Epilogo

Anonymous oggi

> *Sono arrivato ad apprezzare la segretezza. Mi sembra l'unica cosa capace di rendere misteriosa o meravigliosa la vita moderna. La cosa più mondana diventa deliziosa quando gli altri la ignorano.*
> –Oscar Wilde

> *I tecnici apolitici hanno un'educazione politica straordinaria.*
> –Julian Assange

Quanto descritto fin qui potrebbe sembrare a molti il periodo di maggior splendore per le attività di Anonymous: il ruolo di sostegno ai vari movimenti coinvolti nella Primavera Araba; l'attenzione mediatica di alto profilo conquistata dagli spavaldi hack di LulzSec e AntiSec; il crescente impegno a sostegno della giustizia sociale negli Stati Uniti, oltre alla concreta opposizione alla cultura dello stupro e alla brutalità della polizia.

Ovviamente questa nutrita ondata di proteste è andata scontrandosi con la repressione, parimenti copiosa, delle forze dell'ordine. Complessivamente, tra Europa, Asia, Australia e Americhe, sono stati arrestati oltre un centinaio di attivisti legati ad Anonymous – compresi alcuni già menzionati nelle pagine precedenti, tra cui Jeremy Hammond e John Borell negli Stati Uniti, Ryan Ackroyd e Mustafa Al-Bassam nel Regno Unito. Altri geek vennero arrestati semplicemente per aver prestato una piccola porzione dei loro computer alle campagne DDoS organizzate dal collettivo nel tentativo di colpire collettivamente gli istituti finanziari come PayPal, quando cedettero alle pressioni del governo Usa bloccando tutti i loro servizi a WikiLeaks, già sotto assedio su vari fronti.

Rispetto a ogni altra nazione del mondo occidentale, gli Stati Uniti sono stati i più aggressivi nel perseguire penalmente gli hacktivisti di Anonymous, con condanne ben più lunghe accompagnate da multe astronomiche. Non solo gli attivisti, tra cui Jeremy Hammond, ma anche i collaboratori esterni, come Barrett Brown, hanno ricevuto pene severe a seguito del caso Stratfor (maggiori dettagli più avanti). Quando usciranno dal carcere, costoro continueranno a pagare per quanto hanno fatto per via degli enormi debiti imposti dalla stessa sentenza.

Questa serie di condanne, unite al fatto che per mesi l'Fbi ha convinto Sabu, figura centrale del gruppo, a riferire loro quanto accadeva internamente, hanno portato alla diffusione di sfiducia, sospetti e timori tra gli stessi Anon. Temendo la presenza di infiltrati a ogni angolo, gli hacker si sono fatti sempre più paranoici, diminuendo la partecipazione e innalzando la sicurezza delle operazioni. Fatto importante, hanno anche attenuato i toni da smargiassi.

Pur se meno frequenti e con minor clamore, dal 2013 non sono certo mancate le intrusioni online, come i DDoS degli Anon italiani e l'Operazione diritti verdi, che ha visto il defacing di decine di siti web di aziende nemiche dell'ambiente, in particolare la Monsanto (operazioni che, per motivi a me incomprensibili, non hanno mai attirato particolare attenzione o stimolato inchieste a livello mediatico). Tuttavia a partire dal 2014 è divenuto chiaro che le attività più visibili di Anonymous in Nord America e in

Europa puntavano alla visibilità pubblica anziché all'azione diretta, con l'evidente obiettivo di far crescere la consapevolezza pubblica su casi specifici. Nel Regno Unito, l'Operation Death Eaters mirava a mettere in luce la questione dello sfruttamento sessuale infantile e l'insabbiamento delle attività pedofile di alcune potenti figure pubbliche. Negli Stati Uniti, la OpFerguson è nata per sostenere e pubblicizzare le diffuse proteste popolari seguite all'uccisione del diciottenne afro-americano Michael Brown da parte di un poliziotto in Missouri nell'agosto 2014. L'OpISIS, per molti versi allineata con gli interessi delle potenze occidentali, puntava invece a identificare account Twitter e siti web legati all'Isis, in modo da poter essere oscurati dalle autorità.

La spettacolarità operativa che aveva consentito ad Anonymous di ottenere visibilità sui media tradizionali continuò a garantirgli i titoli dei giornali – ma in gran parte come riflesso degli hack condotti da altri team indipendenti. Per lo più questi ultimi avevano ben poco in comune con l'azione politica diretta o con altri interventi degli Anon a sostegno della giustizia sociale. Molte di queste intrusioni erano anzi di segno decisamente opposto. Nel 2014, il sito web della Sony Pictures Entertainment subì l'attacco dei misteriosi Guardiani della pace, che si appropriarono di un'ampia mole di dati aziendali, presumibilmente come rappresaglia per il previsto lancio di un film che proponeva la satira del governo nord-coreano. Gli hacker diffusero pubblicamente quel materiale, che includeva un po' di tutto, dalle copie di film in uscita a comunicati ed email interne. Nel periodo natalizio dello stesso anno, la Sony venne nuovamente presa di mira, quando la Lizard Squad (aggregazione che in parte ricordava LulzSec ma privo di finalità politiche) suscitò un certo clamore su Twitter riuscendo a disabilitare temporaneamente il PlayStation Network con un massiccio attacco DDoS arrivato nel giorno di Natale. Nel 2015, alcuni hacker pro-ISIS, noti come il CyberCaliphate, si appropriarono di un account Twitter delle autorità Usa a gennaio e il mese successivo di un account della rivista *Newsweek,* per poi assumere il pieno controllo di una rete tv francese ad aprile.

Ma l'apparenza può trarre in inganno. Più che diminuito, l'attivismo online di Anonymous era divenuto semplicemente meno visibile. Fu soprattutto in Asia e in America latina, dove gli hacker del collettivo operavano già da qualche tempo, che aumentarono le intrusioni nei sistemi informatici di obiettivi specifici. Uno dei team più prolifici, LulzSec Peru, diede vita a decine di operazioni, inclusa l'appropriazione dell'account Twitter del presidente venezuelano, Nicolas Maduro, e la sottrazione di documenti dell'aviazione cilena. L'hack più esaltante fu quello dell'11 febbraio 2014, quando divulgarono pubblicamente le email che provavano l'estesa corruzione del governo peruviano. Non appena queste vennero rilanciate da Frank Bajak dell'Associated Press, ci fu una sorta di «sollevazione popolare a livello nazionale» e vennero confermate «le accuse secondo cui i ministri più importanti erano al servizio delle lobby industriali anziché della cittadinanza. Ciò contribuì al voto di sfiducia in parlamento ... a cui il governo sopravvisse per puro miracolo[1]».

Pur se quest'ultimo exploit riuscì a risvegliare l'attenzione dei giornalisti anglofoni, la maggior parte dei media occidentali rimase indifferente di fronte alle attività internazionali di Anonymous. Ciò anche per via delle tipiche lacune evidenziate dai giornalisti interessati a seguire certe vicende "estere", mentre le barriere linguistiche e la difficoltà di entrare in contatto con gli hacker, sempre più reticenti dopo le recenti ondate di arresti, resero difficile replicare l'ampia copertura mediatica avutasi nel periodo di

LulzSec.

Più che il segnale del rallentamento dell'attività di Anonymous, questa parziale mancanza di attenzione mediatica ne rivela l'accresciuta capacità di sopravvivenza. Pur se è vero che le iniziative di AntiSec e LulzSec acquistarono forza proprio grazie alla visibilità pubblica, alla fin fine quest'ultima ne mise anche a nudo le maggiori debolezze. In altri termini, è arduo valutare adeguatamente i pro e i contro di una determinata situazione. Conquistando l'attenzione generale, LulzSec e AntiSec diedero impeto alle cause per cui si battevano, incoraggiando inoltre tanti altri ad aderirvi. Trovandosi però a operare sotto l'occhio attento dei media, del pubblico e, soprattutto, delle autorità, questi gruppi stabili divennero sempre più suscettibili agli interventi repressivi. Con ogni hack e ogni scherno ai danni di entità pubbliche montava la pressione generale per identificare e imbavagliare questi attivisti anonimi.

Ma, un po' come per ogni movimento politico emergente animato da stili e strategie innovative, i flirt di Anonymous con la fama e simili tattiche audaci non potevano che essere sperimentali. Non c'è da meravigliarsi se i risultati rivelavano un'alternanza tra spettacolari successi e fallimenti ugualmente impressionanti. E con le inevitabili sviste sono arrivati pure i danni collaterali – anche se gli attivisti sanno imparare rapidamente dagli errori propri come da quelli altrui.

Sembra comunque che almeno qualcuno abbia continuato a prestare attenzione. Prendiamo, per esempio, l'attacco condotto nel 2014 contro il Gamma Group, produttore britannico di spyware specializzato nella vendita di «tecniche di sorveglianze avanzate e soluzioni per il monitoraggio»[2] alle autorità di vari Stati, compresi regimi dittatoriali e repressivi noti per aver usato tali strumenti contro oppositori e attivisti interni. Nel 2011 l'opinione pubblica venne a sapere dell'esistenza di quell'azienda quando WikiLeaks ne divulgò uno dei video promozionali, insieme alle presentazioni che spiegavano come utilizzarne il software per infettare i computer altrui[3]. Poco dopo due esperti di sicurezza suggerirono che probabilmente le autorità del Bahrein avevano applicato quei metodi, installando nei computer degli attivisti locali un programma chiamato FinFisher, a loro insaputa e tramite un file allegato alle email. (Per tutta risposta, i dirigenti del Gamma Group dichiararono che non avevano mai venduto quel programma al Bahrein e qualcuno poteva averne rubata e diffusa una loro copia[4]).

Il 3 agosto 2014, un hacker ignoto a tutti e auto-indentificatosi come Phineas Fisher (nella mitologia greca, Finea è il nome di un indovino) annunciò su vari social media di apprestarsi a divulgare quaranta gigabyte di dati relativi a FinFisher, dopo essere penetrato nel sistema informatico del Gamma Group. L'ampia documentazione così diffusa includeva materiale tecnico (prototipi software, codici sorgenti, documentazione, analisi sull'utilizzo), oltre a elenchi dei clienti, listino prezzi, dimostrativi e altro. Fra le varie rivelazioni, l'hack di Phineas Fisher rafforzò il sospetto che le autorità del Bahrein avessero usato quel programma contro gli attivisti locali[5].

In una dichiarazione a supporto dell'operazione, Phineas Fisher esortava i colleghi hacker a darsi da fare, proponendo un'apposita "guida fai-da te per chi non ha la pazienza di aspettare i whistleblower", in cui spiccava questo consiglio:

> Fintanto che si segue il buon senso di non attaccare nessun sito al di fuori di Whonix[6], non fare mai nulla di strano all'interno di Whonix, non menzionare mai dettagli sulla propria vita privata parlando con altri hacker, e non vantarsi di aver compiuto

> intrusioni illegali con gli amici nella vita reale, allora puoi fare tranquillamente tutto quello che vuoi senza temere di essere v& [*vanned*: termine per indicare qualcuno che viene perquisito o arrestato][7].

Pur senza nominare esplicitamente alcuna affiliazione con Anonymous, l'hack di Phineas Fisher ne incarnava lo spirito e senza dubbio s'ispirava allo stile inaugurato da LulzSec e da altri team all'interno del collettivo. (Phineas Fisher rivelò inoltre un'ottima conoscenza del lulz, scrivendo nella sua guida: «è stato soltanto dopo aver fallito il colpo pieno contro il Gamma, ritrovandomi tra le mani un'interessante documentazione ma nessuna copia del software FinSpy, che ho dovuto accontentarmi di un livello minore di lulz, limitandomi a divulgare quella roba e a prenderli in giro su twitter»[8]). Nel contesto della recente impennata dei "leak", particolarmente da parte di coraggiosi cittadini quali Chelsea Manning ed Edward Snowden, la modalità operativa scelta da Anonymous si distingueva per una caratteristica fondamentale: anziché divulgare materiale affidato loro da fonti esterne, penetravano nelle reti informatiche di governi e corporation onde ricavarne informazioni relative alle aziende operanti nel campo della sicurezza e dell'intelligence.

Anche se con metodi e obiettivi analoghi a quelli di LulzSec e AntiSec, l'operazione di Phineas Fisher rivelava molta più cautela, precisione e attenzione di quanto non avesse mai fatto Anonymous. E anziché usare quel momento di gloria per farsi auto-promozione, divulgò i dati su Twitter e reddit, s'impegnò ad attirare l'attenzione su quel materiale per cinque giorni e poi sparì nel nulla.

O meglio, fino al 5 luglio 2015, quando rivendicò un hack simile, stavolta ai danni di un altro fornitore di cyber-armi, perfino più odioso, l'azienda milanese Hacking Team. Questo produttore di software di sicurezza vende quelle che definisce "soluzioni offensive" a una clientela alquanto vasta, dall'Fbi all'esercito americano[9]. Stavolta Phineas Fisher riuscì a impadronirsi del loro account Twitter, modificandone il nome in Hacked Team e diffondendo il seguente messaggio: «dato che non abbiamo nulla da nascondere, a questo link […] troverete tutte le email, i file e i codici sorgenti aziendali»[10]. Fino al momento dell'intrusione, questi mercenari tecnologi avevano fatto tutto il possibile per nascondere la particolare natura dei servizi offerti, come anche degli affari e dei clienti interni – un quadro destinato a cambiare grazie alla divulgazione di qualcosa come 400 gigabyte di materiale vario. Come nel caso del GammaGroup, l'Hacking Team ribadì pubblicamente di non aver mai venduto alcunché ai regimi repressivi. Oggi sappiamo che così non era: secondo i dati interni poi resi pubblici, l'azienda aveva fatto affari con governi senza scrupoli ed era coinvolta in pratiche discutibili, tra cui lo stoccaggio e l'incetta di vulnerabilità relative a svariati programmi (comprese due presenti nel player Flash di Adobe, assai diffuso online) da poter usare eventualmente contro milioni di utenti internet[11].

Per confermare di essere davvero Phineas Fisher (suggerendo altresì l'arrivo di ulteriori operazioni), l'hacker fece partire il seguente messaggio dall'account attivato in precedenza a parodia del Gamma Group ("GammaGroupPR"): «gamma e HT fuori uso, ancora qualcun altro da colpire :)»[12]. Vi aggiunge nuovamente il link al suo manuale/manifesto fai-da-te – le cui massime, va notato, sono tutt'altro che nuove e girano da tempo nei circoli hacker, compresa l'élite di Anonymous.

Vista comunque la difficoltà di implementare certe misure di sicurezza e gli arresti

che hanno colpito gli hacker del collettivo (pur se parecchi di loro, va aggiunto, non sono mai stati individuati e restano quindi in libertà), torna sicuramente utile ribadirne più volte i principi fondamentali. E come Phineas Fisher ha richiamato i colleghi hacker a pratiche di sicurezza straordinarie, oggi anche Anonymous, memore del Sabutage del 2012, avvisa i nuovi arrivati ad applicare continuamente serie misure di sicurezza. Come si leggeva in un tweet di Anon2earth: «Se sei nuovo qui, allora rilassati e dà prima un'occhiata in giro. Non partecipare a nessuna op se non sai esattamente cosa cavolo stai facendo. Tutelati[13]». Nei vari gruppi di Anonymous, consigli e ammonimenti sulla sicurezza adesso compaiono regolarmente in ogni conversazione quotidiana.

Lungi dall'essere semplici slogan, queste lezioni vengono continuamente rilanciate non solo da hacker come Phineas Fisher, ma anche nei vari livelli di Anonymous. È per esempio il caso della OpCyberPrivacy, una campagna d'opposizione alle norme sulla sorveglianza proposte in vari Paesi occidentali, come il disegno di legge in discussione al parlamento canadese (Bill C-51) fin dall'inizio del 2015, e criticato da accademici, avvocati, giornalisti e decine di gruppi della società civile per i poteri illimitati che assegna alle forze dell'ordine e alle agenzie di spionaggio.

Inizialmente gli Anon provarono ad affondare la proposta soltanto rendendone pubblici gli aspetti controversi, ma non riuscendo a conquistare la necessaria attenzione mediatica, tornarono alla loro strategia più classica: gli attacchi DDoS. Il 17 giugno 2015, Anonymous rese inaccessibili decine di siti web del governo canadese, compresi quello dei servizi segreti e dei Ministeri di giustizia, industria, commercio e sviluppo, risorse naturali, affari esteri. Ancor più importante, riuscirono a bloccare le comunicazioni elettroniche colpendo intenzionalmente il server della posta. La campagna ottenne così ampi rilanci sui media, e secondo il quotidiano nazionale *The Globe and Mail*, «si trattò del cyber-attacco di maggior profilo avutosi nel Paese dopo quello dell'anno scorso in cui degli hacker al servizio delle autorità cinesi penetrarono nel sistema dell'agenzia della ricerca scientifica del premier»[14]. Uno degli organizzatori della campagna mi spiegò poi che «erano circa sei mesi … che il maggior gruppo di lavoro era impegnato» su svariate operazioni: «dalla caccia ai poliziotti di Ferguson alla rivoluzione ucraina, dalle stronzate del Ku Klux Klan ai pedofili e alla privacy». Per vari Anon si trattava delle prime esperienze sul campo, mentre il nucleo centrale era composto per lo più da veterani. In netto contrasto con Operation PayBack contro PayPal del dicembre 2010, che portò all'arresto di numerosi partecipanti, egli mi ribadì che la sicurezza era divenuta una priorità assoluta, al punto tale che uno degli obiettivi dichiarati imponeva di evitare qualsiasi danno collaterale – per intendere qualsiasi cosa che potesse essere usata dalla polizia per far scattare un loro intervento. Nel concludere la chat, l'Anon sottolineò orgogliosamente che «finora non c'è stato alcun problema di sicurezza, fatto assai positivo». In una successiva occasione, aggiunse che in passato avevamo già parlato in chat ma all'epoca usava un diverso nickname, informandomi che d'ora in poi gli pseudonimi sarebbero stati trattati come i cellulari usa e getta: periodicamente ogni attivista avrebbe cambiato nick, così da sembrare un nuovo arrivato e impossibile da collegare a qualche operazione precedente.

Senza l'ondata di arresti del 2011 e 2012 non si sarebbe mai arrivati a simili precauzioni, e comunque la loro efficacia va ancora verificata. Sembra che parecchi Anon preferiscano comunque rischiare e capire qual è veramente la posta in gioco, e buona parte di queste valutazioni dipenderanno dal trattamento e dall'esito legale di quanti sono

già in galera.

Riguardo al caso dei PayPal14, la maggior parte degli accusati ha evitato il carcere per un pelo. Undici di loro si sono dichiarati colpevoli di un reato serio e uno minore, e il primo è stato poi derubricato in base al patteggiamento. Gli altri due indiziati sono stati condannati a tre e quattro mesi di servizi sociali, evitando così la condanna per reati gravi. Ciascuno di loro dovrà comunque sborsare 5.600 dollari come risarcimento danni a favore di eBay (all'epoca azienda madre di PayPal), e quelli che non possono permettersi un pagamento unico saranno soggetti a rate mensili di 100 dollari. L'ultimo del gruppo, Dennis Owen Collins, era tra i più attivi di AnonOps (in questo libro compare come "Fred" e "Owen"). Condannato a un anno di arresti domiciliari, è deceduto il 16 luglio 2015, all'età di 54 anni, a causa di un'estenuante e cronica malattia polmonare da cui era affetto.

Fra tutti i casi giudiziari contro gli attivisti statunitensi di Anonymous ne rimane aperto ancora uno, quello contro Barrett Brown. Il 22 gennaio 2015, in un affollatissimo tribunale di Dallas, il giornalista e attivista si è visto appioppare una pesante condanna dal giudice Samuel Lindsay. Brown, che al momento della sentenza aveva già trascorso due anni dietro le sbarre, è stato condannato a ulteriori 35 mesi di carcere e al pagamento di quasi un milione di dollari per i danni subiti dalla Stratfor, l'azienda di intelligence con base ad Austin, in Texas, vittima dell'attacco di Anonymous. Gli iniziali 17 capi d'imputazione, con pena massima di otto anni, erano stati poi ridotti a tre grazie al patteggiamento: minacce contro gli agenti dell'Fbi, intralcio al mandato di perquisizione, assistenza agli hacker di Anonymous che avevano compromesso il sistema informatico della Stratfor.

L'aspetto più incredibile, e più opinabile, dell'intera faccenda fu l'affermazione del giudice secondo cui Brown «non si era limitato semplicemente a informare sulle attività degli hacker», ma più precisamente aveva contribuito a organizzarle: «la corte stabilisce che Brown ha collaborato e appoggiato gli hacker, fornendo consigli, strategie e assistenza nella pianificazione delle loro attività»[15]. Eppure rimane il fatto che Brown non era un hacker né è stato incriminato per reati connessi a intrusioni non autorizzate. All'interno di Anonymous svolgeva il ruolo di un arguto stratega, e non esistono prove solide sul fatto che abbia coordinato l'attacco contro la Stratfor del dicembre 2011, e ancor meno che vi abbia perso parte. Il suo interesse si concentrava soprattutto sulle email, pur avendo condiviso il link all'elenco delle carte di credito rubate dagli hacker di Anonymous, reato per cui a un certo punto venne indiziato. Tra i 17 capi d'imputazione di cui doveva rispondere inizialmente, era anzi questo il più controverso: Brown non aveva né rubato né usato i dati delle carte di credito, limitandosi piuttosto a condividere un link già ampiamente noto da una chat room a un'altra. Pur se quest'accusa venne poi derubricata nel marzo 2014, il giudice abbracciò comunque la tesi della pubblica accusa secondo cui, ripubblicando quel link, Brown aveva dato una mano agli hacker, e quindi ciò ebbe particolare rilevanza per la sentenza finale. Secondo il giudice, quell'atto era «ben più che la semplice condivisione di un link, ma rivela il suo coinvolgimento con gli altri già parte della stessa attività». Così, pur non dovendo più formalmente rispondere di quell'accusa, è proprio in base a quest'ultima che Brown ha ricevuto comunque una condanna assai severa[16].

Questi contorsionismi e ambiguità legali finiscono chiaramente per limitare la libertà d'espressione – creando una situazione dove altri giornalisti saranno meno inclini a

condividere un link, temendo che questo gesto possa essere interpretato dai giudici come un reato aggravante (all'indomani della sentenza, Quinn Norton annunciò che non avrebbe più seguito temi legati a intrusioni, cyber-sicurezza o sulle attività degli hacker, temendo di subire analoghi trattamenti da parte delle autorità Usa). Al pari di tanti altri hacker, whistleblower, reporter e hacktivisti che avevano rischiato tutto pur di affermare la libertà d'informazione, Brown ne sta pagando un prezzo salato; la sua sentenza dimostra la precisa volontà delle autorità di incriminare non soltanto gli hacker motivati politicamente bensì anche quei geek e giornalisti che si muovono al loro fianco.

Il pesante trattamento penale riservato ad attivisti e sostenitori statunitensi come Hammond, Brown e altri è al centro di un caso ancora in sospeso alla stesura di questo epilogo (e della sua traduzione italiana). Sul capo dell'hacker britannico Lauri Love, arrestato 15 luglio 2015, pende tuttora la richiesta di estradizione negli Stati Uniti: in base al Computer Fraud and Abuse Act, è stato indiziato in New Jersey per essere penetrato illegalmente nei sistemi della Nasa, dell'esercito e della Federal Reserve come parte della OpLastResort di Anonymous, catalizzata dal suicidio dell'attivista Aaron Swartz[17]. C'è parecchio fermento per impedire questa estradizione, viste le pene ben più pesanti previste dalla normativa statunitense, oltre al fantasma della tragica decisione dello stesso Swartz. Secondo gli attivisti, «l'estradizione di Lauri Love negli Stati Uniti sarebbe un'evidente violazione dei suoi diritti umani e civili»[18].

Da tempo le istituzioni si affidano alla longa manus del sistema giuridico e agli interventi repressive per creare un clima di paura capace di tenere sotto controllo i movimenti politici, o quantomeno di contenerne la crescita. È perciò interessante notare come questi interventi delle forze dell'ordine non solo abbiano avuto scarsi effetti contro geek e hacker, ma li hanno anzi galvanizzati a entrare in azione. In particolare, per costoro le rivelazioni di Snowden vengono considerate una chiamata alle armi di portata storica e urgente – rilanciando con rinnovato impeto e vigore l'attivismo pro-privacy per la messa a punto di nuovi strumenti di crittazione.

Pur dopo le ondate di arresti, molti ex-membri di Anonymous, LulzSec e AntiSec hanno continuato ad alimentare senza posa questo movimento a tutela della privacy. Nell'estate 2015, Donncha O'Cearbhaill è stato scelto da Tor, il maggior progetto in corso per garantire comunicazioni online anonimi e crittate, per uno stage estivo sotto la guida degli sviluppatori più esperti. In un'intervista con l'organizzazione, gli fu chiesto: «Quali sono i tuoi eroi, se ne hai, nel campo del software per la libertà online?». Nella sua replica, O'Cearbhaill ha voluto rendere onore a coloro con cui aveva collaborato direttamente nonché alla comunità degli hacker in generale: «Trovo ispirazione nel lavoro di tanta gente impegnata a difendere la libertà online. Sono particolarmente grato a persone quali Edward Snowden, Julian Assange e Jeremy Hammond, che hanno fatto sacrifici enormi per mettere in luce la diffusa sorveglianza imposta dalle autorità statali. Mi ispiro anche agli sviluppatori del software libero e agli attivisti impegnati ovunque su questi temi»[19]. Mustafa Al-Bassam, un altro stagista presso l'organizzazione inglese Privacy International, ha invece deciso di offrire contributi diversificati. Quando i documenti interni della Hacking Team vennero resi pubblici, decise di ospitarli sul suo sito web, onde che garantire che fosse sempre possibile scaricarli. Per giorni il sito ricevette una mole enorme di visite da ogni parte del mondo, e Al-Bassam dovette lavorare a tempo pieno per garantirne l'accesso ininterrotto. Egli avviò inoltre collaborazioni con vari ricercatori e altri ex-Anon, tra cui Darren Martyn, tramite un

think-tank informale chiamato LizardHQ. Sono così riusciti ad attirare l'attenzione mediatica su controversi software di sorveglianza e le annesse vulnerabilità, tra cui: Hola (network privato gratuita con 10 milioni di utenti che prevede perfino una backdoor per coinvolgere surrettiziamente in qualche botnet i computer su cui è installata); E-Detective (programma legale d'intercettazione usato dal regime cinese e da oltre un centinaio di forze di polizia internazionali); e Impero (spyware utilizzato in varie scuole britanniche per spiare gli studenti). Al-Bassam mi ha poi spiegato che le attività della LizardHQ puntano a «esporre le vulnerabilità di questi progetti in modo che gli utenti possano fare scelte consapevoli rispetto al sistema che pensano possano proteggerne al meglio le libertà civili ... Noi informiamo pubblicamente su queste falle senza alcun contatto preventivo con i produttori di spyware, perché altrimenti creeremmo un precedente negativo suggerendo che i ricercatori sono combutta con i produttori».

Come confermato da numerosi studi e sondaggi, dopo le rivelazioni di Snowden l'opinione pubblica americana è più che mai interessata alla tutela della privacy[20]. E sulla questione hanno preso posizione perfino le Nazioni Unite, con un rapporto stilato dall'Alto commissariato per i diritti umani che difende la santità democratica della crittazione, perché «garantisce la privacy e la sicurezza necessarie per esercitare il diritto alla libertà d'espressione nell'era digitale».

Eppure, mentre l'opinione pubblica sta cambiando posizione, le autorità statali e le forze di polizia restano ancorate a strategie prevedibili – come hanno fatto per decenni – demonizzando sia le tecnologie di crittazione che i conseguenti ideali dell'anonimato. Adeguandosi alle forti richieste degli utenti, noti produttori di software proprietario come Apple e Google hanno fatto grossi passi in avanti per garantire la sicurezza degli utenti – suscitando l'insistente risposta dell'Fbi e di altri apparati investigativi secondo cui le corporation hanno invece il dovere di «impedire con ogni mezzo la diffusione della crittazione». Nell'ottobre 2014, il direttore dell'Fbi tenne un intervento sulla privacy dai toni allarmisti e caustici al Brookings Institution di Washington, affermando fra l'altro: «favorendo questo 'restare al buio', quanti tra noi operano nel campo delle forze dell'ordine e della sicurezza pubblica non riuscirebbero più a bloccare i predatori sessuali che approfittano degli individui più vulnerabili della società... a prevenire i violenti criminali che prendono di mira le nostre comunità... a individuare una cellula terrorista che usa i social media per assoldare fiancheggiatori, pianificare e portare avanti un attentato»[21].

In altri termini, va crescendo il confronto sui diritti civili per il futuro della privacy e dell'anonimato. Pur trattandosi di una battaglia tutt'altro che nuova, solo recentemente la questione ha superato l'ambito degli addetti ai lavori, ovvero studiosi di diritto, legislatori, tecnologi e accademici, per entrare nel più ampio dibattito sociale che interessa tecnologi, avvocati, giornalisti, registi, hacker, sviluppatori di software e produttori di hardware, enti non governativi e privati cittadini. Analogamente all'ideale della libertà di parola, che colpì la coscienza pubblica all'apice di accese battaglie politiche nella società statunitense (come l'istituzione del sindacato operaio dell'Industrial Workers of the World all'inizio del 1900 o il movimento di protesta degli anni '60 partito da Berkeley), anche queste iniziative di base a sostegno della privacy sembrano sul punto di raggiungere una massa critica.

La posizione di Anonymous all'interno di questo variegato movimento pro-privacy merita ulteriori approfondimenti. Visto il nome e il simbolismo di cui si è appropriato, la

stessa esistenza del collettivo ne conferma il pieno appoggio a questi valori oggi sotto assedio. Quando però un'entità come Anonymous si lega così intimamente a un movimento sociale, ciò diventa per molti versi un'arma a doppio taglio: pur portando in primo piano certe tematiche e conquistando nuovi aderenti e simpatizzanti, la sua presenza finisce per attirare le critiche dei detrattori. E comunque ciò non è certo una sorpresa, vista la sua propensione a suscitare conflitti. Non c'è modo di evitare le controversie evidenziate da Anonymous, e perfino quando proprio questo ne è l'obiettivo, i risultati possono rivelarsi imprevedibili, improduttivi e talvolta finanche dannosi.

Comunque sia, più di qualsiasi movimento politico passato o presente, Anonymous incarna il caso perfetto tramite cui studiare l'operatività, i benefici, le contraddizioni e le limitazioni dell'applicazione concreta dell'anonimato. E con la crescita di questo movimento pro-privacy, ho notato l'emergere di una forte tensione tra quanti considerano l'anonimato come strumento politico di indubbia utilità. Anche quando i tanti attivisti con tendenze liberali e sinistroidi sostengono inequivocabilmente il diritto al software di crittazione, a volte esprimono profondo disagio di fronte all'uso della segretezza tra gli stessi attivisti, al ruolo dell'anonimato in generale e alla funzione di Anonymous in particolare. Mettendola in maniera leggermente diversa, molti sono infastiditi dal fatto che Anonymous in sé, e ogni comportamento anonimo in generale, rivela una mancanza di responsabilità personale; anzi, in una versione più tagliente della stessa critica, dimostrano vera e propria vigliaccheria. Tempo fa un accademico ha espresso senza mezzi termini questo disagio dichiarando che «l'opposto dell'anonimato è la responsabilità».

Mentre il rapporto tra anonimato e assenza di responsabilità appare ben più complesso di quanto possa implicare tale dichiarazione, è innegabile che la caratteristica fondamentale dell'occultamento intenzionale sia quella di evadere la responsabilità individuale. La studiosa della privacy Helen Nissenbaum ha difeso l'anonimato proprio in base a queste posizioni, spiegando che «il valore dell'anonimato sta non tanto nella capacità di rimanere senza nome, bensì nella possibilità di agire o partecipare rimanendo irraggiungibile»[22].

Pur se forme limitate di segretezza e schermatura dalle ripercussioni legali restano vitali per Anonymous, gli arresti di LulzSec e altri partecipanti hanno chiarito agli odierni attivisti che l'anonimato non è mai qualcosa di assoluto. Oggi gli Anon sono consapevoli di questo rischio, e quindi agiscono tenendo sempre a mente le possibili conseguenze di ogni operazione – comportandosi come se loro attività verranno sicuramente scoperte, pur augurandosi che ciò non avvenga. E, in alcuni casi, costoro rifuggono perfino da quest'anonimato di tipo stringente, tecnico e motivato dalla sicurezza – abbracciando soltanto l'anonimato sociale che consente loro d'interagire con gli altri membri del collettivo in maniera paritaria. Keith Wilson Downey, uno del gruppo di PayPal 14, ha ammesso questa situazione razionalizzando come segue il suo coinvolgimento in Operation Payback: «come fervente sostenitore della libertà d'informazione per oltre un decennio, decisi di fare qualcosa di più che stare solo a parlarne. Così il 9 dicembre 2010 ho scaricato il Loic, partecipando direttamente alle proteste contro PayPal. Va notato che ho scelto di non coprire le mie tracce perché l'ho considerato un legittimo atto di protesta per il quale valeva la pena di correre dei rischi. Una decisione che ha trasformato completamente i miei tre anni successivi[23]. Downey considerava dunque l'anonimato non come uno scudo per sfuggire alla responsabilità individuale, bensì un contesto per dare

impeto all'azione.

Non è facile condensare i meccanismi dell'anonimato all'interno di Anonymous in una logica univoca: qualunque sia la definizione scelta, questa può essere adottata e riformulata, in forme diverse e verso obiettivi differenti, da chiunque voglia farne uso. Non può mai essere privatizzata, e ancor meno tenuta sotto controllo, perché qualsiasi tentativo in tal senso la modifica immancabilmente in qualcosa diverso dall'anonimato. E quindi, per molti versi, l'ideale stesso è incorruttibile (oppure, corruttibile all'infinito) – comunque al di fuori della longa manus del potere, pur se quanti prendono parte a quell'esperienza temporanea, o credono di prendervi parte, finiscono per essere beccati. In ogni caso, Anonymous ha chiaramente reso possibile l'emergere di un nuovo soggetto politico, il cui obiettivo di fondo è quello di non limitarsi a parlarne, come spiegava Downey, per passare piuttosto all'*azione*. E pur essendo possibile giudicare tali azioni, c'è accordo generale sul fatto che i nomi degli autori – pur quando di fatto questi sono identificabili e rischiano il carcere – rivestono un'importanza minore rispetto alle attività intraprese. È così che, anche quando il nome di qualche attivista viene allo scoperto, il valore dell'anonimato viene comunque preservato nelle azioni compiute proprio grazie alla sua spinta. Basta credere nell'idea di Anonymous per motivare all'azione, pur se l'anonimato totale non è l'obiettivo finale né qualcosa di raggiungibile.

Nonostante i membri di Anonymous siano protetti da uno pseudonimo quando agiscono in pubblico, va altresì ribadito che la maggioranza delle operazioni in quanto tali non vengono affatto condotte in segreto. Questi attivisti si organizzano su canali irc pubblici, diffondono comunicati stampa, creano spettacolari video per annunciare e motivare le loro iniziative. Generalmente sono anche in stretto contatto con attivisti e giornalisti che non appartengono al circuito di Anonymous. Nei primi giorni della OpFerguson, per esempio, la CNN ne seguiva i partecipanti su irc, cercando di convincerli ad apparire in Tv dal vivo. È difficile immaginare che un giornalista possa avere un accesso così immediato a terroristi o hacker criminali che cercano di evitare a tutti i costi qualsiasi contatto con le autorità e il pubblico in generale. In altre parole, la maggioranza degli Anon non si nasconde nell'equivalente online delle caverne afgane di Tora Bora per pianificare attentati nel buio totale. Preferiscono agire alla luce del sole, pur se dietro un certo velo di sicurezza, appena sufficiente per consentire loro di passare all'azione.

Un altro elemento di confusione è inoltre la tendenza diffusa ad associare particolari operazioni con altrettanti gruppi, account Twitter, canali irc o individui specifici. È questo il caso, per citare un solo caso, della OpCyberPrivacy. Non appena il team dietro quest'operazione condusse una serie di hack per protestare contro la proposta di legge canadese C-51, un altro hacker di Anonymous noto come ro0ted annunciò di aver bucato il sito web del governo, divulgandone nomi e credenziali degli impiegati. Inizialmente, i giornalisti assegnarono l'hack agli Anon di OpCyberPrivacy, ma costoro non c'entravano nulla e anzi lo criticarono aspramente, ritenendolo un caso di irresponsabile violazione della privacy – chiedendo così ai giornalisti di pubblicare un'immediata smentita. Sarebbe bastata una rapida verifica per notare che ro0ted aveva sostenuto correttamente di far parte di Anonymous, ma non certo di OpCyberPrivacy, essendo coinvolto nella rete di cyber-guerriglia del collettivo[24]. La maggior parte degli articoli online sulla vicenda vennero rapidamente corretti, e la caratteristica di Anonymous emerse chiaramente a chiunque fosse disposto a prestarvi un attimo d'attenzione: era possibile affermare la

responsabilità individuale perfino per chi si trovava parzialmente coinvolto in operazioni anonime[25].

Pur potendo ricondurre la maggioranza delle iniziative portate avanti sotto il manto di Anonymous a una qualche entità responsabile, molti osservatori restano interdetti in assenza di qualsiasi ricorso finale a un'identità legale. Una delle domande che mi venivano rivolte più frequentemente era: se Anonymous è clandestino, come fanno gli attivisti a rispondere del loro operato alle comunità in cui operano?

Forse è il caso capire meglio fino a che punto può arrivare tale responsabilità in quegli ambiti dove vige massima trasparenza. È questo il caso, per esempio, del giornalismo, un campo spesso sbandierato come la quintessenza della trasparenza. I giornalisti firmano gli articoli con il proprio nome e cognome e la credibilità della testata dipende dal fatto che dicono cose vere e non bugie. Eppure si accetta come una necessità – anzi perfino come un sacrosanto diritto – quella di ricorrere talvolta a fonti anonime, in particolare per raccogliere informazioni altrimenti inaccessibili.

Può però capitare che qualche giornalista commetta lo stesso errore imputato ad Anonymous: rivelare e mettere a rischio queste fonti anonime – ovvero, il doxing. Si tratta (comprensibilmente) di una tattica alquanto controversa e a volte profondamente disgustosa tra quelle applicate da Anonymous. Come illustrato in precedenza, ciò fa irritare non poco gli Anon, soprattutto quando qualcuno divulga i nomi di osservatori innocenti oppure attribuisce una certa azione alla persona sbagliata. È quanto accaduto durante l'OpFerguson, quando un account Twitter di Anonymous, TheAnonMessage, diffuse foto e generalità di un poliziotto erroneamente ritenuto quello che aveva sparato a Michael Brown[26].

Anche se i giornalisti non vengono mai accusati di praticare il doxing di per sé, spesso l'effetto finale è identico, ed è un errore in cui cadono non soltanto i tabloid o le testate online come Gawker, il cui fondatore notoriamente sosteneva: «a livello editoriale, ho un semplice banco di prova: è tutto vero, ed è interessante?»[27]. Pochi mesi prima che Anonymous prendesse quell'abbaglio sul poliziotto di Ferguson, emerse il caso più clamoroso di doxing di tutto l'anno – e non fu opera di un manipolo di Anon, bensì del noto settimanale *Newsweek*.

Annunciando con gran frastuono il ritorno in edicola (dal dicembre 2012 usciva soltanto in edizione digitale), all'inizio del marzo 2014 la rivista presentò un'eclatante servizio di copertina: i suoi giornalisti avevano presumibilmente individuato il vero Satoshi Nakomoto, il famoso pseudonimo dietro cui si nascondeva l'ideatore della crypto-moneta bitcoin. *Newsweek* era convinto che quello pseudonimo online non fosse tale: si trattava proprio di Dorian Nakamoto, un anziano ingegnere giapponese-americano residente nella California meridionale, l'uomo elusivo che aveva ideato la popolare valuta digitale. L'inchiesta, come anche le indagini preparatorie e le ricadute successive, rivelarono un'operazione assolutamente intrusiva – incarnando la forma e la logica tipica del doxing istigato dagli hacker. Il giornalista responsabile dell'indagine, Leah McGrath Goodman, diffuse online la fotografia della casa in cui viveva Nakamoto, corredata dall'indirizzo e dalla targa della macchina ben leggibile. Rintracciarlo divenne così un gioco da ragazzi, e non tardarono ad arrivare dettagli privati relativi alle sue condizioni economiche, allo stato di salute e finanche ai guai coniugali – il tutto tranquillamente in bella vista per milioni d'ignari americani. Ciò spinse diverse testate d'informazione, tra cui il *Los Angeles Times*, a lanciare una sorta di "caccia a bitcon", con giornalisti e

fotografi che presero letteralmente d'assedio l'abitazione di Dorian, inseguendolo fin dentro un ascensore e tempestandolo di domande. Salvo poi lo deriderlo nell'articolo per aver offerto un'intervista al primo reporter che gli pagava il pranzo.

Innumerevoli esperti, giornalisti e osservatori non hanno risparmiato accuse a *Newsweek* per le prove fallaci addotte a giustificazione di quella presunta identificazione*;* ma nonostante le diffuse critiche ricevute, a tutt'oggi *Newsweek* continua a difendere l'inchiesta con un inopportuno riferimento all'interesse pubblico: «abbiamo stabilito che fosse nell'interesse pubblico venire a conoscenza di certi dettagli importanti su bitcoin e informare al meglio chi fosse interessato a fare degli investimenti»[28]. Pur nel caso che quei reporter avessero effettivamente identificato la persona giusta, restano assai dubbiose le giustificazioni etiche per divulgarne ai quattro venti la vita privata. L'ideatore di bitcoin ha ripetutamente espresso il desiderio di rimanere anonimo; ancor più importante, le sue azioni non hanno provocato danni o problemi a chicchessia, e non è affatto necessario conoscerne certi dettagli privati per fare "investimenti corretti" in bitcoin, come suggerisce il direttore di *Newsweek.*

Trattandosi di una testata pubblica registrata a norma di legge, ovviamente è possibile querelare *Newsweek*, opzione che nel 2014 Nakamoto sembrò prendere in considerazione. Invece è praticamente impossibile denunciare un collettivo senza volto per un caso di doxing, a meno che il colpevole non venga prima catturato dalla polizia oppure segnalato da qualcuno del gruppo. Per il potenziale errore e la violazione della privacy commessi da *Newsweek,* Nakamoto potrebbe ricevere un sostanzioso risarcimento danni,[29] mentre per il poliziotto erroneamente identificato da Anonymous, a cui arrivarono anche minacce di morte, non ci sono possibilità di riparare il torto subito.

La contrapposizione tra questi casi mette in luce importanti differenze tra la responsabilità di Anonymous, un gruppo di attivisti mimetizzato e una persona reale o un'entità pubblica. Tuttavia non mancano gli esempi di posizioni inaccurate, superficialità o imprecisioni a livello giornalistico che hanno provocato danni collaterali assai più gravi di quelli che possa mai causare Anonymous. Mentre un doxing sbagliato da parte di quest'ultimo può incautamente mettere in pericolo poche persone, affermazioni irresponsabili che vengono riprese tali e quali dalle grandi testate possono portare potenzialmente a decisioni che alterano il destino di intere nazioni. L'esempio più eclatante e insidioso dell'ultimo decennio è ormai noto a tutti, cioè quando il *New York Times* pubblicò nel 2002 un articolo esclusivo che riprendeva, senza ulteriori critiche o verifiche, la posizione delle autorità Usa secondo cui Saddam Hussein fosse in possesso di armi di distruzione di massa. Come hanno poi sottolineato diversi esperti, quell'unico articolo contribuì non poco a giustificare la guerra atroce ed onerosa contro l'Iraq, innescando una serie di eventi che nessuna querela o intervento della società civile potrà mai sanare.

Pur se quest'esempio potrà apparire fin troppo estremo, non mancano i casi più banali di dannosi passi falsi giornalistici basati su affermazioni sconsiderate, spesso proprio nell'ambito del tecno-attivismo. Molti giornali britannici hanno pubblicato articoli che diffamano Edward Snowden come spia russa, senza neppure cercare di fornire uno straccio di prova. Julian Assange, spesso accusato di essere un irresponsabile per le rivelazioni di WikiLeaks, ha criticato aspramente un giornalista del *Guardian* per aver pubblicato la password riservata in un libro che ne raccontava la collaborazione con WikiLeaks. A detta di Assange, ciò provocò «la divulgazione online di centinaia di

migliaia di cablogrammi del Dipartimento di stato Usa senza quelle rimozioni selettive dei testi che erano state attentamente predisposte»[30]. Assange aveva fornito la password a pochi giornalisti fidati con l'esplicito avvertimento che si trattava di materiale da verificare prima della pubblicazione, proprio per evitare l'involontaria divulgazione di informazioni sensitive relative a persone innocenti.

Esaminiamo infine un caso direttamente legato ad Anonymous, e già menzionato nell'introduzione. Il 21 febbraio 2012 – all'apice della popolarità del gruppo stesso, quando alcuni politici polacchi indossarono la maschera di Guy Fawkes per manifestare l'opposizione a un trattato commerciale internazionale – la giornalista Siobhan Gorman pubblicò sul *Wall Street Journal* un articolo in cui gli hacktivisti venivano descritti come pericolosi estremisti – scrivendo che «nel giro di uno o due anni Anonymous potrebbe acquisire la capacità di provocare limitate interruzioni di corrente elettrica tramite un qualche tipo di cyber-attacco». A sostegno di quell'affermazione ci si limitava a una sola battuta: «Questa la valutazione fornita dal generale Keith Alexander [allora direttore della National Security Agency] nel corso di riunioni segrete alla Casa Bianca e in altre incontri privati, secondo quanto sostenuto da fonti a conoscenza della vicenda»[31]. Non soltanto si tratta di una prova chiaramente insufficiente, ma quell'eventualità apparve talmente fuori luogo rispetto al comportamento pubblico di Anonymous da far perdere credibilità all'intero articolo. Se invece l'affermazione fosse stata presa sul serio, avrebbe potuto invalidare gli sforzi di un intero movimento politico per contribuire positivamente a svariati problemi sociali.

Anonymous a volte commette degli errori, e lo stesso fanno i giornalisti. Ma quando è una testata prestigiosa a sbagliare, generalmente non si prende di mira l'intero settore del giornalismo e neppure la casa editrice, bensì soltanto l'articolo, l'autore o il redattore-capo direttamente coinvolti. Perché dovrebbe essere diverso per Anonymous? Ogni specifico errore, che venga commesso dal *New York Times,* da *Newsweek* o da Anonymous, merita critiche motivate. Ed è esattamente quanto accadde nel caso dell'OpFerguson, quando TheAnonMessage divulgò quel nominativo sbagliato. Stavo seguendo la discussione in corso su irc quando costui annunciò di voler divulgare le generalità di quel poliziotto. Essendo mattina presto, la maggior parte degli attivisti direttamente coinvolti erano assenti o inattivi. In genere un'operazione di doxing viene decisa in privato, e stavolta la cosa era inusuale perché stranamente TheAnonMessage agì senza consultare il gruppo centrale, cosa che normalmente avviene a porte chiuse nei canali privati. Non appena divulgò quel nome, e fu chiaro che si trattava di un errore, quasi tutti i membri coinvolti nell'operazione andarono su tutte le furie e criticarono aspramente l'Anon in questione. Uno dei critici più spietati fu Crypt0nymous, rispettato autore di video/media nel collettivo, che su Twitter lanciò una lunga filippica contro @TheAnonMessage[32] – con decine di messaggi sulle sue uscite scadenti e irresponsabili che, secondo Crypt0nymous, andavano imputate al suo desiderio di fama e onori. Non sempre questo tipo di censura e condanna informale riesce a rimediare a tutti gli sbagli, ma comunque sia i rimproveri informali producono effetti concreti sulle attività future, generalmente in senso positivo.

Questa serie di esempi a livello giornalistico non vuole certo giustificare le dannose conseguenze dovute al doxing errato di Anonymous. Servono piuttosto a sottolineare il fatto che, anche operando in un contesto di massima trasparenza, non sempre è possibile garantire che si arrivi a rispondere dei danni provocati. Infatti, quando prestigiose testate,

come il *New York Times* oppure il *Wall Street Journal*, pubblicano frottole o storie corroborate da scarse prove concrete, le conseguenze possono rivelarsi assai più devastanti di quanto non accada con un'entità quale Anonymous. Queste testate sono considerate un veicolo di obiettività e di verità, con una solida reputazione alla spalle difficile da infangare. All'opposto, spesso le affermazioni di Anonymous vengono prese con più di un granello di sale, perfino dai suoi stessi sostenitori.

È comunque lodevole che Anonymous continui a segnalare i pregiudizi e le prospettive inerenti a ogni fonte d'informazione, prescindendo dal fatto che ciò sia dovuto a dei limiti cognitivi, all'eccesso d'informazione, ai preconcetti inerenti allo stesso processo produttivo, a dei dati originari poco chiari oppure alla manipolazione vera e propria. Sapere che gli Anon possono sbagliare è un elemento positivo in quanto tale; non sostengono certo essere corretti e oggettivi, bensì solo degli attivisti impegnati a fare del loro meglio (oltre che a essere oltraggiosi). I loro errori non possono provocare troppi danni, perché non ci si aspetta che quelle affermazioni siano sempre corrette al 100 per cento, diversamente da una testata prestigiosa come il *New York Times*.

Comunque sia, il confronto tra Anonymous e giornalismo regge solo fino a un certo punto. La portata delle attività svolte in questo che rimane un movimento politico finalizzato all'azione diretta, è ben più ampia di quella assegnata a un organo d'informazione, il cui obiettivo si limita alla divulgazione delle notizie.

In molti casi, dunque, Anonymous risponde pubblicamente delle proprie azioni, pur se in maniera anonima e come team operativo, mentre in altre situazioni le sue manifestazioni più radicali e basate sull'azione diretta poggiano direttamente sulla segretezza e sull'anonimato, anche nei confronti di altri Anon. Spesso le attività particolarmente rischiose vengono elaborate e promosse in ambiti segreti, come le "combriccole all'interno delle combriccole" descritte in precedenza. Un altro obiettivo del ricorso alla segretezza riguarda meno la sicurezza e più il mantenimento dell'armonia sociale interna: gli Anon ostracizzano quanti provano a darsi delle arie, spesso chiedendo di sublimare l'identità individuale non soltanto per la propria sicurezza, bensì anche e soprattutto per tenere fuorigioco il proprio ego.

Questi due indicatori di offuscamento forniscono gli esempi di quella che lo studioso Jack Bratich definisce positivamente come «segretezza popolare minore … utile per contrastare ogni politica basata sull'identità e sulla rappresentatività»[33]. Aggiungendo che, non di rado, quando i movimenti sociali provano a conquistare visibilità e rappresentanza, non lo fanno tanto per imporre certe richieste politiche quanto piuttosto per renderle comprensibili ai meccanismi statali, così da farle proprie oppure respingerle[34]. Sottolineando che lo stato «aborrisce ogni maschera che non sia la propria», Bratich suggerisce l'esistenza di un'enorme disparità di forze tra il modo in cui le istituzioni "demonizzano" le maschere usate dai cittadini e il continuo rifiuto a togliersi invece le proprie. Come risultato, egli sostiene che l'attivismo di sinistra debba riservare alla segretezza uno spazio ridotto ma importante. Quando costoro rinunciano a ogni tipo di segreto, tendono a rafforzare inavvertitamente il potere statale; la loro trasparenza ne espone le vulnerabilità a un nemico mascherato pronto a sfruttarle o a cooptarle da una posizione vantaggiosa.

Cosa possono guadagnare gli attivisti da forme di segretezza limitate, soprattutto se fortificate da un'etica di offuscamento dell'ego per incoraggiare la parità interna? Ed è forse possibile giustificare moralmente quando ad applicarla sono gruppi politici

marginali, e va invece sempre condannata quando viene invece applicata da coloro che, come nel caso delle istituzioni e dei colossi dell'economia, esercitano già un vantaggio o un monopolio di potere? Quando ad appropriarsi della segretezza sono le nazioni-stato non solo in senso strumentale ma anche come norma operativa generale e in continua espansione (com'è particolarmente il caso con le agenzie d'intelligence dotate di risorse tecniche ed economiche apparentemente illimitate), spesso i suoi effetti si oppongono direttamente all'interesse pubblico[35]. D'altra parte il segreto offre agli attivisti con scarse risorse a disposizione, come avviene con Anonymous, la possibilità di colpire adeguatamente i più potenti, livellando il campo d'azione. Se usato in maniera limitata, il segreto può alterare positivamente il quadro politico, attivando le condizioni strutturali capaci di dar vita a interventi motivati, anziché limitarsi a produrre solo deliberazioni e comunicazioni di principio, fino a rappresentare una forma di azione diretta in quanto tale. Come ha detto Julian Assange, «la crittografia è la forma definitiva di azione diretta non-violenta»[36].

Vanno poi considerati i costi dell'inazione politica. Quando si tendono a privilegiare le forme tipiche della politica progressista – cioè il dibattito, le riforme e la visibilità, rispetto invece alla partecipazione diretta per il cambiamento – diventa difficile capire da dove possa emergere questo cambiamento nel caso in cui le istituzioni decidano di non prestare ascolto. La nostra società privilegia la trasparenza e il dibattitto civile in quanto meccanismi preferenziali per creare quella pressione politica capace di spingere i legislatori a innescare il cambiamento. Pur se informare al meglio l'opinione pubblica e dare spazio al dibattitto sono valori innegabilmente positivi, per fare in modo che l'informazione assuma un significato politicamente significativo a volte occorre affiancarla all'azione concreta – deve cioè essere trasformata in richieste impossibili da ignorare[37].

La disobbedienza civile è un modo per fare proprio questo, e la sua applicazione può servire come modello per garantire a un'ampia fetta di partecipanti – coloro che non hanno voce nella politica tradizionale oppure le minoranze soffocate da rigide convenzioni normative – un percorso tramite contribuire in maniera diretta al processo politico. Come ha spiegato Robin Celikates, studioso della disobbedienza civile, «anche le forme di azione politica episodiche, informali e extra- o anti-istituzionali consentono ai cittadini di protestare e partecipare, quando, com'è spesso il caso nelle democrazie rappresentative, i canali istituzionali ufficiali e comuni sono chiusi nei loro confronti e inefficaci nel convogliare adeguatamente le loro obiezioni»[38].

Ci si potrebbe opporre del tutto al ricorso alla disobbedienza civile da parte delle minoranze. In fondo, non è forse che la loro opinione sia poco condivisa proprio perché indesiderabile? In realtà questo è un punto di vista ingannevole. Anche quando funziona, la disobbedienza civile serve soltanto per attirare l'attenzione su una certa posizione – che però deve attirare molta altra gente per potersi trasformare in un attivismo di più ampia portata e quindi cambiare il consenso generale. Le posizioni di individui come Chelsea Manning, Jeremy Hammond e Edward Snowden erano quasi sconosciute finché i loro gesti coraggiosi non hanno creato spazio per i rispettivi interventi politici, incoraggiando altri che erano d'accordo con loro ad emularne le gesta. (C'è almeno un altro individuo che sta fornendo i documenti della Nsa a svariate piattaforme editoriali[39], mentre è probabile che Phineas Fisher si sia ispirato agli hack di Anonymous contro le aziende di sicurezza informatica). Atti coraggiosi di questa natura, anonimi o meno,

costringono la gente a confrontarvisi e talvolta a compiacersene. In altri termini, la disobbedienza civile crea un ambiente favorevole allo sviluppo di ampi movimenti sociali di base.

Anonymous è l'esempio perfetto di questa logica in atto. Quanti partecipano direttamente al doxing, alle intrusioni informatiche o agli attacchi DDoS sono una minoranza. Ma così facendo contribuiscono ad attirare spettatori e nuovi partecipanti, inclusi quanti non sono d'accordo con le loro strategie o finalità[40].

Eppure su questo fronte i critici, inclusi quanti difendono il ricorso alla disobbedienza civile da parte di altri movimenti sociali, insistono con la questione della responsabilità di Anonymous. La disobbedienza civile, sostengono costoro, perde legittimità qualora non venga condotta sulla base dell'identità personale – se, cioè, non viene legittimata dal rischio della condanna individuale. Ma come ha sostenuto a ragione Molly Sauter, questa è una concezione ristretta (e limitata) della disobbedienza civile fondata su circostanze storiche specifiche. Si tratta di una concezione, chiarisce la studiosa canadese, «profondamente radicata nell'idea del martirio cristiano e della superiorità morale della disobbedienza civile non-violenta nei confronti dell'oppositore ... e ritenere che gli attivisti politici online debbano esporsi agli interventi punitivi spesso estremi imposti dalle autorità fa in modo che soltanto quanti hanno concezioni estremiste e ben poco da perdere (ovvero quanti non si sentono parte attiva della società) finiscano per coinvolgersi in quelle azioni»[41].

Man mano che Anonymous prosegue con le sue richieste specifiche alle istituzioni, s'impegna per eliminare la corruzione e collabora con altri attivisti nel fornire assistenza a battaglie politiche piccole e grandi, continua a decolonizzare una soggettività dalle radici profonde: osa lavorare a favore del bene comune senza bisogno di un riconoscimento personale o di un marchio individuale. In fondo il collettivo è costituito per lo più da cittadini consapevoli e rispettosi delle leggi che, potendo scegliere, preferirebbero ricevere una qualche forma di apprezzamento pubblico e personale in cambio del loro contributo. E invece insistono sul "diritto all'opacità", nell'accezione formulata dal saggista francese Edouard Glissant[42]. L'atto di nascondersi dietro una maschera, troppo spesso considerato soltanto in termini negativi, può tuttavia innescare una morale positiva e costruttiva tesa a un'interazione concreta che si oppone alle istituzioni, alle corporation e al colonialismo. Questo diritto incarna anzi una serie di rifiuti provocatori e motivati: il rifiuto a consentire che le istituzioni possano sorvegliare i cittadini; il rifiuto a permettere alle corporation di convertire le comunicazioni personali in tornaconto economico o di manipolarne i desideri intimi; il rifiuto a capitalizzare il nostro lavoro a favore di entità esterne; in sostanza, il rifiuto ad accettare l'estinzione di un'idea davvero potente – che siamo e possiamo essere anonimi.

Luglio 2015

Note

[1] Frank Bajak, "Top South American Hackers Rattle Peru's Cabinet", bigstory.ap.org, 2 settembre 2014.
[2] https://www.gammagroup.com/ (consultato il 21 luglio 2015).
[3] https://wikileaks.org/spyfiles/list/tags/gamma-finfisher-trojan.html (consultato il 21 luglio 2015).
[4] Morgan Marquis-Boire e Bill Marczak, *From Bahrain With Love: FinFisher's Spy Kit Exposed?*, The

Citizen Lab, 25 luglio 2012: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/. Pur se i ricercatori non ne trovarono le prove concrete, il sospetto nasce dal fatto che i dati raccolti dal software venivano poi inviati a un indirizzo Ip del Bahrein. Per la dichiarazione della Gamma, si veda: "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy", bloomberg.com, 27 luglio 2012.

[5] Cora Currier e Morgan Marquis-Boire, "Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters", firstlook.org/theintercept, 7 agosto 2014.

[6] Una distribuzione del sistema Gnu/Linux che garantisce privacy, sicurezza e anonimato online. Per ulteriori dettagli si veda: https://en.wikipedia.org/wiki/Whonix.

[7] http://0x27.me/HackBack/0x00.txt (consultato il 21 luglio 2015).

[8] Ibid.

[9] Cora Currier e Morgan Marquis-Boire, "Leaked Documents Show FBI, DEA and US Army Buying Italian Spyware", firstlook.org/theintercept, 6 luglio 2015.

[10] http://core0.staticworld.net/images/article/2015/07/hackingteam_1-100594937-orig.jpg (consultato il 21 luglio 2015).

[11] Al momento di questa traduzione italiana (novembre 2015), i leak su Hacking Team sono ancora in corso. Secondo i documenti divulgati finora e mai smentiti, l'azienda milanese avrebbe venduto i suoi prodotti, tramite una serie di opachi intermediari e grazie a legami con le multinazionali della sorveglianza (quali Verint e NICE Systems) a Paesi come Azerbaigian, Kazakistan, Sudan, Etiopia, Bahrein, Arabia Saudita e altri. Per ulteriori dettagli e aggiornamenti sul tema si veda: http://www.danemblog.com/2015/07/quella-storia-da-film-di-hacking-team.html?spref=tw

[12] https://twitter.com/GammaGroupPR/status/617937092497178624.

[13] https://twitter.com/Anon2earth/status/614279036278284288.

[14] Steven Chase, "Cyberattack Deals Crippling Blow to Canadian Government Websites", theglobeandmail.com, 17 giugno 2015.

[15] https://pdf.yt/d/0SWY7AoPOoovRD_a (consultato il 21 luglio 2015).

[16] Ibid.

[17] Per ulteriori dettagli su Aaron Swartz si veda: http://aaronswartztributo.tumblr.com/.

[18] Per aggiornamenti sul caso di Lauri Love si veda: https://freelauri.com/.

[19] https://blog.torproject.org/blog/interview-tor-summer-privacy-student-donncha-ocearbhaill (consultato il 21 luglio 2015).

[20] http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

[21] https:// www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and- public-safety-on-a-collision-course (consultato il 21 luglio 2015).

[22] Helen Nissenbaum, "The Meaning of Anonymity in an Information Age", *Information Society*, vol. 15, no. 2 (maggio 1999).

[23] https://thepaypal14.com/story-keth.htm (consultato il 21 luglio 2015).

[24] https://twitter.com/ro0ted (consultato il 23 luglio 2015).

[25] Si veda la correzione inserita in calce all'articolo di Matthew Braga, "Anonymous Claims It Leaked Passwords and Credit Card Info of Canadian Officials", motherboard.vice.com, 23 giugno 2015.

[26] Il diciottenne afro-americano ucciso dalla polizia Usa il 9 agosto 2014 a Ferguson, Missouri, evento che provocò un'ondata di forti proteste in tutto il Paese e online, inclusa la OpFerguson di Anonymous più volte menzionata nel libro. Per ulteriori dettagli si veda: https://it.wikipedia.org/wiki/Omicidio_di_Michael_Brown.

[27] Peter Sterne, "Gawker in the Fight of Its Life with Hulk Hogan Sex-Tape Suit", capitalnewyork.com, 12 giugno 2015.

[28] "*Newsweek*'s Statement on the Bitcoin Story", newsweek. com, 7 marzo 2014.

[29] Pur se poi non è arrivata nessuna querela, alcuni sostenitori di bitcoin hanno poi organizzato una campagna di raccolta fondi per aiutare Nakamoto, raccogliendo l'equivalente di circa 14.000 dollari in bitcoin. Si veda: "Dorian Nakamoto—Thank You, Bitcoin Community", video caricato su YouTube da aantonop, 22 aprile 2014: https://www.youtube.com/ watch?v=w7YmJZ-qVW8 (consultato il 23 luglio 2015).

[30] Julian Assange, "Assange: How 'The Guardian' Milked Edward Snowden's Story", newsweek.com, 20 aprile 2015.

[31] Siobhan Gorman, "Alert on Hacker Power Play", wsj.com, 21 febbraio 2012.

[32] https://twitter.com/Crypt0nymous/status/ 499937201825001472.
[33] Jack Bratich, "Popular Secrecy and Occultural Studies", *Cultural Studies*, vol. 21, no. 1 (gennaio 2007).

[34] Si veda anche: Clare Birchall, "Transparency, Interrupted: Secrets of the Left", *Theory, Culture and Society,* vol. 28, no. 7/8 (dicembre 2011).
[35] Per un'analisi antropologica dell'insidiosa logica contemporanea innescata dalla segretezza nelle istituzioni americane, si veda: Joesph Masco, *The Theater of Operations: National Security Affect from the Cold War to the War on Terror,* Duke University Press, 2014.
[36] Julian Assange, et al*., Cypherpunks: Freedom and the Future of the Internet*, OR Books, 2012 (trad. ital.: *Internet è il nemico*, Feltrinelli, 2013).
[37] Si veda: Darin Barney, "Publics without Politics: Surplus Publicity as Depoliticization", in *Publicity and the Canadian State: Critical Communications Perspectives,* a cura di Kirsten Kozolanka, University of Toronto Press, 2014.
[38] Robin Celikates, "Civil Disobedience as a Practice of Civic Freedom", in *On Global Citizenship: James Tully in Dialogue,* a cura di David Owen, Bloomsbury, 2014.
[39] Ewen MacAskill, "Second Leaker in US Intelligence, Says Glenn Greenwald", theguardian.com, 11 ottobre 2014. Nello stesso contesto, a fine ottobre 2015 il sito web The Intercept ha pubblicato documenti riservati che rivelano i segreti del programma americano per usare i droni contro il terrorismo, dando adito alla presenza di "un nuovo Snowden". Si veda: https://theintercept.com/drone-papers.
[40] Si veda: Fruzsina Eördögh, "How Big Is Anonymous? Maybe Bigger than You Thought", csmonitor.com, 8 luglio 2015. L'articolo dettaglia un recente studio sociologico sulla presenza di Anonymous all'interno di Facebook, dal quale si ricava che la composizione del collettivo è più ampia e globale di quanto ritenuto finora.
[41] Intervista personale con l'autrice, 15 giugno 2015. Molly Sauter è dottoranda alla MacGill University e autrice del libro *The Coming Swarm*, Bloomsbury Academic, 2014.
[42] Si veda: Celia Britton, "Opacity and Transparency: Conceptions of History and Cultural Difference in the Work of Michel Butor and Édouard Glissant", *French Studies*, vol. 49, no. 3, luglio 1995. Per ulteriori dettagli su Édouard Glissant (1928-2011) si veda: https://it.wikipedia.org/wiki/%C3%89douard_Glissant.