Στοιχεία Δικαίου της Πληροφορίας

Ακαδημαϊκό έτος 2024-2025

*DarkNet & Δίκαιο*



Μπαλάση Ηλιάνα 3190303

Παπανικολάου Στέφανος 3200142

Παναγιώτα Φυτάλη 3200215

Περιεχόμενα

1. Εισαγωγή
2. Σύντομη περιγραφή του DarkNet και των λειτουργιών του
3. Γενικό Νομοθετικό Υπόβαθρο
   1. Εθνική Νομοθεσία που αφορά το DarkNet
   2. Εθνική Νομολογία που αφορά το DarkNet
   3. GDPR και Darknet
   4. Ενδεικτικές Οδηγίες (ΕΕ) και Darknet
4. Silk Road – Case Study
5. Συμπέρασμα Ανάλυσης
6. Βιβλιογραφία

Εισαγωγή

Με την ανεξέλεγκτη ανάπτυξη της τεχνολογίας, έχουμε οδηγηθεί πλέον σε διαδικασίες οριοθέτησης των ελευθεριών των χρηστών, προκειμένου να ελαχιστοποιηθούν οι νέοι κίνδυνοι που προκύπτουν καθημερινά. Ένας από τους κινδύνους αυτούς, ονομάζεται DarkNet. Για να είμαστε πιο σαφείς, το DarkNet από μόνο του δεν αποτελεί τον ίδιο τον κίνδυνο, αλλά αυτό που μπορεί να φανεί επιβλαβές για τους χρήστες, είναι οι λειτουργίες που αυτό εξυπηρετεί, αποτελώντας έτσι, μία σύγχρονη τεχνολογία η οποία δημιουργεί νέα προβλήματα αλλά και νέες ανάγκες για προστασία. Πέραν των τεχνολογικών μεθόδων οι οποίες μπορούν να χρησιμοποιηθούν για τον περιορισμό της επιρροής την τεχνολογίας αυτής, υπάρχει και ένα από τα διαχρονικότερα μέσα επιβολής τάξης – ο νόμος. Γι’ αυτόν τον λόγο, έχει μεγάλη σημασία να μελετήσουμε τον βαθμό επιρροής της νομοθεσίας σε σχέση με το DarkNet, ποιοι κανονισμοί μπορούν να εφαρμοσθούν πάνω σε αυτό, τις «γκρι ζώνες», αλλά και σημαντικές υποθέσεις που ο ψηφιακός τόπος τέλεσης τους, ήταν ο σκοτεινός ιστός. Όλα αυτά, ξεκινώντας με τον ορισμό του DarkNet.

Σύντομη περιγραφή του DarkNet και των λειτουργιών του

Αναφερόμενοι στο Dark Web, είναι χρήσιμο αρχικά, να ξεκαθαρίσουμε τις διαφορές μεταξύ του συγκεκριμένου όρου και του Deep Web, οι οποίοι λανθασμένα συγχέονται. Με την έννοια Deep Web αναφερόμαστε στο μέρος του διαδικτύου το οποίο δεν εντοπίζεται από τις μηχανές αναζήτησης και επομένως δεν μπορεί να έχει πρόσβαση ο οποιοσδήποτε με μία απλή αναζήτηση, δηλαδή αναφερόμαστε στις σελίδες που για να προβάλει και να αποκτήσει κανείς πρόσβαση απαιτείται αρχικά κάποια σύνδεση. Πρακτικά, στο παραπάνω υπάγονται σελίδες όπως ο προσωπικός λογαριασμός email, το e-banking κάποιου χρήστη και οποιαδήποτε άλλη σελίδα χρήζει απαραίτητη την παράθεση συγκεκριμένων διαπιστευτηρίων, τα οποία είναι μοναδικά για το κάθε χρήστη [4].Το Dark Web, όμως, ενώ ταυτίζεται με το προηγούμενο όσον αφορά τον εντοπισμό των σελίδων που το αποτελούν, διαφέρει στον τρόπο που μπορεί κάποιος, τελικά, να το επισκεφθεί. Η σύνδεση στο «Σκοτεινό Ιστό» είναι δυνατή μόνο με χρήση εξειδικευμένων λογισμικών, το πιο γνωστό των οποίων είναι το Tor[3]. Μελετώντας το Tor, παρατηρούμε ότι είναι υπεύθυνο για την απόκρυψη του χρήστη, συγκεκριμένα της IP διεύθυνσης του, που πάει να συνδεθεί στην σελίδα, αναμεταδίδοντας το σήμα κάθε φορά σαν να προέρχεται από διαφορετική διεύθυνση, ώστε να μην αναγνωρισθεί η πραγματική πηγή[2] . Με αυτό τον τρόπο σύνδεσης αναγνωρίζουμε το Dark Web ως ένα ανώνυμο διαδικτυακό ιστό. Ο σκοπός ύπαρξης του, ή καλύτερα η «μάσκα» πάνω στην οποία λειτουργεί, είναι η διατήρηση της ανωνυμίας για την αποφυγή λογοκρισίας και ουσιαστικά την προώθηση της ελεύθερης έκφρασης[1] . Ωστόσο, όπως θα δούμε και παρακάτω, υπάρχει ένα μεγάλο φάσμα εγκληματικών ενεργειών που αξιοποιούν το Tor ως μέσο τέλεσης τους. Με άλλα λόγια, παραμένει ακόμη στην «γκρι» ζώνη, όσον αφορά την νομιμότητα της ύπαρξης του, λόγω του ότι μέσω αυτού μπορεί να επιτύχει κανείς την απόκρυψη της ταυτότητας του, η οποία δεν είναι απαραίτητο ότι ωφελεί μόνο παράνομες δραστηριότητες. Ένα παράδειγμα επωφελούς χρήσης του Dark Web, πέρα από αυτή της επίτευξης της ελευθερίας λόγου, είναι η χρήση του από οργανισμούς, όπως ο στρατός, ή άλλων όχι τόσο γνωστών διοργανώσεων, με στόχο την προστασία του κοινωνικού συμφέροντος. Αυτό επιτυγχάνεται, καθώς ο χαρακτήρας του «Σκοτεινού Ιστού», όπως γνωρίζουμε, κάνει δυνατή την «κρυφή» επικοινωνία, το οποίο δίνει το πλεονέκτημα στα στρατεύματα να αναπτύξουν αποτελεσματικές στρατηγικές, ελαχιστοποιώντας τους κινδύνους[4](Chapter 1).

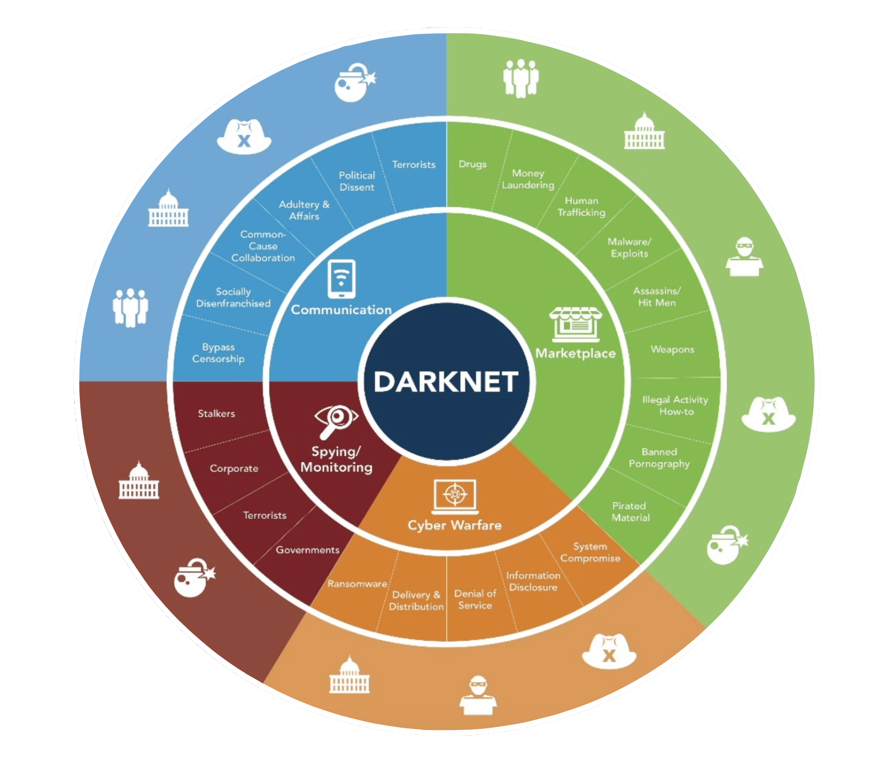
Αναλύοντας την ιστορική αναδρομή διάφορων τεχνολογικών καινοτομιών, παρατηρούμε ότι ο χαρακτήρας των συγκεκριμένων δημιουργημάτων διαμορφώνεται από τον τρόπο χρήσης τους και όχι από τον πρωταρχικό σκοπό υλοποίησης τους. Ο «Σκοτεινός Ιστός» είναι ακριβώς ένα τέτοιο παράδειγμα, με τον χαρακτήρα του ως ένα ανώνυμο δίκτυο και την αδυναμία αναγνώρισης του τελικού χρήστη, να το κάνει έναν ιδανικό χώρο για την προώθηση και την ενίσχυση παράνομων δραστηριοτήτων. Αυτός του ο ρόλος, λοιπόν, είναι και εκείνος που καθιστά επιτακτική ανάγκη την αναγνώριση και την αντιμετώπιση των αναδυόμενων προβλημάτων.

Γενικό Νομοθετικό Υπόβαθρο

Αναλύοντας, ακόμη και επιφανειακά, το DarkNet, προκύπτουν πολλοί προβληματισμοί και κανείς θα περίμενε να υπάρχει ένα ισχυρό σύνολο νόμων και κανονισμών το οποίο θα περιόριζε ή ακόμη και θα απαγόρευε την πρόσβαση σε αυτό.

Η αλήθεια ωστόσο είναι διαφορετική, καθώς δεν υπάρχει κανένας Ευρωπαϊκός Κανονισμός, ούτε κάποιος νόμος, ο οποίος να έχει ως πεδίο εφαρμογής του το DarkNet. Η έλλειψη ειδικών νομοθετημάτων όμως, δεν συνεπάγεται την ασυλία του χρήστη. Η πρόσβαση και η πλοήγηση του χρήστη στο σκοτεινό διαδίκτυο δεν είναι καταρχήν παράνομη, αλλά οι ενέργειες αυτού, μπορούν να του επιφέρουν νομικές κυρώσεις.. Το DarkNet, μπορεί εύκολα να παρομοιαστεί με μία « κακόφημη » γειτονιά μιας μεγάλης πόλης. Ακόμη και εάν γνωρίζει κάποιος ότι σε αυτή τη γειτονιά γίνονται πολλαπλών ειδών παράνομες ενέργειες, διατηρεί αναφαίρετο δικαίωμα να περιπλανηθεί σε αυτή, χωρίς η γνώση του για το τι συμβαίνει και το τι μπορεί να συμβεί εκεί, να λειτουργεί με τρόπο προδικαστικό για τις ενέργειες αυτού. Δηλαδή, ο κάθε χρήστης έχει δικαίωμα πλοήγησης και αναζήτησης μέχρι όποιο βάθος επιθυμεί (και αντέχει), χωρίς να επιβαρύνεται με νομικές ευθύνες. Μέχρι ποιο σημείο όμως φτάνει η ελευθερία αυτή ;

Μέχρι το σημείο στο οποίο το υποκείμενο θα προβεί σε μια ενέργεια ή παράλειψη η οποία θα τον καθιστά εμπλεκόμενο σε μία κατά το νόμο απαγορευμένη συναλλαγή - διαδικασία. Προτού προβούμε όμως σε περεταίρω ανάλυση του τρόπου με τον οποίο ασκείται δικαιοσύνη σε εγκλήματα που διαπράττονται μέσω του DarkNet, ας παραθέσουμε μια εικονογραφία που δημοσίευσε τον Σεπτέμβριο του 2015 στη Νέα Υόρκη, η εταιρία λογισμικού Bat Blue, στην οποία παρουσιάζεται το πλήρες φάσμα των παράνομων λειτουργιών που φιλοξενούνται στο σκοτεινό διαδίκτυο.



“The Underground for the Undergrounds”

Επειδή τα πληροφοριακά συστήματα και τα λογισμικά δεν διαθέτουν ακόμα δική τους νομική προσωπικότητα, πρέπει να εξετάσουμε και τις κατηγορίες των προσώπων που βρίσκονται πίσω από το κύκλωμα αυτό , δηλαδή αυτούς που δημιουργούν ή/και χρησιμοποιούν τα υποσυστήματα του DarkNet. Οι συμμετέχοντες ( actors ) του ευρύτερου συστήματος σύμφωνα με την Blue Bat, είναι οι εξής :

Άρα, το σύνολο των εγκλημάτων που μπορούν να συμβούν μέσα στο DarkNet, περιέχει απο αποκλειστικά ηλεκτρονικά εγκλήματα, όπως παράνομη διάθεση ευαίσθητων πληροφοριών και δεδομένων, κυβερνοεπιθέσεις και κατασκοπίες, μέχρι και εγκλήματα που μπορούν να συμβούν και στον φυσικό μας κόσμο, όπως εμπόριο ναρκωτικών και όπλων, σύναψη συμβολαίων θανάτου, σωματεμπορία και οργάνωση τρομοκρατικών επιθέσεων.

Συνοψίζοντας μέχρι τώρα, έχουμε δύο αντικρουόμενους άξονες, την **ελεύθερη πρόσβαση** στο DarkNet και τον **παράνομο χαρακτήρα των υπηρεσιών** που προσφέρονται από αυτό.

Για την απονομή δικαιοσύνης συνεπώς, αφού δεν υπάρχει συγκεκριμένη νομοθεσία - ή κανονισμός - που βάσει αυτού να περιορίζεται η πρόσβαση στο DarkNet, χρησιμοποιούνται οι νομοθεσίες και οι νομολογίες της εκάστοτε έννομης τάξης, οι Ευρωπαϊκοί κανονισμοί ( εφόσον πρόκειται για χώρα της Ευρωπαϊκής Ένωσης ) αλλά και οι ευρωπαϊκές οδηγίες, εάν πρόκειται για περιπτώσεις άσκησης soft law.

*Εθνική Νομοθεσία που αφορά το DarkNet*

Ένα έγκλημα το οποίο διαπράττεται γενικά μέσω διαδικτύου και ειδικότερα μέσω του DarkNet, περιπλέκει έως ένα βαθμό τον ορισμό του τόπου τέλεσης του εγκλήματος. Για τον ορισμό αυτού, το ελληνικό Δίκαιο, χρησιμοποιεί το συνδυασμό των άρθρων 5 παρ.1 Π.Κ με τίτλο « Εγκλήματα στην ημεδαπή » και του άρθρου 16 Π.Κ με τίτλο « Τόπος τέλεσης της πράξης » όπου κατ’ εφαρμογή των αρχών της εδαφικότητας και της ενότητας, προκύπτει ότι ως *ψηφιακή εδαφικότητα* ενός διαδικτυακού εγκλήματος που επιφέρει ορισμένο αποτέλεσμα, ορίζεται και ο τόπος όπου επήλθε το αξιόποινο αποτέλεσμα πέρα από τον τόπο της ψηφιακής δράσης του υπαιτίου. Με πιο απλά λόγια, είναι αρκετό μόνο το θύμα να είναι φυσικό ή νομικό πρόσωπο, το οποίο εδρεύει στην Ελλάδα , ώστε οι ελληνικές αρχές να μπορέσουν να εξετάσουν στην υπόθεση και μεταγενέστερα το έγκλημα να εκδικαστεί στα ελληνικά ποινικά δικαστήρια.

Αφού έχει προσδιοριστεί η ψηφιακή εδαφικότητα, τότε οι έννομες διαδικασίες που πρόκειται να ακολουθηθούν είναι οι ίδιες με οποιοδήποτε άλλο έγκλημα.

Ωστόσο, το έγκλημα αντιμετωπίζεται ως ένα έγκλημα που διενεργήθηκε με τη χρήση πληροφοριακών συστημάτων μέσω διαδικτύου, έχοντας και την αντίστοιχη ποινική επιβάρυνση σε όσες περιπτώσεις προβλέπεται, όπως για παράδειγμα στο άρθρο 348Α, όπου σύμφωνα με την παρ.1 « *Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο δια θέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων*…» προβλέπεται ποινή πλημμεληματικού βαθμού με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ, ενώ στην παρ.2 όπου σε σχέση με την παρ.1 προστίθεται το εδάφιο *«…μέσω πληροφοριακών συστημάτων…»* , προβλέπεται φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή τριακοσίων χιλιάδων ευρώ.

*Εθνική Νομολογία που αφορά το DarkNet*

Η μοναδική περίπτωση νομολογίας κατά την οποία εμπλέκεται ο σκοτεινός ιστός είναι η απόφαση 10/2024 της Αρχής Προστασίας Δεδομένων, όπου προσωπικά δεδομένα της εταιρίας «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΙΑ» διέρρευσαν στον σκοτεινό ιστό, έπειτα από κακόβουλη επίθεση τρίτων. Στην περίπτωση αυτή βέβαια, η Αρχή εξετάζει τις ενέργειες και τις παραλείψεις της εταιρίας αυτής, όπως και τις ενέργειες και τις παραλείψεις όλων των εκτελούντων της επεξεργασίας και εν τέλει ασκεί τις διορθωτικές της εξουσίες με βάση το άρθρο 58 παρ. 2 στοιχ. θ) του ΓΚΠΔ, χωρίς να στρέφει την προσοχή της στους αυτουργούς της επίθεσης, καθώς δεν κατέχει και τη δικαιοδοσία που απαιτείται ώστε να επέμβει. Για την ιστορία, η Αρχή, ακολουθώντας τις κατευθυντήριες γραμμές 4/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, για τον υπολογισμό των διοικητικών προστίμων, επέβαλε πρόστιμο στην εταιρία ΕΛΤΑ, ύψους δύο εκατομμυρίων εννιακοσίων ενενήντα πέντε χιλιάδων εκατόν σαράντα ευρώ (2.995.140)

*GDPR και DarkNet*

Εξετάζοντας τόσο την εθνική νομοθεσία, όσο και την εθνική νομολογία, παρατηρούμε ότι η μοναδική αναφορά του DarkNet, βρίσκεται στην ως άνω απόφαση ( 10/2024 ). Όπως προαναφέρθηκε, στην συγκεκριμένη απόφαση βρίσκει πεδίο εφαρμογής ο Γενικός Κανονισμός Προστασίας Δεδομένων, του οποίου σκοπός είναι η προστασία των ευαίσθητων προσωπικών δεδομένων των φυσικών και νομικών προσώπων και η διασφάλιση της νόμιμης επεξεργασίας των δεδομένων αυτών. Αφού, λοιπόν, η μοναδική περίπτωση που έχει απασχολήσει το ελληνικό δίκαιο, σχετίζεται με διαρροή προσωπικών δεδομένων στο DarkNet, έχει ενδιαφέρον να αναλύσουμε το πώς η ύπαρξη του σκοτεινού ιστού, μπορεί να προσθέσει ένα επιπλέον βήμα στην διαδικασία προστασίας των προσωπικών δεδομένων από μία εταιρία ή έναν οργανισμό, μέσω του GDPR..

Το πρόβλημα έγκειται στο γεγονός ότι η διαρροή των προσωπικών δεδομένων στον σκοτεινό ιστό, είναι δύσκολο να εντοπιστεί, λόγω των ισχυρών πρωτοκόλλων ανωνυμίας και κρυπτογράφησης, που χρησιμοποιούνται στο υποδίκτυο αυτό. Σύμφωνα με το άρθρο 4 παρ.1 ΓΚΠΔ, ως προσωπικά δεδομένα ορίζονται *« ...κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας,..».* Παράλληλα, στο άρθρο 33 παρ.1 ΓΚΠΔ, αναφέρεται ότι, η αρμόδια εποπτική αρχή θα πρέπει να ενημερωθεί εντός εβδομήντα δύο ωρών από τη στιγμή που γίνεται αντιληπτή η παραβίαση, από τον υπεύθυνο της επεξεργασίας. Επιπλέον, ο κανονισμός προβλέπει ότι η εμφάνιση προσωπικών δεδομένων στο DarkNet συνιστά παραβίασή τους και μπορεί να επιφέρει τις προβλεπόμενες κυρώσεις.. Συνδυάζοντας τις τρεις παραπάνω αναφορές του κανονισμού, με την δυσκολία αναγνώρισης της διαρροής προσωπικών δεδομένων στο DarkNet, δημιουργεί μια νέα απαίτηση για τους υπεύθυνους της επεξεργασίας. Για να υπάρχει πλήρης συμμόρφωση δηλαδή, δεν αρκεί μόνο η θωράκιση των πληροφοριακών συστημάτων του υπευθύνου και του εκτελούντος της επεξεργασίας, αλλά πλέον απαιτείται και η δυνατότητα προληπτικής αναγνώρισης οποιαδήποτε διαρροής προσωπικών δεδομένων στο DarkNet. Για να γίνει αντιληπτή η σημαντικότητα της ανάγκης αυτής, αρκεί να αναφερθεί ότι από το 2018, όπου τέθηκε σε ισχύ ο GDPR, έχει δημιουργηθεί και έχει εξελιχθεί σε μεγάλο βαθμό, η παροχή Dark Net Monitoring υπηρεσιών, από πάρα πολλές εταιρείες που μπορούν να λάβουν τον ρόλο του εκτελούντος της επεξεργασίας.

*Ενδεικτικές Οδηγίες (ΕΕ) και DarkNet*

Εκτός από τον GDPR, υπάρχει και η Οδηγία (ΕΕ) 2017/541{5} του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά την καταπολέμηση της τρομοκρατίας, η οποία περιλαμβάνει διατάξεις που σχετίζονται με την πρόληψη και την δίωξη τρομοκρατικών ενεργειών, συμπεριλαμβανομένων και εκείνων που διεξάγονται μέσω διαδικτύου, όπως είναι και ο σκοτεινός ιστός και η Οδηγία (ΕΕ) 2022/2555{6} σχετικά με τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, η οποία απαιτεί την λήψη κατάλληλων μέτρων για την ασφάλεια στον κυβερνοχώρο στις εθνικές έννομες τάξεις.

Οι Οδηγίες αυτές είναι αποτέλεσμα της ευρύτερης προσπάθειας της Ευρωπαϊκής Ένωσης να ενισχύσει την κυβερνοασφάλεια και κατ΄ επέκταση να καταπολεμήσει το έγκλημα στον κυβερνοχώρο και να προστατέψει τα προσωπικά δεδομένα, στις οποίες ως άνω ενέργειες συμπεριλαμβάνονται και όλες οι δραστηριότητες που λαμβάνουν χώρα στο DarkNet. Η πραγματικότητα είναι πως τα παραπάνω μέτρα δεν στοχεύουν ρητά στα εγκλήματα που διαπράττονται μέσω του DarkNet, αλλά δημιουργούν ένα νομικό πλαίσιο, το οποίο μπορεί να θεωρηθεί αφετηρία στην εκκίνηση νομοθέτησης και ουσιαστικής καταπολέμησης των εγκλημάτων αυτών.

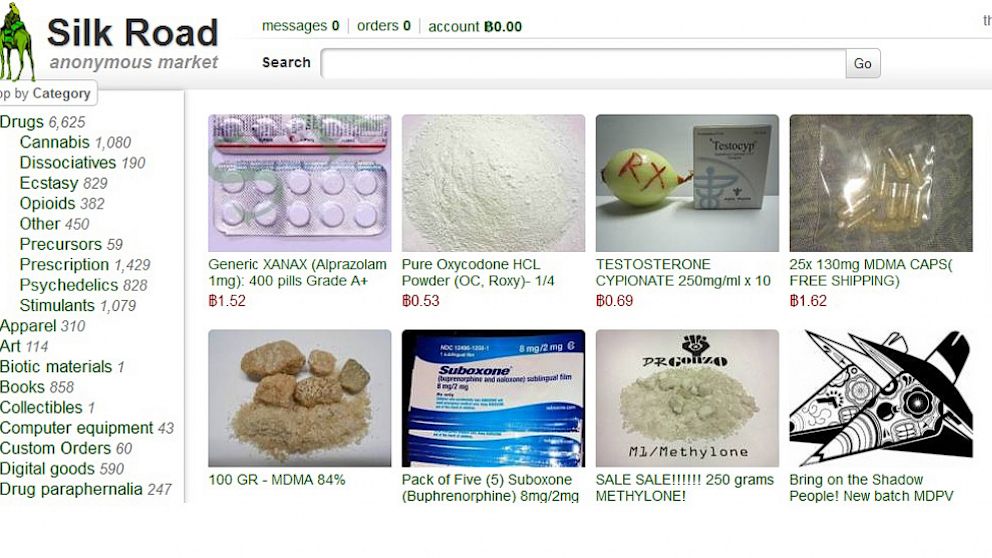
*Συμπέρασμα περί νομοθετικού πλαισίου*

Εξετάζοντας λοιπόν το σύνολο της εθνικής νομοθεσίας και της εθνικής νομολογίας αλλά και το σύνολο των ευρωπαϊκών κανονισμών και οδηγιών, επιστρέφουμε στην αρχική μας παραδοχή, στο ότι το DarkNet, δεν αποτελεί πεδίο εφαρμογής κανενός νόμου ή κανονισμού. Η αιτιολόγηση πίσω απ’ αυτό κρύβεται πιθανότατα στην αργοπορημένη νομοθεσία στο ευρύτερο διαδίκτυο αλλά και την επικρατούσα άποψη στην κοινωνία της Πληροφορικής που θεωρεί το DarkNet, ένα απλό-νόμιμο είδος διαδικτύου. Το παράδοξο που εμπεριέχεται στην κατασκευή του DarkNet, είναι τα πολύ ισχυρά επίπεδα ασφαλείας και κρυπτογράφησης που έρχονται σε αντίθεση με τους παράνομους σκοπούς για τους οποίους χρησιμοποιείται. Εάν η νομοθεσία είχε προλάβει τους εγκληματίες και είχε περιορίσει την πρόσβαση, τότε το DarkNet, δεν θα λεγόταν Dark, και θα μιλούσαμε για ένα υπερ-ασφαλές δίκτυο, το οποίο θα διευκόλυνε μετέπειτα και τη δουλειά του νομοθέτη για ζητήματα όπως για παράδειγμα η προστασία των δεδομένων. Αυτό δεν συνέβη και είναι λογικό, καθώς η ταχύτητα εμφάνισης νέων τεχνολογιών είναι τεράστια και πολλές φορές η κατανόηση τους καθίσταται πολύ δύσκολη ακόμη και για ανθρώπους της επιστήμης της πληροφορικής, πόσω μάλλον για τους νομοθέτες, οι οποίοι όχι μόνο πρέπει να κατανοήσουν, μαζί με τους επιστημονικούς τους συνεργάτες, αλλά και να δώσουν υπόσταση στους πιθανούς κινδύνους που επιφέρουν οι τεχνολογίες αυτές και να προβούν στις κατάλληλες ενέργειες. Ποτέ όμως δεν είναι αργά, αναλογιζόμενοι και την πληροφοριακή και τεχνολογική δύναμη που πλέον διαθέτουν οι κρατικοί μηχανισμοί, ένα νομοθέτημα, κανονισμός ή μια οδηγία, θα μπορούσε να δράσει προληπτικά όσον αφορά τις επερχόμενες αρνητικές εκφάνσεις του σκοτεινού ιστού και μεταγενέστερα να ενισχύσει την αξιοποίηση της σπουδαίας τεχνολογίας που κρύβεται πίσω απ’ αυτόν, για διασφάλιση μεγαλύτερης ασφάλειας στον ψηφιακό κόσμο.

Silk Road – Case Study

Για να δούμε τα αποτελέσματα της έλλειψης ενός ακριβούς νομοθετικού πλαισίου, το οποίο θα έχει πεδίο εφαρμογής τον «Σκοτεινό Ιστό» θα ήταν χρήσιμο να περιγράψουμε μία περίπτωση, όπου τα νομοθετικά όργανα αναγκάστηκαν να αναζητήσουν την «γκρι ζώνη» που βρίσκεται ανάμεσα στη νομιμότητα και την παρανομία.

*Η υπόθεση Silk Road*

Η Silk Road, γνωστή και ως ‘‘Amazon.com των ναρκωτικών’’(Love, D 2013) ξεκίνησε στις αρχές του 2011 ως μια ψηφιακή ‘‘ανώνυμη’’ αγορά για το εμπόριο παράνομων αγαθών, αλλά χρησιμοποιήθηκε κυρίως για την πώληση ναρκωτικών, που κυμαίνονταν από κοκαΐνη, ηρωίνη, μαριχουάνα, μέχρι και LSD. Η Silk Road δεν έβρισκε ούτε προμήθευε αυτά τα ναρκωτικά, αλλά ήταν μια αποτελεσματική πλατφόρμα για διαδικτυακές συναλλαγές. Αυτό γινόταν συνδέοντας αγοραστές με πωλητές και μετά την ολοκλήρωση μιας αγοράς και την επιβεβαίωση της επιτυχημένης παράδοσης, έπαιρνε προμήθεια από κάθε πώληση. Η ιστοσελίδα προσέφερε επίσης υπηρεσίες hacking, κακόβουλο λογισμικό καθώς και προσφορές για την παραγωγή ψευδών εγγράφων ταυτότητας. 

Εικόνα 1: Στιγμιότυπο από την ιστοσελίδα της Silk Road

Η Silk Road ήταν κρυμμένη στο DarkNet του Dark Web και χρησιμοποιούσε το λογισμικό TOR στις λειτουργίες του, όπου τα μηνύματα δρομολογούνταν μέσω πολλαπλών προορισμών, καθιστώντας έτσι σχεδόν αδύνατο να γνωρίζουμε από πού προέρχονται. Για να αποκτήσει ένας χρήστης πρόσβαση στην ιστοσελίδα του Silk Road, χρειαζόταν ειδικό κρυπτογραφικό λογισμικό που συνδύαζε μια ανώνυμη διεπαφή με ανιχνεύσιμες πληρωμές στο ψηφιακό νόμισμα που ονομάζεται Bitcoin. Αυτό επέτρεψε σε χιλιάδες εμπόρους ναρκωτικών και σχεδόν ένα εκατομμύριο πελάτες παγκοσμίως να βρουν ο ένας τον άλλον. Οι περιγραφές προϊόντων και οι αξιολογήσεις χρηστών αποτελούσαν μια ‘‘εγκυκλοπαιδική πηγή πληροφοριών’’, κάτι που με τη σειρά του έφερε περισσότερους χρήστες στον ιστότοπο, διαδίδοντας περαιτέρω την δημοτικότητα του και αυξάνοντας την φήμη του, καθιστώντας έτσι την Silk Road τον κορυφαίο προορισμό για ψηφιακές πωλήσεις ναρκωτικών (Bearman, 2015a). Ενώ βασιζόταν στην ιδέα μιας ‘‘ανοιχτής και ελεύθερης αγοράς’’, ο ιστότοπος είχε πολλούς κανόνες συμπεριλαμβανομένου ενός "Συμφωνητικού Πωλητή" που κάλυπτε ζητήματα από τη συσκευασία και αποστολή των ναρκωτικών έως και την διαδικτυακή ασφάλεια. Ένας από τους ‘‘ιερούς’’ κανόνες ήταν η αυστηρή απαγόρευση της ‘‘αποκάλυψης της ταυτότητας άλλων πωλητών ή αγοραστών του Silk Road’’ (Mullin, 2015). Ωστόσο, ενώ η Silk Road πουλούσε κυρίως ναρκωτικά, οι όροι χρήσης του είχαν απαγορεύσει την πώληση "οτιδήποτε έχει σκοπό να βλάψει ή να εξαπατήσει, όπως κλεμμένες πιστωτικές κάρτες, δολοφονίες και όπλα μαζικής καταστροφής " (Chen, 2011).

Από τον Νοέμβριο του 2011 έως τον Σεπτέμβριο του 2013, οι πράκτορες επιβολής του νόμου έκαναν περισσότερες από 60 ατομικές μυστικές αγορές ελεγχόμενων ουσιών από πωλητές του Silk Road, καθιστώντας την υπόθεση ένα σημαντικό παράδειγμα ειδικών ερευνητικών τεχνικών σύμφωνα με το Άρθρο 20 της Σύμβασης για το Οργανωμένο Έγκλημα. Οι μυστικοί πράκτορες αγόρασαν διάφορα παράνομα ναρκωτικά από πωλητές που βρίσκονταν σε περισσότερες από δέκα διαφορετικές χώρες, συμπεριλαμβανομένων της Αυστρίας, του Καναδά, της Γαλλίας, της Γερμανίας, της Ιρλανδίας, της Ιταλίας, της Ολλανδίας, της Ισπανίας, του Ηνωμένου Βασιλείου και των Ηνωμένων Πολιτειών, δείχνοντας τη διεθνή έκταση των επιχειρήσεων του Silk Road και την εγγενώς διασυνοριακή φύση του κυβερνοεγκλήματος. Περαιτέρω, αποδεικνύοντας τη σοβαρότητα των εγκλημάτων, τα ναρκωτικά που διανέμονταν μέσω του Silk Road έχουν συνδεθεί με τουλάχιστον έξι θανάτους από υπερβολική δόση σε όλο τον κόσμο. Η προσπάθεια των αρχών να εντοπίσουν τη Silk Road οδήγησε στην σύλληψη του Ross Ulbricht και τον Φεβρουάριο του 2015, το Δικαστήριο τον βρήκε ομόφωνα ένοχο, για τη διαχείριση της ιστοσελίδας ως Dread Pirate Roberts. Η ποινική δίωξη του Ulbricht αποτέλεσε μια από τις πιο πολύπλοκες και επίπονες νομικές υποθέσεις της εποχής της, αναδεικνύοντας τις προκλήσεις που αντιμετώπιζαν οι αρχές στον ψηφιακό κόσμο. Το Περιφερειακό Δικαστήριο έπρεπε να αντιμετωπίσει τα ακόλουθα νέα νομικά ζητήματα που δεν είχαν ακόμη εξεταστεί δικαστικά:

1. Αυτοματοποιημένες, ανώνυμες συναλλαγές και κατηγορίες για συνωμοσία
2. Διαχείριση διαδικτυακής αγοράς
3. Χρήση Bitcoin και ξέπλυμα χρήματος

Το Περιφερειακό Δικαστήριο αιτιολόγησε ότι οι συμφωνίες συνωμοσίας δεν απαιτούν απαραίτητα ρητή συμφωνία για όλες τις λεπτομέρειες της συνωμοσίας. Είναι επαρκές να συμφωνήσουν στον στόχο ή στον παράνομο σκοπό της συνωμοσίας. Έμμεσες αποδείξεις που καταδεικνύουν γνώση της εγκληματικής δραστηριότητας ή του σκοπού της συνωμοσίας είναι επαρκείς. Στην παρούσα υπόθεση, η κυβέρνηση μπόρεσε να δείξει ότι ο Ulbricht συγκέντρωσε δεκάδες εκατομμύρια δολάρια σε προμήθειες από παράνομες συναλλαγές ναρκωτικών, καθώς και συναλλαγές για κακόβουλο λογισμικό και ψεύτικα έγγραφα ταυτότητας.

Επομένως, το Περιφερειακό Δικαστήριο διαπίστωσε ότι η απαιτούμενη συμφωνία μπορούσε να τεκμηριωθεί σε περιπτώσεις αυτοματοποιημένων, ανώνυμων συναλλαγών. Ομοίως, το Δικαστήριο έκρινε ότι δεν ήταν απαραίτητο ο Ulbricht να συμμετείχε σε μια συγκεκριμένη μορφή συμπεριφοράς με καθέναν από αυτούς με τους οποίους ενεργούσε σε συνεργασία στη συνεχιζόμενη εγκληματική του επιχείρηση. Ήταν αρκετό να αποδειχθεί ότι χιλιάδες έμποροι ναρκωτικών πραγματοποίησαν συναλλαγές στο Silk Road με χιλιάδες αγοραστές. Το Δικαστήριο διαπίστωσε ότι ο Ulbricht λειτουργούσε σε θέση οργανωτή και διευθυντή της διακίνησης ναρκωτικών που πραγματοποιούνταν στο Silk Road. Όσον αφορά τα Bitcoins, το Δικαστήριο διαπίστωσε ότι η μόνη αξία του Bitcoin είναι να πληρώνει για πράγματα. Το Bitcoin μπορεί να χρησιμοποιηθεί απευθείας για πληρωμές ή να μετατραπεί σε νόμισμα και στη συνέχεια να χρησιμοποιηθεί για πληρωμές. Τα Bitcoins σχεδιάστηκαν ειδικά για να αποκρύπτουν τα έσοδα από παράνομες δραστηριότητες από την ανακάλυψη τρίτων. Ενώ τα Bitcoins μπορεί να μην περιλαμβάνονταν στους παραδοσιακούς ορισμούς του "νομίσματος" ή των "χρηματοοικονομικών συναλλαγών", το Δικαστήριο έκρινε ότι είναι λειτουργικά ισοδύναμα και επομένως μπορούν να χρησιμοποιηθούν για το ξέπλυμα χρήματος.

Ο Ulbricht υποστήριξε ότι τα αποδεικτικά στοιχεία που συλλέχθηκαν μέσω των εντολών παρακολούθησης και των ενταλμάτων για έρευνα στον φορητό του υπολογιστή παραβίασαν τoν νόμο και ζήτησε την απόρριψη των αποδεικτικών στοιχείων που συλλέχθηκαν σε σχέση με την εντολή. Το περιφερειακό δικαστήριο απέρριψε αυτό το αίτημα. Εκτός από τις επτά κατηγορίες για μη βίαια εγκλήματα (διανομή ναρκωτικών, διανομή ναρκωτικών μέσω του Διαδικτύου, συνωμοσία για τη διανομή ναρκωτικών, συμμετοχή σε συνεχιζόμενη εγκληματική επιχείρηση, συνωμοσία για τη διάπραξη hacking, συνωμοσία για τη διακίνηση ψεύτικων εγγράφων ταυτότητας και συνωμοσία για το ξέπλυμα χρήματος), ο κατηγορούμενος ήταν ύποπτος για την οργάνωση πολλαπλών δολοφονιών κατόπιν παραγγελίας εναντίον εκείνων που απειλούσαν την ιδιωτικότητα του ίδιου και των χρηστών του Silk Road. Ωστόσο, δεν υπήρχαν αρκετά αποδεικτικά στοιχεία για να τον κρίνουν ένοχο για αυτές τις κατηγορίες. Για τους παραπάνω λόγους, το Δικαστήριο καταδίκασε τον κατηγορούμενο για τις επτά μη βίαιες κατηγορίες και του επέβαλε ισόβια κάθειρξη.

Ενώ η παράνομη δραστηριότητα συνεχίζεται με ταχύ ρυθμό στο DarkNet, οι αρχές απέδειξαν ότι η ανωνυμία δεν αποτελεί προστατευτική ασπίδα από την σύλληψη και τη δίωξη. Η υπόθεση προκάλεσε έντονες συζητήσεις γύρω από τα νομικά θέματα που προέκυψαν από την λειτουργία της Silk Road, θέτοντας σε πρόκληση στις αρχές και το νομικό σύστημα και προκαλώντας αμφισβήτηση σχετικά με την εφαρμογή των νόμων και την προστασία της ασφάλειας στο διαδίκτυο. Τελικά, η περίπτωση της Silk Road αντιπροσώπευσε μια νίκη για τις αρχές, αλλά και μια επίδειξη των προκλήσεων που αντιμετωπίζουν στην εποχή της ψηφιακής επικοινωνίας και της τεχνολογίας. Η Silk Road υπενθύμισε στους νομοθέτες και τις αρχές τη σημασία της προσαρμογής των νόμων και των διαδικασιών επιβολής τους στις νέες τεχνολογικές πραγματικότητες. Παράλληλα, όμως, αναδείχθηκε η ανάγκη για ισορροπία μεταξύ της προστασίας της ασφάλειας και της ιδιωτικής ζωής των ατόμων, προκειμένου να διασφαλιστεί η ελευθερία και η ασφάλεια στον ψηφιακό κόσμο.

Συμπέρασμα Ανάλυσης

Κάνοντας μία αναδρομή σε ότι έχουμε περιγράψει μέχρι τώρα, σχετικά με τον «Σκοτεινό Ιστό» και το νομοθετικό πλαίσιο που το περικλείει και με την βοήθεια της μελέτης του περιστατικού του Silk Road, απορρέει η ανάγκη για εκσυγχρονισμό και ενίσχυση του νομοθετικού πλαισίου σε σχέση με την πρόσβαση και τις δραστηριότητες στο DarkNet. Όπως μας έγινε πολύ ξεκάθαρο από το παράδειγμα μελέτης, τα νομοθετικά όργανα, για να καταφέρουν να αποδώσουν τις ανάλογες, με τα εγκλήματα, ευθύνες, χρησιμοποιήσαν τεχνάσματα παραλληλισμού των ηλεκτρονικών εγκλημάτων με αυτών, που μπορούν να συμβούν στον φυσικό τόπο όπου η εύρεση της ταυτότητας των υπαιτίων είναι ευκολότερη. Η διαδικασία, όμως, ήταν δυνατή λόγω του ότι κατάφεραν μετά από μία εκτεταμένη έρευνα να αποδείξουν την ταυτότητα ενός από τους δράστες. Δηλαδή είναι φανερό ότι η ανωνυμία που παρέχει ο «Σκοτεινός Ιστός» είναι και αυτή που επιτρέπει όλες τις παράνομες διαδικασίες να συνεχίζουν, ακόμη και αν εν γνώση μας ξέρουμε ότι υφίστανται. Η μόνη μη-ρεαλιστική – για τα σημερινά δεδομένα - λύση που θα μπορούσε να αποδοθεί είναι η πλήρης απαγόρευση του «Σκοτεινού Ιστού» πράγμα που είναι αδύνατο, γιατί όπως γνωρίζουμε η τεχνολογική πρόοδος είναι τέτοια που δεν θα χρειαστούν πάνω από λίγες εβδομάδες, ώστε να ξανά δημιουργηθεί ένα παρόμοιο λειτουργικό περιβάλλον.

Επομένως, αναφερόμαστε στην επιδίωξη μίας πληρέστερης αντιμετώπισης όσων περιστατικών έχουν ως τόπο τέλεσης το DarkNet, χωρίς την απόδοση του ελαφρυντικού ότι υπάρχει έλλειψη συγκεκριμένων Ευρωπαϊκών κανονισμών ή εθνικών νόμων που να εφάπτονται άμεσα αυτού. Το ότι ακόμη δεν έχει υπάρξει ένα ξεκάθαρο νομοθετικό πλαίσιο, εξαιτίας των γνώσεων πάνω στο συγκεκριμένο πεδίο, δεν συνεπάγεται απουσία νομικής ρύθμισης, αλλά την ανάγκη αυστηρότερης εφαρμογής των υπαρχόντων νομικών πλαισίων και της διεύρυνσης τους για να καλύψουν τις νέες προκλήσεις που επιφέρει η τεχνολογική πρόοδος. Αξιολογώντας, βέβαια, την νομοθεσία στον βαθμό που υπάρχει αναφορικά με το DarkNet παρατηρούμε μία σημαντική αντίφαση ως προς την ελευθερία πλοήγησης και αναζήτησης που παρέχεται στον χρήστη και την ποινικοποίηση των δραστηριοτήτων που θεωρούνται παράνομες. Η διαχείριση αυτού του διπλού χαρακτήρα του «Σκοτεινού Ιστού» απαιτεί μια διαρκή ισορροπία μεταξύ προστασίας της ατομικής ελευθερίας και της εξασφάλισης της έννομης ασφάλειας.

Όσον αφορά τη διχογνωμία για το εάν μπορεί να υπάρξει, τελικά, νομοθετικό πλαίσιο που να αφορά αποκλειστικά το DarkNet, καταλήγουμε στο ότι πρέπει να επικεντρωθούμε στην ενίσχυση των υπαρχόντων νομικών εργαλείων και στη δημιουργία νέων κανονισμών που θα ανταποκρίνονται άμεσα στους νέους κινδύνους που προκαλεί η ύπαρξη του DarkNet. Αυτό θα διευκολύνει τις αρχές να ασκήσουν αποτελεσματικότερα τον έλεγχο και την παρέμβαση σε εγκλήματα που διαπράττονται μέσω του DarkNet, διασφαλίζοντας ταυτόχρονα τη νομιμότητα και τη διαφάνεια στην επιβολή του νόμου.

Βιβλιογραφία

[1] [Dark Web: Η ανεξερεύνητη πλευρά του διαδικτύου | OffLine Post](https://www.offlinepost.gr/2020/08/26/dark-web-%ce%b7-%ce%b1%ce%bd%ce%b5%ce%be%ce%b5%cf%81%ce%b5%cf%8d%ce%bd%ce%b7%cf%84%ce%b7-%cf%80%ce%bb%ce%b5%cf%85%cf%81%ce%ac-%cf%84%ce%bf%cf%85-%ce%b4%ce%b9%ce%b1%ce%b4%ce%b9%ce%ba%cf%84%cf%8d/) (Πολύβιος Κοΐνης 26 Αυγούστου, 2020)

[2][Τι είναι το TOR; (The Onion Router) Γλωσσάρι VPN (websiterating.com)](https://www.websiterating.com/el/vpn/glossary/what-is-tor/#:~:text=%CE%A4%CE%B9%20%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9%20%CF%84%CE%BF%20TOR%3B%201%20%CE%95%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7%20%CE%A4%CE%BF%20TOR%2C,%CE%A0%CF%8E%CF%82%20%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF%20%CF%84%CE%BF%20TOR%20...%204%20%CE%A3%CF%85%CE%BC%CF%80%CE%AD%CF%81%CE%B1%CF%83%CE%BC%CE%B1%20) (Τελευταία πρόσβαση: 14.05.2024)

[3] [Dark Web - Βικιπαίδεια (wikipedia.org)](https://el.wikipedia.org/wiki/Dark_Web) (Τελευταία πρόσβαση: 14.05.2024)

[4] Συντάκτες: Austin A Mardon, Kauthar Mohammad, khushi shah, amna abuaskar. Έτος δημιοσίευσης: 2021. (Συμπεριλάβαμε πληροφορίες από το πρώτο κεφάλαιο)

[The Dark Web: The Enigmatic Digital World | Austin A Mardon, Kauthar Mohammad, khushi shah, and amna abuaskar - Academia.edu](https://www.academia.edu/56064859/The_Dark_Web_The_Enigmatic_Digital_World?auto=download)

[5] <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32017L0541&qid=1715712030565> (Τελευταία πρόσβαση 15.05.2024)

[6] <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32022L2555&qid=1715711956601> (Τελευταία πρόσβαση 15.05.2024)

[7] Anthony Minnaar 2017 Online ‘underground’ marketplaces for illicit drugs: The protype case of the dark web website ‘Silk Road’.Διαθέσιμο στο: [https://www.academia.edu/](https://www.academia.edu/40211472/ONLINE_UNDERGROUND_MARKETPLACES_FOR_ILLICIT_DRUGS_THE_PROTOTYPE_CASE_OF_THE_DARK_WEB_WEBSITE_SILK_ROAD)

[8] *Edwards, J*. 2013a. This is the physics student and used book seller who allegedly ran the 'SilkRoad' market for drugs and assassins. *Business Insider*. Διαθέσιμο στο:[http://www.businessinsider.com/meet-ross-ulbricht](http://www.businessinsider.com/meet-ross-ulbricht-the-brilliant-alleged-mastermind-ofsilk-road-2013-10%20)

[9] *Love, D*. 2013. There's a secret internet for drug dealers, assassins, and pedophiles. *Business Insider.* Διαθέσιμο στο: [http://www.businessinsider.com/tor-silk-road-deep-web](http://www.businessinsider.com/tor-silk-road-deep-web-2013-3)

[10] *Mullin, J*. 2015. Sunk: How Ross Ulbricht ended up in prison for life –Inside the

trial that brought down a darknet pirate. *ARS TECHNICA*. Διαθέσιμο στο: <http://arstechnica.com/tech-policy/2015/05/sunk-how-ross-ulbricht-ended-up-in-prisonfor-life>

[11] Sherloc, UNODC (United Nations Office on Drugs and Crime)

Διαθέσιμο στο: [*https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united\_states\_of\_america*](https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america)