DigitCult | Scientific Journal on Digital Cultures

La nostra sicurezza e la privacy dei criminali
Lo scontro tra gli Stati e i giganti del digitale

Enrico Pedemonte
Zerozerouno.news

Abstract

Le piattaforme digitali applicano codici crittografici inviolabili e non vogliono fornire accesso alle forze dell'ordine per difendere la privacy. Ma in questo modo lasciano spazio alle reti della criminalità e dei pedofili. Ora persino un potente servizio segreto Usa riconosce che queste aziende stanno diventando più potenti dello Stato. E propone loro un patto. Vogliamo davvero che lo Stato abdichi il suo ruolo di controllo?

Our Security and Privacy of Criminals.
The Clash between States and the Digital Giants

Digital platforms apply inviolable cryptographic codes and do not want to provide access to the police to defend privacy. But in this way they leave room for crime and pedophile networks. Now even a powerful US secret service recognizes that these companies are becoming more powerful than the State. And he proposes them a deal. Do we really want the state to abdicate its controlling role?

Published 30 December 2019

Correspondence should be addressed to Enrico Pedemonte, zerozerouno.news. Email: enrico.pedemonte@gmail.com

DigitCult, Scientific Journal on Digital Cultures is an academic journal of international scope, peer-reviewed and open access, aiming to value international research and to present current debate on digital culture, technological innovation and social change. ISSN: 2531-5994. URL: http://www.digitcult.it

 doi:10.4399/97888255301551

Con il Volume 4 numero 3 si inaugura la collaborazione tra il journal DigitCult e il blog "Zerozerouno - un blog sui nuovi poteri digitali" http://zerozerouno.news diretto da Paolo Bottazzini e Enrico Pedemonte. In ogni nuovo numero del journal, nella sezione "Provocations and Dialogues", Zerozerouno pubblicherà un articolo che approfondirà uno dei temi affrontati dal blog, suggerendo ulteriori letture. Su DigitCult, dove accademici ed esperti verranno invitati a dialogare sul tema specifico. Sul blog Zerozerouno, dove il lettore potrà trovare ulteriori articoli e prospettive di analisi.

Introduzione

Il problema può essere visto da diverse prospettive. Per esempio quella di un agente dell'antiterrorismo che vuole dare un'occhiata a quello che c'è dentro il vostro cellulare, per verificare se avete contatti con l'Isis. O quella di un giudice che indaga su una rete di pedofili e chiede di sbirciare dentro i vostri messaggi Whatsapp.

Ma ci sono altri punti di vista. Per esempio quello di un cittadino così diffidente nei confronti dello Stato da pretendere che il suo cellulare sia inviolabile. E quello delle aziende hi-tech che vogliono mettere sotto chiave l'intero sistema delle comunicazioni.

L'argomento può apparire un po' astruso perché ha a che fare con un problema – la crittografia – tecnicamente complesso. Ma in realtà è semplice e si può riassumere in una domanda chiara come il vetro: è giusto che il nostro cellulare sia inviolabile?

Intorno a questa domanda è in corso una battaglia che va avanti da trent'anni: protagonisti principali, lo Stato e la Silicon Valley. Ma a questo punto – con l'avvento della tecnologia 5G – è diventato così urgente e strategico – come vedremo - da spingere i vertici della NSA (la National Security Agency) a scrivere un lunghissimo appello sul New York Times per invitare le grandi aziende tecnologiche a collaborare con lo Stato. Perché la rapidità con cui evolve l'innovazione tecnologica non sta solo mettendo a rischio i cittadini, ma sta anche mutando la stessa forma della società, indebolendo drammaticamente il ruolo dello Stato rispetto ai privati. E questo non è un problema solo americano: ci riguarda tutti.

Ma andiamo con ordine e facciamo qualche passo indietro..

1994, l'anno del Clipper Chip

È il 1994, Bill Clinton è presidente da appena un anno e si cimenta in una scelta che si dimostra subito impraticabile: annuncia l'approvazione del Clipper Chip, cioè di un microprocessore, progettato dalla NSA, il servizio segreto più segreto d'America, che dovrebbe consentire al governo una via d'accesso alle comunicazioni cellulari dei cittadini[1].

Il problema è sul tappeto da anni e angustia i servizi segreti e le forze dell'ordine. I telefoni mobili sono ancora grandi come un mattone, ma si prevede che in pochi anni potranno essere infilati in tasca, costeranno poche decine di dollari e saranno più diffusi dei computer. I servizi segreti sono preoccupati perché le tecniche di crittografia consentono ormai – grazie alla tecnica delle "due chiavi" inventata negli anni Settanta – comunicazioni praticamente inviolabili: un regalo ai delinquenti e ai terroristi che potranno comunicare impunemente.

La soluzione suggerita dalla Nsa è un microchip inattaccabile da chiunque ma accessibile alle forze dell'ordine – con l'autorizzazione di un giudice – attraverso una backdoor, un termine utilizzato per indicare una porta secondaria di accesso grazie a una chiave segreta. Il progetto prevede di distribuire molte migliaia di cellulari di questo tipo, a un prezzo molto scontato, in modo da imporre questa tecnologia come standard universale sul mercato.

Ma è una strategia ingenua, destinata al fallimento. Contro il Clipper Chip si schierano non solo molti conservatori ma anche una parte dei parlamentari democratici, oltre alle associazioni per i diritti civili, il mondo della Silicon Valley e i cyberpunk, che sono pochi ma fanno molto

[1] https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

rumore. Per il presidente Clinton, che interviene personalmente in difesa del Clipper Chip, è una sconfitta che brucia.

Il problema resta aperto. La crittografia è un problema di sicurezza nazionale, strettamente legato alla sicurezza degli arsenali nucleari. Per l'NSA è stato il primo punto all'ordine del giorno fin dalla sua fondazione, nel 1952. Sono tecnologie top secret, la cui esportazione è stata fin qui proibita. Fino a pochi anni prima l'NSA dominava il settore e aveva a libro paga quasi tutti gli esperti del ramo. Ma quel monopolio è ormai un ricordo e gli esperti in materia si sono moltiplicati anche nel privato (soprattutto al Mit e nelle aziende della Silicon Valley) e non considerano più un dovere patriottico collaborare con i servizi segreti.

A proposito del Clipper Chip il direttore dell'Fbi dichiara, durante un'audizione al Congresso: "Conservare la capacità di intercettare legalmente le comunicazioni è oggi il problema principale delle forze dell'ordine e della sicurezza nazionale". E Stewart A. Baker, consigliere legale della NSA, spiega al New York Times: "In una decina d'anni avremo telefoni che costeranno 75 dollari e ognuno di questi avrà un bottone per comunicare in modo criptato con qualunque altro telefono: improvvisamente scopriremo che il nostro intero sistema di comunicazione sarà usato in modo profondamente antisociale".

Era il 1994, ma era già chiaro quello che sarebbe successo. E una ventina di anni dopo il problema riemerge in modo ancora più clamoroso.

2015, accade a San Bernardino

È il 2 dicembre 2015. Alle 11 del mattino Syed Farook e sua moglie Tashfeen Malik, cittadini americani di origine pakistana, entrano all'Inland Regional Center, un centro sociale per disabili di San Bernardino, in California[2].

Sono armati e mascherati. In pochi minuti uccidono 14 persone e ne feriscono 24, tra cui due poliziotti. Poi fuggono ma vengono uccisi a due chilometri dal luogo della strage in uno scontro con le forze dell'ordine. La polizia irrompe nella loro abitazione e scopre che i due avevano distrutto sia i cellulari sia il computer. Sull'auto di Farook trovano un iPhone, ma la polizia non riesce ad accedervi: è un Ios8, commercializzato nel 2014 con una campagna di marketing che ne garantisce l'assoluta impenetrabilità. Neanche la Apple può rompere il codice crittografico che lo protegge: almeno, questo è quanto dichiara la casa di Cupertino.

L'Fbi chiede aiuto ad Apple per rompere il codice crittografico dell'iPhone: ci sono ragioni di sicurezza nazionale. Apple risponde picche.

Allora l'Fbi ricorre alla magistratura e un giudice emette una sentenza che – in teoria – dovrebbe obbligare Apple a obbedire, accusando l'azienda di anteporre la sua strategia di marketing rispetto a un'inchiesta sul terrorismo. Infatti Apple promuove se stessa come la "privacy company" in alternativa ad altre società digitali, come Google e Facebook, che campano sui dati degli utenti.

Per essere precisi, la polizia non chiede di essere aiutata a forzare il codice, ma chiede ad Apple di creare un nuovo sistema operativo, con una backdoor che consenta all'azienda, nel caso in cui il magistrato lo chieda – di accedere ai dati e consegnarli alle forze dell'ordine. Ma il rifiuto di Apple è netto: è una delle società più capitalizzate al mondo (in quel momento vale 600 miliardi di dollari, oggi vale il doppio) e non teme uno scontro diretto con lo Stato.

Quel giorno appare evidente come l'interesse pubblico (la lotta contro la criminalità) stia divergendo da quello delle piattaforme digitali che forniscono servizi agli utenti.

A marzo il presidente Obama interviene personalmente schierandosi a favore dell'FBI, in un discorso che molti giudicano storico, al South by Southwest Festival di Austin (Texas), di fronte a oltre duemila imprenditori nel settore tecnologico che lo ascoltano in un imbarazzato silenzio. Obama dice: "Se da un punto di vista tecnologico è possibile costruire un sistema impenetrabile, con una crittografia così potente da non poter essere in nessun modo craccata, come possiamo arrestare i pedofili? Come possiamo individuare un complotto terroristico?". (https://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html)

Anche Obama, come Clinton ventidue anni prima, esce sconfitto da questa sfida.

D'altra parte, neppure all'interno della sua amministrazione esiste consenso sulla questione. Il ministro della Difesa Ashton Carter, per esempio, si dichiara favorevole all'uso di sistemi di crittografia inviolabili, memore di quanto aveva fatto Edward Snowden, che nel 2013 –

[2] https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

 doi:10.4399/97888255301551

quando era contrattista della CIA - aveva diffuso documenti top secret della NSA. Da parte sua Snowden, in un'opinione pubblicata dal New York Times[3], afferma che "la sicurezza delle comunicazioni su Internet è più importante delle esigenze delle forze dell'ordine".

Se si vuole tracciare un confine rozzo tra i due schieramenti, si può dire che la Silicon Valley, i liberal e le associazioni in difesa per i diritti civili, stanno dalla parte di Apple, mentre i conservatori e le forze dell'ordine si schierano con la polizia.

I due fronti usano tutti gli argomenti possibili in una battaglia muro contro muro.

Il procuratore generale di Manhattan Cyrus Vance dice di avere 205 iPhones solo nel suo ufficio che aspettano di essere craccati per fornire informazioni su indagini in corso, molte delle quali sui cartelli della droga e su reti di pedofili.

Apple risponde che l'atteggiamento del governo è pericoloso e poco lungimirante: se l'azienda capitolasse negli Usa, dovrebbe farlo anche in Cina e in altri paesi autoritari, consegnando ai governi le chiavi per accedere ai cellulari degli oppositori.

Ma presto il braccio di ferro si conclude, forse anche perché l'Fbi non vuole esacerbare lo scontro. L'agenzia rivela di avere trovato una soluzione per accedere al telefonino di Farook: le è costato 1,3 milioni di dollari, forse il prezzo pagato a un'azienda specializzata che ha individuato un baco nel software di Apple, ma si tratta solo di voci. Alcuni analisti scrivono che forse quello dell'FBI è stato solo un avvertimento alle aziende di Silicon Valley, affinché queste non mettano in campo tecnologie ancora più inviolabili. Ma è come fermare il vento con le mani.

Recentemente Zuckerberg ha ribadito di voler criptare i video e le telefonate sui propri social suscitando l'ira di molte autorità di controllo e riaccendendo la discussione sulla crittografia end-to-end[4].

La battaglia va avanti, tra mille contraddizioni.

È contraddittorio il comportamento di Facebook, che oggi progetta di estendere da Whatsapp a tutte le altre sue applicazioni la crittografia end-to-end in nome del rispetto della privacy: proprio lei che per anni ha venduto la privacy degli utenti ai propri inserzionisti (e per questo ha subito multe miliardarie)[5].

Ed è contraddittorio il comportamento del governo americano che per anni ha finanziato applicazioni inviolabili, per garantire la sicurezza delle agenzie statali e la libertà di parola nei paesi autoritari e ha regalato quelle applicazioni a ogni sorta di criminali.

È il caso di Tor, che consente di navigare sul web in modo anonimo: era stato sviluppato negli anni Novanta da un gruppo di tecnici del US Naval Research Laboratory per proteggere le comunicazioni online dei servizi di intelligence e oggi è largamente usato dai cartelli della droga e dalle reti di pedofili per navigare sul "dark web" e sfuggire a ogni controllo.

Un altro esempio è ChatSecure, progettato grazie a un finanziamento del Congresso Usa (sette milioni di dollari) per consentire ai cittadini di comunicare liberamente all'interno dei paesi autoritari: il software – scaricabile liberamente dal web - si diffuse rapidamente tra i movimenti di protesta in Iran, Egitto, Libia, Tibet, ma presto è diventato uno dei sistemi più consigliati e utilizzati dalla Jihad[6].

Uno, due, cento Internet

Lo scontro che si è acceso negli Stati Uniti a partire dagli anni Novanta viene affrontato con minor clamore in altri paesi del mondo. Australia e Gran Bretagna, per esempio, hanno approvato leggi che dovrebbero rendere più facile per le forze dell'ordine obbligare le aziende hi-tech consegnare le informazioni in loro possesso. L'India sta considerando una legge per dare alle autorità accesso ai dati di WhatsApp all'interno dei confini nazionali. Ma per ora si tratta di dichiarazioni teoriche, facili da applicare quando le informazioni richieste sono all'interno delle cloud, più difficili da perseguire quando hanno a che fare con servizi (come Whatsapp) a cui è applicata una crittografia end-to-end. Per ora Facebook si è limitata a

[3] https://www.nytimes.com/2015/06/05/opinion/edward-snowden-the-world-says-no-to-surveillance.html
[4] https://www.socialmediatoday.com/news/facebook-launches-next-steps-in-full-messaging-encryption-plan/566695/
[5] https://www.reuters.com/article/us-facebook-ftc/facebook-to-pay-record-5-billion-us-fine-over-privacy-faces-antitrust-probe-idUSKCN1UJ1L9
[6] https://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096

rispondere che un approccio simile "comprometterebbe la privacy dei cittadini e ci obbligherebbe a riprogettare il software"[7].

Diverso il caso della Cina che recentemente ha approvato una legge per regolare l'uso della crittografia che entrerà in funzione il primo gennaio 2020. La legge crea tre categorie di crittografia: per i documenti top secret, quelli semplicemente segreti e quelli commerciali. Tutte e tre dovranno essere approvate e autenticate dal governo che potrà accedere a qualunque documento in caso di emergenza[8]. Quest taglia corto con le polemiche occidentali su Facebook (che in Cina non c'è) e apre un problema con Apple. Ma qui entriamo in un altro contesto, quello degli Stati autoritari che proprio per i problemi di controllo (e di censura) legati alla rete stanno spezzando l'Internet mondiale in diversi sottoinsiemi regolati da diverse norme.

Libertà o impunità?

Ma torniamo al mondo libero, con il suo delicato problema di coniugare la libertà dei cittadini con il controllo dello Stato.

Negli ultimi mesi la questione è riemersa in modo vigoroso grazie ad alcuni dati sulla circolazione di materiali particolarmente inquietanti nella rete: nell'ultimo anno le compagnie hi-tech hanno rintracciato online e segnalato alle forze dell'ordine circa 45 milioni di foto o video contenenti abusi sessuali: il 90 per cento sui social legati a Facebook (di cui due terzi sul Messenger)[9].

Le posizioni delle associazioni per le libertà civili non si sono ammorbidite. Erica Portnoy, della Electronic Frontier Foundation, ha dichiarato che le comunicazioni devono consentire lo stesso livello di privacy di cui godiamo nel salotto di casa: "Il Dipartimento di Giustizia vorrebbe mettere una telecamera nel salotto di ciascuno di noi per prendere pochi pedofili".

Ma è sensato voler applicare al web le stesse norme che si applicano al nostro salotto? Infatti le legge prevede che, con il permesso della magistratura, la polizia possa installare cimici nelle abitazioni. Perché Internet deve essere una terra di nessuno che offre ai criminali possibilità di agire inesistenti nel mondo reale? Fernando Ruiz Pérez (direttore dell'European Cybercrime Center dell'Europol) ha dichiarato che se Facebook applicherà la crittografia end-to-end a tutti i suoi prodotti "svanirà la possibilità di segnalare le immagini che descrivono abusi sessuali".

Cosa cambia con il 5G

Ma le discussioni fin qui descritte potrebbero presto apparire vecchie di fronte al cambiamento radicale ormai dietro l'angolo: il decollo delle tecnologie 5G nel 2020, una svolta che non è stata ancora abbastanza elaborata né dalla politica né dall'opinione pubblica.

Per spiegarla in modo elementare, si può dire che il 5G rappresenta un salto notevole rispetto alle tecnologie attuali (3G e 4G) perché consente di operare a frequenze più alte, offre una banda più larga e promette di essere la tecnologia appropriata per la prossima generazione di applicazioni digitali che connetteranno gli oggetti della nostra vita quotidiana, le auto che si guidano da sole, i macchinari industriali. Il numero di informazioni raccolte sul territorio – e memorizzate nei cloud delle grandi aziende digitali – crescerà di diversi ordini di grandezza. È difficile prevedere l'impatto reale di una tecnologia che non c'è ancora: nessuno può immaginare quali nuovi servizi nasceranno a vantaggio della nostra qualità di vita e quali abusi saranno perpetrati.

Le implicazioni di questa svolta appaiono così profonde da spingere la NSA a far pubblicare un lungo intervento sul New York Times (il 10 settembre)[10] per chiedere alle aziende di Silicon Valley un'alleanza in nome della sicurezza nazionale. Più che una richiesta sembra una preghiera, in ginocchio.

[7] https://www.wsj.com/articles/apple-and-facebook-fighting-international-encryption-battle-11551177000
[8] https://thediplomat.com/2019/10/decoding-chinas-cryptography-law/
[9] https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html
[10] https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html

 doi:10.4399/97888255301551

L'intervento è firmato da Glenn S. Gerstell, uno dei direttori della NSA, ma è ragionevole pensare che sia stato soppesato, parola per parola, da tutto il vertice del servizio segreto e probabilmente anche da diversi esponenti del governo centrale.

Vale la pena di seguire il suo ragionamento perché, se si può dissentire sulla terapia proposta, è difficile non essere d'accordo con la diagnosi.

Il futuro descritto da Gerstell è popolato da reti di sensori, network, algoritmi, macchie guidate da sistemi di intelligenza artificiale: quello che in gergo viene definito "Internet delle cose" che, insieme a molti vantaggi per la nostra vita, presenta anche molti lati oscuri. È un mondo sempre più interconnesso dove tutti i servizi messi a disposizione dalla modernità, dalle reti per l'energia ai sistemi di telecomunicazione, potranno essere attaccati in ogni momento.

Gerstell dice che "dobbiamo prepararci a un mondo di incessante cyberconflitto in ogni aspetto della nostra vita quotidiana e commerciale". Gli strumenti per attaccarci saranno nelle mani di una miriade di delinquenti comuni o gruppi di terroristi, e non più solo di pochi Stati.

In questo mondo, secondo Gerstell, il rapporto tra Stato e privati sarà alterato in un modo molto profondo a favore dei secondi perché il governo avrà sempre meno la leadership in molte aree della sicurezza nazionale. Già oggi – ammette Gerstell – le agenzie legate al Pentagono non sono più all'avanguardia nell'informatica e nella progettazione di algoritmi perché l'eccellenza si è spostata verso alcuni laboratori universitari e, soprattutto, verso le aziende della Silicon Valley.

Gerstell ammette che il settore privato ha già (e sempre più avrà) a disposizione una messe di dati sui singoli individui enormemente superiore rispetto a quello che il governo ha mai potuto o potrà ottenere. E i venditori di antivirus ne sanno di più, su quello che accade su Internet, di quanto possa sapere qualunque agenzia di sorveglianza.

(Questa osservazione la dice lunga sui cambiamenti avvenuti nell'opinione pubblica, che per decenni si è inalberata per l'intrusività dello Stato nella propria vita, e oggi non mostra alcuna reazione tangibile di fronte alla raccolta quotidiana di dati da parte dei privati).

Di fronte a questo scenario lo Stato – secondo Gerstell - non può fare altro che piegarsi all'inedito potere delle aziende digitali private, che però devono accettare di diventare parte integrante dei sistemi di sicurezza pubblica, fornendo al governo le informazioni sui crimini che avvengono in rete. Gerstell non cita la parola crittografia, ma è ovvio che è quello il suo obiettivo principale.

Gerstell va oltre e le sue grida di allarme rasentano il catastrofismo. Dice che che Internet può avere un effetto pernicioso sulle democrazie perché chiunque, soprattutto alcuni Stati stranieri, possono far circolare informazioni per ingannare i sistemi di analisi degli Stati democratici. Anche a causa di questa continua opera di disinformazione le agenzie di governo – e i governi stessi - trovano sempre più difficile riscuotere fiducia nella popolazione. L'abuso delle tecnologie digitali può creare un clima generale di incertezza, e può minare le alleanze internazionali, che sulla fiducia reciproca sono basate.

In questo scenario un drammatico punto di discontinuità potrebbe manifestarsi il giorno in cui i computer quantistici diventassero realtà, con la loro immensa potenza di calcolo e la loro capacità di rompere qualunque protezione basata sulla crittografia. Gerstell mette sull'avviso sul rischio che sia la Cina ad avere la leadership nel settore, con toni che ricordano quelli usati dal governo americano negli anni Quaranta, quando si temeva che i tedeschi arrivassero per primi alla bomba atomica. Allora il governo chiese aiuto agli scienziati più prestigiosi, oggi – attraverso Gerstell - porge la mano alle aziende più potenti, riconoscendo loro uno statuto speciale ma invocando il ruolo guida dello Stato. In pratica dice: alleiamoci, forniteci i dati che siete in grado di raccogliere, consentiteci di entrare nei cellulati dei delinquenti e in cambio vi aiuteremo a conservare i vostri primati finanziando le vostre ricerche che sono di fondamentale importanza per la sicurezza collettiva.

Chi comanda?

Molti hanno paragonato i toni dell'intervento di Gerstell a quelli usati dall'amministrazione Bush dopo l'attentato dell'11 settembre 2001: la volontà di alzare il livello di allerta per spingere le piattaforme tecnologiche a una santa alleanza in nome della sicurezza nazionale. Ma nella sua lettera al New York Time, ci sono diversi altri spunti che fanno riflettere e che vanno ben oltre la dinamica interna ai Poteri forti di quel paese.

La prima, e più importante, è che lo Stato (anche lo Stato più potente del mondo) si sente disarmato di fronte all'impetuosa crescita dei colossi digitali che sfuggono ormai al controllo

dell'autorità centrale. Lo scontro sull'accesso ai codici crittografici, in una società sempre più irrorata da informazioni digitali in ogni sua articolazione, sta diventando la chiave per capire se esisterà ancora un'autorità di controllo, soggetta ai governi democratici, o se il controllo passerà ai consigli di amministrazione di alcune aziende.

Vogliamo che sia lo stato democratico, controllato dai cittadini, a regolare lo sviluppo di tecnologie così importanti, o lo Stato deve passare la mano rinunciando al proprio primato nel determinare l'evoluzione delle norme sociali? E ancora: è sensato che alcune aziende stiano diventando così potenti da suggerire l'interrogativo precedente? Dobbiamo fare qualcosa per fermarle?

 doi:10.4399/97888255301551

Bibliografia

Shearer, Jenny, e Peter Gutmann. "Government, Cryptography, and the Right To Privacy" in *Journal of Universal Computer Science (J.UCS), Volume 2, No.3 (Marzo 1996)* https://www.cs.auckland.ac.nz/~pgut001/pubs/jucs96.pdf

Falk, Courtney. *The Ethics of Cryptography*. Available at https://www.researchgate.net/publication/237217965_The_Ethics_of_Cryptography

Rogaway, Phillip The Moral Character of Cryptographic Work, 2015. Available at https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Commissione Europea, *Ethics and data protection*, 14 novembre 2018. Available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf