PREMIO PULITZER 2014

GLENN GREENWALD

NO PLACE TO HIDE

EDWARD SNOWDEN E LA SORVEGLIANZA DI MASSA

SOTTO CONTROLLO

Rizzoli


PREMIO PULITZER 2014
GLENN GREENWALD
NO PLACE TO HIDE
EDWARD SNOWDEN
E LA SORVEGLIANZA DI MASSA
SOTTO CONTROLLO
Rizzoli

Il primo dicembre 2012, Glenn Greenwald, giornalista americano da anni in prima fila nella difesa delle libertà civili, rice
un'email firmata "Cincinnatus": il suo interlocutore vuole "che le persone possano comunicare in piena sicurezza" e
propone di dotarsi di un efficace sistema di cifratura, senza il quale "chiunque si metta in contatto con lui corre gravi risch
Solo così "Cincinnatus" potrà fornirgli alcune informazioni di sicuro interesse.
Qualche mese più tardi quelle "informazioni" inonderanno per settimane telegiornali, quotidiani, siti intern
sconvolgeranno la politica americana, chiameranno in causa Google, Facebook, Yahoo, Microsoft, Apple e scuoteranno
relazioni tra gli Stati Uniti e i loro principali alleati. "Cincinnatus", infatti, è Edward Snowden, un giovane informatico c
ha lavorato per la CIA e la NSA, l'onnipotente Agenzia per la Sicurezza Nazionale, ed è disposto a rinunciare alla ragazza c
ama, agli amici e a un ottimo stipendio, rischiando l'ergastolo e forse la vita, pur di rivelare al mondo il più gigantes
programma di sorveglianza di massa mai concepito e realizzato: la NSA ha obbligato le società telefoniche a fornire i tabul
di tutte le comunicazioni tra cittadini americani e con l'estero, ha acquisito dati dai server dei giganti dell'informatica e
internet, ha spiato leader politici o funzionari europei o aziende concorrenti di società americane, può accedere ai testi
miliardi di email, può entrare in cellulari e computer in tutto il mondo… Greenwald racconta i primi contatti con Snowde
l'incontro in una stanza d'albergo di Hong Kong, la serie di scoop con cui, a partire dal 5 giugno 2013, il "Guardian" pubbli
le segretissime carte della NSA, la fuga a Mosca, e soprattutto le implicazioni della mole di documenti portati alla luce, c
dimostrano una verità ineludibile: "il governo statunitense ha creato un sistema finalizzato alla totale eliminazione de
riservatezza telematica in tutto il pianeta". Sembra un romanzo di spionaggio, e lo è. Solo che ciò di cui si parla è successo
succede davvero, e riguarda tutti noi.

GLENN GREENWALD (New York 1967), firma di punta del "Guardian" fino a ottobre 2013, ha da poco fondato la testa
online The intercept. Tra i suoi bestseller, *A Tragic Legacy* (2007) sulla presidenza di George W. Bush, e *With Liberty and Just*
for Some (2011).
La rivista "Foreign Policy" l'ha inserito nella lista dei 100 pensatori più influenti del 2013. Grazie alle sue rivelazioni s
programma di sorveglianza della National Security Agency, il "Gardian" ha vinto il premio Pulitzer 2014.

Glenn Greenwald

Sotto controllo

Edward Snowden e la sorveglianza di massa

Rizzoli

ISBN 978-88-58-67085-9

Prima edizione digitale 2014 da edizione maggio 2014

Titolo originale:
NO PLACE TO HIDE.
EDWARD SNOWDEN, THE NSA,
AND THE U.S. SURVEILLANCE STATE

Le fonti e le note di questo libro sono consultabili al sito www.glenngreenwald.net
Traduzione di: Irene Annoni (Studio Editoriale Littera) e Francesco Peri

In copertina:
Art Director: Francesca Leoneschi
Graphic Designer: Laura Dal Maso / *the*World*of*DOT

www.rizzoli.eu

Questo libro è dedicato a tutti coloro che hanno tentato di far luce sui sistemi di sorveglianza di massa del governo degli Stati Uniti, soprattutto alle coraggiose «gole profonde» che, per farlo, hanno rischiato la libertà.

Il governo degli Stati Uniti ha perfezionato una capacità tecnologica che ci permette di monitorare i messaggi che attraversano l'etere […]. Questa facoltà potrebbe ritorcersi contro il popolo americano in qualsiasi momento e tale è la capacità di monitoraggio che a nessun cittadino resterebbe alcuna privacy: conversazioni telefoniche, telegrammi […]. Non ci sarebbe alcun posto in cui nascondersi.

Senatore Frank Church, presidente della Commissione speciale del Senato per l'esame delle operazioni governative in merito all'attività d'intelligence, 1975

Introduzione

Nell'autunno del 2005, senza nutrire particolari aspettative, decisi di aprire un blog argomento politico. All'epoca non potevo immaginare quanto quel gesto avrebbe cambiato mia vita. La ragione che mi aveva spinto a farlo era il crescente disagio che provavo per politiche radicali ed estremiste alle quali il governo statunitense si era avvicina all'indomani dell'11 settembre. Speravo che affrontare certi temi su internet mi avreb consentito di raggiungere più persone rispetto alla mia professione di allora, quella avvocato specializzato in diritti costituzionali e civili.

Un mese e mezzo dopo il «New York Times» uscì con una rivelazione sconvolgente: n 2001, riferiva il quotidiano, l'amministrazione Bush aveva segretamente ingiunto al National Security Agency (NSA) di intercettare le telecomunicazioni elettroniche dei cittadi americani, esentandola dalla necessità di procurarsi i mandati previsti in questi casi dal dirit penale statunitense. Quando la notizia era trapelata le intercettazioni senza mandato erano corso ormai da quattro anni, e varie migliaia di cittadini americani erano già stati spiati.

Era un tema che mi interessava molto e che ben conoscevo vista la mia preparazion giuridica. Il governo stava cercando di legittimare un programma clandestino della NS invocando proprio quella concezione estremista del potere esecutivo che mi aveva indotto a aprire il blog: l'idea che la minaccia terroristica conferisse al presidente prerogativ istituzionali pressoché incondizionate e la possibilità di fare qualunque cosa – persino viola la legge – pur di «tutelare la sicurezza del Paese». Il dibattito scaturito da quelle rivelazio portò in luce problemi complessi di diritto costituzionale e giurisprudenza, che la m formazione di legale mi aveva preparato ad affrontare nel merito.

Per due anni esaminai da ogni punto di vista lo scandalo delle intercettazioni sen mandato della NSA, scrivendone sul mio blog e poi in un libro che nel 2006 sarebbe diventa un bestseller. La mia posizione era semplice e lineare: disponendo quelle intercettazio illegali il presidente aveva violato la legge e doveva rendere conto del proprio operato nel sedi competenti. Dato il clima politico da Far West che aveva preso piede in America, sempr più ottuso e opprimente, un'idea simile non poteva che scontrarsi con resistenze di ogni sort

Sarebbe stato quel precedente a indurre Edward Snowden a scegliere me come prim interlocutore quando, alcuni anni più tardi, si trattò di portare in luce nuovi abusi perpetra dalla NSA su una scala ancora più stupefacente. Snowden si diceva convinto di poter conta su di me: sentiva che avrei colto i rischi insiti in quel progetto di sorveglianza di massa e quella pratica oltranzista della nontrasparenza, e sapeva che non ero tipo da tirarmi indiet di fronte alle pressioni del governo e dei suoi molti fautori, nei media e non solo.

La quantità stupefacente di documenti segretissimi che Snowden mi ha fatto avere e drammatica vicenda umana che lo vede come protagonista hanno risvegliato in tutto il mond un interesse di tipo nuovo per la minaccia della sorveglianza elettronica di massa, mostran che valore prezioso sia la riservatezza nell'era digitale. I problemi che quello scanda

sottintendeva, però, con gli anni si erano andati cronicizzando, quasi sempre all'insaputa d
cittadini.

Molti aspetti del dibattito in corso sulla NSA, inutile specificarlo, sono del tutto *sui gener*
al giorno d'oggi la tecnologia ha reso possibile un tipo di sorveglianza permanente e pervasiv
che fino a pochi anni fa era appannaggio dei più audaci autori di fantascienza. Va inolt
ricordato il clima instauratosi con gli attentati dell'11 settembre, improntato al culto del
sicurezza a qualunque prezzo e favorevole al proliferare degli abusi di potere. Grazie
coraggio dimostrato da Snowden e alla relativa facilità con la quale si possono copiare i da
in formato digitale, infine, abbiamo potuto vedere per la prima volta con i nostri occhi com
funziona davvero, nel dettaglio, un simile sistema di sorveglianza.

Al tempo stesso molti degli interrogativi suscitati dalla vicenda NSA richiamano episo
storici già noti. Non va dimenticato, per esempio, che uno dei momenti fondanti nella gene
degli Stati Uniti d'America è stata proprio la lotta contro l'invasione della privacy da parte d
governo: i coloni americani non erano disposti a tollerare che le autorità britannich
perquisissero le abitazioni private quando e come volevano. Potevano ammettere che in cer
casi, in presenza di indizi probanti, lo Stato si munisse di mandati *ad personam* e perquisis
specifici individui sospettati di attività criminali; anche e soprattutto per questo, però,
concetto di «mandato generale» – cioè l'autorizzazione a procedere indiscriminatamente
controllo dell'intera popolazione – risultava intrinsecamente contraddittorio.

Il Quarto emendamento alla Costituzione statunitense ha tradotto quel principio in legg
La formulazione è limpida e concisa: «Nessuno potrà ledere il diritto dei cittadini americani
non vedere sottoposte a perquisizioni e sequestri arbitrari le loro persone, le loro abitazion
le loro carte e i loro effetti personali, e non verranno emessi mandati in quel senso se non
presenza di fondati sospetti, ratificati da un giuramento o da una deposizione ufficia
contenenti indicazioni sul luogo da perquisire e le persone o le cose da porre sotto sequestro
Il Quarto emendamento doveva impedire una volta per tutte al governo americano
sottoporre i suoi cittadini a una sorveglianza generalizzata e sommaria, sganciata
motivazioni specifiche.

Nel Diciottesimo secolo il dibattito in materia concerneva soprattutto la perquisizione fisi
di abitazioni, ma le pratiche di sorveglianza si sono evolute di pari passo con le nuov
tecnologie. Intorno alla metà del Diciannovesimo secolo, quando l'espansione della re
ferroviaria ha iniziato a rendere possibile un sistema di recapito postale rapido ed economic
il Regno Unito fu travolto da uno scandalo sconcertante: era emerso che il governo britanni
apriva a propria discrezione la corrispondenza dei cittadini. Nei primi decenni del Ventesim
secolo il Bureau of Investigation degli Stati Uniti, prima incarnazione dell'odierna FB
intercettava le comunicazioni in transito sui cavi telefonici e telegrafici, sorvegliava
servizio postale e assoldava informatori per tenere sotto controllo chi contestava le politich
del governo in carica.

A prescindere dalle specifiche tecnologie di volta in volta utilizzate, la questione del
sorveglianza di massa presenta alcuni attributi costanti nel tempo. Tanto per cominciare, son
di norma i dissidenti e gli emarginati a fare le spese di quelle pratiche, e questo induce
simpatizzanti del governo e i qualunquisti a credere – sbagliando – di essere al sicuro. I
storia, inoltre, insegna che la pura e semplice esistenza di un apparato di sorveglianza
massa, qualunque sia nel concreto il suo utilizzo, basta a soffocare la dissidenza. Un

popolazione che si sente osservata giorno e notte non tarderà a trasformarsi in una socie malleabile e pavida.

Verso la metà degli anni Settanta, un'indagine condotta da Frank Church sullo spionagg dell'FBI ha portato a galla una verità sconvolgente: l'agenzia statunitense aveva schedato com potenziali «sovversivi» mezzo milione di cittadini americani e spiava con regolarità alcun categorie di persone sulla sola base delle loro convinzioni politiche. (Gli obbiettivi di quel pratiche andavano da Martin Luther King a John Lennon, passando per il Women's Liberatio Movement e un'associazione anticomunista come la John Birch Society.) Non si può cert affermare, in compenso, che il flagello dell'abuso di sorveglianza sia storicament un'esclusiva americana. Al contrario, il controllo di massa è una tentazione alla qua soggiace fin dall'alba dei tempi qualunque assetto di potere troppo spregiudicato. L'obbiettiv è sempre lo stesso: stroncare il dissenso e imporre l'obbedienza.

La pratica della sorveglianza è un tratto che accomuna dottrine politiche anch sensibilmente diverse tra loro. Nei primi anni del Ventesimo secolo gli imperi colonia francese e britannico hanno avviato dipartimenti *ad hoc* al solo scopo di tenere sott osservazione i movimenti anticoloniali, percepiti come una minaccia. Nel secondo dopoguer il ministero per la Sicurezza di Stato della Germania dell'Est, meglio conosciuto come Stas sarebbe diventato addirittura sinonimo dell'intrusione di un potere governativo nella vi privata delle persone. Più di recente, nei mesi in cui le proteste popolari note com Primavera araba mettevano in discussione la legittimità di certi dittatori aggrappati al poltrona, i regimi al potere in Siria, Egitto e Libia si sono adoperati per tenere d'occhio l'us che i dissidenti interni facevano di internet.

Alcune indagini condotte da Bloomberg News e dal «Wall Street Journal» hanno mostra che quei regimi autoritari hanno fatto letteralmente incetta di prodotti di sorveglianz acquistati da società di tecnologia occidentali nel momento stesso in cui venivano cin d'assedio dai manifestanti. In Siria il regime di Assad ha fatto venire in aereo alcu dipendenti della società di sorveglianza italiana Area Spa, spiegando che le autorità siriar avevano «urgente bisogno di seguire gli spostamenti di certe persone». In Egitto la poliz segreta di Mubarak si è dotata di costosi strumenti per scardinare le protezioni crittografich di Skype e intercettare le telefonate degli attivisti. In Libia, secondo quanto riferito dal «Wa Street Journal», i giornalisti e i ribelli penetrati nel centro di monitoraggio del governo n 2011 si sono trovati davanti «un muro di apparecchiature nere grandi come frigoriferi», con marchio della società di sorveglianza francese Amesys. Quelle apparecchiature «controllavan il traffico telematico» del principale fornitore di servizi internet della Libia, «aprendo messaggi di posta elettronica, risalendo alle password, ficcando il naso nelle chat in rete mappando i rapporti tra le varie persone sospette».

Possedere i mezzi per intercettare le telecomunicazioni della gente conferisce un pote immenso ai depositari di quel privilegio. Se quel potere non è tenuto a freno da rigoros procedure di supervisione e da una forte responsabilità istituzionale, chi ne dispone finis quasi certamente per abusarne. Credere che il governo statunitense potesse far funziona una colossale e segretissima macchina di controllo senza cedere a simili tentazioni significav ignorare la storia e sottovalutare ciò che sappiamo sulla natura umana.

Già prima delle rivelazioni di Snowden, in effetti, molti di noi avevano capito che parla della sorveglianza esercitata dagli Stati Uniti come di un'eccezione o un caso a parte e

peccare di ingenuità. Nel 2006, durante un dibattito al Congresso intitolato *Internet in Cin Strumento di libertà o di repressione?*, gli oratori si erano alternati per condannare le azienc tecnologiche americane, accusate di aiutare la Cina a mettere a tacere le voci di dissenso rete. Il deputato repubblicano del New Jersey Christopher Smith, presidente della sedut paragonò la cooperazione di Yahoo con il governo cinese all'operato della polizia segreta ch aveva consegnato Anna Frank ai nazisti. Fu un'arringa in piena regola, come sempre accad quando un funzionario americano parla di un regime non allineato alle politiche statunitensi.

Neanche ai presenti, però, poteva sfuggire il fatto che quel dibattito al Congresso si apriv a neppure due mesi dall'articolo con il quale il «New York Times» aveva smascherato grande programma di intercettazioni senza mandato promosso dall'amministrazione Bus Alla luce di quanto emerso, puntare il dito contro altri Paesi per accusarli di seguire in cas propria le stesse procedure rischiava di non suonare molto convincente. Il deputat democratico californiano Brad Sherman, che prese la parola dopo Smith, osservò come società di servizi telematici invitate a resistere al regime cinese avrebbero dovuto fa attenzione anche al proprio governo. «Altrimenti» ammonì con parole rivelatesi profetich «mentre la riservatezza dei cinesi viene violata nel modo più odioso, anche noi, qui negli Sta Uniti, potremmo scoprire un brutto giorno che un presidente sta leggendo la nostra pos elettronica accampando improbabili interpretazioni della Costituzione, e io preferirei ch questo non accadesse senza un mandato.»

Nel corso degli ultimi decenni i leader statunitensi hanno cavalcato la paura del terrorism continuamente rintuzzata da notizie ansiogene che ingigantiscono la reale entità del minaccia, per giustificare un ampio ventaglio di politiche estremiste. Quella paura è servita legittimare guerre di aggressione, un regime di tortura con ramificazioni sull'intero pianeta la detenzione (se non l'assassinio) di cittadini stranieri e americani anche senza precisi capi imputazione. Uno dei suoi effetti più duraturi, però, potrebbe essere proprio il sistem onnipresente e segreto per la sorveglianza di cittadini innocenti che quella paura h contribuito a instaurare; perché nonostante i molti paralleli storici, l'attuale scandalo del NSA presenta alcuni aspetti del tutto inediti, legati al ruolo che internet ha assunto nella nost vita quotidiana.

Internet non è un mondo a parte; soprattutto per le generazioni più giovani è il luog deputato all'esercizio di alcune funzioni vitali. Internet è molto più del nostro ufficio posta o del nostro telefono: è l'epicentro del mondo in cui viviamo. Attraverso di esso si esplic praticamente qualunque attività che ci riguarda. In rete conosciamo nuovi amici, scegliam che libri leggere e che film guardare, organizziamo la nostra partecipazione politica, creiam e archiviamo i nostri dati più riservati. Navigando nella rete sviluppiamo ed esprimiamo nostra stessa personalità e il nostro senso dell'io.

Trasformare tutto questo in un sistema di controllo di massa ha implicazioni impossibili d ricondurre a quelle di qualsiasi precedente programma di sorveglianza di Stato. Tutti i siste di spionaggio del passato erano, per ovvi limiti tecnologici, più circoscritti e quindi più fac da eludere. Consentire che la pratica della sorveglianza sulla rete metta radici, invec significherebbe sottoporre a un minuzioso controllo di Stato tutte le forme di interazione pianificazione, forse addirittura lo stesso pensiero umano.

Fin dal suo primo apparire internet è stato descritto da molti come un'opportuni straordinaria, in grado di liberare centinaia di milioni di persone democratizzando il discor

politico e riequilibrando i rapporti tra i potenti e gli indifesi. Quella promessa, però, irrealizzabile senza la garanzia della libertà, cioè senza la possibilità di proteggere l'utilizzo internet da vincoli istituzionali, procedure di controllo sociale o statale e soprattutto da u senso di paura costante. Trasformare il web in un sistema di sorveglianza, in altri termin equivale a stroncare il suo potenziale più prezioso. Peggio ancora, vuol dire trasformare rete in un dispositivo di repressione che prefigura lo strumento di intrusione di Stato p estremo e opprimente che la storia del genere umano abbia mai conosciuto.

Per questo le rivelazioni di Snowden sono così sconvolgenti, dirompenti e important Trovando il coraggio di denunciare le sbalorditive tecnologie di vigilanza messe a punto dal NSA e le sue sconcertanti ambizioni per il futuro, Snowden ci ha mostrato che la storia si trov oggi di fronte a un bivio. Vogliamo che l'era digitale sia l'alba dell'emancipazione individua e delle libertà politiche, resa possibile dalle inedite potenzialità di internet, oppure siam disposti ad accettare un sistema di monitoraggio e controllo onnipervasivo che neppure i p sadici tiranni del passato avrebbero osato sognare? Oggi come oggi, entrambe le alternativ sono possibili. Saranno le nostre azioni a decidere che cosa sarà di noi.

Il contatto

Edward Snowden mi ha contattato per la prima volta il 1° dicembre 2012, anche se allora no sapevo che l'autore del messaggio fosse lui.

Si era fatto vivo mandandomi una e-mail firmata «Cincinnatus», uno pseudonimo ch alludeva a Lucio Quinzio Cincinnato, l'agricoltore dell'antica Roma che nel Quinto secolo a.C fu nominato dittatore per respingere un attacco degli Equi. Lo si ricorda soprattutto perch dopo aver sconfitto gli avversari dell'Urbe, rinunciò a ogni carica istituzionale per tornare suo lavoro nei campi. La figura di Cincinnato è considerata un modello di virtù civica incarna la nobiltà d'animo di chi, nell'interesse della collettività, limita la propria autorità addirittura vi rinuncia.

Il messaggio si apriva con queste parole: «Per me è molto importante che le person possano comunicare in piena sicurezza». L'anonimo autore mi suggeriva di installare programma di cifratura PGP, così da potermi trasmettere alcune informazioni che di sicuro m avrebbero interessato. PGP, ovvero Pretty Good Privacy («riservatezza più che discreta»), è u programma nato nel 1991 per proteggere la posta elettronica e altre forme di comunicazion in rete dalla pirateria informatica e dagli strumenti di sorveglianza. Nelle sue varie versioni diventato sempre più sofisticato e oggi è il più diffuso al mondo. In sostanza blinda ciascu messaggio con un codice formato da centinaia, se non addirittura migliaia, di cifre e caratte minuscoli o maiuscoli che fungono da scudo protettivo.

Le agenzie di spionaggio tecnologicamente più avanzate al mondo – e la National Securit Agency (NSA) è indubbiamente una di queste – dispongono di software in grado di forzar l'accesso a contenuti protetti da password generando fino a un miliardo di ipotesi al second I codici PGP, però, sono così lunghi e di struttura talmente arbitraria che perfino i programm più sofisticati impiegano anni a decodificarli. Chi ha buone ragioni per temere che le su telecomunicazioni siano tenute sotto sorveglianza (come per esempio gli agenti segreti, spie, gli attivisti per i diritti umani e gli hacker) protegge i propri messaggi con software criptazione di questo genere.

Cincinnatus mi diceva di aver cercato, senza trovarla, la mia «chiave pubblica» PGP, u codice che consente agli utenti di scambiare messaggi di posta elettronica protetti c cifratura. Ne aveva dedotto che non mi servivo abitualmente di programmi crittografici, teneva a farmi sapere che «chiunque si metta in contatto con lei corre gravi rischi. Non le s dicendo di proteggere tutti i messaggi in arrivo o in uscita dalla sua casella di posta, ma s non altro dovrebbe offrire questa possibilità ai suoi interlocutori».

Cincinnatus portava l'esempio dello scandalo a sfondo sessuale che aveva travolto generale David Petraeus, la cui carriera militare era stata stroncata dalla scoperta della su relazione clandestina con la giornalista Paula Broadwell; la vicenda era emersa quando g

inquirenti erano risaliti ad alcuni messaggi di posta elettronica scambiati dai due amanti s
Gmail o conservati nella cartelletta «bozze». Se Petraeus avesse cifrato i suoi messagg
spiegava Cincinnatus, nessun ispettore avrebbe mai potuto intercettarli. «La cifratura
importante, non serve soltanto alle spie e ai mariti fedifraghi.» Criptare le mail, continuava
lettera, «è una misura di sicurezza indispensabile per chiunque desideri mettersi in contat
con lei».

Per invitarmi a seguire il suo consiglio aggiungeva: «Là fuori ci sono persone con cui
interesserebbe avere a che fare, ma che mai e poi mai si metteranno in contatto con lei finch
non avranno la certezza che i loro messaggi non vengano intercettati».

A quel punto Cincinnatus si offriva di aiutarmi a installare il software: «Se le serve un
mano me lo faccia sapere, oppure chieda aiuto su Twitter. Molti dei suoi follower son
persone preparatissime in campo informatico e le offriranno di sicuro assistenza tecnica». Pe
finire si congedava: «Grazie, C.».

Già in passato mi ero ripromesso di installare un programma per criptare le mail. Da an
scrivevo articoli su WikiLeaks, su informatori e gole profonde, sul collettivo di hacker not
come Anonymous e su altri argomenti piuttosto delicati; inoltre, di tanto in tanto, ero entra
in contatto con agenti della National Security Agency. La maggior parte di quelle person
tenevano moltissimo alla riservatezza delle loro comunicazioni e prendevano precauzioni pe
depistare eventuali osservatori indesiderati. Le applicazioni di quel genere, però, sono molt
difficili da utilizzare, soprattutto per chi, come il sottoscritto, non se la cavava troppo ben
con i computer. Insomma, era uno di quei buoni propositi per cui non si trova mai il tempo.

La lettera di Cincinnatus non mi smosse da quell'apatia. Dal momento che sono noto pe
volermi occupare di tutte quelle storie che il resto dei media passano sotto silenzio, mi capi
spesso di venire contattato da gente che mi promette uno «scoop colossale», ma il più del
volte quell'esclusiva si riduce a un pugno di mosche. Senza contare che di solito lavor
contemporaneamente a più articoli di quelli che riesco a gestire. Per convincermi a
accantonare i progetti in corso e lanciarmi su una nuova pista occorrono prove concrete, e
lettera di Cincinnatus non conteneva nulla di particolarmente stimolante, al di là di qualch
vaga allusione a «persone là fuori» con le quali sarei stato interessato ad «avere a che fare
Lessi la mail, ma non mi presi neppure la briga di rispondere.

Tre giorni dopo, Cincinnatus mi scrisse di nuovo chiedendomi di confermargli che avev
ricevuto e letto il precedente messaggio. Questa volta risposi, ma in modo sbrigativo: «Tutt
chiaro, cercherò di organizzarmi. Non ho una chiave PGP e non so come procurarmene un
ma vedrò di trovare qualcuno che possa darmi una mano».

Replicò nel giro di qualche ora mandandomi una guida molto dettagliata del programm
PGP: *La cifratura per negati*. Insieme alle istruzioni, che trovai comunque ostiche e poc
illuminanti a causa della mia totale ignoranza in materia, Cincinnatus precisava che quel
erano solo «i primissimi rudimenti». «Se non riesce a trovare qualcuno che possa aiutarla
installare il programma, generare una chiave e usarla» scriveva, «me lo faccia sapere: poss
metterla in contatto con persone che se ne intendono di queste cose in qualunque parte d
mondo, o quasi.»

Questa volta la formula di congedo era più eloquente: «Crittograficamente su
Cincinnatus».

Nonostante la mia buona volontà, non riuscii a trovare il tempo per occuparmi d

problema della crittografia. Lasciai passare ben sette settimane, pur sentendomi un po' colpa per non avere ancora provveduto. E se quella persona avesse davvero avuto per le ma uno scoop da propormi? Se mi fossi lasciato sfuggire una notizia importante soltanto perch non sapevo installare un programma? Inoltre, anche se quel Cincinnatus si fosse rivelato u falsa pista, un protocollo di cifratura mi sarebbe sempre tornato utile.

Il 28 gennaio 2013 scrissi a Cincinnatus, per fargli sapere che intendevo farmi aiutare qualcuno e che speravo di venirne a capo in un paio di giorni o poco più.

Rispose l'indomani: «Queste sì che sono ottime notizie! Se le serve altro aiuto, o se futuro si troverà in difficoltà, non esiti a contattarmi in qualunque momento. La prego accettare i miei più sinceri ringraziamenti per il suo impegno a favore di telecomunicazio più sicure! Cincinnatus».

Invece anche quella volta lasciai passare del tempo senza fare concretamente nulla, pres com'ero da altri servizi e non del tutto convinto che Cincinnatus avesse qualcosa per cui valesse la pena. Non fu una decisione consapevole: semplicemente, nella mia lista semp troppo lunga di cose da fare, installare un programma di cifratura su richiesta di un perfet sconosciuto non arrivò mai abbastanza in alto da indurmi a mettere da parte altre faccende dedicarmici.

Io e Cincinnatus dunque eravamo prigionieri di un circolo vizioso, una sorta di «comm 22»: lui non era disposto a sbottonarsi sul materiale in suo possesso e neppure a dirmi chi e e dove lavorava finché non mi fossi dotato di un sistema di cifratura; io, senza lo stimolo elementi concreti, non ritenevo una priorità assecondare le sue richieste e rimandavo giorno in giorno l'installazione di quel programma.

Di fronte al mio temporeggiamento, Cincinnatus rinnovò i suoi sforzi. Produsse un video dieci minuti intitolato *PGP per giornalisti*. Parlando attraverso un modulatore di voce, nel vide spiegava passo passo e con istruzioni semplici come installare un programma di crittografi con tanto di grafici ed esempi.

Non mossi un dito neppure quella volta. Fu allora che Cincinnatus, come più tardi avrebbe confidato, iniziò a perdere la pazienza. Forse si diceva: «Io sono qui, pronto a paga con la mia libertà, e forse addirittura con la vita, pur di passare a quel tizio migliaia documenti riservatissimi prelevati negli archivi dell'agenzia più segreta del Paese, u soffiata che promette decine se non centinaia di colossali scoop giornalistici, e quello non spreca neppure a installare un programmino per criptare la posta elettronica».

Per un pelo, insomma, non ho rischiato di perdere l'esclusiva su una delle maggiori fughe notizie nell'intera storia della National Security Agency, nonché una delle più gravide conseguenze.

Per una decina di settimane non ricevetti altre notizie. Il 18 aprile decollai da Rio de Janeir dove abito, e atterrai a New York per presenziare ad alcune conferenze sui rischi del segre istituzionale e sulla violazione delle libertà civili in nome della Guerra al terrorismo.

Quando atterrai all'aeroporto JFK trovai un messaggio da parte della documentarista Lau Poitras. Diceva: «Per caso sarai negli Stati Uniti la prossima settimana? Mi piacerebbe fare punto con te su una certa faccenda, ma sarebbe meglio vedersi di persona».

Prendo sempre molto sul serio i messaggi di Laura, perché è una delle persone p determinate, impavide e indipendenti che io conosca. Aveva girato moltissimi reportage nel

circostanze più rischiose, senza il supporto di una troupe e la tutela di giornali o re televisive, contando solo su un budget modesto, una videocamera e la sua forza di volontà. è avventurata nel Triangolo sunnita nei giorni più violenti della guerra in Iraq per girare *M Country, My Country*, un docufilm molto crudo sulle condizioni di vita degli iracheni sot l'occupazione statunitense, che è stato candidato agli Academy Award.

Per realizzare il suo successivo reportage, *The Oath*, Laura si è trasferita nello Yemen, dov ha seguito per mesi due cittadini del Paese: la guardia del corpo di Osama bin Laden e il su autista. Un paio di anni più tardi ha iniziato a lavorare a un documentario sulla sorveglianz della NSA. A causa di questi tre docufilm – una sorta di trilogia sulla gestione da parte deg Stati Uniti della Guerra al terrorismo – Laura è stata costretta a subire continue vessazioni d parte delle autorità governative ogni volta che entrava o usciva dagli Stati Uniti.

Quando ci siamo incontrati per la prima volta, nel 2010, era già stata fermata neg aeroporti in più di una trentina di occasioni dal Dipartimento della sicurezza interna mentre accingeva a rientrare negli Stati Uniti o a partire per l'estero. L'avevano interrogata minacciata; le avevano sequestrato il suo materiale di lavoro, inclusi il laptop, le macchin fotografiche e i computer portatili, eppure lei aveva deciso di non denunciare pubblicamente soprusi di cui era vittima perché temeva che le ripercussioni di quel gesto le avrebber impedito di lavorare. Laura però cambiò idea dopo un interrogatorio più duro del soli all'aeroporto di Newark. Ne aveva avuto abbastanza: «Stare zitta non migliora le cose, anz le peggiora». Era pronta per affidare la sua storia alla mia penna.

L'articolo che pubblicai sulla rivista online «Salon», con tutti i dettagli sui numero interrogatori ai quali Laura Poitras era stata sottoposta, ebbe un buon successo p visualizzazioni e commenti. Molti lettori si schierarono a favore di Laura manifestando la lor solidarietà per le persecuzioni che aveva subito. Quando lei partì nuovamente per l'estero d un aeroporto americano, nessuno la interrogò o sequestrò i suoi materiali. Per un paio di me la lasciarono in pace. Per la prima volta da anni Laura era libera di viaggiare.

La lezione che avevo imparato era chiara: i funzionari della National Security Agency no amano le luci della ribalta. Prevaricano e trattano la gente con prepotenza soltanto quand sanno di trovarsi al sicuro, protetti dal silenzio. È nella segretezza che s'annida l'abuso d potere, è da essa che trae la forza che lo rende possibile. L'unico antidoto che funziona, i questi casi, è la trasparenza.

Appena lessi il messaggio di Laura, ancora sulla pista dell'aeroporto JFK, risposi: «Ch coincidenza, sono appena atterrato negli Stati Uniti… Tu dove sei?». Fissammo u appuntamento per il giorno dopo al ristorante dell'hotel Marriott di Yonkers, dove mi er sistemato. Una volta seduti al tavolo, però, lei insistette per ben due volte per cambiare post e iniziammo a parlare soltanto quando fu sicura che nessuno potesse origliare. Venne subit al dunque. Voleva discutere con me di «un problema estremamente importante e delicato», la riservatezza era un requisito fondamentale.

Avevo con me il mio telefono cellulare. Laura mi pregò di estrarre la batteria o di portar in camera. «Ti sembrerò paranoica» disse, e mi spiegò che il governo disponeva del tecnologia necessaria per attivare a distanza telefoni cellulari e computer portatili p trasformarli in strumenti con cui spiare la gente. Spegnere il cellulare o il computer no bastava: bisognava togliere la batteria.

Avevo già sentito raccontare storie simili da attivisti per la trasparenza e hacker, ma er convinto che si trattasse di scrupoli eccessivi. Questa volta, però, presi sul ser l'avvertimento perché proveniva da Laura. Quando scoprii che la batteria del mio telefor era fissa portai il cellulare in camera e poi tornai al ristorante.

Prese quelle precauzioni, Laura iniziò a raccontarmi che aveva ricevuto alcune e-ma anonime da una persona che le era sembrata credibile. L'autore di quei messaggi sosteneva aver accesso a documenti segretissimi che accusavano il governo statunitense di spiare propri cittadini e il resto del mondo. L'anonimo corrispondente era deciso a rendere pubblic documenti e aveva espressamente chiesto a Laura di collaborare con me per farli circolare realizzare un reportage. Non mi venne neppure in mente che l'informatore potesse esse Cincinnatus, perché avevo archiviato quella storia in un angolo della mia mente.

Laura tirò fuori dal suo zaino alcuni fogli: erano pagine tratte da due e-mail dell'anonim corrispondente. Le lessi dalla prima all'ultima parola.

Era roba da mozzare il fiato.

La seconda delle e-mail, inviata ad alcune settimane dalla prima, cominciava con: «Anco qui». In risposta alla domanda che più mi interessava – «Quando sarebbe pronto per fornirc documenti?» – il mittente scriveva: «Tutto ciò che posso dire è: "Presto"».

Dopo averla esortata a togliere le batterie dai cellulari prima di trattare argomenti delica – o almeno a mettere i telefoni in freezer, dove la capacità d'intercettazione sarebbe sta intralciata – l'informatore esprimeva la volontà che Laura lavorasse con me su qu documenti. Giungeva poi al punto di quella che considerava la sua missione:

> Lo shock di questa prima fase [dopo le prime rivelazioni] produrrà il sostegno necessario a costruire un internet più equo, ma questa non andrà a vantaggio del cittadino medio a meno che la scienza non corra più veloce della legge. Comprendendo i meccanismi attraverso i quali è violata la nostra privacy qui possiamo vincere, possiamo garantire a tutte le persone un'eguale difesa da una vigilanza assurda in virtù di leggi universali, ma solo se la comunità tecnologica sarà disposta ad affrontare la minaccia e a impegnarsi per attuare soluzioni sovra-ingegnerizzate. Dobbiamo far valere un principio secondo il quale il potente potrà godere della propria privacy solo nel momento in cui sarà accessibile nello stesso modo all'uomo della strada: quello imposto dalle leggi di natura anziché da politiche di umana concezione.

«Questo non è un impostore» commentai quando ebbi finito di leggere. «Non saprei dir esattamente perché, ma il mio intuito mi dice che sta parlando sul serio, che è la persona ch sostiene di essere.»

«Lo credo anch'io» confermò Laura. «Non ho praticamente più dubbi.»

Da persone ragionevoli e razionali, Laura e io sapevamo che la nostra fiducia nel credibilità di quell'informatore poteva rivelarsi malriposta. Non avevamo la più pallida ide di chi si nascondesse dietro quelle e-mail. Poteva trattarsi di chiunque. Nulla escludeva ch l'anonimo si fosse inventato tutto, dalla prima all'ultima parola. Poteva perfino trattarsi una macchinazione del governo, che ci tentava per poi coglierci con le mani nel sacc complici di una fuga illegale di notizie. Forse all'origine di tutto c'era un avversario, ch tramava per ledere la nostra credibilità di giornalisti trasmettendoci documenti falsi chiedendoci di pubblicarli.

Valutammo insieme tutte le possibilità. Sapevamo che nel 2008 un rapporto segre

dell'esercito americano aveva dichiarato WikiLeaks nemico di Stato, proponendo strumen per «colpire e possibilmente distruggere» l'organizzazione ostile. Quel testo (reso pubblic ironia della sorte, proprio da WikiLeaks) contemplava la possibilità di mettere in circolazion documenti falsi. Se WikiLeaks li avesse pubblicati spacciandoli per autentici, l'attendibili del portale avrebbe accusato un duro colpo.

Io e Laura ci rendevamo conto di tutti i possibili trabocchetti, ma quella ci sembrav un'eventualità remota e inoltre ci fidavamo del nostro istinto. Da quei messaggi trapelava un forza tale da persuaderci entrambi della sincerità dell'autore: sembrava credere con tutto s stesso alla minaccia rappresentata da istituzioni poco trasparenti e dallo spionagg indiscriminato verso chiunque; riconoscevo in lui la passione politica che lo animava. Sent che qualcosa mi legava al nostro anonimo corrispondente, alla sua visione del mondo, senso d'impazienza che si avvertiva leggendo le sue righe, e che lo stava divorando.

Negli ultimi sette anni, spinto dalle stesse convinzioni, avevo scritto quasi ogni giorno sul derive più inquietanti del segreto istituzionale, sulle teorie del potere esecutivo radicale, sug abusi delle pratiche di sorveglianza e di detenzione, sul militarismo e sulla violazione del libertà civili. C'è un'intonazione, un atteggiamento morale di fondo che accomuna giornalisti, gli attivisti e i lettori che condividono la stessa preoccupazione per simi fenomeni. Imitare quel tono in modo così preciso e con un simile effetto di autenticità, n dicevo, sarebbe stato molto difficile per chi non avesse creduto sinceramente a quei pericoli non ne avvertisse l'urgenza.

In uno dei passaggi conclusivi dell'ultima lettera ricevuta da Laura, il corrispondente senz nome scriveva di essere quasi pronto a fornirci la documentazione promessa: restavano c sbrigare alcune formalità. Ci sarebbero volute altre quattro-sei settimane, al termine del quali avrebbe provveduto lui stesso a ricontattarci. Ci chiedeva soltanto di essere pazienti prometteva che non ci avrebbe deluso.

Tre giorni dopo rividi Laura, questa volta a Manhattan. L'anonimo informatore si era fatt vivo con una nuova e-mail, nella quale spiegava perché era disposto a mettere a repentagl la sua libertà pur di rendere pubblici quei documenti, esponendosi al rischio concreto di un pena detentiva. Ora ero del tutto certo: la nostra fonte faceva sul serio. Come spiegai al m compagno David Miranda sull'aereo che ci riportava in Brasile, però, non volevo pensa troppo a quella storia. «La cosa potrebbe non andare in porto. L'informatore potrebb cambiare idea. Oppure potrebbero arrestarlo.» David è una persona dotata di grande intuit e in quell'occasione si dimostrò particolarmente sicuro del suo giudizio: «Non è un montatura. Il tipo fa sul serio. Vedrai che si farà vivo con i documenti e sarà lo scoop d secolo».

Rientrato a Rio, per tre settimane non ricevetti altre notizie. Non trascorsi molto temp pensando alla nostra fonte perché l'unica cosa che potessi fare era aspettare. Poi, l'11 maggi mi scrisse un esperto di informatica con il quale Laura e io avevamo già collaborato passato. Le sue parole erano piuttosto sibilline, ma il messaggio era chiaro: «Ciao Glenn, ricontatto per la storia del PGP che volevi imparare a usare. Mi dai il tuo indirizzo di casa Così la settimana prossima posso spedirti qualcosa che ti aiuterà a muovere i primi passi».

Di sicuro voleva mandarmi qualcosa di cui avrei avuto bisogno per iniziare a lavorare s documenti del nostro informatore. Questo significava che Laura aveva avuto notizie dal su

corrispondente anonimo e aveva ricevuto ciò che stavamo aspettando.

Il tecnico informatico mi spedì un pacco via FedEx e mi fece sapere che lo avrei ricevu nel giro di due giorni. Non sapevo che cosa aspettarmi: un programma da installare o documenti stessi? Per le successive quarantotto ore non riuscii a concentrarmi su nient'altr Alle 17:30 del giorno in cui sarebbe dovuto arrivare il materiale, però, non era ancora passa alcun fattorino. Contattai gli uffici della FedEx e venni a sapere che il pacco era stat trattenuto alla dogana per «ragioni non meglio precisate».

Trascorsero due giorni. Poi altri cinque. Quindi un'intera settimana. Ogni volta quelli del FedEx mi rispondevano la stessa cosa: il pacco era fermo in dogana per ragioni non megl precisate.

Mi ritrovai a temere che le autorità governative (americane, brasiliane o altre) fosser responsabili del ritardo perché sospettavano qualcosa, ma non volevo rinunciare al spiegazione molto più plausibile che si trattasse di una mera coincidenza, uno di quei disgu burocratici che possono capitare a tutti.

Nel frattempo, però, Laura aveva deciso di non parlare di quella storia né per telefono n via internet, per cui io non sapevo esattamente quale fosse il contenuto del pacco.

Infine, dopo circa dieci giorni dalla spedizione, un fattorino FedEx mi consegnò il pacc Lacerai la busta e trovai al suo interno due chiavette USB e una nota dattiloscritta co informazioni dettagliate sull'utilizzo di programmi volti a garantire la massima sicurezza del comunicazioni, oltre a varie *passphrase* per l'accesso a caselle di posta elettronica criptate e a altri programmi che non avevo mai sentito nominare.

Non conoscevo gli specifici programmi di cifratura. Però sapevo che cos'è una *passphrase*: tratta di una password molto lunga generata automaticamente e composta da maiuscol minuscole e segni di interpunzione, combinati in modo tale da renderne molto difficile l forzatura. Ora che Laura Poitras non voleva parlare per telefono o tramite internet, n sentivo frustrato quanto prima: avevo finalmente per le mani il materiale tanto atteso, m non avevo la più pallida idea di dove mi avrebbe portato.

Lo avrei scoperto molto presto, e grazie alla migliore delle guide.

Il giorno dopo aver ricevuto il pacco, durante la settimana del 20 maggio, Laura mi fec sapere che aveva urgente bisogno di parlarmi, ma era disposta a farlo soltanto su una ch OTR (*off the record*, cioè «a microfono spento»: un protocollo crittografico che serve comunicare su internet in modo sicuro). In precedenza avevo già utilizzato OTR e, servendom di Google, riuscii a installare correttamente l'applicazione necessaria, quindi m'iscrissi servizio e aggiunsi il nome di Laura alla mia «lista degli amici». Lei mi contat immediatamente.

Le domandai come avrei potuto accedere ai documenti segreti. Mi spiegò che li avr ricevuti soltanto dalla fonte, non da lei. Laura aggiunse qualche ulteriore informazione: fors saremmo dovuti partire immediatamente per Hong Kong per incontrare la nostra fonte.

Rimasi di sasso. Che cosa ci faceva a Hong Kong una persona che poteva accedere documenti segretissimi del governo statunitense? Che cosa c'entrava adesso Hong Kong? Er sempre stato convinto che la nostra fonte anonima risiedesse nel Maryland o nel Nord del Virginia. Che cosa aveva a che fare con questa storia un tizio che viveva, fra tutti i Pae possibili, proprio a Hong Kong? Ero pronto a partire per qualunque destinazion naturalmente, ma prima volevo saperne di più sulle ragioni di quel viaggio. Dal momento ch

Laura non poteva parlare liberamente, fu necessario rimandare le spiegazioni. Mi chiese s
fossi disposto a recarmi a Hong Kong nei giorni successivi. Io volevo esser certo che n
valesse la pena. In altre parole: aveva verificato che la fonte fosse autentica? Rispos
soltanto: «Certo! Altrimenti non ti trascinerei fin là!». Diedi per scontato che avesse ottenu
qualche documento probante dalla fonte stessa.

Laura però mi informò anche che era insorto un problema. L'informatore era indispetti
da come stavano andando le cose, soprattutto da una novità: il possibile coinvolgimento d
«Washington Post». Mi disse che era fondamentale che io gli parlassi direttamente p
rassicurarlo.

Nel giro di un'ora la fonte scrisse al mio indirizzo di posta elettronica. La e-mail proveniv
dall'indirizzo verax@[redacted].net. In latino *verax* significa «colui che dice la verità
L'oggetto era: «Dobbiamo parlare».

«Ultimamente ho lavorato a un grande progetto con un amico comune» esordiva il tes
della e-mail. Era un modo per farmi sapere che era proprio lui, la fonte anonima, quello
contatto con Laura.

«Di recente si è rifiutato di partire per l'estero con un preavviso minimo per incontrarm
ma è indispensabile che anche lei collabori su questo dossier» scriveva. «Sarebbe possibi
parlarne entro breve? Mi sembra di capire che non sia molto attrezzato in materia di re
sicure, ma cercherò di farmi bastare gli strumenti di cui dispone.» Propose di comunica
tramite un protocollo OTR e mi fornì il suo user name.

Non ero sicuro di sapere cosa intendesse lui per «partire con un preavviso minimo» e,
effetti, mi ero chiesto perché si trovasse proprio a Hong Kong, ma di sicuro non mi ero tirat
indietro. Attribuii queste incomprensioni a una cattiva comunicazione e gli risposi subit
«Sono deciso a fare quanto possibile per partecipare a questo progetto» lo rassicura
proponendogli di sentirci immediatamente via OTR. Aggiunsi il suo nome alla lista degli ami
sulla chat e attesi.

Una quindicina di minuti più tardi il mio computer emise un rintocco come di campana: e
il segnale che l'altro si era collegato. Un po' nervoso, cliccai sul suo nome e digitai: «Ciao
Lui rispose, e così mi ritrovai a comunicare senza intermediari con una persona che, a qu
punto, ero certo essere in possesso di un numero imprecisato di documenti segreti relativi
programmi di sorveglianza degli Stati Uniti e decisa a renderne pubblica almeno una parte.

Come prima cosa, gli feci sapere che il mio impegno era incondizionato. «Sono deciso a fa
tutto il necessario pur di scrivere su questa vicenda.» La fonte – della quale ignoravo ancora
nome, la professione, l'età e altre caratteristiche – mi chiese se fossi disposto a raggiungerlo
Hong Kong. Mi trattenni dal domandargli che cosa ci facesse là, volevo evitare di sembra
un giornalista importuno a caccia di informazioni.

Inoltre, stabilii fin dall'inizio di lasciare che fosse lui a prendere l'iniziativa. Se aves
voluto spiegarmi perché si trovava a Hong Kong, lo avrebbe fatto. Se desiderava farmi sape
quali documenti possedeva e progettava di farmi visionare, me ne avrebbe parlato lui. M
sentivo a disagio in quel ruolo passivo. Sono abituato a interrogare le persone anche in mod
piuttosto veemente quando voglio delle risposte – non per nulla sono un ex avvocato passa
al giornalismo d'inchiesta – e le domande che avrei voluto porgli erano centinaia. Al temp
stesso ero perfettamente consapevole che lui si trovava in una posizione molto delicata.
prescindere da altre considerazioni, sapevo che aveva deciso di commettere quello che

governo degli Stati Uniti avrebbe considerato un crimine gravissimo. Inoltre la su competenza in campo di comunicazioni sicure dava fondatezza a tutte quelle precauzioni. D momento che sapevo poco o nulla sul conto del mio interlocutore, sul suo modo di pensar sulle motivazioni che lo spingevano ad agire e sulle sue paure, era indispensabile da parte m procedere con cautela e discrezione. Non dovevo spaventarlo. Mi sforzai di lasciare che informazioni venissero a me, piuttosto che allungare la mano per afferrarle.

«Certo che verrò a Hong Kong» dissi, pur sapendone quanto prima sulle ragioni del trasferta e sul perché voleva che lo raggiungessi laggiù.

Quel giorno chattammo per due ore. A preoccuparlo era più che altro sapere cosa sarebb successo ai documenti della NSA di cui Laura Poitras, con il suo consenso, aveva parlato Barton Gellman, reporter del «Washington Post». Il materiale era relativo a un programm denominato PRISM che consentiva alla NSA di attingere alle comunicazioni private direttamen dai server delle principali società mondiali di servizi telematici, tra cui Facebook, Googl Yahoo! e Skype.

Invece di scriverne immediatamente e in modo incisivo, il «Washington Post» aveva riuni una nutrita squadra di avvocati che ora stavano sollevando un'infinità di cavilli. La fon interpretava quel comportamento come un segnale del fatto che il «Post», dopo essersi vis servire su un piatto d'argento uno scoop giornalistico senza precedenti, almeno secondo il su giudizio, si era lasciato intimorire agendo senza determinazione. Era anche furioso per il fat che il «Post» avesse coinvolto tante persone e temeva che ciò potesse ledere alla sua sicurez personale.

«Non mi piace la piega che la cosa sta prendendo» mi confidò. «Volevo che qualcun altro occupasse di PRISM così che lei potesse dedicarsi al resto dell'archivio e alla sorveglianza massa, ma ora tengo davvero a che sia lei in persona a rendere noto quel materiale. Leggo suoi articoli da molto tempo» spiegò, «e so che lei ne scriverà in modo grintoso e senz lasciarsi spaventare.»

«Mi sento pronto e sono impaziente di mettermi al lavoro» gli assicurai. «Stabiliamo fin c subito come muoverci.»

«La primissima cosa da fare è venire a Hong Kong» ribadì. Insistette più volte su qu punto: «Venga immediatamente a Hong Kong».

Il fatto che Gellman si fosse rifiutato di prendere un aereo per incontrarlo, adducend quelli che la fonte giudicava improbabili pretesti giuridici confezionati ad arte dai legali d «Washington Post» per dimostrare che si trattava di una mossa sconsiderata e rischiosa, indispettiva tremendamente. Gli garantii che io non mi sarei tirato indietro per così poco.

L'altro grande argomento che affrontammo in quella prima conversazione online erano suoi obbiettivi. Avendo letto le e-mail mostratemi da Laura, capivo che sentiva il bisogno far sapere al mondo come il governo statunitense stesse costruendo in gran segreto u ciclopico apparato di sorveglianza. Lui, però, cosa sperava di ottenere?

«Voglio innescare un dibattito a livello mondiale su problemi come la privacy, la libertà rete e i pericoli della sorveglianza di Stato» disse. «Non ho paura di quello che pot accadermi. Mi sono rassegnato all'idea che dopo aver fatto ciò che intendo fare mol probabilmente la mia vita non sarà mai più la stessa. Me ne sono fatto una ragione. So che la cosa giusta.» A quel punto aggiunse un dettaglio sconvolgente: «Ho intenzione di far sape a tutti che il responsabile della fuga di notizie sono io. Credo di aver l'obbligo morale

spiegare perché lo sto facendo e che cosa spero di ottenere». Mi disse di aver già redatto u documento che prevedeva di pubblicare in rete dopo essersi autodenunciato come fonte: trattava di un manifesto a favore della privacy e contro la sorveglianza, che i cittadini di tut il mondo avrebbero potuto firmare per dimostrare l'esistenza di un movimento globale favore della riservatezza. Il prezzo da pagare per quell'autodenuncia era evidente (nel cas migliore una lunga pena detentiva), ma la fonte ripeté più volte di essersi «fatto una ragione delle conseguenze.

«Il mio unico timore» aggiunse, «è che la gente possa leggere quei documenti e scrollare spalle, pensando: "Sapevamo già che stava succedendo qualcosa del genere e non ce importa più di tanto". L'unica cosa che mi preoccupa è l'idea di fare tutto questo per nulla.»

«Dubito fortemente che possa andare così» lo rassicurai, ma in cuor mio non ne ero d tutto certo. Scrivo da anni sugli abusi di potere della NSA e so per esperienza diretta che difficile far prendere alla gente seriamente coscienza del fatto che la sorveglianza segreta Stato è un problema anche loro: violazione della privacy e abuso di potere sono spes percepiti come un'astrazione, difficili da prendere visceralmente a cuore. Del resto il tema sempre ricchissimo di risvolti complessi e ciò rende ancor più arduo coinvolgere ampie fas di opinione pubblica.

Sentivo però che stavolta il caso era diverso. Quando c'è una fuga di notizie top secret media non possono fare finta di niente. Il fatto che la messa in guardia provenisse da u esponente dello stesso apparato di sicurezza nazionale, piuttosto che da un legale dell'ACL (American Civil Liberties Union) o da un militante per le libertà civili, inoltre, conferiva al vicenda un peso indubbiamente maggiore.

Quella sera parlai con David dell'opportunità di partire subito per Hong Kong. Esitav ancora di fronte alla prospettiva di accantonare tutti i lavori in corso per volare dall'alt parte del globo al solo scopo di incontrare una persona di cui non sapevo nulla, neppure nome. Per giunta non avevo nemmeno una prova concreta del fatto che lui fosse davvero c diceva di essere. Poteva rivelarsi una grossa perdita di tempo oppure una trappola o u qualche subdola macchinazione.

«Rispondigli che prima vuoi vedere qualche documento, per capire se fa sul serio e se p te ne vale la pena» propose David.

Come sempre in questi casi, seguii il suo consiglio. La mattina seguente, quando mi colleg alla chat OTR, feci sapere al mio interlocutore che sarei partito per Hong Kong entro qualch giorno, ma che prima volevo vedere dei documenti per capire che genere di rivelazioni avev intenzione di fare.

Se volevo i documenti, mi rispose, dovevo prima installare i programmi di crittografi Trascorsi un paio di giorni in chat, mentre la fonte mi guidava passo passo nell'installazione nell'utilizzo dei software, tra cui finalmente anche PGP Encryption. Fu molto paziente, perch sapeva che ero un neofita. Arrivò perfino a darmi istruzioni del tipo: «Fai *clic* sul pulsan azzurro; adesso premi OK e passa alla schermata successiva».

Io mi scusavo di continuo per la mia scarsa dimestichezza con gli strumenti informatici: stavo costringendo a impiegare ore del suo tempo a insegnarmi l'abc della comunicazion sicura. «Non si preoccupi» mi disse, «sono programmi poco intuitivi. E in questo momento h molto tempo libero.»

Quando le applicazioni si furono configurate, ricevetti un file compresso che contenev