ISSN 2037-6677

Apple v. FBI: i valori costituzionali in gioco

di Giulio Enea Vigevani

1 – Molto rumore per nulla? Nel febbraio 2016, un frastuono di voci si era alzato dopo che l'amministratore delegato di Apple Tim Cook aveva reagito - con una lettera aperta ai propri clienti[1]- all'ordine di un giudice del Distretto Centrale della California, che aveva imposto all'azienda di Cupertino di aiutare l'FBI a decrittare lo smartphone di un terrorista[2].

Si preannunciava una battaglia giudiziaria campale, destinata a finire sul tavolo della Corte Suprema, tra le istituzioni politiche e la più nota e celebrata tra le *tech companies*, con in gioco una posta particolarmente alta: la sicurezza della Nazione per il Governo, l'integrità dei sistemi informatici che proteggono la privacy dei consumatori per Apple.

Due squadre sembravano già formarsi nel mondo della politica, del diritto e degli informatici, nonché nella stessa società, non solo in America: da un lato, chi riteneva che l'interesse, di rilievo costituzionale, alla prevenzione e alla repressione di

[1] T. Cook, *A Message to Our Customers*, consultabile all'indirizzo <www.apple.com/customer-letter/ (16 febbraio 2016)>.

[2] Il provvedimento del giudice Sheri Pym del 16 febbraio 2016, *In the Matter of the Search of an Apple iPhone*, n. ED 15-0451M, U.S. D.C., Centr. D. Ca. Feb. 16, 2016, è consultabile all'indirizzo <www.documentcloud.org/documents/2714001-SB-Shooter-Order-Compelling-Apple-Asst-iPhone.html>.

reati gravissimi dovesse in sé prevalere su interessi di natura prevalentemente commerciale; dall'altro chi avvertiva che si sarebbe creato un pericoloso precedente, che estendeva a dismisura i poteri dell'amministrazione nei confronti di cittadini e imprese.

Dopo circa un mese, il 28 marzo 2016, la questione si è risolta quasi nell'ombra, quando alcuni funzionari del Governo federale dichiararono di essere riusciti, con l'aiuto di una società specializzata, a decrittare il dispositivo. Di conseguenza, il Dipartimento della Giustizia degli Stati Uniti decise di abbandonare la causa[3].

La vicenda, pur nota, merita una breve sintesi: nelle indagini successive alla strage di San Bernardino del dicembre 2015, gli inquirenti rinvennero un iPhone 5-C di un attentatore, il cui contenuto era protetto da una password di quattro cifre. Tale versione è programmata per distruggere automaticamente i dati che custodisce, dopo alcuni tentativi andati a vuoto di accedere al dispositivo. Per evitare tale eventualità, che avrebbe privato la polizia di una possibile fonte di spunti investigativi circa i movimenti e i contatti precedenti e successivi alla strage, l'FBI chiese a Apple di disabilitare le misure di sicurezza installate sul telefono e, in particolare, la funzione di auto-distruzione dei dati.

La società dichiarò di non essere in grado di collaborare, come pure avvenuto in casi non dissimili in passato. Infatti, anche a seguito delle rivelazioni di Edward Snowden, che fecero conoscere l'esistenza di programmi governativi segreti di sorveglianza e di intercettazioni di massa[4], Apple aveva introdotto nei propri sistemi operativi più recenti nuove misure di sicurezza, che essa stessa non poteva eludere o violare. Dunque, ogni ipotesi di collaborazione informale con l'FBI era impedita dallo sviluppo tecnologico, che rendeva "unreasonably burdensome" il comportamento richiesto.

---

[3] Per un dettagliato resoconto si rinvia a <www.digitaltrends.com/mobile/apple-encryption-court-order-news/#ixzz4B5m8QWLK>; nonché a M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in corso di pubblicazione in F. Pizzolato, P. Costa, (a cura di), collettanea dei *Quaderni di diritto dell'economia* del Dipartimento di sc. ec.-az. e diritto per l'economia dell'Università degli studi di Milano-Bicocca, Milano, Giuffré, 2016.

[4] Su tale vicenda si rinvia a F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *Federalismi.it* (26 giugno 2013) e a L. P. Vanoni, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e datagate: Security v. Privacy*, in *Federalismi.it* (27 febbraio 2015).

Di fronte al rifiuto di cooperazione dell'azienda californiana, il Dipartimento di Giustizia ottenne dal *U.S. Magistrate Judge* della *U.S. District Court* del *Central District* della California Sheri Pym l'emissione *ex parte*, ovvero in assenza di contradditorio, di un *Order* che imponeva ad Apple un "facere", ossia creare un *software* che consentisse l'accesso alla memoria dell'iPhone in questione. In pratica, si trattava di realizzare una "porta di servizio" che neutralizzasse il meccanismo di cancellazione dei dati e consentisse alla polizia federale di cercare senza limiti la password.

L'ordinanza fu emessa sulla base dell'*All Writs Act* del 1789, una antica legge federale che autorizza le corti federali a emettere «tutti i provvedimenti necessari o appropriati in ausilio delle rispettive giurisdizioni e conformi agli usi e ai principi generali del diritto»[5]. Tale normativa attribuisce al giudice ampi poteri per assicurare che le sue decisioni siano adempiute, tra cui *inter alia*, secondo l'interpretazione della Corte Suprema, quello di chiedere l'assistenza tecnica di terzi, purché vi sia una relazione tra la materia e il destinatario dell'atto e l'intervento sia necessario e non si risolva in un sacrificio eccessivamente gravoso[6].

La lettera di Tim Cook è, come accennato, la reazione a questa ordinanza. Secondo Apple, allo stato della tecnica non esiste la possibilità di fornire un sistema che "apra" un solo apparecchio; ciò che essa potrebbe fornire è una sorta di *passe-partout* per l'accesso a tutti i dispositivi in commercio. E questo non vuole farlo[7]. L'azienda, che sta andando nella direzione opposta, ovvero quella di realizzare strumenti dotati di impostazioni sulla privacy che nemmeno il produttore possa eludere, non intende creare un *software* che permetta di spiare ogni attività effettuata, ogni comunicazione inviata e ricevuta e ogni movimento di ogni singolo

[5] Sulla portata e i limiti di tale rimedio, si rinvia a D.D. Portnoi, *Resorting to Extraordinary Writs: How the All Writ Act Rises to Fill the Gaps in the Right of Enemy Combatants*, in *NY Law Rev.*, vol. n. 83, 2008, pp. 293 ss. e a G. Resta, *Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza*, in <www.eticaeconomia.it/il-caso-usa-v-apple-e-il-dilemma-dei-diritti-nella-societa-della-sorveglianza/> (29 febbraio 2016), il quale ultimo sottolinea che «L'indeterminatezza del dettato legislativo ne ha reso particolarmente problematica l'attuazione pratica ed ha richiesto vari interventi chiarificatori delle corti». In particolare, Giorgio Resta ricorda che «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)]».

[6] *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172-3 (1977), per la quale si rinvia alla approfondita analisi di Marco Orofino in questa stessa *Rivista*.

[7] Un ingegnere di Apple ha paragonato tale ordine a quello rivolto a un costruttore di case a cui si chieda la chiave per entrare nell'abitazione del proprietario all'insaputa di questi.

possessore di iPhone. Tale *passe-partout* sarebbe massimamente pericoloso se finisse in possesso di Stati autoritari o di criminali. Ma anche nelle mani della democratica amministrazione americana, conclude Cook, la chiave anti-privacy costituirebbe una minaccia «*a quelle stesse libertà che il nostro governo ha il compito e il dovere di proteggere*». Dunque, secondo l'amministratore di Apple, è più che mai necessario aprire un pubblico dibattito per far comprendere ai cittadini le conseguenze sulla sfera dei diritti individuali che un precedente di tal genere potrebbe determinare.

Sul piano giudiziario, Apple, supportata dalle maggiori società informatiche, che intervennero in qualità di *amici curiae*, presentò il 25 febbraio un atto[8] con il quale richiedeva di revocare l'ordinanza del giudice Sheri Pym[9]. L'udienza, fissata per il 22 marzo, fu rinviata su richiesta del Governo che, qualche giorno dopo, annunciò che il sistema di sicurezza era stato superato e che dunque rinunciava all'azione.

Forse non estranea alla scelta dell'amministrazione di abbandonare il caso è stata la decisione di un altro giudice, James Orenstein della *District Court* dell'*Eastern District* di New York, che il 29 febbraio 2016, dunque nel mezzo della battaglia legale che si svolgeva in California, ha respinto un'analoga richiesta governativa di concessione di un ordine *ex parte*, sempre nei confronti di Apple, di decrittazione di un cellulare di un soggetto implicato in un'indagine sul traffico di droga. Il giudice Orenstein ha ritenuto infatti che la misura richiesta violasse il principio di separazione dei poteri, sottolineando come il Congresso avesse in passato preso in esame proposte di legge che avrebbero consentito la concessione dell'*Order*, ma non le avesse mai approvate; dunque l'*All Writs Act* «cannot be a means for the executive branch to achieve a legislative goal that Congress has considered and rejected»[10].

---

[8] *Apple Inc's Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search, and Opposition to Governement's Motion to Compel Assistance* (C.D. Cal. Feb. 25, 2016), consultabile in https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf.

[9] Per una ampia analisi di tale atto difensivo, cfr. A. Serena, Apple v. FBI*, or the Role of Technology on the Functioning of the Law*, in <www.medialaws.eu/apple-v-fbi-or-the-role-of-technology-on-the-functioning-of-the-law/> (Law and Media Working Paper Series no. 3/2016), pp. 2 ss.

[10] *In Re Order requiring Apple Inc. to assist in the execution of a search warrant issued by the court*, *Memorandum and Order*, James Orenstein, Magistrate Judge, U.S. District Court, Eastern District of New York (Brooklyn), 1:15-mc-1902 (JO), February 29, 2016, p. 26. Su tale controversia, si v. A. Serena, Apple v. FBI*, or the Role of Technology on the Functioning of the Law*, cit., pp. 3-4 e M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea* , cit.

Tale decisione fu impugnata dal Dipartimento della Giustizia, ma anche tale caso fu infine abbandonato, dopo che si riuscì a sbloccare altrimenti il dispositivo.

2. – La questione alla base del caso *Apple v. FBI* era se ed entro quali limiti una Corte federale potesse imporre ai fabbricanti di cellulari di aiutare la polizia a sbloccare dispositivi il cui contenuto è protetto attraverso la crittografia. Tale questione, a prima vista tutta interna all'ordinamento statunitense, affascina e turba lo studioso delle Costituzioni, anche europeo, per più di un motivo.

In primis, *Apple v. FBI* è un caso che concerne l'equilibrio tra sicurezza e sfera privata delle persone.

Il dilemma "sicurezza v. privacy" è noto. La tecnologia oggi ha la possibilità di fornire al potere strumenti che consentono un controllo davvero capillare delle "vite degli altri". Dunque, la misura della sorveglianza sugli individui non è più una questione tecnica ma in primo luogo politica e costituzionale. Da un lato, vi è uno Stato che, invocando le esigenze di lotta alla criminalità e specie al terrorismo internazionale, in modo quasi paternalistico chiede a tutti i "cittadini onesti", di sacrificare la segretezza dei propri dati per un bene superiore. Dall'altra, vi è una accresciuta consapevolezza che una progressiva estensione di forme di controllo generalizzate, attraverso il "*data mining*", finisce con il mortificare la libertà e la dignità dei cittadini. Dunque, lo scontro tra giustizia americana e Apple può inquadrarsi nel secolare conflitto ideale e politico tra la tendenza degli inquirenti a superare ogni impedimento che ostacoli l'individuazione dei colpevoli dei reati più gravi e l'esigenza di protezione della sfera di libertà della persona, fisica e giuridica[11].

Al contempo, costituisce un assaggio di una battaglia che si combatterà nelle aule di giustizia, all'interno del conflitto che forse sta maggiormente connotando il XXI secolo, quello appunto tra privacy e sicurezza o, forse meglio, tra sicurezza e libertà dell'individuo da un lato e sicurezza collettiva dall'altro. E l'esito di tale conflitto finirà con l'incidere non solo sulla relazione tra Stato e individuo, ma altresì

[11] Sul tema, si rinvia al bel saggio di L. P. Vanoni, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e datagate: Security v. Privacy*, cit. L'Autore, interrogandosi sul possibile giusto equilibrio tra *privacy* e *security* nell'era del terrorismo digitale, osserva che: «*Come testimonia la storia americana, la risposta a queste domande non è univoca, e segue un andamento costante che vede ampliarsi considerevolmente i poteri del Governo ogni volta che la minaccia terroristica è più pressante, per comprimersi a vantaggio della privacy una volta che essa diventa meno attuale*», p. 34.

sul rapporto di forza tra il sovrano del XX secolo, lo Stato nazionale, e i soggetti che più sembrano insidiare tale predominio, ovvero i giganti delle comunicazioni della West Coast americana[12].

Il caso *Apple v. FBI* sembra confermare l'emergere di un conflitto sempre più palese tra gli interessi dell'amministrazione pubblica e quelli dei giganti della comunicazione; questi ultimi, infatti, hanno ormai acquisito la consapevolezza che la collaborazione con l'*intelligence* nella lotta al terrorismo tecnologico ha un costo non irrisorio sul piano dell'immagine. Infatti, la reputazione delle *tech companies* si fonda sempre più «sull'elevato livello di sicurezza dei propri sistemi informatici e sulla promessa di rispetto della privacy degli utenti»[13], che attraverso lo smartphone compiono buona parte delle loro attività quotidiane, dalle operazioni bancarie alla gestione dei file personali. In questo quadro, non appare irrealistico ritenere che i le grandi società dell'elettronica avranno un ruolo nel decidere quali diritti umani siano effettivamente meritevoli di protezione e che saranno anche le contrattazioni tra Stati e queste ultime a definire paese per paese l'intensità della tutela dei diritti fondamentali.

Il caso suggerisce altre riflessioni sul rapporto tra i poteri e tra questi e i cittadini.

Apple v. FBI pone in luce il tema del bilanciamento tra *national security* e *cybersecurity*, tra l'interesse degli investigatori ad accedere ai sistemi informatici, anche attraverso la collaborazione di terzi, e la legittima aspettativa dei singoli che le misure di sicurezza che proteggono i loro dati personali non siano violate sistematicamente[14].

---

[12] Andrea Serena sottolinea acutamente come «*this trial can be seen as a manifestation of the endless fight between East Coast code (legal regulatory design) and West Coast Code (environmental regulatory design), between the governmental agencies from Washington, D.C. and the tech companies from Silicon Valley, in a battle that will shape our fundamental rights in the future*»; A. Serena, Apple v. FBI, *or the Role of Technology on the Functioning of the Law*, cit., p. 6.

[13] G. Resta, *Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza*, cit., p. 1.

[14] Così Peter Swire, che in un'intervista pubblicata su techpolicy.com (<www.techpolicy.com/Blog/February-2016/Peter-Swire-Says-It-s-a-Case-of-National-Security.aspx>) definisce esplicitamente la questione una «*security issue, not a privacy issue*», aggiungendo altresì che «*The ethical concern is we use phones the way we use laptops; we use them for our banking, we use them for our most important activities in life. And our laptops now can routinely be encrypted by default. And Apple and Google now do phones encrypted by default. And if we break that, then we're breaking the fundamental security of our banking system, of our corporate secrets, of our personal security around all our communications*».

Il caso solleva poi più di un dubbio circa il rispetto del I Emendamento della Costituzione americana che, *inter alia*, impedisce ai pubblici poteri di costringere a parlare chi non vuole. Secondo la giurisprudenza[15], anche i *software* rientrano nella sfera protetta dalla libertà di espressione e dunque l'obbligo a carico di Apple di crearne uno nuovo che neutralizzi il suo protocollo di crittazione costituisce «a compelled speech and viewpoint discrimination in violation of the First Amendment»[16].

Apple v. FBI coinvolge poi anche il profilo della divisione dei poteri tra legislativo e giudiziario[17]. Nel caso in esame non pare priva di senso l'opinione di chi ha sostenuto che il giudice abbia quasi voluto rinvenire a tutti i costi, frugando nelle pieghe più nascoste della legislazione, strumenti che consentissero di rispondere all'emergenza terroristica, dilatando l'ambito di applicazione dell'*All Writs Act* e ampliando le competenze delle corti federali. Si assiste, in altri termini, a una sorta di supplenza del potere giudiziario, che si sostituisce a un Congresso che discute da tempo, senza decidere, sull'estensione del potere dei giudici di ordinare a terzi di collaborare alla decrittazione di dati.

In questa prospettiva, qualora la posizione del giudice Orenstein del *New York District* finisca con l'affermarsi, dovrà essere il legislatore ad assumersi la responsabilità di individuare le regole in materia di decrittazione coattiva, tenendo in conto anche i diritti di cittadini e imprese, senza lasciare alle corti la risoluzione di una questione che è ad alto contenuto politico[18]. Come bene osserva Monica Bonini, «non modificare l'AWA esclude il legislatore federale da ogni decisione relativa, senza risolvere il problema a monte dell'intera questione: la sicurezza (intesa come bene giuridico che, non entrando nel bilanciamento perfetto con i diritti

[15] D. J. Bernstein et al., v. U.S. Department of State et al. 176 F.3d 1132 (9th Cir. May 6, 1999), citato in A. Serena, Apple v. FBI, *or the Role of Technology on the Functioning of the Law*, cit., pp. 4-5.
[16] Cfr. A. Serena, Apple v. FBI, *or the Role of Technology on the Functioning of the Law*, cit., pp. 4-5.
[17] Sulla questione, si vedano le articolate riflessioni di M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, cit., la quale pone il dubbio che «*il Governo degli Stati Uniti si sia rivolto alla magistratura per evitare il confronto democratico e l'eventuale legge federale adottata nel pieno rispetto delle garanzie procedimentali fornite dall'iter parlamentare*».
[18] Per il dibattito federale e statale su una nuova legislazione in materia di crittografia, si rinvia al già menzionato saggio di Marco Orofino in questa *Rivista*.

costituzionali, in modo solo limitato può limitarli) può essere garantita esclusivamente nel rispetto della separazione dei poteri»[19].

Apple v. FBI è, infine, un caso che riguarda la legittimazione del potere. Un noto studioso del diritto della rete, Yochai Benkler, ha osservato che: «The showdown between Apple and the FBI is not, as many now claim, a conflict between privacy and security. It is a conflict about legitimacy». Egli ritiene, infatti che «Apple's design of an operating system impervious even to its own efforts to crack it was a response to a global loss of trust in the institutions of surveillance oversight. It embodied an ethic that said: "You don't have to trust us; you don't have to trust the democratic oversight processes of our government. You simply have to have confidence in our math"»[20]. In altri termini, senza un chiaro impegno delle istituzioni democratiche a realizzare un sistema di potere trasparente e a rendere conto dei propri comportamenti, i cittadini troveranno rifugio nelle tecnologie.

E tale crisi di fiducia negli organi di governo non pare certo una questione solo americana. Anche in Europa vi sono segnali di crisi dell'ideale del "governo del potere pubblico in pubblico" che connota la democrazia moderna[21]. Lo sviluppo della rete aveva illuso molti che si sarebbero determinate una sempre maggiore trasparenza e *accountability* nell'azione dei pubblici poteri. Le emergenze securitarie tendono invece, da un lato, a favorire il ritorno degli *arcana imperii* e, dall'altro, a giustificare intrusioni nella sfera privata proprio attraverso l'uso delle tecnologie.

Di qui l'impressione – forse non ingiustificata – di un controllo pervasivo, da parte di uno Stato percepito come ostile, di comunicazioni, movimenti, contatti e più in generale di tutti i dati ricavabili dai cellulari di ultima generazione. In altri termini, cittadini insicuri dell'effettività della protezione costituzionale della loro privacy e della loro proprietà, confidano maggiormente nella tecnologia che nelle leggi e nelle istituzioni preposte al rispetto delle stesse e chiedono ai colossi informatici di tutelare la loro sfera personale contro il loro stesso Stato.

---

[19] M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, cit.

[20] Y. Benkler, *We cannot trust our government, so we must trust the technology*, in <www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi> (22 febbraio 2016).

[21] N. Bobbio, *Il futuro della democrazia*, Torino, 1995, pp. 86 ss.

E di qui l'obbligo per gli Stati democratici di garantire quantomeno il diritto dei cittadini di conoscere l'entità dei sacrifici ai diritti individuali richiesti a ciascuno a garanzia della sicurezza collettiva, senza che i cittadini vivano nel timore di essere sorvegliati in ogni attività quotidiana. In assenza di trasparenza, non sembra inverosimile che le *tech companies* diverranno sempre più i soggetti cui si rivolgeranno gli utenti in cerca di protezione.

3. – Apple v. FBI resta senza dubbio, con le parole di Giorgio Resta, un *hard case*[22], sul piano legale e tecnologico, con in gioco una pluralità di interessi di rilievo costituzionale.

Ma la novità più rilevante è costituita, forse, dai protagonisti di questo scontro: non lo Stato e i suoi cittadini ma il potere statuale e un altro potere non meno forte, ovvero una grande multinazionale che gestisce dati a livello globale. Ed è probabile che il comportamento di Apple nella vicenda non sia stato ispirato solo da aneliti libertari: la protezione degli iPhone dalle possibili intrusioni di un governo appare finalizzata principalmente a rafforzare il *brand* e il rapporto fiduciario con i clienti, a cui Cook non a caso si rivolge.

In ogni caso, che sia voluto o che sia una eterogenesi dei fini, gli interessi commerciali dell'azienda hanno finito con il costituire un baluardo per la sfera privata del cittadino contro la naturale invadenza dello Stato. E confermano, dopo due secoli e mezzo, la validità dell'intuizione di Montesquieu che più il potere è diviso, più la libertà dei singoli è salvaguardata[23].

[22] G. Resta, *Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza*, cit., p. 1. Sul rilievo del caso, si veda anche l'editoriale di Guido Rossi, *Un «nuovo» Stato per tutelare la privacy*, in *Il Sole 24 Ore*, 28 febbraio 2016, p. 1.

[23] Così C. Melzi d'Eril - G.E. Vigevani, *In gioco c'è la libertà dei singoli*, in *Il Sole 24 Ore*, 19 febbraio 2016, p. 19.