

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, riceve un'email firmata "Cincinnatus": il suo interlocutore vuole "che le persone possano comunicare in piena sicurezza" e gli propone di dotarsi di un efficace sistema di cifratura, senza il quale "chiunque si metta in contatto con lui corre gravi rischi". Solo così "Cincinnatus" potrà fornirgli alcune informazioni di sicuro interesse.

Qualche mese più tardi quelle "informazioni" inonderanno per settimane telegiornali, quotidiani, siti internet e sconvolgeranno la politica americana, chiameranno in causa Google, Facebook, Yahoo, Microsoft, Apple e scuoteranno le relazioni tra gli Stati Uniti e i loro principali alleati. "Cincinnatus", infatti, è Edward Snowden, un giovane informatico che ha lavorato per la CIA e la NSA, l'onnipotente Agenzia per la Sicurezza Nazionale, ed è disposto a rinunciare alla ragazza che ama, agli amici e a un ottimo stipendio, rischiando l'ergastolo e forse la vita, pur di rivelare al mondo il più gigantesco programma di sorveglianza di massa mai concepito e realizzato: la NSA ha obbligato le società telefoniche a fornire i tabulati di tutte le comunicazioni tra cittadini americani e con l'estero, ha acquisito dati dai server dei giganti dell'informatica e di internet, ha spiato leader politici o funzionari europei o aziende concorrenti di società americane, può accedere ai testi di miliardi di email, può entrare in cellulari e computer in tutto il mondo... Greenwald racconta i primi contatti con Snowden, l'incontro in una stanza d'albergo di Hong Kong, la serie di scoop con cui, a partire dal 5 giugno 2013, il "Guardian" pubblica le segretissime carte della NSA, la fuga a Mosca, e soprattutto le implicazioni della mole di documenti portati alla luce, che dimostrano una verità ineludibile: "il governo statunitense ha creato un sistema finalizzato alla totale eliminazione della riservatezza telematica in tutto il pianeta". Sembra un romanzo di spionaggio, e lo è. Solo che ciò di cui si parla è successo davvero, e riguarda tutti noi.

GLENN GREENWALD (New York 1967), firma di punta del “Guardian” fino a ottobre 2013, ha da poco fondato la testata online [The Intercept](#). Tra i suoi bestseller, *A Tragic Legacy* (2007) sulla presidenza di George W. Bush, e *With Liberty and Justice for Some* (2011).

La rivista “Foreign Policy” l’ha inserito nella lista dei 100 pensatori più influenti del 2013. Grazie alle sue rivelazioni sul programma di sorveglianza della National Security Agency, il “Guardian” ha vinto il premio Pulitzer 2014.

Glenn Greenwald

Sotto controllo

Edward Snowden e la sorveglianza di massa

Rizzoli

Proprietà letteraria riservata

© Glenn Greenwald 2014

Published by arrangement with Metropolitan Books, an imprint of Henry Holt and Company, LLC., New York, and Marco

Vigevani & Associati Agenzia Letteraria.

All rights reserved.

© 2014 RCS Libri S.p.A., Milano

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 / *theWorldofDOT*

www.rizzoli.eu

Quest'opera è protetta dalla Legge sul diritto d'autore.

È vietata ogni duplicazione, anche parziale, non autorizzata.

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

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 avvicinato all'indomani dell'11 settembre. Speravo che affrontare certi temi su internet mi avrebbe consentito di raggiungere più persone rispetto alla mia professione di allora, quella di avvocato specializzato in diritti costituzionali e civili.

Un mese e mezzo dopo il «New York Times» uscì con una rivelazione sconvolgente: nel 2001, riferiva il quotidiano, l'amministrazione Bush aveva segretamente ingiunto alla National Security Agency (NSA) di intercettare le telecomunicazioni elettroniche dei cittadini americani, esentandola dalla necessità di procurarsi i mandati previsti in questi casi dal diritto penale statunitense. Quando la notizia era trapelata le intercettazioni senza mandato erano in 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 preparazione giuridica. Il governo stava cercando di legittimare un programma clandestino della NSA 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 prerogative istituzionali pressoché incondizionate e la possibilità di fare qualunque cosa – persino violare la legge – pur di «tutelare la sicurezza del Paese». Il dibattito scaturito da quelle rivelazioni portò in luce problemi complessi di diritto costituzionale e giurisprudenza, che la mia formazione di legale mi aveva preparato ad affrontare nel merito.

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

Sarebbe stato quel precedente a indurre Edward Snowden a scegliere me come primo interlocutore quando, alcuni anni più tardi, si trattò di portare in luce nuovi abusi perpetrati dalla NSA su una scala ancora più stupefacente. Snowden si diceva convinto di poter contare 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 indietro 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 la drammatica vicenda umana che lo vede come protagonista hanno risvegliato in tutto il mondo un interesse di tipo nuovo per la minaccia della sorveglianza elettronica di massa, mostrando che valore prezioso sia la riservatezza nell'era digitale. I problemi che quello scandalo

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

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

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

Il Quarto emendamento alla Costituzione statunitense ha tradotto quel principio in legge. La formulazione è limpida e concisa: «Nessuno potrà ledere il diritto dei cittadini americani di non vedere sottoposte a perquisizioni e sequestri arbitrari le loro persone, le loro abitazioni, le loro carte e i loro effetti personali, e non verranno emessi mandati in quel senso se non in presenza di fondati sospetti, ratificati da un giuramento o da una deposizione ufficiale 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 di sottoporre i suoi cittadini a una sorveglianza generalizzata e sommaria, sganciata da motivazioni specifiche.

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

A prescindere dalle specifiche tecnologie di volta in volta utilizzate, la questione della sorveglianza di massa presenta alcuni attributi costanti nel tempo. Tanto per cominciare, sono di norma i dissidenti e gli emarginati a fare le spese di quelle pratiche, e questo induce i simpatizzanti del governo e i qualunquisti a credere – sbagliando – di essere al sicuro. La storia, inoltre, insegna che la pura e semplice esistenza di un apparato di sorveglianza di 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 società malleabile e pavida.

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

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

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

Possedere i mezzi per intercettare le telecomunicazioni della gente conferisce un potere immenso ai depositari di quel privilegio. Se quel potere non è tenuto a freno da rigorose procedure di supervisione e da una forte responsabilità istituzionale, chi ne dispone finisce quasi certamente per abusarne. Credere che il governo statunitense potesse far funzionare una colossale e segretissima macchina di controllo senza cedere a simili tentazioni significa 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 parlare della sorveglianza esercitata dagli Stati Uniti come di un'eccezione o un caso a parte era

peccare di ingenuità. Nel 2006, durante un dibattito al Congresso intitolato *Internet in Cina: Strumento di libertà o di repressione?*, gli oratori si erano alternati per condannare le aziende tecnologiche americane, accusate di aiutare la Cina a mettere a tacere le voci di dissenso nelle reti. Il deputato repubblicano del New Jersey Christopher Smith, presidente della seduta, paragonò la cooperazione di Yahoo con il governo cinese all'operato della polizia segreta che aveva consegnato Anna Frank ai nazisti. Fu un'arringa in piena regola, come sempre accade 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 aprì a neppure due mesi dall'articolo con il quale il «New York Times» aveva smascherato un grande programma di intercettazioni senza mandato promosso dall'amministrazione Bush. Alla luce di quanto emerso, puntare il dito contro altri Paesi per accusarli di seguire in campo proprio le stesse procedure rischiava di non suonare molto convincente. Il deputato democratico californiano Brad Sherman, che prese la parola dopo Smith, osservò come le società di servizi telematici invitate a resistere al regime cinese avrebbero dovuto fare attenzione anche al proprio governo. «Altrimenti» ammonì con parole rivelatesi profetiche «mentre la riservatezza dei cinesi viene violata nel modo più odioso, anche noi, qui negli Stati Uniti, potremmo scoprire un brutto giorno che un presidente sta leggendo la nostra posta elettronica accampando improbabili interpretazioni della Costituzione, e io preferirei che questo non accadesse senza un mandato.»

Nel corso degli ultimi decenni i leader statunitensi hanno cavalcato la paura del terrorismo continuamente rintuzzata da notizie ansiogene che ingigantiscono la reale entità della minaccia, per giustificare un ampio ventaglio di politiche estremiste. Quella paura è servita a 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 di imputazione. Uno dei suoi effetti più duraturi, però, potrebbe essere proprio il sistema onnipotente e segreto per la sorveglianza di cittadini innocenti che quella paura ha contribuito a instaurare; perché nonostante i molti paralleli storici, l'attuale scandalo della NSA presenta alcuni aspetti del tutto inediti, legati al ruolo che internet ha assunto nella nostra vita quotidiana.

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

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

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

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 un senso di paura costante. Trasformare il web in un sistema di sorveglianza, in altri termini equivale a stroncare il suo potenziale più prezioso. Peggio ancora, vuol dire trasformare le reti in un dispositivo di repressione che prefigura lo strumento di intrusione di Stato più estremo e opprimente che la storia del genere umano abbia mai conosciuto.

Per questo le rivelazioni di Snowden sono così sconvolgenti, dirompenti e importanti. Trovando il coraggio di denunciare le sbalorditive tecnologie di vigilanza messe a punto dalla NSA e le sue sconcertanti ambizioni per il futuro, Snowden ci ha mostrato che la storia si trova oggi di fronte a un bivio. Vogliamo che l'era digitale sia l'alba dell'emancipazione individuale e delle libertà politiche, resa possibile dalle inedite potenzialità di internet, oppure siamo disposti ad accettare un sistema di monitoraggio e controllo onnipervasivo che neppure i più sadici tiranni del passato avrebbero osato sognare? Oggi come oggi, entrambe le alternative 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 non sapevo che l'autore del messaggio fosse lui.

Si era fatto vivo mandandomi una e-mail firmata «Cincinnatus», uno pseudonimo che 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 perché dopo aver sconfitto gli avversari dell'Urbe, rinunciò a ogni carica istituzionale per tornare al 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 e addirittura vi rinuncia.

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

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

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

Cincinnatus portava l'esempio dello scandalo a sfondo sessuale che aveva travolto il generale David Petraeus, la cui carriera militare era stata stroncata dalla scoperta della sua 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 su Gmail o conservati nella cartelletta «bozze». Se Petraeus avesse cifrato i suoi messaggi spiegava Cincinnatus, nessun ispettore avrebbe mai potuto intercettarli. «La cifratura importante, non serve soltanto alle spie e ai mariti fedifraghi.» Criptare le mail, continuava la lettera, «è una misura di sicurezza indispensabile per chiunque desideri mettersi in contatto 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 finché 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 una mano me lo faccia sapere, oppure chiedi aiuto su Twitter. Molti dei suoi follower sono persone preparatissime in campo informatico e le offriranno di sicuro assistenza tecnica». Poi finì congedando: «Grazie, C.».

Già in passato mi ero ripromesso di installare un programma per criptare le mail. Da anni scrivevo articoli su WikiLeaks, su informatori e gole profonde, sul collettivo di hacker noto come Anonymous e su altri argomenti piuttosto delicati; inoltre, di tanto in tanto, ero entrato in contatto con agenti della National Security Agency. La maggior parte di quelle persone tenevano moltissimo alla riservatezza delle loro comunicazioni e prendevano precauzioni per depistare eventuali osservatori indesiderati. Le applicazioni di quel genere, però, sono molto difficili da utilizzare, soprattutto per chi, come il sottoscritto, non se la cavava troppo bene 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 per voler occuparmi di tutte quelle storie che il resto dei media passano sotto silenzio, mi capita spesso di venire contattato da gente che mi promette uno «scoop colossale», ma il più delle volte quell'esclusiva si riduce a un pugno di mosche. Senza contare che di solito lavoro 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 la lettera di Cincinnatus non conteneva nulla di particolarmente stimolante, al di là di qualche 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 confermarle che avevo ricevuto e letto il precedente messaggio. Questa volta risposi, ma in modo sbrigativo: «Tutto chiaro, cercherò di organizzarmi. Non ho una chiave PGP e non so come procurarmene una, ma vedrò di trovare qualcuno che possa darmi una mano».

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

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 mani uno scoop da propormi? Se mi fossi lasciato sfuggire una notizia importante soltanto perché non sapevo installare un programma? Inoltre, anche se quel Cincinnatus si fosse rivelato una 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 da 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 in futuro si troverà in difficoltà, non esiti a contattarmi in qualunque momento. La prego di accettare i miei più sinceri ringraziamenti per il suo impegno a favore di telecomunicazioni più sicure! Cincinnatus».

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

Io e Cincinnatus dunque eravamo prigionieri di un circolo vizioso, una sorta di «cammie 22»: lui non era disposto a sbottonarsi sul materiale in suo possesso e neppure a dirmi chi era e dove lavorava finché non mi fossi dotato di un sistema di cifratura; io, senza lo stimolo di 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 di dieci minuti intitolato *PGP per giornalisti*. Parlando attraverso un modulatore di voce, nel video spiegava passo passo e con istruzioni semplici come installare un programma di crittografia con tanto di grafici ed esempi.

Non mossi un dito neppure quella volta. Fu allora che Cincinnatus, come più tardi mi avrebbe confidato, iniziò a perdere la pazienza. Forse si diceva: «Io sono qui, pronto a pagare con la mia libertà, e forse addirittura con la vita, pur di passare a quel tizio migliaia di documenti riservatissimi prelevati negli archivi dell'agenzia più segreta del Paese, un soffio 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 di 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 Janeiro dove abito, e atterrai a New York per presenziare ad alcune conferenze sui rischi del segreto 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 Laura Poitras. Diceva: «Per caso sarai negli Stati Uniti la prossima settimana? Mi piacerebbe fare un 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 più 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 reti 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 *My Country, My Country*, un docufilm molto crudo sulle condizioni di vita degli iracheni sotto l'occupazione statunitense, che è stato candidato agli Academy Award.

Per realizzare il suo successivo reportage, *The Oath*, Laura si è trasferita nello Yemen, dove ha seguito per mesi due cittadini del Paese: la guardia del corpo di Osama bin Laden e il suo autista. Un paio di anni più tardi ha iniziato a lavorare a un documentario sulla sorveglianza della NSA. A causa di questi tre docufilm – una sorta di trilogia sulla gestione da parte degli Stati Uniti della Guerra al terrorismo – Laura è stata costretta a subire continue vessazioni da 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 negli 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 e minacciata; le avevano sequestrato il suo materiale di lavoro, inclusi il laptop, le macchine fotografiche e i computer portatili, eppure lei aveva deciso di non denunciare pubblicamente i soprusi di cui era vittima perché temeva che le ripercussioni di quel gesto le avrebbero impedito di lavorare. Laura però cambiò idea dopo un interrogatorio più duro del solito all'aeroporto di Newark. Ne aveva avuto abbastanza: «Stare zitta non migliora le cose, anzi 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 numerosi interrogatori ai quali Laura Poitras era stata sottoposta, ebbe un buon successo per visualizzazioni e commenti. Molti lettori si schierarono a favore di Laura manifestando la loro solidarietà per le persecuzioni che aveva subito. Quando lei partì nuovamente per l'estero da un aeroporto americano, nessuno la interrogò o sequestrò i suoi materiali. Per un paio di mesi 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 non amano le luci della ribalta. Prevaricano e trattano la gente con prepotenza soltanto quando sanno di trovarsi al sicuro, protetti dal silenzio. È nella segretezza che s'annida l'abuso di potere, è da essa che trae la forza che lo rende possibile. L'unico antidoto che funziona, in questi casi, è la trasparenza.

Appena lessi il messaggio di Laura, ancora sulla pista dell'aeroporto JFK, risposi: «Che coincidenza, sono appena atterrato negli Stati Uniti... Tu dove sei?». Fissammo un appuntamento per il giorno dopo al ristorante dell'hotel Marriott di Yonkers, dove mi era sistemato. Una volta seduti al tavolo, però, lei insistette per ben due volte per cambiare posto e iniziammo a parlare soltanto quando fu sicura che nessuno potesse origliare. Venne subito 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 portarlo in camera. «Ti sembrerò paranoica» disse, e mi spiegò che il governo disponeva della tecnologia necessaria per attivare a distanza telefoni cellulari e computer portatili per trasformarli in strumenti con cui spiare la gente. Spegnerne il cellulare o il computer non bastava: bisognava togliere la batteria.

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

Prese quelle precauzioni, Laura iniziò a raccontarmi che aveva ricevuto alcune e-mail anonime da una persona che le era sembrata credibile. L'autore di quei messaggi sosteneva di aver accesso a documenti segretissimi che accusavano il governo statunitense di spiare i propri cittadini e il resto del mondo. L'anonimo corrispondente era deciso a rendere pubblici i documenti e aveva espressamente chiesto a Laura di collaborare con me per farli circolare e realizzare un reportage. Non mi venne neppure in mente che l'informatore potesse essere 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'anonimo 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: «Ancora qui». In risposta alla domanda che più mi interessava – «Quando sarebbe pronto per fornirci i documenti?» – il mittente scriveva: «Tutto ciò che posso dire è: "Presto"».

Dopo averla esortata a togliere le batterie dai cellulari prima di trattare argomenti delicati – o almeno a mettere i telefoni in freezer, dove la capacità d'intercettazione sarebbe stata intralciata – l'informatore esprimeva la volontà che Laura lavorasse con me su quei 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 dirti esattamente perché, ma il mio intuito mi dice che sta parlando sul serio, che è la persona che 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 nella credibilità di quell'informatore poteva rivelarsi malriposta. Non avevamo la più pallida idea di chi si nascondesse dietro quelle e-mail. Poteva trattarsi di chiunque. Nulla escludeva che l'anonimo si fosse inventato tutto, dalla prima all'ultima parola. Poteva perfino trattarsi di una macchinazione del governo, che ci tentava per poi coglierci con le mani nel sacco come complici di una fuga illegale di notizie. Forse all'origine di tutto c'era un avversario, che 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 segreto

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

Io e Laura ci rendevamo conto di tutti i possibili trabocchetti, ma quella ci sembrava un'eventualità remota e inoltre ci fidavamo del nostro istinto. Da quei messaggi trapelava una forza tale da persuaderci entrambi della sincerità dell'autore: sembrava credere con tutto il cuore, allo stesso modo della minaccia rappresentata da istituzioni poco trasparenti e dallo spionaggio indiscriminato verso chiunque; riconoscevo in lui la passione politica che lo animava. Sentivo che qualcosa mi legava al nostro anonimo corrispondente, alla sua visione del mondo, al suo 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 sulle derive più inquietanti del segreto istituzionale, sulle teorie del potere esecutivo radicale, sugli abusi delle pratiche di sorveglianza e di detenzione, sul militarismo e sulla violazione della libertà civili. C'è un'intonazione, un atteggiamento morale di fondo che accomuna i giornalisti, gli attivisti e i lettori che condividono la stessa preoccupazione per simili fenomeni. Imitare quel tono in modo così preciso e con un simile effetto di autenticità, non dicevo, sarebbe stato molto difficile per chi non avesse creduto sinceramente a quei pericoli e non ne avvertisse l'urgenza.

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

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

Rientrato a Rio, per tre settimane non ricevetti altre notizie. Non trascorsi molto tempo pensando alla nostra fonte perché l'unica cosa che potessi fare era aspettare. Poi, l'11 maggio, mi scrisse un esperto di informatica con il quale Laura e io avevamo già collaborato nel passato. Le sue parole erano piuttosto sibilline, ma il messaggio era chiaro: «Ciao Glenn, ho 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 sui documenti del nostro informatore. Questo significava che Laura aveva avuto notizie dal suo

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 ricevuto 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'altro. Alle 17:30 del giorno in cui sarebbe dovuto arrivare il materiale, però, non era ancora passato alcun fattorino. Contattai gli uffici della FedEx e venni a sapere che il pacco era stato trattenuto alla dogana per «ragioni non meglio precisate».

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

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

Nel frattempo, però, Laura aveva deciso di non parlare di quella storia né per telefono né 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 pacco. Lacerai la busta e trovai al suo interno due chiavette USB e una nota dattiloscritta con informazioni dettagliate sull'utilizzo di programmi volti a garantire la massima sicurezza delle comunicazioni, oltre a varie *passphrase* per l'accesso a caselle di posta elettronica criptate e ad 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 maiuscole, minuscole e segni di interpunzione, combinati in modo tale da renderne molto difficile la forzatura. Ora che Laura Poitras non voleva parlare per telefono o tramite internet, mi sentivo frustrato quanto prima: avevo finalmente per le mani il materiale tanto atteso, ma 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 fece sapere che aveva urgente bisogno di parlarmi, ma era disposta a farlo soltanto su una chat OTR (*off the record*, cioè «a microfono spento»: un protocollo crittografico che serve a comunicare su internet in modo sicuro). In precedenza avevo già utilizzato OTR e, servendomi di Google, riuscii a installare correttamente l'applicazione necessaria, quindi m'iscrissi al servizio e aggiunsi il nome di Laura alla mia «lista degli amici». Lei mi contattò immediatamente.

Le domandai come avrei potuto accedere ai documenti segreti. Mi spiegò che li avrei ricevuti soltanto dalla fonte, non da lei. Laura aggiunse qualche ulteriore informazione: forse 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 ai documenti segretissimi del governo statunitense? Che cosa c'entrava adesso Hong Kong? Ero sempre stato convinto che la nostra fonte anonima risiedesse nel Maryland o nel Nord della Virginia. Che cosa aveva a che fare con questa storia un tizio che viveva, fra tutti i Paesi possibili, proprio a Hong Kong? Ero pronto a partire per qualunque destinazione naturalmente, ma prima volevo saperne di più sulle ragioni di quel viaggio. Dal momento che

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

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

Nel giro di un'ora la fonte scrisse al mio indirizzo di posta elettronica. La e-mail proveniva 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 testo della e-mail. Era un modo per farmi sapere che era proprio lui, la fonte anonima, quello che aveva avuto il contatto con Laura.

«Di recente si è rifiutato di partire per l'estero con un preavviso minimo per incontrarmi, ma è indispensabile che anche lei collabori su questo dossier» scriveva. «Sarebbe possibile parlarne entro breve? Mi sembra di capire che non sia molto attrezzato in materia di relazioni sicure, ma cercherò di farmi bastare gli strumenti di cui dispone.» Propose di comunicare 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, per gli effetti, mi ero chiesto perché si trovasse proprio a Hong Kong, ma di sicuro non mi ero tirato indietro. Attribuii queste incomprensioni a una cattiva comunicazione e gli risposi subito: «Sono deciso a fare quanto possibile per partecipare a questo progetto» lo rassicurai proponendogli di sentirci immediatamente via OTR. Aggiunsi il suo nome alla lista degli amici sulla chat e attesi.

Una quindicina di minuti più tardi il mio computer emise un rintocco come di campana: era 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 quel punto, ero certo essere in possesso di un numero imprecisato di documenti segreti relativi a 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 fare tutto il necessario pur di scrivere su questa vicenda.» La fonte – della quale ignoravo ancora il nome, la professione, l'età e altre caratteristiche – mi chiese se fossi disposto a raggiungerlo a Hong Kong. Mi trattenni dal domandargli che cosa ci facesse là, volevo evitare di sembrare un giornalista importuno a caccia di informazioni.

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

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

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

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

Invece di scriverne immediatamente e in modo incisivo, il «Washington Post» aveva riunito una nutrita squadra di avvocati che ora stavano sollevando un'infinità di cavilli. La fonte interpretava quel comportamento come un segnale del fatto che il «Post», dopo essersi visto servire su un piatto d'argento uno scoop giornalistico senza precedenti, almeno secondo il suo giudizio, si era lasciato intimorire agendo senza determinazione. Era anche furioso per il fatto che il «Post» avesse coinvolto tante persone e temeva che ciò potesse ledere alla sua sicurezza 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 di massa, ma ora tengo davvero a che sia lei in persona a rendere noto quel materiale. Leggo i suoi articoli da molto tempo» spiegò, «e so che lei ne scriverà in modo grintoso e senza lasciarsi spaventare.»

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

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

Il fatto che Gellman si fosse rifiutato di prendere un aereo per incontrarlo, adducendo quelli che la fonte giudicava improbabili pretesti giuridici confezionati ad arte dai legali del «Washington Post» per dimostrare che si trattava di una mossa sconsiderata e rischiosa, mi indispettava 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 i suoi obiettivi. Avendo letto le e-mail mostratemi da Laura, capivo che sentiva il bisogno di far sapere al mondo come il governo statunitense stesse costruendo in gran segreto un gigantesco apparato di sorveglianza. Lui, però, cosa sperava di ottenere?

«Voglio innescare un dibattito a livello mondiale su problemi come la privacy, la libertà di rete e i pericoli della sorveglianza di Stato» disse. «Non ho paura di quello che potrebbe accadermi. Mi sono rassegnato all'idea che dopo aver fatto ciò che intendo fare molto probabilmente la mia vita non sarà mai più la stessa. Me ne sono fatto una ragione. So che è la cosa giusta.» A quel punto aggiunse un dettaglio sconvolgente: «Ho intenzione di far sapere 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 un 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 tutto il mondo avrebbero potuto firmare per dimostrare l'esistenza di un movimento globale a favore della riservatezza. Il prezzo da pagare per quell'autodenuncia era evidente (nel caso peggiore 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 le spalle, pensando: "Sapevamo già che stava succedendo qualcosa del genere e non ce ne 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 del tutto certo. Scrivo da anni sugli abusi di potere della NSA e so per esperienza diretta che è difficile far prendere alla gente seriamente coscienza del fatto che la sorveglianza segreta dello Stato è un problema anche loro: violazione della privacy e abuso di potere sono spesso percepiti come un'astrazione, difficili da prendere visceralmente a cuore. Del resto il tema è sempre ricchissimo di risvolti complessi e ciò rende ancor più arduo coinvolgere ampie fasce di opinione pubblica.

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

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

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

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

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

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

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

- [click *Les rebelles : Une anthologie*](#)
- [read *The Second Tree: Of Clones, Chimeras and Quests for Immortality*](#)
- [download *Coalition of Lions \(Arthurian Sequence Series, Book 2\)*](#)
- [read online *Poems Collection of Su Shi \(Chinese classical literature series\)* \(ä, -
å, ½, å, •, ¢, å, ..., æ, †, å, å, ¨, æ, œ, -ä, ›, ä, !, è, •, è, ½, ¼, è, -—, é, †\)](#)
- <http://aseasonedman.com/ebooks/Les-rebelles---Une-anthologie.pdf>
- <http://monkeybubblemedia.com/lib/The-Foundation-of-the-Unconscious--Schelling--Freud-and-the-Birth-of-the-Modern-Psyche.pdf>
- <http://www.experienceolvera.co.uk/library/Coalition-of-Lions--Arthurian-Sequence-Series--Book-2-.pdf>
- <http://wind-in-herleshausen.de/?freebooks/Poems-Collection-of-Su-Shi--Chinese-classical-literature-series---ae-----ae--ae----->