West, S. (2017). *Survival of the Cryptic*. Limn¹.

O'Brien, K. J. (2015). Why Encryption Is Crucial for All News Organizations. *Columbia Journalism Review*¹.

Oakley, E. and A. Myers (2004) 'The UK: Public Concern at Work', in R. Calland and G. Dehn (eds.) *Whistleblowing around the world, law, culture and practice*. London: The Open Democracy Advice Centre.

Paul, R. J., & Townsend, J. B. (1996). Don't kill the messenger! Whistleblowing in America—A review with recommendations. *Employee Responsibilities and Rights Journal*, 9(2), 149–161.

Phillips, D. J. (2001). *Cryptography, Secrets, and the Structuring of Trust*. In P. E. Agre and M. Rotenberg (Eds.), (1998). *Technology and Privacy: The New Landscape*. Cambridge, MA: The MIT Press¹.

Rehg, M. T., Miceli, M. P., Near, J. P., & Van Scotter, J. R. (2008). Antecedents and outcomes of retaliation against whistleblowers: Gender differences and power relationships. *Organization Science*, 19(2), 221–240.

Rhee, M. Y. (2003). *Internet Security. Cryptographic Principles, Algorithms and Protocols*. Hoken: Wiley¹.

Rosenblum, A. (2016). Moxie Marlinspike Makes Encryption for Everyone Popular Science¹.

Ruby, F., Goggin, G. and Keane, j. (2017). “Comparative Silence” Still? Journalism, Academia, and the Five Eyes of Edward Snowden. *Digital Journalism*¹.

Schneier, B. (2015). *Data and Goliath. The Hidden Battle to Collect Your Data and Control Your World*. New York: Norton¹.

Sifry, M. L. (2011). *Wikileaks and the Age of Transparency*. Yale University Press¹.

Simon, J. (2015). *The New Censorship. Inside the Global Battle for Media Freedom*. New York: Columbia Journalism Review Books¹.

Singel, R. (2007, November 14). Sensitive Guantanamo Bay Manual Leaked Through Wiki Site. *Wired.com*¹.

Skivenes, M. and S. Trygstad (2010) ‘When whistleblowing works: The Norwegian case’, *Human Relations*, 63(7): 1071-1097.

Snowden, E. (2019). *Permanent Record*. Pan Macmillan.

Tigas, M. (2016). *A More Secure and Anonymous ProPublica Using Tor Hidden Services*. ProPublica¹.

Thorsen, E. (2019). *Surveillance of Journalists/Encryption Issues*. The International Encyclopedia of Journalism Studies. Hoboken: Wiley¹.

Tsui, L., and 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*¹.

Vandekerckhove, W., James, C., and West, F. (2013) *Whistleblowing: The Inside Story - A study of the Experiences of 1000 Whistleblowers*¹.

Vinten, G. (1994) *Whistleblowing, subversion or corporate citizenship?* London: Paul Chapman Publishing Ltd.

Weiskopf, R., & Tobias-Miersch, Y. (2016). Whistleblowing, parrhesia and the contestation of truth in the workplace. *Organization Studies*, 37(11), 1621–1640.

Wolfe, S., Worth, M., Dreyfus, S., and Brown, A. J. (2014). *Whistleblower Protection Laws in G20 Countries*¹.

Παραπομπές

1. Όπως αναφέρεται στο Di Salvo 2020.
2. <https://www.acfe.com/default.aspx>
3. <https://www.britannica.com/biography/Daniel-Ellsberg>
4. <https://www.britannica.com/biography/Chelsea-Manning>
5. <https://www.ellsberg.net/bio/>
6. <https://twitter.com/Snowden>
7. <https://securedrop.org/overview/no-third-parties-can-secretly-be-subpoenaed/>
8. <https://securedrop.org/overview/limits-metadata-trail-much-possible/>
9. <https://securedrop.org/overview/protects-against-hackers/>
10. <https://securedrop.org/overview/encrypted-and-air-gapped/>
11. <https://securedrop.org/overview/free-and-open-source-software/>

12. <https://tails.boum.org/about/index.en.html>
13. <https://www.hmdc.harvard.edu/securedrop.html>
14. <https://www.theguardian.com/world/ng-interactive/2020/oct/15/justice-on-trial-three-years-after-murder-daphne-caruana-galizia>
15. <https://balkaninsight.com/2020/08/05/jan-kuciak-a-murder-that-changed-slovakia/>
16. <https://www.npr.org/sections/thetwo-way/2018/03/15/593803439/slovakias-prime-minister-offers-to-resign-amid-protest-over-journalist-s-murder?t=1613315594048>
17. <https://www.theguardian.com/politics/2019/dec/01/malta-pm-joseph-muscat-quits-daphne-caruana-galizia>
18. <https://www.opendemocracy.net/en/can-europe-make-it/whistleblower-maria-efimova-fears-her-safety-amid-threats-and-new-arrest-warrants/>
19. <https://www.vice.com/el/article/mbkdq3/mia-aytoktonia-poy-htan-dolofonia-h-istoria-twn-ellhnikwn-ypoklopwn>
- <http://news.bbc.co.uk/2/hi/europe/4838552.stm>
20. <https://www.kathimerini.gr/investigations/832716/amerikanoi-kai-ellines-xekinisan-mazitis-ypoklopes-toy-2004/#fifthPage>
21. <https://www.theguardian.com/news/series/cambridge-analytica-files>

<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>

Σημειώσεις

i) Ο Aaron Swartz ήταν ένας Αμερικανός προγραμματιστής ο οποίος συνέδεσε άρρηκτα το όνομά του με την ελεύθερη διακίνηση της πληροφορίας στο Διαδίκτυο. Ο Swartz συμμετείχε σε πολλά projects και διαδικτυακές καμπάνιες για την ελευθερία στο internet, την ελευθερία του λόγου και τα ψηφιακά δικαιώματα. Μεταξύ άλλων ήταν ο σχεδιαστής του κώδικα RSS και ένας από τους προγραμματιστές του Reddit. Συμμετείχε στο σχεδιασμό των Creative Commons, για τα πνευματικά δικαιώματα, σε συνεργασία με τον καθηγητή Lawrence Lessig και στην κίνηση ενάντια στις νομοθετικές πράξεις SOPA και PIPA, οι οποίες προκαλούσαν κλυδωνισμούς στη διαδικτυακή ελευθερία. Υπερασπίστηκε μέχρις εσχάτων την ελεύθερη πρόσβαση στην ακαδημαϊκή έρευνα. Το 2011 μπήκε κρυφά στον χώρο όπου στεγαζόταν ο κεντρικός server της ψηφιακής βιβλιοθήκης JSTOR, η οποία παρέχει κυρίως άρθρα ακαδημαϊκής έρευνας, και κατέβασε σε σκληρό δίσκο χιλιάδες έγγραφα τα οποία ήταν προσβάσιμα επί πληρωμή στο κοινό. Στόχος του ήταν να τα ανεβάσει στο διαδίκτυο με ελεύθερη πρόσβαση. Η ενέργειά του αυτή τον οδήγησε στη σύλληψη και στην απαγγελία κατηγοριών που επέσυραν πολυετή κάθειρξη και υπέρογκα χρηματικά πρόστιμα. Στις 11 Ιανουαρίου 2013 βρέθηκε απαγχονισμένος στο διαμέρισμά του. Η επίσημη εκδοχή είναι ότι έδωσε μόνος του τέλος στη ζωή του στα 27 του χρόνια, χωρίς να αφήσει οποιοδήποτε μήνυμα ή εξήγηση. Οι αγώνες και το έργο του, πέρα από τις σημαντικές κατακτήσεις τους, αποτελούν πηγή έμπνευσης για όσους πιστεύουν στην αξία της ελεύθερης διακίνησης της γνώσης.

ii) Η απώλεια της δουλειάς και η αλλαγή καριέρας συνέβη βέβαια και στην περίπτωση του Edward Snowden, καθώς το ιστορικό του whistleblower δε μπορεί να συμπεριστεί με το επάγγελμα του πράκτορα. Όμως αυτό υπήρξε συνειδητή επιλογή του αμερικανού IT expert. Όπως ο ίδιος επισημαίνει στο moto του στο twitter “I used to work for the government, now I work for the public”.

iii) Έντεκα μήνες μετά τη δολοφονία Τσαλικίδη, στις 2 Φεβρουαρίου 2006, οι υπουργοί Δημόσιας Τάξης, Γιώργος Βουλγαράκης, Δικαιοσύνης, Αναστάσιος Παπαληγούρας και Επικρατείας, Θεόδωρος Ρουσόπουλος δίνουν κοινή συνέντευξη τύπου στην οποία αποκαλύπτουν το μεγαλύτερο σκάνδαλο κατασκοπείας που έχει καταγραφεί στη σύγχρονη ελληνική ιστορία. Πρόκειται για την παρακολούθηση των τηλεφώνων περισσότερων από 100

Βασιλική Διονυσοπούλου, Πλατφόρμες Ασφαλούς Επικοινωνίας

πολιτών και κρατικών αξιωματούχων, μεταξύ των οποίων και ο πρωθυπουργός Κώστας Καραμανλής. Ο Κώστας Τσαλικίδης, μετά από 11 χρόνια στη Vodafone, είχε υποβάλλει την παραίτησή του, 40 ημέρες πριν το θάνατό του. Τότε είχε εκμυστηρευτεί στο στενό του κύκλο ότι είναι ζήτημα ζωής και θανάτου να φύγει από την εταιρεία. Η τελευταία του είχε ζητήσει να μείνει μέχρι να βρει αντικαταστάτη. Η έρευνα που διεξήχθη, οδήγησε στο συμπέρασμα ότι είχε εντοπίσει την τρύπα ασφαλείας στο δίκτυο της εταιρείας. Την παραμονή της δολοφονίας του Τσαλικίδη, ο CEO της εταιρείας στην Ελλάδα, Γιώργος Κορωνιάς, δίνει εντολή να απεγκατασταθεί το αποκαλυφθέν παράνομο λογισμικό από το δίκτυο της εταιρείας, ενέργεια για την οποία δέχθηκε δριμεία κριτική, καθώς εμπόδισε τη διεξαγωγή έρευνας που θα μπορούσε να οδηγήσει στους δράστες. Ο CEO της Vodafone ζήτησε εκτάκτως ακρόαση από την κυβέρνηση, την επομένη του θανάτου του Τσαλικίδη, όπου αποκάλυψε την ανακάλυψη παράνομου λογισμικού, με αποτέλεσμα την έναρξη μυστικής εισαγγελικής έρευνας. Όπως αποκαλύφθηκε αργότερα, από τα έγγραφα που έδωσε στη δημοσιότητα το Edward Snowden, οι παρακολουθήσεις στην Ελλάδα αποτελούσαν κοινό έργο της ΕΥΠ και του NSA, έπειτα από αίτημα των αμερικανικών μυστικών υπηρεσιών, στα πλαίσια της αποτροπής τρομοκρατικών επιθέσεων, κατά τη διάρκεια διεξαγωγής των Ολυμπιακών Αγώνων. Η συνέχιση βέβαια των παρακολουθήσεων, πέντε μήνες μετά τη λήξη τους, ξεφεύγει από τον παραπάνω στόχο. Η σοβαρότητα της υπόθεσης φαίνεται και από την ψήφιση του απαραίτητου Προεδρικού Διατάγματος, για την κοινή συνεργασία μεταξύ της ΕΥΠ και του NSA με στόχο την πραγματοποίηση παρακολουθήσεων κατά τη διάρκεια των Ολυμπιακών Αγώνων του 2004, μόλις την επομένη της δολοφονίας Τσαλικίδη, στις 10 Μαρτίου 2005.

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.