Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza

Categories : Istituzioni e regole

Tagged as : Giorgio Resta, Menabò n. 38

Date : 29 Febbraio 2016

1. *Hard cases,* si sa, *make bad law.* La controversia che vede contrapposti il governo USA e la società Apple ha tutti gli elementi del 'caso difficile'. Da un lato troviamo l'interesse di un'impresa, che ha costruito la sua reputazione commerciale (anche) sull'elevato livello di sicurezza dei propri sistemi informatici e sulla promessa di rispetto della *privacy* degli utenti, e a cui viene ora ingiunto di elaborare un *software* capace di 'aggirare' il dispositivo criptografico posto a garanzia dell'inviolabilità dei suoi prodotti. Dall'altro v'è l'interesse, altrettanto legittimo, alla corretta amministrazione della giustizia, e in particolare alla repressione dei reati, peraltro in questo caso particolarmente efferati. Da un lato, dunque, un interesse alla segretezza e all'integrità dei sistemi informatici, che, pur vantato da Apple per ragioni economiche, si espande indirettamente sino a coprire il pubblico indifferenziato dei consumatori, i quali confidano sull'alto livello di protezione dei prodotti tecnologici prescelti. Dall'altro un interesse all'accesso, fatto valere dagli organi inquirenti e, per il loro tramite, dai familiari delle vittime della strage di San Bernardino e dall'intera cittadinanza. Tale è la rilevanza delle posizioni in gioco, che il conflitto ha assunto immediatamente una visibilità globale, dividendo equamente l'opinione pubblica tra i 'favorevoli' e i 'contrari' all'ordine di decriptazione emesso dal giudice federale Sheri Pym lo scorso 16 febbraio. Essendo fuor di dubbio che si tratti di un *hard case,* è possibile affermare che la soluzione adottata integri un *bad law*? I tempi sono certo prematuri per offrire una risposta univoca a un siffatto interrogativo, da un lato perché l'ordine è stato emesso *ex parte,* cioè in assenza di contradditorio, e Apple non ha ancora spiegato le proprie difese (quindi i fatti non possono ritenersi chiariti); dall'altro, perché è probabile che la controversia, ove l'ordine in esame sia confermato, approdi sui banchi della Corte Suprema USA. Non lo sono, invece, per iniziare a ragionare in maniera più distaccata sulle questioni giuridiche coinvolte e sulle loro implicazioni.

2. L'intera vicenda ha origine all'indomani della strage di San Bernardino (CA), allorché Syed Rizwan Farook e la moglie uccisero 14 persone e ne ferirono gravemente 23 in un centro per disabili, rimanendo a loro volta uccisi, al momento della fuga, nel conflitto a fuoco con la polizia. Nell'autovettura impiegata dai terroristi, fu ritrovato un iPhone, il quale fu debitamente sequestrato previo regolare mandato giudiziario. Tuttavia, il suo contenuto risultò inaccessibile, in ragione del particolare sistema di protezione adottato dalla Apple. Questo consiste nell'applicazione combinata del codice di 4 cifre, stabilito dall'utente al primo utilizzo del telefono, e di una chiave crittografica. A fronte delle 9.999 combinazioni possibili, gli attuali elaboratori elettronici riuscirebbero in pochi secondi a individuare il codice corretto. Tuttavia il sistema operativo Apple concede solo 10 tentativi inesatti di accesso, dopo di che si innesta automaticamente il *reset* del dispositivo, che determina la cancellazione di tutti i dati dello *smartphone*. Inoltre, è previsto un lasso di attesa minimo tra ogni tentativo di accesso, che cresce progressivamente, sino a raggiungere la durata di un'ora con il nono tentativo. Di conseguenza, mentre è stato possibile per gli investigatori acquisire i dati di traffico e (dalla stessa Apple) le informazioni di *backup* conservate in iCloud, i contenuti digitali del telefono sono risultati inaccessibili.

Falliti i tentativi di collaborazione in via ufficiosa, il governo USA si è rivolto alla corte distrettuale federale del Central District (CA), al fine di ottenere un ordine di *facere* in capo alla società di Cupertino. A questa veniva richiesto di prestare ausilio tecnico al fine di violare il sistema di protezione del suddetto iPhone, e

segnatamente di mettere a disposizione degli inquirenti un *software* in grado di disabilitare la funzione di auto-cancellazione dei dati e eliminare il tempo di attesa minimo tra ogni successivo reinserimento delle combinazioni. Tali domande sono state integralmente accolte dal giudice Sheri Pym, con un provvedimento di poche righe, lo scorso 16 febbraio [*In the Matter of the Search of an Apple iPhone*, n. ED 15-0451M, U.S. D.C., Centr. D. Ca., Feb. 16, 2016]. Apple ha la facoltà di opporsi a tale provvedimento, dimostrando che esso sia "irragionevolmente oneroso".

È importante soffermarsi sulla base normativa addotta a sostegno del suddetto ordine di *facere.* Si tratta dell'*All Writs Act*, un testo legislativo originariamente integrato nella sect. 14 del *Judiciary Act* del 1789, che autorizza la Corte Suprema e tutte le altre corti federali ad emettere "tutti i provvedimenti necessari o appropriati in ausilio delle rispettive giurisdizioni e conformi agli usi e ai principi generali del diritto". L'indeterminatezza del dettato legislativo ne ha reso particolarmente problematica l'attuazione pratica ed ha richiesto vari interventi chiarificatori delle corti. La Corte Suprema, in particolare, ha precisato che la concessione di un *writ* 'atipico' sia possibile ogniqualvolta ciò sia necessario "per assicurare l'attuazione, o prevenire l'aggiramento, di ordini precedentemente emanati nell'esercizio di prerogative giurisdizionali conferite da altre norme" [*U.S. v. New York Tel. Co*., 434 U.S. 159, 172 (1977)]. Di conseguenza, tale base normativa non può essere invocata al fine di estendere la competenza delle corti, o di fondare autonomi poteri d'azione, ma presuppone la sussistenza di una norma primaria attributiva della giurisdizione [J. Steinman, *The Newest Frontier of Judicial Activism: Removal under the All Writs Act,* in 80 *Boston U. L. Rev.* 773, 780 (2000)]. Ancora, si è stabilito che a tale disposizione non potrebbe farsi ricorso per arricchire in via interpretativa una disciplina legislativa, introducendo in maniera surrettizia un rimedio che il Congresso aveva intenzionalmente omesso di prevedere [*Pennsylvania Bureau of Correction v. US Marshal Services,* 474 U.S. 34, 43 (1985)].

Quest'ultimo punto risulta particolarmente rilevante per la controversia in questione, poichè il *Communications Assistance for Law Enforcement Act* del 1994, a differenza di quanto espressamente previsto dall'analoga normativa britannica (cfr. sect. 49 del *Regulation of Investigatory Powers Act*), pur prevedendo l'obbligo per i providers di telecomunicazioni di adottare sistemi *surveillance-friendly,* non aveva conferito all'autorità giudiziaria il potere di ordinare coattivamente la decriptazione di un messaggio cifrato [B.M. Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption,* 75 *Brooklyn L. Rev.* 345 (2009)]. In seguito sono stati presentati diversi disegni di legge volti a colmare tali lacune e a estendere i poteri d'intercettazione anche alle nuove forme di comunicazione digitale, come le piattaforme multimediali o i servizi VoIP. Tuttavia tali proposte non hanno avuto seguito, sicché la questione della 'decriptazione coattiva' è stata di fatto integralmente rimessa in capo alle corti.

Il problema che è stato più frequentemente dibattuto, con esiti alterni, concerne i limiti di ammissibilità degli ordini volti a ottenere le chiavi di decriptazione direttamente dai soggetti indagati; di tali ordini si è, infatti, frequentemente predicata l'illiceità per contrasto con le garanzie contro l'auto-incriminazione poste dal Quinto Emendamento [J. Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment,* 24 *Public Interest L. J.* 53 (2015)].

L'altra questione che è recentemente emersa è quella della legittimità degli ordini rivolti a un soggetto terzo, detentore di particolari informazioni o *expertise* tecnologica. È questo, in particolare, il caso della società Apple, in quanto produttore dei dispositivi, come l'iPhone, inaccessibili da parte di chi non conosca le chiavi di decriptazione.

Si deve notare che la questione della legittimità di tali ordini di decrittazione non si pone oggi per la prima volta. Già nell'ottobre 2015, il governo USA aveva presentato un'analoga istanza di fronte ad altra corte distrettuale, quella dell'Eastern District New York, al fine di ottenere, lo sblocco dell'iPhone di un supposto trafficante di droga, Jun Feng. In tal caso il giudice Orenstein, differentemente da quanto ora deciso dal giudice Pym, ha negato la concessione *ex parte* dell'ordine, instaurando un contradditorio sulla

proporzionalità del rimedio [*In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court,* n. 15-mc-1902 (U.S. D.C., East. Dist. N.Y., Oct. 9, 2015)].

Tre ordini di circostanze osterebbero, secondo la corte, all'applicabilità dell'*All Writs Act*: *a*) Apple, diversamente dalle compagnie di telecomunicazione, non esercita un pubblico servizio, ma è un soggetto privato, libero di "attribuire maggior peso all'interesse alla *privacy* dei consumatori rispetto a quello del *law enforcement*"; *b*) Apple non è il proprietario dell'apparecchio sequestrato; *c*) l'*All Writs Act* non può essere invocato per esercitare un potere che "il Congresso ha scelto di non concedere".

Se ne desume che la base giuridica invocata a sostegno di tali ordini di decrittazione è alquanto incerta e controvertibile. Inoltre, a conferma della rilevanza meta-soggettiva degli interessi fatti valere dall'opponente, si deve notare che sia l'*American Civil Liberties Union*, sia l'*Electronic Frontier Foundation*, sono intervenute nel procedimento in veste di *amici curiae*, presentando una memoria a sostegno di Apple. La decisione finale del giudice Orenstein, sollecitata in punto di diritto dalle stesse parti, è attesa per le prossime settimane.

3. Il caso *U.S.A. v. Apple* costituisce, quindi, un caso di altissimo profilo, che può contribuire a far chiarezza circa il rapporto tra garanzie del giusto processo, integrità dei sistemi informatici e libertà d'impresa nell'era dei *big data*. L'assenza di orientamenti giurisprudenziali condivisi in materia di "decrittazione coattiva", assieme alla consapevolezza della particolare rilevanza delle questioni coinvolte, suggeriscono di guardarsi dalle tesi di chi vorrebbe ridurre l'intera questione ad un netto conflitto tra 'stato' e 'mercato', o, all'opposto, tra 'società della sorveglianza' e 'diritti di libertà'. *Apple* rappresenta un caso 'difficile', come lo sono molti altri casi recenti, che hanno posto all'attenzione dell'interprete la questione cruciale dell'impatto delle tecnologie della sorveglianza sulle garanzie dei diritti di libertà. Come tale, gli interessi in gioco meritano di essere valutati e ponderati con attenzione.

Si deve riconoscere, ad esempio, che un siffatto ordine di decriptazione non suscita le stesse obiezioni di principio a suo tempo avanzate nei confronti dei programmi di sorveglianza di massa della NSA [su cui v. F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* 78 *Law & Cont. Prob's* 101 (2015)]. Qui, infatti, siamo al cospetto di un ordine puntuale (e non generalizzato), emanato da una corte 'ordinaria' (e non speciale, né operante in segreto, come il Foreign Intelligence Surveillance Court), e non troppo dissimile, nella sostanza, da altri ordini di esibizione rivolti alle banche o ai fornitori di servizi di telecomunicazione.

D'altra parte, vi sono alcuni elementi che inducono a tenere nella massima considerazione gli argomenti avanzati da chi si opponga alla logica della 'decriptazione coattiva'. In primo luogo appare problematica la base normativa invocata a sostegno dell'ordine giudiziale: come si è detto, la concessione di un rimedio in base all'*All Writs Act* presuppone la sussistenza di una serie di requisiti, tra i quali anche l'assenza di una "eccessiva onerosità" in capo al suo destinatario, alquanto controvertibili nel caso in esame. Peraltro non deve sottovalutarsi il profilo della ripartizione di competenze tra poteri dello stato, ben presente alla giurisprudenza sull'*All Writs Act*: su un tema così delicato, che coinvolge i diritti fondamentali dei cittadini e delle imprese, sarebbe opportuno invocare un intervento del legislatore, che valuti attentamente costi e benefici di ciascuna opzione regolatoria. In secondo luogo, non può ignorarsi il problema, di carattere prettamente tecnologico, derivante dalla predisposizione di un *software* in grado di violare il dispositivo di protezione. Mentre il governo ritiene che sia possibile elaborare un programma in grado di sbloccare il *singolo* apparecchio, senza compromettere l'integrità di tutti gli altri dispositivi della stessa serie, Apple contesta tale assunto, sostenendo che, una volta elaborato un sistema di decrittazione, esso apra una porta d'ingresso (*back door)* potenzialmente suscettibile di usi illimitati. Su questo punto, evidentemente, il giurista deve invocare l'ausilio di altre discipline, e in primo luogo dell'informatica. In terzo luogo, v'è un problema di ordine più generale relativo all'effetto di precedente di una decisione favorevole. Come escludere che, una volta affermato il principio dell'obbligo di

decrittazione, questo non venga poi invocato in maniera seriale, magari sotto l'egida del secreto, come avvenuto nell'ambito del programma PRISM?

Si tratta, evidentemente, di questioni complesse, per le quali è indispensabile un dibattito pubblico informato e trasparente. La lettera aperta di Tim Cook costituisce un'acuta mossa di *marketing,* che risponde a una precisa strategia commerciale di Apple. E tuttavia è innegabile che essa abbia contribuito in maniera decisiva a innescare una riflessione articolata, e non limitata alle frontiere statunitensi, sui temi in esame.