Παρακολουθήσεις εκτός συνόρων ή «για λόγους εθνικής ασφάλειας»

διαμαρτυρία στο Ευρωπαϊκό Κοινοβούλιο, Μάρτιος 2014

Προηγούμενες αναρτήσεις από το μάθημα Surveillance Law του Coursera:
Νομοθεσία των ΗΠΑ περί παρακολουθήσεων (εβδομάδα 1)
Τηλεφωνικές παρακολουθήσεις εντός ΗΠΑ (εβδομάδα 2)
Υποκλοπές e-mail (εβδομάδα 3α)
Πλοήγηση στον Ιστό, υποκλοπές από κινητά & κυβερνητικό χάκινγκ (εβδομάδα 3β)
Εξαναγκασμός εταιρειών και ατόμων να συνεργάζονται στις

παρακολουθήσεις (εβδομάδα 4)

Όλα όσα αναλύθηκαν τις τελευταίες εβδομάδες μέσα από τη σειρά των αναρτήσεων για τη νομοθεσία των ΗΠΑ περί παρακολουθήσεων - δηλαδή οι προστασίες του συντάγματος, το νομικό πλαίσιο και οι ερμηνείες που οριοθετούν την εφαρμογή του- ουσιαστικά εξουδετερώνονται στην περίπτωση που ο παρακολουθούμενος δεν είναι πολίτης ή κάτοικος των ΗΠΑ και αν η παρακολούθησή του γίνεται εκτός συνόρων ΗΠΑ. Με δυο λόγια, **οι ΗΠΑ δεν προστατεύουν την ιδιωτικότητα των επικοινωνιών ξένων υπηκόων εκτός των συνόρων τους. Το ίδιο ισχύει, όμως, και για τα δεδομένα των επικοινωνιών που είναι αποθηκευμένα σε αμερικάνικους cloud servers, όταν ο κάτοχός τους είναι ξένος.**

Αυτό, όμως, δεν κάνει ούτε τους Αμερικανούς προνομιούχους, αφού μέσω της συγκεκριμένης εξαίρεσης, η χώρα τους **έχει βρει τον τρόπο να παρακάμπτει τους νομικούς περιορισμούς και να παρακολουθεί και τον δικό της πληθυσμό**. Επικαλούμενο **λόγους «εθνικής ασφάλειας»** -ένα δόγμα που κυριάρχησε σε κάθε πεδίο όπου το χρειάστηκαν οι εξουσίες, μετά την 11η Σεπτεμβρίου του 2001- **το πολιτικό και δικαστικό σύστημα των ΗΠΑ έχει αποδεχτεί τα τελευταία χρόνια την εγκατάσταση ενός παγκόσμιου συστήματος μυστικών υποκλοπών των επικοινωνιών της υφηλίου.** Μέχρι να έρθουν οι αποκαλύψεις του Έντουαρντ Σνόουντεν, το καλοκαίρι του 2013, υπήρχαν διαρροές που καταδείκνυαν πτυχές αυτού του συστήματος. Οι συγκεκριμένες διαρροές, ωστόσο, δεν ήταν αρκετές για να τεκμηριώσουν το συγκλονιστικό εύρος και το βάθος της διείσδυσής του, όπως τα γνωρίζουμε σήμερα.

Επιπλέον, μεγάλο μέρος του νομικού πλαισίου που καθορίζει τη νομιμότητα των παρακολουθήσεων εκτός συνόρων έχει διαμορφωθεί **μέσα από διαδικασίες «ex parte», δηλαδή με δίκες στις οποίες υπό την επίκληση λόγων εθνικής ασφάλειας δεν παρίσταται και δεν ακούγεται από τον δικαστή πάρα μόνο η πλευρά της κυβέρνησης.** Το δικαστικό αυτό παράδοξο, που μοιάζει με σεναριακή υπερβολή όταν το βλέπεις σε αμερικάνικες τηλεοπτικές

σειρές, είναι ένα πραγματικό εργαλείο συγκάλυψης τερατουργημάτων της ελίτ που κυβερνά τις ΗΠΑ, σε βάρος κάθε έννοιας δημοκρατίας, διαφάνειας και ελέγχου της εξουσίας.

Όποιος παρακολουθεί τη σειρά των συγκεκριμένων αναρτήσεων από το μάθημα Surveillance Law, ίσως να θυμάται πως **μια από τις βασικές προϋποθέσεις για να στραφεί κανείς δικαστικά κατά των αρχών των ΗΠΑ, αν πιστεύει ότι παρακολουθείται καθ'υπέρβαση του νόμου, είναι το να αποδείξει κατ'αρχήν ότι έχει πέσει θύμα παρακολούθησης. Όμως, λόγω της μυστικότητας που περιβάλει τη λειτουργία αυτού του συστήματος υποκλοπών, κάτι τέτοιο ήταν ουσιαστικά αδύνατο μέχρι να έρθουν οι αποκαλύψεις Σνόουντεν**, επισημαίνει ο Τζόναθαν Μάγιερ. Τώρα πια, αφού αποδεικνύεται πως τα προγράμματα μαζικών υποκλοπών επηρεάζουν στην πραγματικότητα το σύνολο των πολιτών ακόμη και εντός αμερικανικών συνόρων, δυνητικά ανοίγει ένας δρόμος για δικαστικές προσφυγές που θα μπορούν να βασίζονται σε επίκληση αυτών των αποκαλύψεων. Αν κατανοήσει κανείς αυτή τη λεπτομέρεια, καταλαβαίνει γιατί οι αποκαλύψεις του συγκεκριμένου πρώην συνεργάτη της NSA για τη δράση της, αφενός οδήγησαν στη λυσσαλέα δίωξή του, αφετέρου προσέφεραν ένα σπουδαίο όπλο στην κοινωνία των πολιτών.

Όταν ο στόχος ή το αντικείμενο των υποκλοπών είναι εκτός συνόρων ΗΠΑ

Η εξαίρεση ή όχι από τις προστασίες του συντάγματος των ΗΠΑ εξαρτάται από τους δεσμούς που έχει κανείς με τη συγκεκριμένη χώρα. Εκτός από τους πολίτες της, έχει κριθεί δικαστικά ότι μπορεί να προστατεύεται και κάποιος που έχει εισέλθει στην επικράτειά της και έχει αναπτύξει ουσιαστικούς δεσμούς μαζί της. Ουσιαστικά, δηλαδή, προστατεύονται και οι μόνιμοι κάτοικοι, καθώς και κάποιοι προσωρινά διαμένοντες, υπό προϋποθέσεις (και υπό την κρίση κάθε δικαστηρίου). Αυτό όμως, ισχύει μόνο αν η παρακολούθηση συμβεί εντός των ΗΠΑ. **Τα δεδομένα αλλάζουν όταν η παρακολούθηση γίνεται στο εξωτερικό, ή αν οι βάσεις δεδομένων των παρακολουθούμενων επικοινωνιών βρίσκονται στο εξωτερικό.**

Τοποθεσία του στόχου

Το πρώτο που εξετάζεται είναι η τοποθεσία του στόχου, δηλαδή του ατόμου που παρακολουθείται. **Αν πρόκειται για αμερικανό πολίτη, εξακολουθεί να ισχύει η προστασία του συντάγματος, αλλά χαλαρώνουν οι απαιτήσεις για αιτιολόγηση της παρακολούθησης και για έκδοση εντάλματος**. Έτσι, π.χ. για να τεθεί υπό παρακολούθηση ένας αμερικανός πολίτης που κάνει διακοπές ή δουλεύει στο εξωτερικό, δεν χρειάζεται συνήθως ένταλμα, αλλά μια πιο ευέλικτη αιτιολόγηση που να στηρίζεται σε **κάποιου είδους σύνδεση των επικοινωνιών του με μια «πιθανή αιτία»** κάποιας εγκληματικής ενέργειας. Ή, αν στην υπόθεση εμπλέκονται και οι αστυνομικές αρχές της χώρας όπου βρίσκεται ο στόχος, μπορεί οι ΗΠΑ να δεσμεύονται να εφαρμόσουν την εκάστοτε τοπική νομοθεσία περί παρακολουθήσεων.

Αν πρόκειται για μη αμερικανό πολίτη, δηλαδή για τον υπόλοιπο πληθυσμό του πλανήτη, δεν αναγνωρίζεται καμία προστασία ιδιωτικότητας. Έτσι, αν π.χ. κάποιος ευρωπαίος χρήστης αμερικανικής υπηρεσίας e-mail ζημιωθεί από κάποια ενέργεια των αμερικανικών αρχών, όπως συμβαίνει με τις υποκλοπές της Εθνικής Υπηρεσίας Ασφαλείας (National Security Agency ή NSA), δεν μπορεί να επικαλεστεί την Τέταρτη Τροποποίηση του αμερικανικού συντάγματος για να προστατευτεί.

Τοποθεσία των δεδομένων του στόχου

Σημασία, ωστόσο, δεν έχει μόνο η τοποθεσία του στόχου, αλλά και η τοποθεσία των δεδομένων του, καθώς ζούμε στην εποχή της πληροφορίας. Τα δεδομένα κάθε κίνησής μας μέσω ίντερνετ, αλλά και κάθε ψηφιακής επικοινωνίας μας, αποθηκεύονται σε πολλούς σέρβερ ανά τον πλανήτη, και μάλιστα σε πολλαπλά αντίγραφα, για λόγους ασφαλείας, με αποτέλεσμα να αγνοούμε πού βρίσκονται και από ποιούς είναι προσβάσιμα.

Στην περίπτωση των αμερικανών πολιτών, η συνταγματική προστασία αλλάζει ανάλογα με το πού βρίσκονται τα δεδομένα. Αν οι σέρβερ είναι στις ΗΠΑ, εξακολουθεί να ισχύει η Τέταρτη Τροποποίηση. Αν βρίσκονται σε άλλη χώρα, αρκεί να κρίνεται ότι

αυτός είναι ο κατάλληλος τρόπος να υπηρετηθεί μια έρευνα (δες «εύλογο πρότυπο» – **εβδομάδα 2**) ώστε να παραδοθούν τα δεδομένα στο FBI ή στη CIA. Ή, πάλι μπορεί να τεθούν αυστηρότεροι όροι, αν αυτό καθορίζεται από την τοπική νομοθεσία περί παρακολουθήσεων.

Στην περίπτωση των μη αμερικανών, δεν ισχύει καμμία συνταγματική προστασία, εκτός αν τόσο ο στόχος όσο και τα δεδομένα βρίσκονται εντός των ΗΠΑ. Για όλες τις υπόλοιπες περιπτώσεις, δηλαδή για τη συντριπτική πλειοψηφία του παγκόσμιου πληθυσμού και για την συντριπτική πλειονότητα των ψηφιακών δεδομένων που υπάρχουν αποθηκευμένα οπουδήποτε, δεν ισχύει η Τέταρτη Τροποποίηση, περί ιδιωτικότητας.

Εξίσου σημαντικό, όμως, είναι και το τι συμβαίνει στις περιπτώσεις που οι αμερικανικές αρχές κάνουν λάθος και διεξάγουν παρακολουθήσεις που εκ των υστέρων κρίνονται παράνομες, ή αν στο πλαίσιο μια έρευνας συλλέξουν «κατά λάθος» και δεδομένα ανθρώπων που δεν θεωρούνται στόχοι. Τουλάχιστον σε μία περίπτωση ένα αμερικανικό δικαστήριο έκρινε ότι δεδομένα που συλλέχθηκαν από λάθος ή παράλειψη έπρεπε να διαγραφούν αμέσως. **Η κυρίαρχη θεώρηση, πάντως, είναι ότι το κράτος συγχωρείται να κάνει μερικά λάθη, και ότι αν παρακολουθούνται κατά σύμπτωση και κάποιοι που συνομιλούν με «στόχους», αναγκαστικά εκτίθενται κι αυτοί στις παρακολουθήσεις.** Μια μειοψηφία νομικών, πάντως, εγείρει σοβαρές ενστάσεις, επισημαίνοντας ότι οι η ιδιωτικότητα αυτών των μη-στόχων, πρέπει να γίνεται σεβαστή.

Τοποθεσία συλλογής ή τοποθεσία ανάλυσης των δεδομένων;

Ένα άλλο ζήτημα είναι το **τι συμβαίνει όταν τα δεδομένα συλλέγονται σε άλλη τοποθεσία από αυτή όπου τα αναλύουν οι αμερικανικές υπηρεσίες**. Η κυβερνητική θεώρηση είναι ότι δεν έχει σημασία πού αναλύονται, αλλά το πού έγινε η κατάσχεσή τους. Καθόλου αναπάντεχη προσέγγιση, αν θυμηθεί κανείς ότι, σύμφωνα με τις αποκαλύψεις Σνόουντεν, μεγάλο μέρος των δεδομένων (και από τους σέρβερ των ΗΠΑ) γίνεται μέσω του

διατλαντικού δικτύου υποκλοπών που έχει στηθεί σε συνεργασία με τη Μ.Βρετανία. Με απλά λόγια, **η NSA θα χρειαζόταν ένταλμα ή κλήτευση για να συλλέξει εντός της επικράτειας των ΗΠΑ δεδομένα από τις επικοινωνίες π.χ. ενός Αμερικανού που χρησιμοποιεί αμερικάνικο email. Αλλά δεν χρειάζεται καμμία έγκριση για να τα ζητήσει και να τα λάβει μέσω της βρετανικής μυστικής υπηρεσίας GCHQ, ώστε να μπορεί να τα επεξεργαστεί με την ησυχία της στις εγκαταστάσεις της στις ΗΠΑ.**

Και ο νόμος FISA, εξάλλου, ενισχύει αυτή την προσέγγιση, προσδιορίζοντας τα όρια της προστασίας της ιδιωτικότητας με βάση την τοποθεσία που γίνεται η κατάσχεση των δεδομένων και όχι την τοποθεσία της ανάλυσής τους. Μπορεί κανείς να διανοηθεί πόσο διευκολύνει αυτό τις υποκλοπές που διεξάγουν από κοινού οι ΗΠΑ και η Μ.Βρετανία, αν σκεφτεί ότι το 25% της τρέχουσας παγκόσμιας διαδικτυακής κίνησης περνά από το βρετανικό έδαφος μέσω καλωδίων τηλεπικοινωνιών που συνδέουν τις ανατολικές ακτές των ΗΠΑ με την Ευρώπη, την Αφρική και τον υπόλοιπο κόσμο, όπως επισημαίνει ο Λουκ Χάρντινγκ στον **«Φάκελο Σνόουντεν»**.

Ο πολιτειακός θεσμός που έχει την εξουσία και θα μπορούσε αν ήθελε να διασφαλίσει μια πιο εκτεταμένη προστασία της ιδιωτικότητας, είναι το αμερικανικό Κογκρέσο, επισημαίνει ο Τζόναθαν Μέγιερ. Τόσο ο νόμος ECPA, όσο και ο FISA, αφορούν το σύνολο των δεδομένων, ακόμη κι αν αυτά αφορούν μη-αμερικανούς πολίτες, ή αν βρίσκονται εκτός συνόρων. Συνεπώς θα αρκούσε μια σχετική ερμηνεία των νόμων ώστε να επεκταθεί η προστασία της ιδιωτικότητας των δεδομένων όλων των χρηστών του πλανήτη όταν αυτά αποθηκεύουν σε σέρβερ αμερικανικών τεχνολογικών εταιρειών.

Ο νόμος FISA και οι «λόγοι εθνικής ασφάλειας»

Στην πράξη, ωστόσο, το πολιτικό και δικαστικό σύστημα έχει λειτουργήσει σε βάρος των δικαιωμάτων των πολιτών. Ο **Νόμος περί Παρακολουθήσεων Αντικατασκοπείας (Foreign Intelligence Surveillance Act ή FISA)**, ο αντίστοιχος του νόμου ECPA στις

υποθέσεις όπου εμπλέκονται οι μυστικές υπηρεσίες, έχει αποτελέσει το κλειδί στη χαλάρωση της συνταγματικής προστασίας, με την επίκληση «λόγων εθνικής ασφαλείας». Επιπλέον, νομιμοποίησε για πρώτη φορά τις μαζικές (bulk) υποκλοπές, εντός και εκτός συνόρων, για παρελθοντικές ή/και μελλοντικές επικοινωνίες.

Ειδικότερα, ο FISA ρυθμίζει τους όρους διεξαγωγής των επιχειρήσεων παρακολούθησης εντός της επικράτειας των ΗΠΑ, καθώς και τις επιχειρήσεις ηλεκτρονικών παρακολουθήσεων εκτός επικράτειας αν αυτές αφορούν αμερικανούς πολίτες. Για τις υπόλοιπες επιχειρήσεις, δηλαδή για την κατασκοπεία εκτός συνόρων, υπάρχει η **Εκτελεστική Εντολή 12333 (Executive Order 12333)**, το πλαίσιο που καθορίζει τη συνεργασία των ομοσπονδιακών υπηρεσιών με την CIA.

Οι ομοσπονδιακές υπηρεσίες είναι οι πολυάριθμοι δορυφόροι της NSA (η οποία ιδρύθηκε το 1952 και υπάγεται στο υπ. Εθνικής Άμυνας). Στενοί συνεργάτες της NSA είναι οι μυστικές υπηρεσίες των άλλων χωρών μελών της συμφωνίας **"Five Eyes" (επισήμως "UKUSA Agreement")**: η **GCHQ** της Μ.Βρετανίας, η **CSE** του Καναδά, η **ASD** της Αυστραλίας, και η **GCSB** της Ν.Ζηλανδίας.

Εξαιρέσεις από την ιδιωτικότητα «για λόγους εθνικής ασφαλείας»

Εξαιρέσεις στην προστασία της ιδιωτικότητας των πολιτών «για λόγους εθνικής ασφάλειας» είχαν αναγνωρίσει διάφορα δικαστήρια από το 1967 και μετά, δηλαδή πριν συνταχθεί ο FISA. Σήμερα η κυρίαρχη θεώρηση είναι ότι αυτές οι εξαιρέσεις μπορούν να ισχύσουν ακόμη και σε υποθέσεις όπου δεν κρίνεται αποκλειστικά η εθνική ασφάλεια, αλλά που η εθνική ασφάλεια είναι ένας από τους «πρωταρχικούς σκοπούς» ή και απλώς ένας «σημαντικός σκοπός» της έρευνας. Στην πράξη, όπως αποδεικνύεται, **μπορεί οι αρχές να επικαλούνται λόγους εθνικής ασφαλείας απλώς για να κάνουν ευκολότερη τη δουλειά τους**.

Ο FISA αποτελεί την κορύφωση της «επαγγελματικής κατασκοπείας» που ανέπτυξαν οι ΗΠΑ τις τελευταίες δεκαετίες. Μέχρι το 1952

και επί δύο αιώνες που προηγήθηκαν, η κατασκοπεία ήταν αντικείμενο μόνο της εκτελεστικής εξουσίας και του στρατού, χωρίς να υπάγεται στον έλεγχο της δικαστικής και νομοθετικής εξουσίας. Η αρμοδιότητα της εκτελεστικής εξουσίας να πραγματοποιεί παρακολουθήσεις στο πλαίσιο επιχειρήσεων κατασκοπείας πήγαζε από το άρθρο ΙΙ του συντάγματος (που περιλαμβάνει και την Τέταρτη Τροποποίηση), **όπως το ερμήνευε η ίδια η εκτελεστική εξουσία εν κρυπτώ**. Το ίδιο ουσιαστικά ισχύει και σήμερα, διευκρινίζει ο Μάγιερ, με την εφαρμογή της Εκτελεστικής Εντολής 12333.

Μαζικές υποκλοπές με δικαστική επίβλεψη

Οι πρώτες επιτροπές νομοθετών που έλεγχαν τις κυβερνητικές υπηρεσίες πληροφοριών συγκροτήθηκαν μετά από μια σειρά δυσάρεστων αποκαλύψεων για παράνομες (μαζικές, χωρίς εντάλματα κλπ) υποκλοπές επικοινωνιών που είχαν διεξάγει η NSA, το FBI και η CIA, αλλά και μετά από σκάνδαλα όπως το Watergate. Η δημόσια οργή έφερε τη σύσταση της **SSCI** και της **HPSCI** που υποτίθεται ότι έχουν τη δυνατότητα να αναλύουν, να κατανούν και να ελέγχουν, για λογαριασμό των νομοθετών (Γερουσίας και Βουλής), τη λειτουργία του συστήματος παρακολουθήσεων. Οι δύο επιτροπές, ωστόσο, αποδείχτηκε ότι στην πορεία έγιναν υποχείρια των μυστικων υπηρεσιών, εγκρίνοντας ουσιαστικά όλα τους τα σχέδια μέχρι σήμερα.

Την ίδια περίοδο της κριτικής για τις παράνομες υποκλοπές, **το 1978, το Κογκρέσο συνέταξε το νόμο FISA**, επιχειρώντας να συμβιβάσει τα πράγματα, και **καθόρισε ότι οι παρακολουθήσεις θα εξακολουθούσαν να πραγματοποιούνται από τα όργανα της εκτελεστικής εξουσίας αλλά θα το έκαναν υπό δικαστική επίβλεψη**.

Έκτοτε, οι υποκλοπές υπό τον FISA απαιτούν την έκδοση ενός είδους εντάλματος, μια **Foreign Intelligence Wiretap Order**. Σε αντίθεση με τις αντίστοιχες Εντολές Υποκλοπών (Wiretap Orders) που εκδίδονται βάσει της ECPA, **οι εντολές βάσει FISA δεν απαιτούν πιθανή αιτιολόγηση εγκληματικής δραστηριότητας του**

στόχου, αλλά πιθανή αιτιολόγηση ότι ο στόχος είναι «ξένη δύναμη» (“foreign power”) ή «πράκτορας ξένης δύναμης» (“agent of foreign power”), ένας ορισμός που περιλαμβάνει τόσο τις άλλες χώρες όσο και τρομοκρατικές οργανώσεις.

Δικαστήρια περί «εθνικής ασφάλειας»

Τις προσφυγές που γίνονται βάσει του FISA, τις εξετάζουν ειδικά δικαστήρια, το πρωτοβάθμιο Foreign Intelligence Surveillance Court (FISC) και το Foreign Intelligence Surveillance Court of Review (FISCR) όταν γίνεται έφεση. Τυχόν περαιτέρω προσφυγές τις εξετάζει το Ανώτατο Δικαστήριο των ΗΠΑ.

Κανονικά τα ειδικά δικαστήρια του FISA εξέταζαν μόνο τα γεγονότα και δεν μπορούσαν να δίνουν ερμηνείες στο Νόμο. Αυτό άλλαξε με τον τροποποιητικό USA Patriot ACT, τον Πατριωτικό Νόμο που ήρθε μετά την 11η Σεπτεμβρίου. **Μετά το 2001, όλο και συχνότερα οι δικαστές των FISC και FISCR εξετάζουν νομικά επιχειρήματα, αλλά το κάνουν κυρίως σε δίκες “ex parte”, που γίνονται εν κρυπτώ, εξετάζοντας απόρρητα στοιχεία, με τη ακρόαση μόνο της κυβερνητικής πλευράς ως διαδίκου, οι αποφάσεις των οποίων κατά κανόνα δεν δημοσιοποιούνται**. Γι’αυτό και τα δικαστήρια FISC και FISCR αποκαλούνται και «**μυστικά δικαστήρια**».

Μια σημαντική λεπτομέρεια είναι ότι τους δικαστές των μυστικών αυτών δικαστηρίων τους επιλέγει ο Αρχιδικαστής του Ανωτάτου Δικαστηρίου, μια θέση που ελέγχεται από τους Ρεπουμπλικανούς όλα αυτά τα χρόνια που εφαρμόζεται ο FISA. Έτσι, δεν θεωρείται τυχαίο που οι αποφάσεις των FISC και FISCR αντανακλούν συντηρητισμό και συμπάθεια για τις θέσεις του λόμπι υπέρ των παρακολουθήσεων.

πηγή *φωτό:* ***https://www.flickr.com/photos/greensefa/13105939224/in/photostream/***

Στην επόμενη και τελευταία ανάρτηση: Τα αμφιλεγόμενα προγράμματα παρακολούθησης της NSA