

Edward Snowden, il protagonista delle rivelazioni sullo spionaggio di massa della *privacy* individuale, in parte illegale, delle agenzie di *intelligence* statunitensi (National Security Agency – NSA) e britanniche (GCHQ), ma anche quelle australiane e di altri governi alleati, attraverso l'uso delle tecnologie digitali, vive da 10 anni in esilio in Russia, e oggi afferma che la sorveglianza da lui denunciata nel giugno 2013 “*sembra un gioco da ragazzi*” rispetto alle attuali tecnologie avanzate e invadenti utilizzabili dai governi e dalle *global corporations* del “*capitalismo della sorveglianza*”. Oggi, infatti, i governi e le aziende che vogliono infrangere la nostra *privacy* hanno a disposizione milioni di telecamere di videosorveglianza, il riconoscimento facciale¹, l'intelligenza artificiale² e *spyware* intrusivi come Pegasus utilizzato contro dissidenti e giornalisti³.

Il quarantenne Snowden ha preso la cittadinanza russa nel 2022 in quanto era l'unica alternativa al carcere che gli sarebbe toccato negli Stati Uniti (potenzialmente rischia ancora 30 anni di carcere ai sensi dell'*Espionage Act* del 1917, in questo in una condizione simile a quella in cui si trova Julian Assange⁴). Vive in Russia insieme alla moglie e due figli piccoli⁵ e negli ultimi due anni ha ridotto il suo profilo pubblico, tenendo meno discorsi e ritirandosi dalle interviste alla stampa e dai social media.

Alcuni lo considerano un eroe, l'informatore più importante da quando Daniel Ellsberg pubblicò i Pentagon Papers sulla guerra in Vietnam. Ma l'ex vicepresidente Dick Cheney, uno dei massimi architetti dello “*Stato di sorveglianza*” messo in piedi negli Stati Uniti dopo l'11 settembre 2001⁶, lo ha definito un “*traditore*” che “*ha commesso dei crimini*”. Questo punto di vista è ancora prevalente nell'*establishment* della sicurezza nazionale statunitense. Snowden ha ripetutamente affermato di non avere rimpianti per aver agito secondo la sua coscienza e aver reso pubblici i *file* della NSA. Come Ellsberg, avrebbe desiderato fare queste rivelazioni prima.

Nel 2013 – esattamente 10 anni fa – era fuggito dalle Hawaii ad Hong Kong dove aveva incontrato tre giornalisti – Ewen MacAskill del Guardian, l'editorialista Glenn Greenwald e la regista Laura Poitras – ai quali aveva consegnato decine di migliaia di documenti *top secret*. Attraverso le sue rivelazioni bomba ha costretto le agenzie di *intelligence* angloamericane ad ammettere un ampio spionaggio sui propri cittadini, intercettando, elaborando e archiviando i loro dati e condividendo queste informazioni.

Snowden è cresciuto nella Carolina del Nord e nella periferia di Washington, dove suo padre prestava servizio nella Guardia Costiera degli Stati Uniti e sua madre lavorava come impiegata presso la NSA. La sua ossessione per la tecnologia – ha violato la rete dei laboratori nucleari di Los Alamos da adolescente – lo ha portato a una carriera come ingegnere di sistemi della CIA e della NSA. Nel 2013, era stato assunto da un appaltatore della NSA, Booz Allen Hamilton, dopo un precedente impiego con Dell e la CIA.

Snowden è rimasto turbato nel vedere come gli analisti della NSA hanno utilizzato i poteri del governo per leggere le e-mail di persone legate sul piano affettivo o ex partner per poi perseguitarli online. Un particolare programma della NSA, noto come XKeyscore, ha permesso al governo USA di setacciare la storia di americani comuni su Internet, raccogliendo praticamente qualsiasi dato personale che li riguardasse⁷.

Snowden ha concluso che la comunità dell'*intelligence* - che avrebbe dovuto proteggere gli americani e prevenire il ripetersi degli attacchi terroristici dell'11 settembre 2001 - aveva *"hackerato la costituzione"* ed era diventata essa stessa una minaccia per le libertà civili. Snowden ha affermato di essere gradualmente rimasto deluso dai programmi in cui era coinvolto e di aver cercato di manifestare le sue preoccupazioni etiche attraverso canali interni, ma di essere stato ignorato. Per cui, ha deciso di fare una denuncia pubblica, sapendo che la sua vita e la sua carriera sarebbero state sconvolte. Ha svuotato i suoi conti in banca, ha messo i soldi in una scatola di munizioni d'acciaio per la sua ragazza e ha cancellato e crittografato i suoi vecchi computer. Il 20 maggio 2013, Snowden è volato a Hong Kong dove ha convocato i tre giornalisti per rivelare segreti riservati sull'ampia raccolta del governo di e-mail, chiamate telefoniche e attività su Internet fatta in nome della sicurezza nazionale.

Il 6 giugno 2013, il Guardian ha pubblicato la prima storia basata sulle rivelazioni di Snowden, rivelando che un'ordinanza segreta del tribunale consentiva al governo degli Stati Uniti di costringere Verizon a condividere i tabulati telefonici di milioni di americani. Il giorno successivo il giornale ha riferito di *Prism*, un sistema per aspirare dati dai giganti di Internet statunitensi tra cui Google e Facebook.

L'impatto è stato drammatico. James Clapper, il direttore dell'intelligence nazionale, che all'inizio di quell'anno aveva testimoniato al Congresso che la NSA non raccoglieva dati su milioni di americani, fu costretto a scusarsi e ad ammettere che la sua dichiarazione era stata *"chiaramente errata"*⁸.

L'American Civil Liberties Union (ACLU) ha intentato una causa costituzionale presso una corte federale. Un'azione legale che alla fine ha portato a una sentenza secondo cui il programma di raccolta di dati e conversazioni telefoniche di milioni di americani da parte della NSA era ed era sempre stato illegale⁹.

Il 9 giugno 2013, il Guardian ha rivelato l'identità di Snowden su sua richiesta. Ha detto: *"Non ho intenzione di nascondere chi sono perché so di non aver fatto nulla di male"*. L'allora 29enne Snowden ha spiegato le sue motivazioni, parlato del suo futuro incerto e del perché non avesse mai avuto intenzione di nascondersi nell'ombra. *"Non voglio vivere in un mondo in cui tutto ciò che faccio e dico viene registrato. Il mio unico motivo è informare il pubblico su ciò che viene fatto in loro nome e ciò che viene fatto contro di loro"*. *"Non posso*

in buona coscienza permettere al governo degli Stati Uniti di distruggere la privacy, la libertà di Internet e le libertà fondamentali per le persone di tutto il mondo con questa imponente macchina di sorveglianza che stanno segretamente costruendo". "Il panico [dopo l'11 settembre] ci ha resi politicamente vulnerabili. Quella vulnerabilità è stata sfruttata dal nostro stesso governo per autorizzarsi dei poteri radicalmente espansi che per decenni erano stati fuori portata. Avremmo dovuto sapere cosa sarebbe successo e, guardando indietro alla documentazione pubblica, penso che a livello intellettuale molti di noi lo sapessero. Ma le élite politiche e mediatiche hanno ripetuto incessantemente che la scelta qui era ovvia: una garanzia di vita o una certezza di morte", ha detto Snowden.

Articoli successivi su Guardian, Washington Post, New York Times e ProPublica – nonostante i tentativi dei governi di bloccare la pubblicazione dei materiali¹⁰ – hanno rivelato altre attività di spionaggio e come le agenzie statunitensi e britanniche avevano avuto accesso alle informazioni dai cavi che trasportavano il traffico telefonico e Internet mondiale. Le rivelazioni hanno confermato quello che gli attivisti pacifisti che negli anni '60 protestavano contro la guerra del Vietnam avevano sempre pensato e sostenuto – che la loro posta venisse letta e che le loro conversazioni telefoniche venissero intercettate – e ha innescato un dibattito nazionale sull'entità della sorveglianza del governo che ha scioccato l'opinione pubblica statunitense e mondiale.

L'amministrazione del presidente Barack Obama ha affermato che le fughe di notizie hanno causato danni alla sicurezza nazionale, inclusa la segnalazione di al-Qaeda e altri gruppi terroristici a specifici tipi di sorveglianza elettronica statunitense¹¹. Ma la pressione di attivisti e membri del Congresso ha costretto la Casa Bianca a declassificare molti dei dettagli che circondavano i programmi di sorveglianza e il modo in cui funzionavano, nel tentativo di rassicurare gli americani che la NSA non li stava spiando direttamente.

Pochi i cambiamenti positivi e un aumento dei pericoli negli ultimi 10 anni

Quello che certamente è cambiato rispetto al 2013 è che allora la stragrande maggioranza dei cittadini si fidava del proprio governo che invece li spiava legalmente e illegalmente, come si fidava delle aziende tecnologiche che collaboravano nell'attività di spionaggio. Oggi, invece, la sfiducia e la diffidenza sono estremamente diffuse tra i cittadini nonostante siano state emanate alcune riforme che hanno introdotto nuovi vincoli di trasparenza e supervisione, insieme alla crescita della tecnologia crittografata, che hanno fatto pendere la bilancia verso la tutela della *privacy*. L'impulso degli individui a proteggersi dalle intercettazioni statali è diventato così intenso che i giganti della tecnologia sono stati costretti a rispondere e nel 2016, per la prima volta da quando è stato creato, Internet ha trasportato più dati crittografati che non crittografati. In ultima analisi, lo "*Stato di sorveglianza*" degli Stati Uniti è riuscito a operare in totale segreto per così tanti anni dopo l'11 settembre 2001 che questo porta molti a domandarsi: siamo ancora tenuti all'oscuro?

L'amministrazione Obama aveva nominato una commissione di alto livello per esaminare le pratiche di sicurezza informatica, *intelligence* e sorveglianza; il *panel* ha raccomandato cambiamenti radicali, alcuni dei quali sono stati adottati¹². E per la prima volta dagli anni '70, il Congresso ha legiferato per restringere, piuttosto che ampliare, i poteri di sorveglianza della comunità dell'*intelligence*. Era assolutamente chiaro che Snowden aveva rivelato informazioni che non avrebbero dovuto essere segrete, che il pubblico aveva il diritto di conoscere.

Oggi, l'importanza delle rivelazioni di Snowden è difficile da contestare perché i tribunali federali hanno invalidato i principali programmi di sorveglianza del governo a causa di tali rivelazioni. Il Congresso ha cambiato la legge a causa di tali rivelazioni. Lo *USA Freedom Act* nel 2015 ha ridotto alcune delle pratiche sui metadati della NSA, passando l'archiviazione di tabulati telefonici in blocco dall'agenzia alle compagnie telefoniche e aprendo il tribunale di sorveglianza dell'*intelligence* straniera a un minimo di controllo pubblico. Il presidente Obama ha rivisto un ordine esecutivo che riguardava il modo in cui il governo degli Stati Uniti si occupava delle comunicazioni dei non americani. Tutto questo non sarebbe successo senza quelle rivelazioni.

Nel Regno Unito si sono svolte tre inchieste. La prima è stata fatta dal Comitato di intelligence e sicurezza del parlamento (ISC). Ha fatto poco per investigare su ciò che le spie stavano effettivamente facendo, pur riconoscendo che era necessaria una nuova legislazione. Una inchiesta di David Anderson QC, il revisore indipendente della legislazione sul terrorismo, è stata più circospetta e ha suggerito una serie di miglioramenti. Infine, il Ministero dell'Interno ha convocato un *panel* che ha prodotto un rapporto e una serie di raccomandazioni. Questi tre rapporti alla fine hanno portato all'approvazione nel 2016 dell'*Investigatory Powers Act*, che ha chiarito quali tipi di sorveglianza statale erano consentiti e come questi dovevano essere autorizzati. L'atto ha consentito le intercettazioni di massa - con grande sgomento degli attivisti per la privacy - ma ha cambiato il processo che regolava il modo in cui questa intercettazione veniva autorizzata. Ciò significava che mentre un segretario di stato poteva firmare un mandato che giustificava i poteri più intrusivi, quel mandato doveva essere approvato anche da un commissario giudiziario indipendente.

Da questo punto di vista, l'eredità delle fughe di notizie di Snowden è mista. L'intercettazione e la sorveglianza di massa non si sono fermate, nonostante ora ci sia maggiore trasparenza e maggiore controllo. Ci sono alcune garanzie in più, ma per lo più continua. La più grande eredità delle fughe di notizie di Snowden sono le sfide legali che hanno reso possibili. Fino a queste rivelazioni, era quasi impossibile intentare una causa legale contro la sorveglianza statale. Ora ci sono state diverse cause legali di successo sia negli USA sia in UK sia nella UE¹³.

Rispetto a 10 anni fa, Snowden vede l'uso diffuso della crittografia *end-to-end* come una delle eredità positive delle fughe di notizie. Le società Big Tech sono state imbarazzate dalle rivelazioni secondo cui avevano consegnato dati personali alla NSA. Un imbarazzo che si è poi trasformato in rabbia quando ulteriori fughe di notizie hanno rivelato che, nonostante tale collaborazione, la NSA era riuscita ad ottenere dati dalle società Big Tech attraverso vulnerabilità *backdoor*. In risposta, nonostante l'opposizione delle agenzie, le aziende si sono precipitate nella crittografia *end-to-end* anni prima del previsto.

Prima della crittografia *end-to-end* un'enorme frazione del traffico Internet globale viaggiava elettronicamente senza alcuna protezione. Ma i progressi tecnologici continuano a corrodere la privacy. Secondo Snowden, *"l'idea che dopo le rivelazioni del 2013 ci sarebbero stati arcobaleni e unicorni il giorno successivo non era realistica. È un processo continuo. E dovremo lavorarci per il resto della nostra vita e per la vita dei nostri figli e oltre"*. Dal suo punto di vista, comunque, la sorveglianza di massa è ora prevalentemente eseguita da *"società amorali di telecomunicazioni e sorveglianza mascherate da attività commerciali e pubblicitarie. Sfruttano le debolezze delle nostre leggi, dispositivi e reti per riempire i loro dossier e poi venderli ai governi"*.

Le agenzie di *intelligence* negli Stati Uniti e nel Regno Unito continuano a sostenere che le rivelazioni di Snowden hanno arrecato loro un grave danno. L'MI6 britannico ha dovuto chiudere le operazioni di *intelligence* umana. L'altra loro lamentela è che la narrazione del 2013 ritraeva la NSA e il GCHQ come gli unici attori malvagi, ignorando ciò che Russia e Cina stavano facendo su Internet. Snowden contesta tali affermazioni. Ha detto che nessuno all'epoca pensava che Russia e Cina fossero angeli. Per quanto riguarda i danni, ha affermato che le agenzie non hanno mai citato alcuna prova concreta. *"Rottura di un sistema? Certo, è plausibile", ha detto. "Ma è difficile rivendicare un 'danno' se, nonostante 10 anni di crisi isteriche, il cielo non è mai caduto"*.

Secondo Snowden, ora l'attenzione dovrebbe essere concentrata su cos'altro debba essere fatto per garantire che le attività di sorveglianza dei governi (e delle imprese loro alleate) siano soggette al controllo democratico. Le riforme legali e politiche che sono arrivate sulla scia delle rivelazioni di Snowden probabilmente hanno appena scalfito gli elementi critici della questione. Molte di queste riforme sono state troppo modeste per affrontare la portata del problema della sorveglianza (fisica e digitale). Secondo alcuni osservatori lo *"Stato della sicurezza nazionale"* sarebbe diventato ancora più subdolo e potente. La tecnologia è migliorata e una delle cose che lo *"Stato di sorveglianza"* degli Stati Uniti è esperto nel fare, e lo è stato da quando è stato creato alla fine della seconda guerra mondiale, è garantire che gli americani abbiano sempre un nuovo nemico da temere e abbiano sempre una ragione per credere che sia necessario che il governo possa operare in segreto e spiare e avere poteri illimitati.

Mentre Snowden ha sensibilizzato l'opinione pubblica sulla sorveglianza di massa come mai prima di allora, gli elettori e coloro che eleggono non hanno necessariamente agito di conseguenza. Ci sono state solo modifiche modeste a ciò che la NSA poteva o non poteva fare, doveva rivelare o meno, protocolli per mandati FISA (*Foreign Intelligence Surveillance Act*), quindi il dibattito pubblico è stato aperto ma non ha portato a una significativa riduzione dei poteri del governo americano. C'è una sorta di consenso *bipartisan* sulla sicurezza nazionale, e sia i democratici che i repubblicani, alla fine hanno lasciato i poteri della NSA per lo più intatti. I cambiamenti istituzionali, politici e legali negli USA, come in altri Paesi, si sono dimostrati molto più difficili da realizzare rispetto al semplice sollevare domande critiche¹⁴.

Qualcosa è cambiato per quanto riguarda i media statunitensi e britannici che erano stati in precedenza criticati come troppo deferenti nei confronti delle autorità governative, ad esempio durante la guerra in Iraq, ma anche in relazione alle prime segnalazioni del sistema spionistico messo in piedi dalla NSA¹⁵. Una delle più importanti eredità del caso Snowden è stata la diffusione di un nuovo spirito di impavidità. Il coraggio che i giornalisti e gli editori del *Guardian* hanno mostrato di fronte a un'incredibile pressione non è stato solo significativo all'epoca – alla fine, il *Guardian* e il *Washington Post* hanno condiviso il premio Pulitzer 2014 per l'inchiesta¹⁶ –, ma ha effettivamente incoraggiato, almeno negli Stati Uniti e nel Regno Unito, un po' tutti i media. Quindi, una delle eredità delle rivelazioni di Snowden è un sistema dei media che si dimostra più aggressivo e più attento a riferire sui segreti della sicurezza nazionale, nonostante che vi siano stati anche una serie di tentativi da parte dei governi di introdurre dei meccanismi per assicurarsi che i giornalisti non potessero mai più fare ciò che il *Guardian* e altri media hanno fatto 10 anni fa. L'informazione relativa alla guerra in Ucraina è stata criticata per essere troppo allineata alle posizioni del Pentagono e dell'amministrazione Biden, con il caso clamoroso dell'inchiesta sulla distruzione del gasdotto Nord Stream da parte delle forze militari degli Stati Uniti che il premio Pulitzer Seymour Hersh ha dovuto pubblicare in un blog e non su un giornale come il *New York Times*.

Alessandro Scassellati

1. Lo scorso novembre, un giovane afroamericano, Randal Quran Reid, è stato fermato dalla polizia di Stato in Georgia mentre stava guidando verso Atlanta. È stato arrestato in base a dei mandati emessi dalla polizia della Louisiana per due casi di furto a New Orleans. Reid non era mai stato in Louisiana, men che meno a New Orleans. Le sue proteste non hanno avuto successo ed è stato in prigione per sei giorni mentre la sua famiglia ha speso migliaia di dollari assumendo avvocati sia in Georgia che in Louisiana per cercare di liberarlo. È emerso che i mandati d'arresto erano basati esclusivamente su una (falsa) corrispondenza di riconoscimento facciale, sebbene questo non fosse mai menzionato in nessun documento della polizia; i mandati affermavano che "una fonte credibile" aveva identificato Reid come il colpevole. La corrispondenza del riconoscimento facciale non era corretta, il caso alla fine è andato in pezzi e Reid è stato rilasciato. È stato fortunato. Aveva la famiglia e le risorse per scovare la verità. Milioni di americani non avrebbero avuto tali risorse sociali e finanziarie. Reid, tuttavia, non è l'unica vittima di un falso riconoscimento facciale. I numeri sono piccoli, ma finora tutti gli arrestati negli Usa dopo un falso riscontro erano afroamericani. Il che non sorprende dato che sappiamo non solo che il design stesso del

software di riconoscimento facciale rende più difficile identificare correttamente le persone di colore, ma anche che gli algoritmi replicano i pregiudizi del mondo umano.[←]

2. Poco più di due settimane fa, membri di spicco della comunità tecnologica, tra cui Sam Altman, CEO di OpenAI, che crea ChatGPT, Demis Hassabis, CEO di Google DeepMind, e Geoffrey Hinton e Yoshua Bengio, spesso considerati come i padrini dell'IA moderna, hanno rilasciato una dichiarazione affermando che l'IA potrebbe annunciare la fine dell'umanità. *"Mitigare il rischio di estinzione da parte dell'IA"*, hanno avvertito, *"dovrebbe essere una priorità globale insieme ad altri rischi su scala sociale come le pandemie e la guerra nucleare"*. Un monito che molti hanno interpretato come un invito ipocrita a regolamentare il settore del capitalismo digitale che finora si è battuto in tutti i modi contro qualsiasi tentativo di regolamentazione pubblica. Su questi temi si vedano gli articoli di Roberto Rosso su Transform! Italia, ad esempio, qui, qui, qui e qui.[←]
3. Con l'evolversi della tecnologia, anche la sorveglianza si evolve. Gli Stati hanno trovato nuovi modi per spiare i cittadini, in particolare utilizzando i telefoni cellulari che tutti portano con sé. *Spyware* intrusivi come Pegasus, venduto dalla società di sorveglianza israeliana NSO Group, possono trasformare il telefono di una persona in una macchina di sorveglianza 24 ore su 24. Un'indagine del 2021 del Guardian e di altre organizzazioni mediatiche ha mostrato come attivisti, giornalisti e avvocati fossero stati presi di mira da *malware* acquistati da paesi come Arabia Saudita, Emirati Arabi Uniti, Ungheria e India.[←]
4. Julian Assange è un cittadino australiano che viene perseguito dal governo degli Stati Uniti per aver pubblicato informazioni classificate sulla condotta degli Stati Uniti nelle guerre illegali del paese, comprese prove dirette di crimini di guerra statunitensi e morti civili non segnalate in precedenza. Assange ha pubblicato documenti riservati, in gran parte il risultato di una fuga di notizie da parte dell'ex analista dell'*intelligence* dell'esercito americano Chelsea Manning, condannata a 35 anni di carcere, ma rilasciata dopo che il presidente Barack Obama ha commutato la sua pena nel 2017. Attraverso i cosiddetti *WikiLeaks*, a partire dal 2010 Assange ha svelato innumerevoli crimini di guerra, abusi ed orrori, avendo divulgato più di 700 mila documenti riservati sulle attività militari e diplomatiche statunitensi durante la *"guerra globale al terrorismo"*, soprattutto in Iraq e Afghanistan. Per questo Assange rischia fino a 175 anni di carcere negli USA se sarà estradato dal Regno Unito dove è detenuto da oltre 4 anni. Sulla persecuzione di Assange vedi il nostro articolo qui.[←]
5. Dopo i suoi incontri con i giornalisti a Hong Kong, Snowden aveva intenzione di recarsi, attraverso la Russia, in Ecuador e chiedere asilo. Ma quando il suo aereo è atterrato a Mosca, ha saputo che il suo passaporto americano era stato annullato. Ha trascorso 40 giorni in aeroporto, cercando di negoziare l'asilo e, dopo che questo gli era stato negato da 27 paesi, si è stabilito in Russia. La sua fidanzata di lunga data lo ha raggiunto a Mosca, si sono sposati e ora hanno due figli piccoli. Snowden ha ottenuto la cittadinanza russa per garantire che la famiglia potesse vivere insieme, ma rimane anche cittadino statunitense. Ha parlato in modo critico del regime del presidente Vladimir Putin. Snowden continua a lavorare come attivista per la *privacy* digitale e spesso ha parlato in pubblico online. È stato attivo nello sviluppo di strumenti che i giornalisti possono utilizzare, specialmente nei paesi autoritari, per rilevare se sono sotto sorveglianza.[←]
6. Il *Patriot Act*, che ha spazzato via regole di lunga data che impedivano allo Stato di monitorare i cittadini statunitensi senza *"probabile causa"*, è stato approvato in 45 giorni. La legislazione è diventata legge con un dibattito e un'opposizione minimi al Congresso, concedendo alle forze dell'ordine nazionali ampi poteri. Ha permesso al governo di tracciare il comportamento online degli americani, soprattutto degli americani musulmani, rendendo molto più facile l'acquisizione di un mandato. Ha dato il via libera all'FBI e alla CIA per effettuare *"intercettazioni telefoniche itineranti"* in cui gli agenti potevano seguire le tracce di comunicazione tra telefoni e computer. Ha sventrato il vincolo in vigore dagli anni '70 che proteggeva i cittadini statunitensi dalla sorveglianza straniera. E ha notevolmente aumentato il potere dell'FBI di ottenere i dati personali dei clienti americani da compagnie telefoniche, banche e fornitori di servizi Internet senza l'approvazione del tribunale attraverso le cosiddette *"lettere di sicurezza nazionale"*. I documenti di Snowden hanno dimostrato che entro il 14 settembre 2001- appena tre giorni dopo gli attacchi - l'allora direttore della NSA, Michael Hayden, aveva preso una *"decisione tattica"* per iniziare a ficcare il naso nelle comunicazioni digitali di persone presenti negli Stati Uniti. D'ora in poi, la NSA, senza consultare il Congresso o i tribunali, si è concessa il potere di sorvegliare qualsiasi americano sul suolo statunitense che fosse in contatto digitale con un paese straniero in cui si sapeva che esisteva il terrorismo, senza bisogno di alcun mandato. Il 4 ottobre 2001 la Casa Bianca concesse il permesso, sempre in

segreto e senza consultazione, alla NSA di accendere i riflettori sui cittadini statunitensi in quello che divenne noto come il President's Surveillance Program.[↵]

7. Snowden ha commentato nel 2014: *"Se avessi voluto estrarre una copia dell'e-mail di un giudice o di un senatore, tutto quello che dovevo fare era inserire quel selettore in XKeystore", un programma della NSA che non richiedeva alcun mandato dalla FISA o da qualsiasi altro tribunale*".[↵]
8. Le intercettazioni di massa venivano effettuate senza un mandato democratico e con poche garanzie reali. Quando la portata di questa sorveglianza è venuta alla luce, i funzionari hanno affermato che la maggior parte delle informazioni non era stata *"letta"* e quindi la loro raccolta non violava la *privacy*. Questo era falso; i dati potevano rivelare un'immagine intima della vita di qualcuno, un fatto che è stato confermato in successivi processi, che hanno dimostrato che la sorveglianza violava la privacy e la legge sui diritti umani. È bene ricordare che l'idea che lo Stato non abbia il diritto di entrare in una casa e sequestrare documenti è stata stabilita nella legge inglese nel famoso caso Entick contro Carrington (1765), che in seguito divenne la base per il quarto emendamento della Costituzione statunitense. In un famoso passaggio, Lord Camden dichiarò: *"Per le leggi dell'Inghilterra, ogni invasione della proprietà privata, anche se minima, è una violazione"*.[↵]
9. Sette anni dopo le rivelazioni di Snowden, una corte d'appello degli Stati Uniti ha stabilito che il programma di sorveglianza telefonica della NSA era illegale e che i leader dell'*intelligence* statunitense che lo difendevano pubblicamente non dicevano la verità. Una svolta significativa dato che i programmi di sorveglianza giustificati in base alla sicurezza nazionale erano stati generalmente tenuti fuori dal controllo giudiziario. *"Non avrei mai immaginato che sarei vissuto abbastanza per vedere i nostri tribunali condannare le attività della NSA come illegali e nella stessa sentenza mi attribuiscono il merito di averle smascherate"*, ha detto allora Snowden in un messaggio pubblicato su Twitter.[↵]
10. Il governo britannico credeva che, ordinando la distruzione dei computer del Guardian, avrebbe messo a tacere il giornale. In effetti, il Guardian ha semplicemente trasferito il centro delle pubblicazioni a New York, sotto l'allora redattore statunitense del giornale, Janine Gibson.[↵]
11. Nel 2008, l'allora senatore Barack Obama aveva denunciato le intercettazioni senza mandato dell'amministrazione Bush, assicurandosi l'immagine di campione delle libertà civili. Nella campagna elettorale per la presidenza, Obama aveva promesso *"basta con le intercettazioni illegali di cittadini americani.... Basta ignorare la legge quando è scomodo"*. Sfortunatamente, Obama non ha promesso di non ignorare la legge quando era *"davvero, davvero conveniente"*. Dopo che Obama ha conquistato la nomina presidenziale del Partito Democratico, ha ribaltato la sua posizione e ha votato per la concessione dell'immunità alle società di telecomunicazioni che hanno tradito i propri clienti con le agenzie dell'*intelligence* statunitense. Questo è stato un indicatore delle future depredazioni costituzionali di Obama presidente. Dopo che Obama è entrato in carica, i funzionari della sua amministrazione hanno rapidamente ampliato le appropriazioni dei dati personali degli americani da parte della NSA. Il *Washington Post* ha definito il primo mandato di Obama come *"un periodo di crescita esponenziale per la raccolta domestica della NSA"*. Nel 2010, il *Washington Post* ha riferito che *"ogni giorno, i sistemi di raccolta presso la [NSA] intercettano e archiviano 1,7 miliardi di e-mail, telefonate e altri tipi di comunicazioni"*. Nel 2011, la NSA ha ampliato un programma per fornire informazioni sulla posizione in tempo reale di ogni americano con un telefono cellulare, acquisendo più di un miliardo di tabulati telefonici ogni giorno da AT&T. Indipendentemente da ciò, i media hanno continuato a ritrarre Obama come un salvatore delle libertà civili.[↵]
12. Il *panel* di esperti selezionati da Obama ha riferito che non c'è stato un solo caso in cui la raccolta dei dati telefonici sia stata necessaria per fermare un attacco terroristico. Il rapporto del panel ha anche avvertito: *"Gli americani non devono mai commettere l'errore di fidarsi completamente dei nostri funzionari pubblici"*. Il panel ha concluso che la *"raccolta in blocco dei tabulati telefonici dei cittadini americani ha avuto uno scopo poco utile nella lotta al terrorismo"*, ha riferito ABC News. Ma come ha osservato Snowden, *"Questi programmi non riguardavano mai il terrorismo: riguardavano lo spionaggio economico, il controllo sociale e la manipolazione diplomatica. Riguardano il potere"*.[↵]
13. A partire dal 2013, le organizzazioni per i diritti civili, tra cui PI, Liberty e Big Brother Watch, hanno iniziato a contestare l'intercettazione e la sorveglianza di massa presso la Corte europea dei diritti dell'uomo e i tribunali inglesi. Le sentenze del tribunale per i diritti umani hanno stabilito un precedente in tutta Europa secondo cui tale

spionaggio richiede una previa autorizzazione indipendente o giudiziaria che deve essere significativa, rigorosa e verificare la presenza di adeguate “tutele end-to-end”. All’inizio di quest’anno, il tribunale dei poteri investigativi britannico ha ritenuto che l’MI5 avesse agito illegalmente conservando enormi quantità di dati personali dopo che PI e Liberty avevano intentato una causa. Nessuno di questi casi sarebbe stato possibile se le informazioni di Snowden non fossero venute alla luce, e si spera che abbiano esercitato pressioni sulle agenzie di *intelligence* affinché prestino attenzione alle tutele legali.[↔]

14. Troppo spesso i servizi di sicurezza confondono la protezione di chi detiene il potere con la protezione del pubblico. I politici hanno a lungo utilizzato i loro servizi di sicurezza e i loro poteri di sorveglianza per soffocare la protesta e il dissenso prendendo di mira chiunque potesse legittimamente sfidare (o addirittura mettere in discussione) la loro presa sul potere. Questo è il motivo per cui gli interessi dei servizi di sicurezza vanno così spesso a spese del pubblico. Anche così, il grido di battaglia di proteggere il pubblico è spesso usato per giustificare tale sorveglianza invasiva. Ora è in corso un’altra spinta da parte degli Stati per spiare i loro cittadini con il pretesto della sicurezza online e della legittima preoccupazione del pubblico per il cattivo comportamento online. Strumentalizzando questi temi si cerca di dare ai servizi di sicurezza e/o alle società tecnologiche la possibilità di violare la crittografia *end-to-end*. Ottenere una *backdoor* per *chat* crittografate è stato un obiettivo delle spie quasi da quando è stato inventato Internet. Ma non vi è alcuna garanzia che ciò renderà Internet più sicuro o privo di danni. Non bisogna lasciarsi ingannare dal fatto che la sorveglianza renda più sicuri. La realtà è che niente mette più in pericolo i cittadini.[↔]
15. Quando nel 2005 il New York Times rivelò le intercettazioni senza mandato della NSA, il giornale ammise di essersi seduto sulla storia per un anno per volere della Casa Bianca. Il Los Angeles Times ha bloccato la pubblicazione di una storia portata da un informatore che ha rivelato che la società di telecomunicazioni AT&T aveva consegnato tutto il suo traffico Internet alla NSA. Il giornale era stato sollecitato a censurare le rivelazioni da Hayden e dall’allora direttore dell’*intelligence* nazionale, John Negroponte.[↔]
16. Quando un gruppo di parlamentari chiese che lo Scott Trust (proprietario del Guardian) smettesse di pubblicare il materiale passato da Snowden, il Trust poté onestamente rispondere che non aveva tale potere.[↔]