Francesca Musiani

# La crittografia nei sistemi di messaggistica sicura: le libertà digitali tra sviluppo tecnologico e regolazione

**THE EXPERIENCE OF ENCRYPTION IN SECURE MESSAGING SYSTEMS: DIGITAL LIBERTIES AMONG TECHNICAL DEVELOPMENT CHALLENGES AND REGULATION ATTEMPTS**

This article presents some results of a research conducted from 2016 to 2018 as part of the Nextleap project, which resulted in the publication of the volume *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties* in April 2022. The article makes an argument for studying the experience of encryption in the variety of secure messaging protocols and tools existing today, so as to explore the implications of these socio-technical projects for the «construction» of civil liberties on the Internet. In particular, the article invites to reflect on the importance of analyzing encryption with social science tools. Specifically, it invites to examine how different encrypted messaging solutions are created, developed, implemented and governed and what these different encryption experiences – among the challenges of technical development and those deriving from regulation attempts – mean for digital freedoms.

**KEYWORDS** *Encryption, Secure Messaging, Digital Liberties, Internet Governance, Technical Development.*

## 1. Introduzione

Le rivelazioni di Edward Snowden del 2013 sono state un evento fondamentale nello sviluppo del campo delle comunicazioni sicure (Snowden 2019). Le controversie che tali rivelazioni hanno generato mostrano che la crittografia ha implicazioni fondamentali per le nostre libertà individuali e la presenza collettiva su Internet, e che i tentativi di minare la crittografia equivalgono a

Francesca Musiani, Centre national de la recherche scientifique, Centre Internet et Société – Rue Pouchet, 59-61 – 75017 Paris, Francia, email: francesca.musiani@cnrs.fr, orcid: 0000-0001-8343-6122.


ISSN 2785-0072

rendere gli utenti Internet vulnerabili *by design*. La crittografia è diventata uno dei principali campi di battaglia della governance di Internet.

La crittografia delle comunicazioni su larga scala e in modo *user-friendly* è diventata una questione di interesse pubblico; nuovi immaginari relativi alla crittografia emergono e la comprendono come una precondizione necessaria per la formazione di pubblici in rete (Myers West 2018). Oltre a trasformare la crittografia in una vera e propria questione politica, le rivelazioni di Snowden hanno catalizzato dibattiti di lunga data nel campo della sicurezza dei protocolli di messaggistica. La comunità dei crittografi (in particolare, i collettivi accademici e di software libero) ha rinnovato i propri sforzi per creare una nuova generazione di protocolli di messaggistica, al fine di superare i limiti dei protocolli esistenti, come *Pretty good privacy* (Pgp) e Off-the-record (Otr).

Con eventi quali l'introduzione della crittografia *end-to-end*[1] in WhatsApp, la piattaforma di messaggistica istantanea più popolare (2014), miliardi di utenti hanno iniziato a proteggere le proprie comunicazioni per impostazione predefinita e su base quotidiana, spesso senza rendersene conto. Sebbene il mantra «Non ho niente da nascondere» sia ancora diffuso tra gli utenti di Internet, l'interesse per le modalità di protezione delle comunicazioni online con mezzi come la crittografia è in aumento; un interesse che ha importanti conseguenze socio-tecniche. Se queste conseguenze si applicano in particolare a coloro la cui vita dipende da un'accurata valutazione dei rischi legati alla propria professione o al contesto politico, lo sono sempre di più anche per il «cittadino comune». In risposta alla concezione, sempre più diffusa, della sicurezza nelle comunicazioni online come importante questione sociale e politica, oltre che tecnica, l'uso della crittografia *end-to-end* è un campo vivace e in divenire.

Questo articolo presenta alcuni risultati di una ricerca condotta dal 2016 al 2018 in collaborazione con Ksenia Ermoshina nell'ambito del progetto Nextleap[2], che ha dato luogo nell'aprile 2022 alla pubblicazione del volume *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties*, per i tipi di Mattering Press[3]. Nel contesto sopra descritto, il libro esplora l'esperienza[4] della crittografia nella varietà di protocolli e strumenti di

[1] Si veda https://it.wikipedia.org/wiki/Crittografia_end-to-end.

[2] Si veda nextleap.eu, NEXT-generation techno-social and legal encryption, access and privacy, finanziato dalla Commissione Europea nell'ambito del programma H2020 Collective awareness platforms (Caps).

[3] Disponibile in open access all'indirizzo https://www.matteringpress.org/books/concealing-for-freedom.

[4] Sottolineato in corsivo nel titolo e nel testo per evidenziare che la dimensione delle comunicazioni criptate che questo articolo (e il libro) analizzano non è quella della crittografia «come dovrebbe essere», nelle sue definizioni formali, ma come viene esperita e vis-

messaggistica sicuri esistenti al giorno d'oggi, e le implicazioni di questi progetti socio-tecnici per la «costruzione» delle libertà civili su Internet.

In particolare, l'articolo invita a riflettere sull'importanza di analizzare la crittografia con gli strumenti delle scienze sociali, per esaminare come diverse soluzioni di messaggistica criptata sono create, sviluppate, attuate e governate e cosa significhino queste diverse esperienze di crittografia per le libertà digitali. Come ha affermato, già nel 2003, lo studioso dell'informazione e pioniere di Internet Philip Agre, «l'architettura tecnologica è politica, ma non dovrebbe essere compresa come un sostituto della politica» (Agre 2003, 39). L'articolo suggerisce che è necessario, nel caso della messaggistica criptata, condurre una valutazione dettagliata della misura in cui fattori economici, sociali, legali (e naturalmente, tecnici) complicano la «traduzione» lineare da un'architettura tecnologica decentralizzata verso un sistema socio-economico decentralizzato di successo, o da un modello tecnico centralizzato a una struttura socio-politica *top-down*.

## 2. Per un contributo delle scienze sociali agli studi della crittografia

Per molto tempo, le ricerche sulla crittografia sono state per lo più appannaggio degli informatici, mentre le questioni più «sociali» che la riguardano sono state spesso confinate ai dibattiti sulla *usable security* (cioè alle discussioni che si svolgono all'interno della comunità degli informatici, e che si basano su studi di tipo sondaggistico che mirano a trovare modi per rendere gli strumenti criptati più facili da usare). Dopo le rivelazioni di Snowden, le comunicazioni criptate e gli obiettivi di privacy e sicurezza che esse cercano di potenziare stanno diventando oggetto di un ampio dibattito pubblico. È dunque importante che le scienze sociali raccolgano la sfida di indagare in profondità su come gli strumenti di messaggistica criptata vengono concepiti e sviluppati, su come vengono adottati da diversi profili di utenti, a volte in modo non intenzionale o imprevisto, su come ispirano e sono ispirati da diversi immaginari e su come, infine, gli attori della governance di Internet se ne impossessano. La presente ricerca è in dialogo con i contributi che, recentemente, hanno cercato di applicare alcuni concetti centrali delle scienze sociali, in particolare dei *Science and technology studies* (Sts), allo studio della crittografia.

Come ha sostenuto Sarah Myers West (2018), la crittografia è una questione di immaginari in competizione e di visioni, progetti e implementazio-

suta sia dagli attori sociali che la creano e la sviluppano concretamente in dispositivi e strumenti, sia da coloro che scelgono e si appropriano tali tecnologie nella loro vita quotidiana.

ni che essi co-producono. La crittografia ha costruito i suoi diversi significati nell'ambito della sicurezza nazionale e della segretezza e in quello dei sistemi democratici, in cui consente la comunicazione privata e permette di evitare la sorveglianza e le potenziali sanzioni sociali o politiche. Tecnologie simili possano acquisire significati e ruoli diversi in contesti culturali differenti; dunque, queste tecnologie devono essere comprese non solo in senso tecnico, ma anche negli specifici contesti sociali, culturali e politici in cui vengono utilizzate. Occorre inoltre tenere conto della dimensione storica di questi contesti socioculturali e della loro evoluzione nel tempo, come sottolinea Isadora Hellegren nel suo lavoro che vede il discorso sulla crittografia come un processo contestuale, strutturante e performativo di creazione di significato (Hellegren 2017). Il significato sfaccettato della crittografia evolve non solo secondo le diverse comunità di sviluppatori e utenti, ma anche nel tempo. La comprensione di come i vari attori abbiano costruito specifiche accezioni di libertà in relazione a tecnologie come la crittografia è importante per gli storici di Internet, gli hacker, i programmatori e i politici, poiché tutti questi attori sono coinvolti nella costruzione della forma, della funzione e del significato delle libertà digitali.

La crittografia, e i dibattiti che la circondano, sono il risultato dell'incrociarsi di molteplici sfere pubbliche e circoli di esperti, incorporati in questioni più ampie di Internet e della società come il controllo dei media in rete, la sorveglianza e la protezione dei dati personali. *Crypto-Politics* (2019) di Linda Monsees è un importante contributo allo studio di questi aspetti, che osserva lo svolgersi di discorsi sulla crittografia nel suo insieme, in arene politiche tradizionali e meno tradizionali. Monsees sviluppa la nozione di «*publicness*» per trasmettere l'idea che le controversie politiche sulla crittografia si trovano spesso al di fuori delle istituzioni politiche consolidate (sebbene non debbano essere trascurate quelle che si svolgono in arene politiche più tradizionali): «le controversie sulla crittografia elaborano idee specifiche relative non solo a cosa significhi la 'sicurezza', ma anche a come su queste concezioni si costruiscono idee specifiche di cittadinanza, privacy e 'fare Stato'» (Monsees 2019, 10).

Al di là del dialogo con questo insieme di ricerche recenti sulla crittografia, basate sulle scienze sociali, il nostro lavoro si ispira e cerca ulteriormente di contribuire alla ricerca di numerosi studiosi che operano all'incrocio tra *media studies*, sociologia della tecnologia e informatica, per studiare le tecnologie di comunicazione in rete e le loro implicazioni per la privacy, la sicurezza e la governance di Internet.

Lo sviluppo tecnico di applicazioni e protocolli, e l'insieme delle scelte operanti durante il processo di sviluppo, contribuiscono in modo determinante a dare un senso alla definizione delle libertà digitali, come dovrebbero essere preservate, e chi sono i loro avversari. L'antropologa Gabriella Coleman ha

aperto la strada agli studiosi che cercano di esplorare queste questioni. In particolare, ha esaminato il ruolo della cultura hacker, esplorando cosa gli hacker intendono per libertà e come la mettono in atto in quanto forma di autodeterminazione che considera l'accesso illimitato alla conoscenza una precondizione necessaria per l'evoluzione della loro «arte tecnica» (Coleman 2005). Inoltre, il lavoro di Coleman è di particolare rilevanza per uno studio sulla crittografia basato sulle scienze sociali. Insieme ad Alex Golub, Coleman ha definito la «cripto-libertà» come una particolare forma di pratica hacker, fondata su una comprensione della libertà che pone lo stato come il principale avversario nella battaglia per la privacy online. Questa pratica deriva dal particolare contesto storico e culturale del liberalismo negli Stati Uniti e si basa sulla convinzione che questa libertà dovrebbe essere preservata e promossa principalmente su Internet attraverso lo sviluppo e l'uso delle tecnologie di crittografia (Coleman e Golub 2008).

Dopo le rivelazioni di Snowden, diversi autori hanno inoltre affrontato la questione di cosa significhi essere online come individuo, cittadino e consumatore, in una società sempre più consapevole della misura in cui veniamo sorvegliati. In questo ambito, si sono soffermati sul tema del ruolo svolto dallo sviluppo tecnico delle architetture e delle infrastrutture di comunicazione online.

Come mostrano Stefania Milan e colleghi (ad es. Milan e van der Velden 2018), stiamo assistendo ad una crescente varietà di pratiche di «attivismo dei dati» (*data activism*): un insieme di tattiche socio-tecniche, resistenze e mobilitazioni che adottano un approccio critico alla dataficazione, alla raccolta di dati di massa e alla sorveglianza pervasiva. La lente concettuale della «giustizia dei dati» (*data justice*) è stata proposta da Arne Hintz, Lina Dencik e Karin Wahl-Jorgensen (2019) per illustrare che non solo la cittadinanza e la possibilità di agire dei cittadini nell'Internet di oggi sono profondamente modellate da fenomeni come la massiccia raccolta e mercificazione dei dati, ma anche che i diritti e le pratiche degli utenti in materia di privacy e sorveglianza online sono oggi concepiti in termini altamente individualizzati. Questo problema è importante in relazione alle tecnologie di crittografia e alla loro adozione di massa perché il pubblico di destinazione delle applicazioni di messaggistica sicura nate o sostanzialmente sviluppate dopo Snowden è tutt'altro che limitato a gruppi di esperti di tecnologia e attivisti: diversi progetti mirano a un uso diffuso. Questo è un grande cambiamento nel campo, poiché per molto tempo la maggior parte della comunità tecnica *crypto* ha ritenuto che una maggiore facilità d'uso potesse realizzare in pratica il loro desiderio di adozione su larga scala, considerando allo stesso tempo l'ergonomia e il *comfort* dei problemi secondari rispetto alla solidità della tecnologia.

Infine, un insieme di concetti particolarmente utile agli studi sociali della crittografia si trova in studi incentrati sulla governance di Internet in una prospettiva Sts (ad es. Epstein *et al.* 2016). Complementari agli approcci prevalentemente istituzionali che hanno definito l'agenda di ricerca sulla governance di Internet nei suoi primi passi – approcci che rimangono una delle sue caratteristiche preminenti – gli approcci Sts invitano a prendere in considerazione l'*agency* (capacità di agire) di sviluppatori tecnici, decisori politici e utenti mentre interagiscono, in modo distribuito, con tecnologie, norme e regolamenti. Gli Sts forniscono anche risorse concettuali cruciali per consentire la comprensione della crittografia come luogo di contestazione e conflitto, in particolare con la nozione di controversia sociotecnica. Da un lato, fin dagli albori di Internet, gestire questa «rete di reti» ha significato esercitare il controllo su funzioni particolari che forniscono ad attori specifici il potere e l'opportunità di agire a proprio vantaggio. D'altra parte, molto raramente esiste un unico modo per implementare queste funzioni o un unico attore in grado di controllarle. Internet è quindi controverso e contestato, obiettivo e strumento di governance al tempo stesso, e oggetto di interesse di una miriade di attori, dal più potente e centralizzato al «semplice» utente Internet (Epstein *et al.* 2016). Gli assetti infrastrutturali e architettonici, lo sviluppo e l'attuazione di particolari protocolli, possono essere intesi come delle arene fondamentali per esercitare il potere economico e politico, come abbiamo esaminato altrove (ad es. DeNardis e Musiani 2016).

Internet include un numero crescente di siti di contestazione (Mueller *et al.* 2012; Deibert e Crete-Nishihata 2012; DeNardis e Hackl 2015; Ziewitz 2016; Mager 2012). Inoltre, in Internet e nelle sue applicazioni sono spesso presenti contenziosi politici, sovente legati all'attivismo e alla protesta dei cittadini (Milan e ten Oever 2017). Tra i vari esempi, le tecnologie di crittografia per le comunicazioni online stanno diventando uno dei sistemi principali in cui si esercitano funzioni di governance tramite l'architettura tecnologica, pieno di controversie che riguardano, a loro volta, lo sviluppo di queste tecnologie, la loro implementazione, la loro (a volte sorprendente) appropriazione da parte degli utenti e i tentativi di regolarli.

È interessante notare che, a questo proposito, le rivelazioni di Snowden del 2013 e il successivo allargamento dei dibattiti relativi alla sorveglianza di massa, non solo hanno rivelato la necessità di un'ulteriore riforma legale dei sistemi di *intelligence* e sorveglianza, ma hanno anche messo in evidenza «una varietà di pratiche, politiche e discorsi che possono [...] essere correlati alle controversie post-Snowden» (Pohle e Van Audenhove 2017, 2-3). Uno degli esempi principali è stata la controversia tra Fbi e Apple che ha attraversato il 2015 e il 2016, quando Apple Inc. ha ricevuto diversi ordini dai tribu-

nali distrettuali degli Stati Uniti, finalizzati ad assistere le indagini penali in corso tramite l'estrazione di dati da iPhone con ampie protezioni di sicurezza crittografica. La stessa Apple non poteva violare queste protezioni a meno di non scrivere un nuovo software specifico per consentire alle autorità di aggirare tali barriere. Questo dibattito ha posto la questione se – e in caso affermativo in quale misura – le autorità giudiziarie o governative potessero obbligare gli attori tecnici a fornire assistenza nello sblocco di dispositivi protetti da sistemi di crittografia (vedi anche Schulze 2017). Polemiche come questa hanno contribuito a svelare aspetti dell'*esperienza* della crittografia nell'Internet di oggi e suggeriscono che le questioni più urgenti del nostro tempo relative alla crittografia potrebbero essere non solo legali e tecniche, ma anche sociali.

## 3. Una nota metodologica

Il nostro approccio è basato su diversi filoni della letteratura Sts e delle altre discipline che abbiamo introdotto nella sezione precedente. Tali contributi, proponendo una maggiore attenzione alla molteplicità delle arene di governance, alle «pratiche quotidiane» dello sviluppo tecnologico che sono dotate di valenza politica, e al ruolo controverso dello sviluppo e dell'implementazione delle infrastrutture, permettono di analizzare lo sviluppo delle architetture e delle interfacce delle applicazioni di messaggistica come «punti di incontro» tra gli obiettivi intenzionali degli sviluppatori e le esigenze degli utenti (Oudshoorn e Pinch 2005). In tal modo, abbiamo cercato di fornire un'analisi, basata sul lavoro sul campo, di sistemi emergenti e comunità di pratica attraverso «dense descrizioni analitiche» (per una trattazione recente del concetto, introdotto per la prima volta dall'antropologo Clifford Geertz, si veda Ponterotto 2006) di eventi, manufatti e organizzazioni. In particolare, prestiamo attenzione ai momenti di crisi, dibattito e controversia – per cercare di comprendere la vita di un manufatto tecnico, dalla sua creazione alla sua appropriazione e riconfigurazione da parte degli utenti, al suo divenire oggetto di dibattito pubblico, di governance, di lobbying. La metodologia principale per raggiungere questo obiettivo è stata l'osservazione, per periodi di tempo relativamente prolungati, di gruppi o comunità di casi di studio specifici, conducendo interviste approfondite con i loro membri e leggendo la documentazione appropriata come *release notes* e resoconti di sessioni di lavoro.

In breve, la metodologia usata in questo lavoro può essere descritta come un'etnografia *multi-sito*, poiché abbiamo intrapreso ricerche in e tra diverse località online e offline come parte del nostro studio, e abbiamo anche espli-

citamente considerato specifici protocolli e sistemi tecnici come «parte di un contesto più ampio che supera i confini del sito» (Muir 2011, 1015).

Tra i soggetti delle nostre interviste, gli sviluppatori sono stati per lo più selezionati sulla base di relazioni personali preesistenti che i membri del team di ricerca Nextleap avevano con la comunità di ricerca crittografica. Piuttosto che ricercare artificialmente la massima diversità in termini di profili, origini e genere degli intervistati (obiettivo difficile da raggiungere nel *milieu* dello sviluppo di soluzioni crittografiche per le comunicazioni online), ci è sembrato più significativo ai fini della ricerca massimizzare la varietà, dal punto di vista tecnologico, dei dispositivi che i nostri intervistati contribuivano a sviluppare (architettura tecnologica, trattamento dei dati e dei metadati, etc.) Per i progetti con i quali i membri del team di ricerca non avevano precedenti collegamenti personali, abbiamo anche contattato gli sviluppatori tramite le pagine GitLab e GitHub dei progetti. Le domande poste agli sviluppatori vertevano principalmente sulle ragioni alla base dello sviluppo del loro progetto e delle scelte tecniche, sulla dimensione e l'organizzazione interna del team, sulle scelte relative a questioni tecno-economiche chiave quali il trattamento dei dati, la sicurezza, la standardizzazione e i *business model*, e infine sulle collaborazioni con altri progetti di messaggistica.

Gli studi sugli utenti sono stati invece condotti con individui selezionati in base alla loro partecipazione a eventi di formazione alla crittografia, in diversi luoghi (sia ad alto rischio, nel caso di Ucraina e Russia, sia a basso rischio nel caso di Francia, Germania, Austria e il Regno Unito). La nostra selezione di eventi e conferenze a cui partecipare è stata guidata principalmente dal nostro interesse a parlare con utenti provenienti da contesti ad alto rischio, che non avrebbero potuto esprimersi liberamente nei loro paesi natali; due eventi a cui abbiamo regolarmente assistito sono stati l'Internet freedom festival e RightsCon. Tutte le interviste sono state condotte tra l'autunno 2016 e la fine dell'estate 2018, per un totale di 63 interviste.

## 4. Alcuni risultati della ricerca

### *Il rischio è relazionale, il threat-modelling è cruciale*

Fornendo una serie di esempi relativi ai contesti di utilizzo, alle esigenze percepite degli utenti e alla selezione di strumenti possibilmente appropriati, il nostro lavoro ha dimostrato che nel campo delle comunicazioni online e, in particolare, della messaggistica sicura, il rischio è relazionale e il *threat-model-*

*ling*[5] è fondamentale per scegliere lo strumento giusto per proteggere le proprie comunicazioni. Ad esempio, l'obiettivo principale di un utente può essere di dissimulare alcune delle sue attività online rispetto allo Stato, oppure proteggere le informazioni relative alle sue abitudini in quanto consumatore, e dunque «migrare» da piattaforme *closed-source* con modelli di business che siano basati sui dati degli utenti. L'«avversario» da cui proteggersi può assomigliare a una rete fluida in continua evoluzione che si collega con infrastrutture sia private che istituzionali, o ad un'unica entità con capacità ben definite e dotata di un insieme predeterminato di tecniche e strumenti di sorveglianza e attacco.

I formatori e le organizzazioni che operano per la sicurezza digitale si stanno orientando verso un approccio incentrato sull'utente e sessioni di formazione personalizzate. Allo stesso tempo, affrontano sempre più la sfida di comunicare in maniera adeguata agli individui che formano che gli strumenti di tutela della privacy e di miglioramento della protezione dei dati personali non garantiscono, di per sé, sicurezza assoluta. Le sfide crittografiche ancora irrisolte, come costruire soluzioni facilmente utilizzabili per la conservazione dei metadati, sono in qualche modo «compensate» da un mosaico di tecniche di sicurezza operativa e da una combinazione di strumenti che gli utenti inventano e modificano costantemente. Pertanto, l'identificazione di «da chi ci si deve nascondere» – ottenuta tramite *threat-modelling* e valutazione del rischio – è un processo in continua evoluzione che dipende da un ampio insieme di parametri spesso non tecnici o non crittografici, come il grafo sociale dell'utente (la sua rete di relazioni), genere, norme religiose o etiche, professione, situazione geopolitica/regime politico, e perfino la percezione della reputazione e del carisma dei creatori e sviluppatori dei sistemi di comunicazione. In effetti, la comunicazione crittografata è il prodotto, e talvolta il catalizzatore del cambiamento, di una vasta rete che include istituzioni (o attori che si confrontano o si oppongono ad esse) e, naturalmente, una miriade di infrastrutture e dispositivi tecnici in cui concetti come sicurezza e privacy sono incorporati.

La stessa distinzione tra utenti ad «alto» e «basso» rischio, sebbene operativamente utile per il ricercatore come strumento metodologico pratico per costruire un campione diversificato di utenti per le interviste, mostra i suoi

[5] Applicato al processo di sviluppo del software, il *threat-modelling* è definito come un «processo formale di identificazione, documentazione e mitigazione delle minacce alla sicurezza a un sistema software» (Oladimeji *et al.* 2006, pp. 13-15). Consente agli sviluppatori di esaminare l'applicazione «attraverso gli occhi di un potenziale avversario» al fine di identificare i principali rischi per la sicurezza. Tuttavia, i processi e le tecniche di *threat-modelling* vengono applicati anche agli agenti umani, al fine di trovare falle di sicurezza nei modelli di comportamento degli utenti (sia online che offline), identificare le informazioni sensibili «da proteggere», determinare potenziali avversari, valutarne le capacità e proporre soluzioni per la mitigazione e la protezione dei rischi.

limiti, principalmente a causa della natura relazionale del rischio. Se un utente a basso rischio ha almeno un utente ad alto rischio nel suo grafo sociale, può adottare un livello di protezione più elevato e persino installare uno strumento specifico per comunicare con questo contatto – e viceversa, in contesti sociopolitici specifici, quelle che sono solitamente comprese come informazioni a basso rischio/non sensibili possono infatti collocare le persone a cui fanno riferimento in categorie di rischio più elevato. In ultima analisi, se la progettazione di strumenti per il miglioramento della privacy richiede di immaginare il «peggiore di tutti i mondi possibili», questo potrebbe benissimo essere il mondo di un individuo tra i nostri contatti: la persona che ha più bisogno di dissimulare un'informazione, e talvolta, di nascondersi – virtualmente e fisicamente.

## *Strategie di occultamento come strumenti di integrità (e di potere)*

La crittografia è una questione controversa. Man mano che i nostri casi di studio si svolgevano, abbiamo potuto vedere come diversi team di sviluppatori – e, spesso, gli utenti dei sistemi che sviluppano – gestiscono lo status particolare dei dibattiti sulle politiche relative alla crittografia. Molto spesso, questi dibattiti contrappongono infatti una sicurezza collettiva o sistemica, assicurata dallo Stato a scapito delle libertà civili, e le nuove tecnologie di libertà che possono comportare rischi per tale sicurezza. Mentre i tecnologi, inclusi diversi sviluppatori e formatori di sicurezza, ritengono che senza crittografia il diritto alla privacy rimanga puramente teorico data la facilità di spiare le comunicazioni digitali, la crittografia è spesso definita nei dibattiti politici come un meccanismo che consente ai criminali di nascondere il contenuto delle loro comunicazioni da parte del sistema giudiziario e di polizia.

La nostra ricerca ci ha consentito di evidenziare diverse sfumature di questo dibattito, durante la nostra analisi del «*making of*» della crittografia e la sua interazione con i diritti e le libertà di Internet. Abbiamo osservato come la crittografia non venga utilizzata solo per nascondere informazioni, ovvero per rendere riservati i dati, ma anche per fornire controlli sull'integrità e l'autenticazione dei dati, anche pubblici. Ad esempio, per verificare che i dati non siano stati modificati accidentalmente o con cattive intenzioni, le funzioni *hash* – che riducono i dati ad un codice più sintetico, che può essere verificato indipendentemente – vengono utilizzate per verificare l'integrità dei dati. Tecniche crittografiche che possono essere apparentate a «segreti», chiamati chiavi private, possono essere proposte sia per autenticare che per crittografare i dati. Con le chiavi pubbliche e le funzioni *hash*, è possibile creare firme digitali per assicurarsi di conoscere l'identità dell'entità che origina dati particolari.

Questo approccio, ampiamente utilizzato nella messaggistica sicura, è utile in una varietà di scenari, compresi gli schemi di firma elettronica che possono aiutare a ridurre la burocrazia o prevenire la diffusione di informazioni false. Nasce così il dilemma che, nel campo della messaggistica sicura, è stato esemplificato dal caso *Federal bureau of investigation* (Fbi) contro Apple (Schulze 2017): se un governo attua una politica per ridurre la forza della crittografia in modo che la sua polizia o i suoi servizi di *intelligence* possano «leggere» messaggi digitali, vi è il chiaro pericolo che il governo impedisca accidentalmente altri usi della crittografia che danneggerebbero la capacità degli utenti di riporre fiducia nella circolazione e nell'elaborazione dei dati da parte di terzi, con conseguenze economiche negative di ampio respiro.

Per questo motivo, pur riconoscendo che le rispettive strategie dei team di sviluppatori in termini di scelta dell'architettura o dei processi di standardizzazione variano notevolmente, possiamo riconoscere una tendenza comune nelle diverse storie di sviluppo tecnologico che abbiamo esaminato: una forte resistenza ai tentativi, da parte dei regolatori, di rendere illegale la crittografia dei dati, per qualsiasi motivo. Gli attori nel campo della messaggistica sicura condividono la convinzione che la crittografia debba essere legale poiché le tecnologie digitali non solo aumentano le possibilità di sorveglianza, ma lo fanno in un modo fondamentalmente asimmetrico, incompatibile con la democrazia (vedi anche Bortzmeyer 2019); le piattaforme raccolgono molte informazioni su di noi, ma queste piattaforme sono opache per i cittadini e lo stesso problema vale per varie agenzie di *intelligence* statali; inoltre, tale trattamento dei dati avviene in massa.

## *L' «indebolimento selettivo» della crittografia*

La nostra osservazione dei processi di sviluppo di strumenti di messaggistica sicura come «pratiche localizzate» rivela tutti i limiti del presentare la crittografia principalmente come un meccanismo che impedirà agli stati e alle forze di polizia di condurre correttamente le loro indagini. Mentre seguivamo gli sviluppatori nel loro lavoro, abbiamo potuto vedere che dal loro punto di vista, la crittografia *end-to-end* – in cui gli *endpoint* sono gli utenti, e nessuna entità si frappone ed è dotata di capacità di decrittare il messaggio – intende restaurare una norma sociale di comunicazione privata, nelle modalità che le erano proprie prima dell'avvento della comunicazione digitale, in modo che la provenienza dei messaggi da un particolare mittente sia chiara, e che questi possano essere letti solo da un determinato destinatario, senza interferenze.

Con una rinascita post-Snowden (ad es. Barr 2016), ma che affonda le sue radici in dibattiti accademici e politici di lunga data (Rivest 1998; Sogho-

ian 2010), un'opzione politica fortemente dibattuta e controversa in materia di crittografia è stata ed è il suo «indebolimento selettivo», che consente sia l'uso della crittografia che la sua possibile violazione in casi specifici – ad esempio, in caso di indagine su un caso di terrorismo, l'idea di una *backdoor* per consentire la decrittazione dei messaggi criptati. Dal punto di vista dei tecnologi, questa disposizione è altamente problematica in quanto, indipendentemente dalla scelta dell'architettura tecnica, gli algoritmi matematici che costituiscono il nucleo della crittografia non possono funzionare solo in alcuni casi, ma non in altri: o consentono ai dati di essere accessibile da chiunque abbia la chiave, o hanno un difetto, che è dunque sfruttabile da chiunque ne sia a conoscenza – un argomento che è stato avanzato, in particolare, dal rapporto *Keys under doormats* (Abelson *et al.* 2015). Nelle proposte di *backdoor*, una chiave di decrittazione sarebbe la chiave del legittimo destinatario, ma esisterebbe un'altra chiave avendo il controllo di un *middlebox* che decritta il messaggio e lo re-cripta prima di consegnarlo destinatario previsto. Questa chiave sarebbe in regime di «*key escrow*», il che significa conservata da un terzo, come un'agenzia governativa, e disponibile solo in circostanze speciali. Tuttavia, una tale soluzione, per ragioni abbastanza chiare, non funzionerebbe nei progetti *open source* e di software libero, dove la revisione di qualsiasi codice mostrerebbe la *backdoor*. Potrebbe essere più realistica in contesti in cui l'utente non ha il controllo sul software che sta utilizzando e il software che gli viene fornito può includere la *backdoor* dall'inizio.

Come ha sottolineato uno degli sviluppatori che abbiamo intervistato, tuttavia, «ovviamente, qualsiasi entità che rappresenti una vera minaccia per lo stato non utilizzerà questi ultimi strumenti, ma [cercherà invece] software senza *backdoor*. Ma questo metodo può funzionare con il cittadino onesto che, a differenza del terrorista, si fida del software proprietario e che comunica con gli altri cittadini tramite le piattaforme della Silicon Valley». Quindi, dal punto di vista di questo sviluppatore e di altri tra i nostri intervistati, lo scopo delle campagne anti-crittografia e in favore delle *backdoor* non riguardano, o non riguardano principalmente, la ricerca di soluzioni che consentano alle autorità di decrittare a fini di antiterrorismo, ma sono un modo per fare pressione sulla Silicon Valley e altri attori tecnici affinché includano le *backdoor* nei loro software di comunicazione, al fine di abilitare e/o sostenere sistemi di sorveglianza di massa. La storia recente è utile in questo caso per ricordarci che, in un famigerato caso di sovversione di un ente normativo, il generatore di numeri pseudocasuali Dual Ec (usato per generare chiavi), ratificato dall'agenzia di normalizzazione statunitense Nist, aveva una *backdoor* collocata al suo interno dalla Nsa; questa *backdoor* è stata inserita nei router Juniper ed è stata successivamente sfruttata da un attore sconosciuto per compromettere

questi router e quindi installare la propria *backdoor* (Checkoway *et al.* 2016). In risposta a questo scenario, la Commissione europea ha riconosciuto nella sua recente strategia di sicurezza informatica (Commissione europea 2017) che la crittografia consente di esercitare le proprie libertà fondamentali, e organizzazioni per le libertà digitali come European digital rights (Edri) hanno affermato che, in quanto tale, la crittografia dovrebbe essere riconosciuto come uno strumento per contrastare l'arbitrarietà di alcuni Stati, e di alcuni attori privati in posizione dominante o di monopolio (Edri 2017).

## *Ricerca di standard e di equilibrio tra valori*

Gli sviluppatori di sistemi di messaggistica sicura, nella loro grande varietà, devono far fronte a diversi livelli di complessità. Il loro utilizzo della moderna crittografia e, il più delle volte, di protocolli formalmente verificati, ha lo scopo di ridurre i problemi di sicurezza (ad es. legati alle *backdoor*) e gli errori. Lavorano anche principalmente sul presupposto che la crittografia che sviluppano non debba necessariamente essere compresa dai decisori per essere implementata; come ha affermato uno dei nostri intervistati, «nessun decisore politico dovrebbe conoscere la differenza tra le proprietà Decisional Diffie-Hellman e Computational Diffie-Hellman». Condividono anche per lo più la comprensione del fatto che la privacy è «difficile da ottenere», a causa della varietà di contesti sociali coinvolti (si veda la precedente sezione dedicata). Sono consapevoli che affinché le nozioni di privacy siano significative e applicabili ai processi di sviluppo tecnologico, è necessario definire attentamente il threat-model ed eseguire simulazioni per misurare in modo empirico fenomeni come la prossimità. Infine, diversi sviluppatori sono consapevoli del fatto che per escludere la possibilità di *backdoor* nel proprio o in altri software, gli algoritmi e i protocolli che utilizzano la crittografia devono essere formalmente verificati o sottoposti ad audit da soggetti esterni. Tuttavia, per i motivi sopra menzionati, la privacy è più difficile da verificare effettivamente e non rientra nei quadri di verifica formali; quindi, è complicato determinare esattamente quali tipi di privacy vengano discussi e se un determinato sistema possa supportarla.

Sebbene gli sviluppatori non si aspettino, come detto, che i responsabili politici abbiano conoscenze crittografiche, operano in contesti nazionali e sovranazionali in cui la crittografia, e la capacità di comprometterla, è una questione intensamente politica se non un vero e proprio *proxy* dell'esercizio del potere – cosa che è sempre più vera dopo le rivelazioni di Snowden. Nel 2013, pochi mesi dopo le rivelazioni, fu rivelato che la Nsa aveva fatto pressioni discrete affinché il *National institute of standards and technology* (Nist) degli

Stati Uniti includesse un algoritmo indebolito, forse deliberatamente difettoso, in uno standard di crittografia del 2006 (Greenemeier 2013). E nel 2016, un gruppo del settore finanziario ha proposto un protocollo chiamato eTls, omettendo da esso la funzione di segretezza detta forward secrecy che era stata incorporata nell'ultima versione del protocollo *Transport layer security* (Tls). L'*European telecommunications standards institute* (Etsi) ha rilasciato eTls, poi ribattezzato Ets per ridurre al minimo l'ambiguità, come standard nell'autunno del 2018, con grande controversia (Leyden 2019) e ferma opposizione da parte dell'*Internet engineering task force* (Ietf).

Organismi di standardizzazione come l'Ietf e la sua organizzazione parallela, l'*Internet research task force* (Irtf), hanno dimostrato, nella controversia di cui sopra e in altre, di essere ben posizionati, tramite entità come il gruppo di ricerca CryptoForum fondato dall'Irtf, per emettere pareri autorevoli sulla sicurezza degli algoritmi crittografici. Tuttavia, ci sono altre importanti fonti esperte. In Europa, la promozione delle migliori pratiche nell'uso degli algoritmi crittografici pubblici, nella loro verifica e nella generazione di standard crittografici è stata intrapresa fino a tempi recenti dall'Agenzia dell'Unione europea per la cybersecurity (Enisa, che usa ancora questa sigla, in riferimento al suo nome originario); tuttavia ora questa funzione viene devoluta agli Stati, il che può comportare rischi (come discusso, pressioni per introdurre *backdoor* o livelli irregolari di conoscenza crittografica all'interno di diversi contesti nazionali).

Inoltre, sono in corso diversi dibattiti a livello nazionale nei paesi europei sulla crittografia *end-to-end*, e su come trovare un equilibrio tra la protezione dei diritti digitali e l'applicazione della legge. Nel 2017, il Consiglio digitale francese (Cnnum) ha emesso un parere esperto sulla crittografia, riaffermando l'utilità e la necessità delle tecnologie di crittografia alla luce dei ripetuti tentativi da parte del Ministero dell'Interno di contestarne l'uso a causa del loro potenziale sfruttamento da parte di terroristi e criminali (Cnnum 2017). Nel 2019 segnali nuovi e preoccupanti sono arrivati dalla Germania, dove, dopo oltre vent'anni di inequivocabile supporto ad una crittografia forte (Herpig e Heumann 2019), è allo studio una legge che obbligherebbe i provider di servizi di chat a consegnare, su domanda, conversazioni criptate *end-to-end* in testo normale; questa inclusione dei servizi Internet che forniscono software criptato amplierebbe in modo importante i poteri della legge tedesca, che attualmente consente «solamente» di ispezionare comunicazioni a partire dal dispositivo personale di un sospetto (telefono, computer, tablet; Chapman 2019). Nel Regno Unito, nell'ambito dei dibattiti sull'*Investigatory powers act*[6], il governo

[6] Una legge del Parlamento del Regno Unito (approvata nel 2016) che stabilisce ed amplia i poteri di sorveglianza elettronica dei servizi di *intelligence* e delle forze dell'ordine del paese.

ha emesso una versione rivista del disegno di legge che «chiarisce la posizione del governo sulla crittografia, stipulando che alle aziende può essere chiesto solo di rimuovere la crittografia che esse stesse hanno applicato, e solo dove è possibile farlo» (Carey 2016).

In risposta alla controversia sulla crittografia in Germania, Roman Flepp, sviluppatore di una piattaforma di messaggistica istantanea crittografata *end-to-end* con sede in Svizzera chiamata Threema, popolare tra gli utenti di lingua tedesca, ha affermato che: «In nessun caso siamo disposti a scendere a compromessi al riguardo» (citato in Chapman 2019). Tuttavia, come ha mostrato questa ricerca, la strada verso il «nessun compromesso» è in pratica, per gli sviluppatori di strumenti di messaggistica sicuri, lastricata di compromessi, alcuni dei quali riguardano scelte tecniche, altri il pubblico degli utenti a cui si rivolgono e altri ancora fanno riferimento agli scenari geopolitici più ampi e dibattiti in cui operano. Tali dibattiti continueranno senza dubbio poiché la crittografia rimane una questione di intensa preoccupazione pubblica, in cui i tecnologi sono attivamente coinvolti, sia nelle azioni che nelle parole.

## 5. Conclusioni

La governance di Internet, come suggerisce un corpus di lavori recente e sempre più dinamico, riguarda tanto il lavoro delle istituzioni e i processi legislativi, quanto le «pratiche quotidiane» e l'*agency* di progettisti, sviluppatori, hacker, manutentori e utenti mentre interagiscono, in modo distribuito, con tecnologie, norme e regolamenti, portando a conseguenze sia previste che non intenzionali con effetti sistemici (Epstein *et al.* 2016). Gli approcci Sts possono aiutare nell'analisi empirica delle diverse forme di attività decisionali e di coordinamento che si svolgono oltre confini formali e ben definiti (van Eeten e Mueller 2013).

Tale approccio è particolarmente rilevante in un momento in cui la sorveglianza e la privacy online, e i mezzi tecnologici e legali per limitare la prima e proteggere la seconda, vengono identificati (ad es. da Mueller e Badiei 2020) come una delle questioni pre-eminenti dell'ultimo decennio legate alla governance di Internet. La questione è stata senz'altro spinta ulteriormente alla ribalta dalle rivelazioni di Snowden, ma ha le sue radici in dibattiti di lunga data su dati personali, identità su Internet e crittografia. Probabilmente, l'era inaugurata dalle rivelazioni di Snowden è quella in cui il mondo ha preso piena misura della portata dell'autorità globale esercitata di fatto dagli Stati Uniti, tramite le infrastrutture digitali, su Internet, e in cui è diventato consapevole della profondità dei «legami pericolosi» tra il governo degli Stati Uniti ed in-

termediari privati (Musiani 2013). Ciò ha aperto una grave crisi di legittimità per gli Stati Uniti per continuare a fungere da attore principale nella governance di Internet e probabilmente – anche se il processo era, lentamente ma inesorabilmente, già in corso prima di Snowden – ha contribuito alla cosiddetta «transizione Iana» (dall'acronimo dell'*Internet assigned numbers authority*), il processo attraverso il quale gli Stati Uniti hanno ceduto il controllo della radice del *Domain name system* (Dns) e che ha portato a sostanziali riforme nei meccanismi di responsabilità utilizzati nella sua gestione dall'Internet corporation for assigned names and numbers (Icann). Gli ultimi anni hanno anche assistito all'ascesa di nuove superpotenze nella governance di Internet, in particolare Russia e Cina, la cui strategia predominante è stata quella di raggiungere, in modi diversi, la «sovranità digitale» (Musiani 2022).

In questo multiforme scenario contemporaneo che è la governance di Internet, la crittografia sta diventando una questione centrale. L'analisi dei protocolli e delle applicazioni di messaggistica sicura, man mano che sono sviluppati e fatti propri da diversi gruppi di utenti pionieri, permette di chiarire i molteplici modi in cui la crittografia è «fatta, utilizzata e governata», contribuendo ad articolare e consolidare lo studio delle «pratiche quotidiane» della governance di Internet. Allo stesso tempo, queste pratiche si sviluppano in un continuo intreccio con le arene istituzionali in cui si svolgono le narrazioni politiche e si costruiscono le priorità di regolazione sulla crittografia. Le istituzioni della governance di Internet possono e devono, a loro volta, essere analizzate con l'ausilio degli Sts, che possono aiutare a comprendere l'autorità ed il potere da esse esercitati non come un fatto compiuto, ma come risultato della loro capacità di riconfigurarsi e negoziare la loro identità nei momenti di controversia e destabilizzazione, al fine di mantenere il loro dinamismo e la loro legittimità (Flyverbom 2011; Pohle 2016).

La crittografia può e deve essere compresa come materia di studio completamente interdisciplinare, prerogativa tanto delle scienze sociali quanto dell'informatica e degli studi giuridici, svelando le dimensioni formali e informali degli accordi di potere che la circondano. Dimensioni che sono, entrambe, fondamentali nel co-costruire i nostri diritti e le nostre libertà – come cittadini e comunicatori digitali, e come parti interessate di come Internet è governato oggi e sarà governato domani.

## Riferimenti bibliografici

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schil-

ler, J. I., Schneier, B., Specter, M. e Weitzner, D. J. (2015), *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, MIT CSAIL Technical Report, July 2015, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Agre, P. (2003), *Peer-to-Peer and the Promise of Internet Equality*, in «Communications of the ACM», 46(2), pp. 39-42.

Barr, A. C. (2016), *Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment*, in «Minnesota Law Review», 101(1), pp. 301-339.

Bortzmeyer, S. (2019), *Cyberstructure: L'Internet, un espace politique*, Caen, C & F Éditions.

Carey, S. (2016), *The Snooper's Charter Still Has an Encryption Problem: Parliament Continues to Grapple with End-to-End Encryption in the Investigatory Powers Bill*, in «Computerworld», 19 luglio, https://www.computerworld.com/article/3427168/the-snooper-s-charter-still-has-an-encryption-problem--parliament-continues-to-grapple-with-end-to-e.html.

Chapman, C. (2019), *Mozilla Pens Open Letter to German Policymakers Over Planned Encryption Law*, in «The Daily Swig», 14 giugno, https://portswigger.net/daily-swig/mozilla-pens-open-letter-to-german-policymakers-over-planned-encryption-law.

Checkoway, S. (2016), *A Systematic Analysis of the Juniper Dual EC incident*, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 468-479, doi: 10.1145/2976749.2978395.

Cnnum (2017), *Prédictions, chiffrement et libertés*, Report, Settembre, https://cnnumerique.fr/files/2017-10/CNNum_avis_prédiction_chiffrement_libertés_sept2017.pdf.

Coleman, G. (2005), *The Social Construction of Freedom in Free and Open Source Software: Hackers, Ethics, and the Liberal Tradition*, PhD Thesis, Chicago, The University of Chicago.

Coleman, E. G. e Golub A. (2008), *Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism*, in «Anthropological Theory», 8(3), pp. 255-77.

Commissione europea (2017), *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*, Report, 13 settembre, https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF.

Deibert, R. J. e Crete-Nishihata, M. (2012), *Global Governance and the Spread of Cyberspace Controls*, in «Global Governance: A Review of Multilateralism and International Organizations», 18(3), pp. 339-61.

DeNardis, L. e Hackl, A. M. (2015), *Internet Governance by Social Media Platforms*, in «Telecommunications Policy», doi: 10.1016/j.telpol.2015.04.003.

DeNardis, L. e F. Musiani (2016), *Introduction: Governance by Infrastructure*, in F. Musiani, D. L. Cogburn, L. DeNardis e N. S. Levinson (a cura di), *The Turn to Infrastructure in Internet Governance*, New York, Palgrave Macmillan, pp. 3-21.

Edri (2017), *Encryption Workarounds. A Digital Rights Perspective*, Position Paper, https://edri.org/files/encryption/workarounds_edriposition_20170912.pdf.

Eeten, M. Van e Mueller, M. (2013), *Where is the Governance in Internet Governance?*, in «New Media & Society», 15(5), pp. 720-736.

Epstein, D., Katzenbach, C. e Musiani, F. (2016), *Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions, Special issue*, in «Internet Policy Review», doi:10.14763/2016.3.435.

Ermoshina, K. e Musiani, F. (2022), *Concealing for Freedom: The Making of Encryption, Secure Messaging, and Digital Liberties, Manchester*, Mattering Press.

Flyverbom, M. (2011), *The Power of Networks: Organizing the Global Politics of the Internet*, Cheltenham, Edward Elgar Publishing.

Greenemeier, L. (2013), *NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard*, Scientific American, 18 settembre, https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/.

Hellegren, Z. I. (2017), *A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom*, in «Internet Histories», 1(4), pp. 285-311.

Herpig, S. e Heumann, S. (2019), *The Encryption Debate in Germany, International Encryption Brief*, Carnegie Endowment for International Peace, 30 maggio, https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215.

Hintz, A., Dencik, L., e Wahl-Jorgensen, K. (2018), *Digital Citizenship in a Datafied Society*, Cambridge, Polity Press.

Leyden, J. (2019), *EFF Condemns Financial Think-Tank for Promoting «Weaker» Crypto*, The Daily Swig, 28 febbraio, https://portswigger.net/daily-swig/eff-condemns-financial-think-tank-for-promoting-weaker-crypto.

Mager, A. (2012), *Algorithmic Ideology: How Capitalist Society Shapes Search Engines*, in «Information, Communication & Society», 15(5), pp. 769-787.

Milan, S. e ten Oever, N. (2017), *Coding and Encoding Rights in Internet Infrastructure*, in «Internet Policy Review», doi: 10.14763/2017.1.442.

Milan, S., e van der Velden, L. (2018), *Reversing Data Politics: An Introduction to the Special Issue*, in «Krisis: Journal for Contemporary Philosophy», 1, pp. 1-3.

Monsees, L. (2019), *Crypto-Politics. Encryption and Democratic Practices in the Digital Era*, Abingdon and New York, Routledge.

Mueller, M. L. e Badiei, F. (2020), *Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field*, in L. DeNardis, D. L. Cogburn, N. S. Levinson and F. Musiani (a cura di), *Researching Internet Governance: Methods, Frameworks, Futures*, Cambridge, The MIT Press, pp. 59-83.

Mueller, M. L., Kuehn, A. e Santoso, S. M. (2012), *Policing the Network: Using DPI for Copyright Enforcement*, in «Surveillance & Society», 9(4), 348-364.

Muir, S. (2011), *Multisited Ethnography*, in D. Southerton (a cura di), *Encyclopedia of Consumer Culture*, London, Sage.

Musiani, F. (2022), *Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-based Sociology of Digital Self-determination Practices*, in «Information, Communication & Society», 25(6), pp. 785-800.

Musiani, F. (2013), *Dangerous Liaisons? Governments, Companies and Internet Governance*, in «Internet Policy Review», doi: 10.14763/2013.1.108.

Myers West, S. (2018), *Cryptographic Imaginaries and the Networked Public*, in «Internet Policy Review», doi: 10.14763/2018.2.792.

Oladimeji, E. A., Supakkul, S. e Chung, L. (2006), *Security Threat Modeling and Analysis: A Goal-Oriented Approach*, in Proceedings of the 10th IASTED International Conference on Software Engineering and Applications (SEA), pp. 13-15.

Oudshoorn, N. e Pinch, T. (2005), *How Users Matter: The Co-Construction of Users and Technology*, Cambridge, The MIT Press.

Pohle, J. (2016), *Multistakeholder Governance Processes as Production Sites: Enhanced Cooperation «in the Making»*, in «Internet Policy Review», doi: 10.14763/2016.3.432.

Pohle, J. e Van Audenhove, L. (2017), *Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change*, in «Media and Communication», 5(1), pp. 1-6.

Ponterotto, J. G. (2006), *Brief Note on the Origins, Evolution, and Meaning of the Qualitative Research Concept Thick Description*, in «The Qualitative Report», 11(3), pp. 538-549.

Rivest, R. L. (1998), *The Case against Regulating Encryption Technology*, in «Scientific American», 279(4), pp. 116-117.

Schulze, M. (2017), *Clipper Meets Apple vs FBI: A Comparison of the Cryptography Discourses from 1993 and 2016*, in «Media and Communication», 5(1), pp. 54-62.

Snowden, E. (2019), *Permanent Record*, New York, Henry Holt and Company.

Soghoian, C. (2010), *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, in «Journal on Telecommunications and High Technology», 8, pp. 359-424.

Ziewitz, M. (2016), *Governing Algorithms: Myth, Mess, and Methods*, in «Science, Technology and Human Values», 41(1), pp. 3-16.