FBI v Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime

di Marco Orofino*

SOMMARIO: 1. Premessa. – 2. La crittografia come strumento per la tutela della sicurezza e della privacy o come intralcio alle attività di *law enforcement?*. – 3. Le condizioni che legittimano la richiesta di collaborazione attiva di soggetti terzi ai sensi del *All Writs Act*. – 4. Annotazioni conclusive circa i riflessi del caso FBI vs. Apple sull'ordinamento europeo e sull'ordinamento nazionale. – 4.1 La crittografia nel nuovo Regolamento 2016/679. – 4.2. Gli obblighi di collaborazione attiva.

1. – Premessa

La vicenda da cui trae spunto questo contributo è legata alla contrapposizione tra il *Federal Bureau of Investigation* (FBI) ed Apple, all'indomani della strage di San Bernardino del 2 dicembre 2015, in cui due terroristi, probabilmente affiliati all'ISIS, aprirono il fuoco sugli inermi ospiti di un centro sociale per disabili, uccidendo quattordici persone e ferendone gravemente numerose altre.

Le autorità federali durante la perquisizione della macchina dei terroristi, rimasti anch'essi uccisi nella sparatoria con la polizia, ritrovarono un *i-Phone* che venne sottoposto a sequestro. Su autorizzazione del giudice (cd. *search*) le autorità federali provarono ad ispezionare il telefonino ed ottennero dal *provider* dei servizi telefonici e di internet, i dati relativi alle chiamate effettuate ed i dati di traffico, nonché da *Apple*, i dati, associati al telefonino, memorizzati sulla piattaforma proprietaria di *cloud computing* (*i-Cloud*)[1].

L'FBI non riuscì però ad accedere allo *smartphone* e ad estrarre tutti gli altri dati in esso memorizzati.

*Università degli Studi di Milano. E-mail: marco.orofino@unimi.it. Il contributo riproduce, con alcune integrazioni alla luce dell'entrata in vigore del Regolamento europeo 2016/679, il saggio pubblicato in DPCE Online.

[1] La piattaforma in questione, occorre segnalare, comprende i servizi Mail, Contatti, Calendario, Drive, Trova il mio iPhone, Note, Promemoria, Pages, Number, Keynote, Foto. Essa pertanto può offrire innumerevoli informazioni circa l'utente, a patto naturalmente che egli utilizzi tali servizi e, soprattutto, a patto che la funzione di *back up* non sia stata, come nel caso dell'*i-Phone* sequestrato, disabilitata oppure non più aggiornata per mancanza di spazio.

Il sistema operativo mobile *iOS 08* di *Apple* in uso sull'*i-Phone* sequestrato include, infatti, un sistema di protezione particolarmente avanzato. Tale sistema si fonda su un algoritmo associato ad una chiave crittografica – un codice di quattro cifre – impostata dall'utente e salvata solo localmente sullo *smartphone*. Esso prevede, inoltre, che tutti i dati memorizzati sullo *smartphone,* associati sui *server* di Apple nonché i dati in transito siano automaticamente crittografati con lo stesso codice[2].

Il sistema operativo richiede, all'accensione dell'*i-Phone,* l'inserimento del codice, che non ha solo la funzione di "accendere il telefonino", ma anche di consentire la decrittazione e, quindi, l'utilizzo dei dati in esso memorizzati. In caso di errore nell'inserimento, il sistema operativo permette solo dieci tentativi, intervallati da un lasso di tempo crescente ad ogni errore compiuto[3]. Esauriti i dieci tentativi, il sistema operativo provvede in automatico e senza possibilità di successivo recupero alla cancellazione di tutti i dati memorizzati.

Per questa ragione, dopo aver fallito i primi tentativi l'FBI ha chiesto e ottenuto, in data 16 febbraio 2016, dal giudice distrettuale Sheri Pym un'ingiunzione che, ai sensi del *Writs Act, 28 U.S.C. § 1651(a),* ordinava ad Apple di dare assistenza agli agenti federali nelle operazioni di sblocco del telefonino e consentire l'estrazione dei dati, fornendo un *software* capace di: a) bypassare o disabilitare la funzione di autodistruzione dei dati; b) permettere l'inserimento delle chiavi d'accesso elettronicamente anziché manualmente; c) aggirare il meccanismo presente sul dispositivo che ritarda, progressivamente, dopo ogni tentativo fallito, l'introduzione di un nuovo codice[4].

Il giorno stesso in cui il Governo otteneva l'ingiunzione richiesta, l'AD di Apple Tim Cook, diffondeva *online* una lettera rivolta ai propri consumatori, in cui motivava la decisione dell'azienda di opporsi in giudizio alla richiesta del FBI[5]. I punti salienti

[2] G. Reda, *Two Side to Security: iPhones and the All Writ Act*, in *Lousiana Law Review*, 15 marzo 2016.

[3] Il limite dei dieci tentativi, l'obbligo di inserimento manuale ed il lasso temporale tra un inserimento e l'altro, rendono assai difficoltosa la ricerca di un codice di quattro cifre che altrimenti, essendo possibili solo 9999 combinazioni, sarebbe assai semplice e risolvibile in pochissimi minuti da un qualsiasi programma di rilevamento di codici.

[4] Application, *In Re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203,* No. 15-0415M, 2016 WL 618401, (C.D. Cal. Feb. 16, 2016), pt. 7 e 8.

[5] La lettera è disponibile, sul sito dell'azienda, all'indirizzo http://www.apple.com/customer-letter/

della posizione di Apple, espressi fin da subito nella lettera e poi articolati nell'atto di opposizione depositato il 25 febbraio 2016, sono essenzialmente tre[6].

Il primo punto messo in risalto attiene all'impossibilità tecnica di sviluppare un *software* applicabile, realmente, al solo caso concreto, e cioè solo allo sblocco dell'*iPhone* sequestrato, senza porre in una situazione di grave rischio la sicurezza del sistema operativo in sé e, quindi, la sicurezza dei dati e la *privacy* degli altri possessori di un *device* con il medesimo sistema operativo.

Il secondo, quello più generale, ma oggettivamente assai importante, riguarda i sistemi crittografici e la necessità di non indebolirli, ma al contrario di renderli sempre più sicuri per proteggere la *privacy* degli utenti.

Il terzo, prettamente giuridico e formale, riguarda l'obbligo di assistenza. Essa rappresenterebbe, per Apple, un'illegittima estensione di quanto previsto dal *All Writs Act*, e se accolta un precedente pericoloso, in quanto capace di estendere i poteri del FBI (e del Governo) oltre i limiti posti dalla *Due Process Clause* di cui al Quinto Emendamento della Costituzione degli Stati Uniti d'America.

In data 28 marzo 2016, con il deposito di un atto estremamente sintetico presso il *Central District of California*, il Governo degli Stati Uniti ha comunicato, senza specificare come ciò sia stato possibile e grazie alla collaborazione di quali soggetti, che le autorità preposte erano riuscite ad accedere ai dati registrati sul *i-Phone* sequestrato e che, non avendo quindi più bisogno dell'assistenza di Apple, rinunciavano alla loro precedente richiesta[7].

La rinuncia del Governo statunitense chiude questo specifico caso giudiziario, ma certamente non risolve nessuna delle questioni che la vicenda aveva sollevato, alimentando un ampio ed articolato dibattito sia nell'opinione pubblica sia tra i giuristi[8].

---

[6] *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).

[7] ED No. CM 16-10 (SP) *Government's Status Report. In Re Search of an Apple iPhone* ... cit. Si v. per una attenta ricostruzione della vicenda e delle sue implicazioni legali, l'articolo di S.M. Witzel, J.D. Roth, *Implications of the DOJ and Apple Legal Fight That Wasn't*, in *New York Law Journal*, 255, 86, 5 maggio 2016.

[8] Moltissimi sono stati gli articoli di cronaca apparsi sui quotidiani statunitensi ed europei. Particolarmente interessanti sono inoltre alcune prese di posizioni ufficiali tra cui, in favore di Apple, la lettera di David Kaye, *UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, rivolta al giudice Sheri Pym, *Re: In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203;* l'intervento in giudizio, come *amicus curiae* in favore di Apple, della *American Civil Liberties Union*. Nella letteratura italiana, v. i primi contributi di A. Serena, *Apple v. FBI, or the Role of Technology on the Functioning of the Law*, in *Law and Media Working Paper Series*, no. 3/2014; G.

Occorre inoltre segnalare che la richiesta formulata dal Governo statunitense non è affatto un'eccezione. Infatti, a partire dall'ottobre del 2015, Apple ha ricevuto molte altre richieste di sblocco[9], ed almeno in un altro caso, analogo per tipologia di *smartphone* e per sistema operativo utilizzato, il Governo ha richiesto un ordine di assistenza *ex All Writs Act*, ricevendo, in quel caso, un diniego dal giudice *Orenstein* del *New York District*[10].

Nei paragrafi che seguono, saranno oggetto di alcune riflessioni, necessariamente brevi nell'ambito di questo contributo, due questioni che sembrano rivestire notevole rilevanza, anche aldilà del caso concreto da cui esse sono scaturite.

2. *La crittografia come strumento per la tutela della sicurezza e della privacy o come intralcio alle attività di law enforcement?*

La prima questione riguarda il tema della crittografia[11], l'uso di chiavi crittografiche, come quella approntata da Apple a partire dal sistema operativo iOS 08, e la legittimità di eventuali limitazioni allo sviluppo di sistemi di protezione sempre più efficaci, nel caso in cui essi possano essere di ostacolo alla giustizia.

Innanzitutto, occorre dire che la crittografia è una tecnica antica come l'uomo che, essenzialmente, consente di "cifrare" un qualunque dato, informazione o messaggio per renderlo incomprensibile a tutti fuorché a chi conosce la chiave di lettura. La storia è piena di celebri esempi, dal cifrario assai semplice di Giulio Cesare[12], agli algoritmi, invece, assai complessi usati dai nazisti durante il secondo conflitto bellico e

Resta, *Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza*, in *Menabò di Etica ed Economia*, 38/2016.

[9] I dati sono riportati da B. Chappel, *Apple Has Gotten Federal Orders to Helkp Unlock at Least 13 Devices*, NPR (Feb. 24, 2016), il quale cita ed esibisce documentazione fornita da Apple nell'ambito di un analogo procedimento di fronte al Giudice Orenstein di New York.

[10] *In re Order Requiring Apple, Inc to assist in the Execution of a Search Warrant Issued by this Court*, No. 15-MC-1902(JO), 2016 WL 783565.

[11] V. su questi temi, per tutti, G. Ziccardi, *Crittografia e diritto. Crittografia, diritto, utilizzo e disciplina giurdica, document informatico e firma digitale, segretezza delle informazioni e sorveglianza globale*, Torino, 2003; e più recentemente Id., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

[12] Presumibilmente se Giulio Cesare inviò dei messaggi ai suoi alleati a Roma dopo aver varcato il Rubicone il testo crittografato della sua celebre affermazione *Alea iacta est* dovrebbe essere stato DOHD MDFAD HXA e chissà se qualcuno intercettandolo sia riuscito o meno a scoprire che si trattava di un cifrario a scorrimento con chiave di lettura 3.

recentemente tornati alla ribalta grazie al film *The Imitation Game*, che narra appunto la storia del matematico inglese Alain Touring che riuscì a decrittarli.

Lo sviluppo di elaboratori elettronici, capaci di compiere complesse operazioni matematiche in tempi brevissimi, da un lato, ha certamente contribuito a rendere gli algoritmi crittografici infinitamente più complessi; dall'altro ha reso anche più semplice l'attività di decrittazione. Ciò che la tecnologia non ha modificato è il fondamento dell'operazione crittografica che rimane, infatti, sempre un algoritmo associato ad una chiave di lettura.

La necessità di algoritmi crittografici sempre più sofisticati è cresciuta contemporaneamente con lo sviluppo di elaboratori elettronici capaci di archiviare grandi quantità di dati ed informazioni ed è letteralmente esplosa con Internet, ed in particolare con lo sviluppo del web 2.0 che ha consentito la proliferazione di tutta una serie di servizi che non solo consentono agli utenti di comunicare tra loro, ribaltando su tali comunicazioni le esigenze di segretezza proprie, e costituzionalmente garantite, delle comunicazione interpersonali, ma anche di compiere una miriade di attività (si pensi ad esempio all'*home banking* o all'*e-Health*) che, richiedendo la memorizzazione di molti dati e informazioni relative agli utenti sia sulle diverse piattaforme sia sui terminali di rete (*PC*, *Smartphone*, *Tablet*, *SmartTV*, etc.), necessitano di segretezza al fine di garantire sia la sicurezza delle attività medesime sia delle persone che le compiono[13].

L'enorme quantità di dati, la loro memorizzazione, il loro continuo scambio (più o meno volontario) sollevano, come è ormai noto a tutti, importanti questioni riguardanti la *privacy* delle persone. Meno comprese, ma assai delicate sono le questioni che la circolazione di tali quantità di dati comporta, non tanto in riferimento alla *privacy*, quanto piuttosto alla sicurezza individuale, alla sicurezza delle attività svolte *online* e, evidentemente, alla sicurezza della società nel suo complesso.

Il sistema crittografico, adottato da Apple, rappresenta un deciso avanzamento nel livello di protezione per tre ragioni. In primo luogo perché esso imposta la protezione su

[13] Sia consentito rinviare sull'impatto che il web 2.0 produce sulle libertà e i diritti costituzionalmente garantiti a M. Orofino, *L'inquadramento costituzionale del web 2.0: da nuovo mezzo per la libertà di espressione a presupposto per l'esercizio di una pluralità di diritti costituzionali*, in AA.vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Ravenna, 2013, 33 ss., nonché Id., *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Torino, 2015, spec. 9 ss.

tutti i dati generati e/o memorizzati in modo automatico; si tratta, dunque, di una caratteristica impostazione di *default* del sistema che mira a proteggere qualsiasi utente anche colui che non disporrebbe delle necessarie conoscenze e competenze informatiche per impostare autonomamente tale protezione. In secondo luogo, perché la chiave di accesso, inserita dall'utente come prima operazione, è registrata solo a livello locale (nella memoria dello *smartphone*) e, dunque, essa non è salvata in alcun *server* posto sotto il controllo di Apple. Infine, perché il sistema operativo non prevede alcuna *backdoor* che permetta un accesso da remoto e, pertanto, l'utilizzo di applicazioni (ivi compresi microfoni e telecamere) e dati decrittati, senza l'inserimento della chiave di accesso.

La mancata previsione di una *backdoor* nel sistema operativo, distribuito a partire dal 2 giugno 2014, è evidentemente legata anche alle rilevazioni di Edward Snowden circa il sistema di sorveglianza, noto come PRISM, e alla conferma che le principali aziende del settore hanno trasmesso dati alla *National Security Agency* (NSA)[14].

La scelta compiuta da Apple con il rilascio del sistema operativo iOS 08 deve essere, dunque, inquadrata in questo contesto. Posto, infatti, che l'algoritmo crittografico, per quanto ben congegnato, è sempre individuabile, l'aver spostato la sicurezza sulle chiavi di lettura ha consentito di rimettere, in capo al solo utente, la responsabilità del codice di accesso, della sua gestione e della sua conservazione.

Nel bilanciamento, anche di natura commerciale, compiuto da Apple tra il danno che potrebbe comportare per l'utente la cancellazione definitiva di tutti i suoi dati, magari solo per aver dimenticato il codice, e l'esigenza di assicurare e garantire il più alto livello di sicurezza riguardo ai dati memorizzati, l'azienda ha consapevolmente scelto di privilegiare la seconda opzione.

Il punto in discussione, che evidentemente oltrepassa di molto il caso in questione, è se la scelta compiuta da Apple di massimizzare la protezione sia o meno legittima allorché essa possa avere un impatto negativo sull'attività di prevenzione e di repressione di crimini, anche gravissimi come nel caso della strage di San Bernardino, svolta dalle autorità preposte alla pubblica sicurezza e alla sicurezza nazionale

[14] V. la dichiarazione di Apple, che pur negando di essere a conoscenza di tale programma di sorveglianza ammette di aver dato corso, valutando caso per caso, a richieste di accesso provenineti sia da parte di autorità giudiziarie sia da parte di autorità federali competenti in materia di *national security*. Il testo è disponibile all'indirizzo: http://www.apple.com/apples-commitment-to-customer-privacy/

Molto spesso, ed è accaduto anche nel caso qui in esame, sia da parte di *Apple* sia da parte del FBI nell'audizione del Direttore James Comey presso l'*House Judiciary Committee* del Congresso[15], la questione è stata semplificata nella contrapposizione, ormai tanto utilizzata da apparire abusata, tra *privacy* e sicurezza.

Questa tensione tra esigenze di *privacy* ed esigenze di sicurezza collettiva che pure innegabilmente sussiste, coglie però solo una parte del problema e rischia di essere, infine, fuorviante.

La crittografia, infatti, non serve solo ed esclusivamente a proteggere la *privacy* delle persone, ma mira soprattutto a proteggere la loro libertà e la loro sicurezza individuale. Essa non è, quindi, solo un "ostacolo" all'attività investigativa, volta ad evitare un reato o ad assicurare il colpevole alla giustizia, ma rappresenta una protezione in sé alla messa in essere di condotte criminose sul web. Per questo essa concorre a rafforzare la libertà delle persone di utilizzare i nuovi servizi che, in modo incessante, il web 2.0 continua a rendere disponibili.

D'altra parte, occorre dire che i cd. *cyber crimes* sfruttano talvolta le falle presenti nei sistemi operativi adottati dai produttori di *device* e dai fornitori di servizi e possono essere evitati attraverso il loro rafforzamento. Anche la realizzazione di un *cyber terroristic attack* può richiedere la violazione di una chiave crittografica per l'accesso da remoto a dispositivi militari, come in un attualissimo *remake* del celebre e visionario film *War Games* di John Badham, oppure a dispositivi e strumenti civili capaci, nel caso di un malfunzionamento indotto di mettere a rischio, e su larga scala, la sicurezza delle persone.

Gli esempi fatti non servono a negare quanto è evidente, e cioè che sussista una tensione latente tra sicurezza e *privacy*, in particolar modo laddove si ragiona sui poteri da attribuire alle autorità di sicurezza e sui limiti formali e sostanziali entro cui essi possono essere esercitati, ma servono a mostrare quanto sia riduttivo pensare che la sicurezza delle persone possa essere garantita solo massimizzando i poteri di controllo delle autorità. L'adozione di sistemi crittografici sempre più sicuri concorre, a tutta evidenza, a garantire la sicurezza delle persone e di conseguenza la loro libertà.

Per questa ragione, l'idea che possa essere richiesto dalle autorità di *law enforcement* "l'indebolimento" di un sistema operativo per il sol fatto che il medesimo

[15] Cfr. *Statement Before the House Judiciary Committee*, Washington D.C., 1st March 2016. L'audizione è integralmente disponibile in *streaming* sul sito del Congresso degli Stati Uniti.

sia in grado non solo di ostacolare eventuali malintenzionati, ma anche di opporre resistenza ad una forzatura legittimamente compiuta dalle autorità preposte solleva non poche perplessità. Esse aumentano se si immagina, *de iure condendo*, di imporre ai produttori la creazione di una *backdoor* di sistema. Sarebbe come dire, se è consentita la provocazione, che sono vietate le porte blindate perché rendono difficile l'accesso della polizia oppure come prevedere, legislativamente, che in ogni casa sia lasciato aperto un pertugio utilizzabile all'occorrenza.

La prospettiva criticata non è affatto ipotetica, ma molto reale se si pensa che il Direttore del FBI James Comey ha domandato, proprio nell'ambito dell'audizione del 1 marzo 2016 di fronte all'*House Judiciary Committee*, se una volta che tutti i limiti formali e sostanziali previsti dalla Costituzione e dalla legge fossero stati rispettati, sarebbe accettabile per il Congresso, una tecnologia che ponesse ostacoli nell'assunzione delle prove di un crimine[16].

In questa direzione, si stavano muovendo, peraltro, alcuni Parlamenti statali, ad esempio quello dello Stato della California e quello dello Stato di New York. Le proposte in discussione mirano a dare nuovi poteri, in quegli Stati, alle autorità di polizia e, soprattutto, ad imporre ai produttori di *smartphone* proprio l'obbligo di prevedere una *backdoor* nei loro sistemi operativi[17].

In senso opposto, occorre segnalare che al Congresso è stata presentata una proposta di legge volta a definire unitariamente, a livello federale, la materia. La proposta presentata (*The Act for Ensuring National Constitutional Rights for Your Private Telecommunications, cd. Encrypt Act of 2016*) ha il duplice scopo di evitare il *patchwork* che potrebbe derivare da legislazioni diverse da Stato a Stato e di prevenire gli Stati dal richiedere ai fabbricatori di *device* ed ai fornitori di servizi di alterare i loro prodotti o servizi per creare *backdoor* utili nella ricerca di prove[18].

[16] *Statement Before the House Judiciary Commitee, cit.*

[17] Le proposte cui ci si riferisce nel testo sono "An Act to amend the general business law, in relation to the manufacture and sale of smartphones that are capable of being decrypted and unlocked by the manufacturer" presentata all'Assemblea dello Stato di New York l'8 giugno 2015 e "An act to add Section 22762 to the Business and Profession Code, relating to smartphones", AB 1681, presentata all'Assemblea californinana il 20 gennaio 2016.

[18] La proposta di legge è bipartisan, nel senso che essa è stata presentata da Ted Lieu (Deputato democratico della California) e Blake Farenthold (repubblicano eletto in Texas). Suzan DelBene (democratica di Washington) and Mike Bishop (repubblicano del Michigan) hanno inoltre firmato la proposta come *supporter*.

Il dibattito sulla disciplina della crittografia è quindi apertissimo. È auspicabile, ed anche presumibile, che esso andrà molto oltre la dicotomia *privacy-sicurezza* e toccherà altre questioni, assai sensibili nel dibattito americano, quali la libertà personale, da intendersi anche come il diritto a garantirsi la propria sicurezza individuale, la libertà d'impresa e di commercio.

3. *Le condizioni che legittimano la richiesta di collaborazione attiva di soggetti terzi ai sensi del All Writs Act.*

La seconda questione che si intende affrontare riguarda la controversa legittimità del *All Writs Act*, 28 U.S.C. § 1651(a) come base legale dell'ordine impartito ad Apple, il 16 febbraio 2016, dal giudice distrettuale Sheri Pym. Anche in questo caso, il tema è assai più ampio e tocca il delicato problema della collaborazione attiva (in particolare consistente in un *facere*) che individui o, come nel caso in questione, aziende possono essere chiamati a prestare alle autorità di *law enforcement*, anche laddove essi non siano direttamente coinvolti nella questione giudiziaria o nel fatto che ne è all'origine.

La previsione normativa statunitense di cui al *28 U.S. Code § 1651a* è assai risalente nel tempo e prevede oggi, dopo alcune modifiche, che "the Supreme Court and all Courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principle of law"[19].

Nonostante il suo tenore letterale, la norma non ha, come chiarito dalla Corte Suprema americana in *Pennsylvania Bureau of Correction v. United States Marshals Services*[20], una portata generale, ma solo una applicazione residuale, nel senso che essa è utilizzabile dal giudice per emettere un ordine a carico di un determinato soggetto terzo solo qualora non vi sia un'altra fonte legale che disciplini la specifica questione o lo specifico comportamento richiesto.

L'indubbia originale flessibilità del *writ* in questione, derivante dal fatto di non essere inquadrato in uno schema legale tipizzato, è stata controbilanciata dai requisiti

[19] L'atto, nella sua forma originaria, era parte integrante dello *Judiciary Act of 1789*. La versione odierna approvata nel 1911 è stata successivamente oggetto di modifiche legislative che non hanno inciso sulla sua portata sostanziale.

[20] V. *N. Pa. Bureau of Corr. V. U.S. Marshals*, 474 U.S. 34, 43 (1985)

per la sua adozione che sono stati individuati con precisione dalla sentenza *United States v. New York Telephone Co* del 1977[21].

I fatti di causa sono risalenti, ma meritano di essere brevemente ricostruiti per la loro somiglianza con il caso in questione. Gli agenti del FBI, sospettando che alcuni individui gestissero un'attività illegale di scommesse clandestine, chiesero ed ottennero dalla *District Court* di New York l'autorizzazione ad installare e utilizzare, su due telefoni utilizzati dai sospettati, due dispositivi (cd. *pen register*) capaci di registrare i numeri selezionati. Sulla base di una richiesta avanzata ai sensi del *All Writs Act, 28 U.S.C. § 1651(a)*, il giudice ordinava alla compagnia telefonica *New York Telephone Co*, proprietaria delle due linee telefoniche, di fornire all'FBI l'assistenza necessaria – intesa come informazioni, servizi ed assistenza tecnica – per installare i dispositivi e registrare i numeri selezionati.

La compagnia telefonica si oppose alla richiesta di fornire assistenza tecnica argomentando, in particolare, che tale ordine avrebbe potuto essere imposto solo in collegamento con un ordine di intercettazione adottato dal giudice ai sensi del *Omnibus Crime Control and Safe Streets Act of 1968*.

Questa obiezione non fu accolta in alcun grado di giudizio e la Corte Suprema, confermando che la registrazione dei numeri chiamati non è attività di intercettazione in senso proprio, poiché non consiste nell'ascolto di una chiamata e che, dunque, non può essere ricondotta alle norme specificamente previste per tale attività, specificò che per questa ragione, il giudice poteva legittimamente fare ricorso al potere residuale di cui al *All Writs Act*.

Tuttavia, la Corte Suprema precisò che il potere delle Corti federali di imporre obbligazioni a carico di terze parti, ai sensi del *All Writs Act*, non è affatto da considerarsi come illimitato e che il giudice deve accertare, come condizioni *sine qua non*, che: i) il soggetto terzo a cui viene imposta una obbligazione sia, anche solo in ragione dei servizi che esso offre, coinvolto nella questione[22]; ii) l'intervento del

[21] V. *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172-3 (1977).

[22] Non è in discussione il fatto che il potere conferito dal *All Writ Act* si estenda, a determinate condizioni, a soggetti che pur non essendo parti dell'azione originale, non essendo connesse con essa, non essendo in alcun modo sospettate di alcun illecito, si trovano in una posizione tale da poter frustrare l'esecuzione di un ordine della Corte o l'amministrazione propria della giustizia come in *Mississippi Valley Barge Line Co. v. United States*, 389 U.S. 579 (1968); *Board of Education v. York*, 401 U.S. 954 (1971). Allo stesso modo si estende anche ad ordini nei confronti di persone che non abbiano compiuto

soggetto terzo sia assolutamente necessario; iii) il comportamento richiesto non si traduca in un onere irragionevole.

La Corte Suprema decise che l'ordine imposto alla compagnia telefonica *New York Telephone Co* rispettava tutte e tre le condizioni. La prima condizione, ossia l'esistenza di una connessione tra il soggetto terzo e la fattispecie, era per la Corte Suprema rispettata perché i servizi della compagnia telefonica erano utilizzati su base continuativa per commettere un reato; perché la compagnia svolgeva un servizio pubblico altamente regolato per cui era difficile sostenere che essa avesse un interesse sostanziale a non collaborare; perché la medesima compagnia aveva ammesso di impiegare regolarmente tali dispositivi senza ordine del tribunale ai fini del controllo delle operazioni di fatturazione, individuazione delle frodi, e prevenzione di violazioni di legge. La seconda condizione, ossia il requisito della necessità dell'intervento della compagnia telefonica, risultava provato dal fatto che gli agenti federali, dopo un'accurata ricerca, non erano riusciti ad installare i propri *pen register*. Pertanto, la cooperazione della compagnia era essenziale per il raggiungimento degli obiettivi e per scoprire l'identità delle persone coinvolte con il gioco d'azzardo e, soprattutto, "non c'era modo concepibile attraverso cui l'attività di sorveglianza potesse essere diversamente e con successo realizzata". La terza condizione, vale a dire la non eccessiva gravosità dell'ordine era, infine, facilmente dimostrata secondo la Corte Suprema dal fatto che la compagnia telefonica, nel caso di specie, avrebbe ricevuto un indennizzo per la sua attività e per le linee temporaneamente affittate al FBI.

Nel caso oggetto di questo contributo, *FBI v. Apple*, erano in discussione, nel senso che le parti avevano prodotto memorie di segno opposto, sia l'applicabilità del *All Writs Act* sia la sussistenza delle tre condizioni individuate dalla Corte Suprema.

Per quanto riguarda l'applicabilità in sé del *All Writs Act*, 28 U.S.C. § 1651(a), la questione passa necessariamente dalla verifica della sussistenza o meno di un'altra normativa federale che incida in materia.

La norma "più vicina" in materia è il *Communications Assistance to Law Enforcement Act* of *1994* (CALEA) che ha ad oggetto specificamente il potere delle autorità di *law enforcement*, in seguito ad un ordine di un giudice, di intercettare le

alcuna azione affermativa per ostacolarla come nei casi *United States v. McHie,* 196 F. 586 (ND Ill.1912); *Field v. United States,* 342 U.S. 894 (1951).

comunicazioni attraverso l'utilizzo di tecnologie avanzate e di richiedere l'assistenza degli operatori di telecomunicazione. Non è in discussione, nel senso che né Apple né il Governo hanno sostenuto il contrario, che tale normativa sia dedicata essenzialmente ai fornitori di reti e di servizi e non imponga, quindi, ai produttori di *smartphone* di bypassare le proprie misure di sicurezza per consentire l'accesso ad uno specifico *device*. Il punto discriminante è se tale esclusione sia il frutto di una scelta consapevole orientata dalla volontà di non sottoporre i produttori a tali obblighi, il che impedirebbe l'utilizzo del *All Writs Act*, oppure se essa non sia una scelta, ma una semplice lacuna nell'ambito della legislazione federale che, quindi, aprirebbe la strada all'utilizzo legittimo della normativa residuale[23].

Il punto si presta indubbiamente ad entrambe le letture. Nel "caso gemello" in cui il Giudice Orenstein del Distretto di New York ha negato il *writ*, l'argomentazione principale è stata che il Congresso aveva specificamente considerato la possibilità di estendere anche ai produttori di terminali, gli obblighi legali previsti per i fornitori di servizi dal CALEA, senza però giungere all'adozione degli emendamenti allo scopo presentati[24]. Dunque non si trattava, per il giudice Orenstein, di una lacuna, ma di una scelta precisa del Congresso che impediva il ricorso alla normativa residuale di cui al *All Writs Act*. Non c'è dubbio che questa interpretazione valorizzi assai i lavori parlamentari. Questo non solo, come è nella tradizione americana, per ricostruire la volontà storica del legislatore ai fini dell'interpretazione della disposizione, ma anche, come nel caso di specie, per giustificare l'assenza di una previsione legislativa *ad hoc* sulla volontà del legislatore di non disciplinare la materia.

In *U.S. v. New York Tel. Co*, la Corte Suprema non si era spinta come il giudice Orenstein del Distretto di New York fino a questo punto, limitandosi a verificare, in quel caso, che la normativa in materia di intercettazioni telefoniche non disciplinasse anche la registrazione dei numeri chiamati.

In ogni modo, anche qualora si fosse risolto positivamente il problema interpretativo a monte sull'applicabilità del *All Writs Act*, occorrerebbe comunque sottolineare che la posizione di Apple appare piuttosto diversa da quella della *New York*

[23] G. Reda, *Two Side to Security… cit.*, par. 3.

[24] *In Re Order Requiring Apple, Inc. To Assist in the Execution of a Search Warrant Issued By This Court*, No. 15-MC-1902 (JO), 29 February 2016.

Telephone Company con riferimento ad ognuno delle tre condizioni poste dalla Corte Suprema nel caso *United States v. New York Telephone Co.*

Con riferimento alla connessione di *Apple* con il caso in essere, bisogna considerare che la società di Cupertino è, innanzitutto, un produttore di *device* e di sistemi operativi e, solo secondariamente, anche un fornitore di servizi[25]. Il nesso con l'attività criminosa svolta dai terroristi è, quindi, assai tenue e limitato al fatto che essi avrebbero potuto servirsi di quello specifico *smartphone* per pianificare la strage. Di certo, c'è però che l'attività di Apple non può essere in alcun modo equiparata a quella svolta da una compagnia telefonica che eroga un servizio pubblico regolamentato.

La sussistenza della seconda condizione, che in principio sembrava teoricamente soddisfatta, posta la dichiarazione in cui l'FBI affermava di non poter aggirare il sistema di protezione e, dunque, l'ineludibile necessità di assistenza da parte di Apple, è divenuta assai dubbia nel momento in cui il Governo ha dichiarato, sia pubblicamente sia succintamente nell'atto depositato in giudizio, che il *Federal Bureau* era essere riuscito a fare a meno dell'assistenza di Apple e a decrittare il contenuto dell'*i-Phone*.

Questo proverebbe, a posteriori, che la richiesta non rispettava il criterio della necessità, essendosi poi concretamente giunti al medesimo risultato, che si era dichiarato irraggiungibile, senza l'assistenza di *Apple*. È evidente che la dichiarazione di rinuncia, così come è stata espressa, sembra poter divenire assai controproducente, quasi al pari di un autogol, in casi analoghi, tuttora o in futuro pendenti davanti ad altre corti e riferiti al medesimo sistema operativo iOS 08.

La sussistenza della terza condizione, ossia la non eccessiva onerosità dell'azione, è altrettanto discutibile. Non tanto, o almeno non in modo decisivo, perché l'attività richiesta ad Apple, in buona sostanza la modifica del proprio *software* con la creazione di una *backdoor* di sistema, sia in sé eccessivamente onerosa da realizzare per una società che vanta un fatturato nel solo primo trimestre 2016 pari a 50,6 miliardi di dollari oppure perché non sia prevista compensazione.

L'eccessiva onerosità della richiesta sembra derivare piuttosto dal fatto che essa incide pesantemente sulle scelte d'impresa e di sviluppo dei prodotti aziendali e può generare ricadute economiche assai negative sia in termini di immagine rispetto alla

[25] Non è in discussione che in quanto fornitore del servizio *i-cloud*, l'Apple sia anche fornitore di un servizio, ma occorre ribadire che, in tale veste, l'azienda ha immediatamente cooperato con l'FBI e dato seguito all'ordine del giudice.

promessa fatta da Apple ai consumatori di rendere i loro dati sempre più sicuri, sia in termini di concorrenza rispetto agli altri produttori di *device* e di sistemi operativi, sia in termini giudiziari nell'ipotesi, non così peregrina, che gli acquirenti di un *i-Phone* con sistema operativo *iOS 08*, preoccupati dall'indebolimento del sistema a seguito dell'azione del produttore, volessero intentare un'azione giudiziaria o una *class action*.

L'abbandono della causa da parte del Governo americano ha evidentemente la conseguenza che il giudice non si pronuncerà su questi dubbi né essa potrà arrivare innanzi alla Corte Suprema. Tuttavia sembrano sussistere buone ragioni per ritenere che, almeno sulla base del precedente *United States v. New York Telephone Co*, il Governo americano abbia intrapreso una strada assai ricca di ostacoli e anche che, alcune decisioni adottate nel corso della vicenda abbiano finito con renderla ancora più irta ed accidentata.

4. *Annotazioni conclusive circa i riflessi del caso FBI vs. Apple sull'ordinamento europeo e sull'ordinamento nazionale.*

I due temi trattati, tra i molti che il caso FBI vs. Apple sollevava, e cioè la questione della legittimità di sistemi di sicurezza, come quelli crittografici approntati da Apple, nel caso in cui essi possano essere di ostacolo alla giustizia e la questione degli obblighi che possono essere imposti ai produttori di *device* per coadiuvare le autorità di law *enforcement*, sono evidentemente centrali non solo per gli Stati Uniti, ma per ogni altro Paese[26].

4.1. *La crittografia nel nuovo Regolamento 2016/679.*

Per quanto riguarda la questione della crittografia, è importante che il dibattito si sposti in sede internazionale e, in quella sede, si arricchisca del contributo europeo. Non è, infatti, immaginabile né auspicabile che ogni Stato proceda a definire regole nazionali in un settore che appare ormai fortemente globalizzato.

[26] Questo è chiarissimo, innanzitutto, ad Apple che, pur avendo sede nella Contea di Santa Clara in California, potrebbe trovarsi tanto a fronteggiare differenti legislazioni statali che obbligano produttori di *device* e di sistemi operativi a prevedere delle *backdoor* quanto a rispondere ad una richiesta, simile a quella avanzata dal governo americano, da parte di un qualsiasi altro governo nazionale.

L'Unione europea vanta in proposito una storica attenzione al tema della sicurezza dei terminali e dei servizi di trasmissione sia nella legislazione in materia di comunicazioni elettroniche, sia in quella in materia di protezione dei dati personali.

Già l'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE prevedeva che la Commissione europea potesse stabilire che i dispositivi degli utenti finali fossero "costruiti in modo da contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato"[27]. In questa previsione era già presente, ancorché non esplicitato il concetto di *data protection by design (privacy by design)*, che è stato successivamente ripreso nell'art. 14, par. 3, della direttiva 58/2002, cd. direttiva e-privacy[28].

Il concetto in questione è assolutamente centrale. Esso indica, infatti, la necessità che, fin dalla fase di progettazione del processo di raccolta e trattamento dati, si privilegino quelle opzioni tecniche che consentono una maggiore protezione dei dati personali. A tale concetto si accompagna quello della *data protection by default*, che richiede l'impostazione predefinita delle modalità di trattamento più protettive per l'utente anche quando il medesimo possa successivamente modificarle.

Il recente Regolamento europeo 2016/679 compie un passo ulteriore.

In primo luogo, l'art. 25 disciplina, in modo esplicito, il principio della data *protection by design* e il principio della *data protection by default*[29].

In secondo luogo, adotta un cambiamento notevole di impostazione laddove prevede che il titolare del trattamento non si limiti più a garantire l'osservanza delle norme in materia di protezione dati ma assuma un comportamento proattivo volto dimostrare la conformità del trattamento dati rispetto al nuovo quadro normativo. Per far questo deve adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati *by default*[30].

[27] V. anche in proposito l'art. 8, par. 4., lett. f) e l'art. 13a della direttiva 21/2002/EU sugli obblighi a carico delle imprese che offrono reti e servizi di comunicazione elettronica di adottare misure adeguate di tipo tecnico ed organizzativo per gestire e minimizzare i rischi. Sulla portata di tali obblighi nel settore delle comunicazioni elettroniche sia consentito rinviare a M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Milano, 2008, 135 ss.

[28] V. sul punto, F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, *passim* e spec. 132-133.

[29] Ibidem, 287-289.

[30] V. in generale l'art. 25 ed il considerando 78 e con riferimento ai requisiti richiesti per il trasferimento dati e l'art. 47 sulle "Norme vincolanti d'impresa" ed il considerando 108. Cfr. F. Pizzetti, op.ult.cit., 287-289.

In terzo luogo, il Regolamento indica espressamente la cifratura tra gli strumenti essenziali che il titolare del trattamento e il responsabile del trattamento devono adottare per garantire un livello adeguato di sicurezza nel trattamento dati[31].

Questi obblighi sembrano doversi applicare anche ai produttori di dispositivi e di sistemi operativi, i quali, come già specificato dal *Gruppo articolo 29*[32], nel *Parere 02/2013 sulle applicazioni per dispositivi intelligenti* "devono essere considerati responsabili del trattamento di eventuali dati personali trattati per finalità proprie, di dati generati dall'utente (ad esempio informazioni sull'utente durante la registrazione), di dati generati automaticamente dal dispositivo o di dati personali trattati da produttori di OS o dispositivi in seguito all'installazione o all'utilizzo di applicazioni". Inoltre, nel caso in cui "i produttori di OS o dispositivi offrono funzionalità aggiuntive, quali una funzione di back-up o localizzazione remota, diventano responsabili del trattamento dei dati personali trattati per tale scopo".

4.2. *Gli obblighi di collaborazione attiva.*

Per quanto riguarda, invece, il delicato problema della collaborazione attiva (in particolare consistente in un *facere*) che soggetti terzi, individui o aziende, possono essere chiamati a prestare alle autorità incaricate di compiti di pubblica sicurezza o di polizia giudiziaria (di cd. *law enforcement*), esso dipende, in maggior misura, dalle garanzie costituzionali e dalle leggi nazionali.

Una trattazione esaustiva circa la legittimità degli obblighi di *facere* che possono essere imposti ai produttori di terminali o di sistemi operativi richiederebbe un sviluppo dell'indagine, anche in chiave comparata, che appare incompatibile con la brevità di questo contributo.

[31] V. considerando 83 ed art. 32 del Regolamento 3/2006.

[32] Si tratta del Gruppo di lavoro, istituito dall'art. 29 della direttiva 95/46, di cui fa parte un rappresentante di ogni Autorità di controllo degli Stati membri, un rappresentante della Commissione ed il Presidente dell'Autorità di supervisione sui trattamenti dati dell'ordinamento UE. Tale Gruppo ha la funzione assai rilevante di assicurare un'interpretazione comune da parte delle singole autorità nazionali della normativa europea in materia di protezione dati. Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Vol. I. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., 33-35.

Con riferimento all'ordinamento costituzionale italiano, occorre, però, almeno ricordare i limiti posti dall'art. 23 Cost. che, come noto prevede, che "nessuna prestazione personale o patrimoniale può essere imposta se non in base alla legge".

La norma introduce una riserva di legge che, ancorché sia da considerare come relativa, è rispettata, come specificato dalla Corte costituzionale nella sentenza 115 del 2011, solo se la legge in questione è sufficientemente dettagliata[33]. Ne consegue che il mero richiamo formale ad una prescrizione legislativa generale, orientata ad un principio valore – come è, invece, il *Writs Act, 28 U.S.C. § 1651(a)* – parrebbe di dubbia compatibilità con il nostro ordinamento costituzionale.

Infine, anche nell'ipotesi che, *de iure condendo,* fosse la legge ad imporre ai produttori di *device* e di sistemi operativi obblighi specifici di collaborazione, occorrerebbe in concreto verificare sia la loro compatibilità con l'ordinamento costituzionale sia con l'ordinamento europeo. Con riferimento a quest'ultimo, la decisione della Corte di Giustizia nel caso *Scarlet v. Sabam*[34], che ha dichiarato illegittimo l'obbligo di introdurre un filtro tecnologico a carico degli *Internet Service Provider,* in grado di prevenire scaricamenti illegali di materiale sottoposto a *copyright* perché viola, tra gli altri parametri considerati, il diritto alla protezione dei dati e la libertà d'impresa, è assolutamente paradigmatica[35].

Fatte le debite proporzioni e tenuto conto dalla diversità degli interessi in gioco si può affermare che un obbligo legislativo generalizzato, volto a imporre la previsione di una *backdoor* nei sistemi operativi, potrebbe essere oggetto di analoga valutazione, nel contesto europeo, rispetto alla sua compatibilità con le norme in materia di sicurezza dei terminali e di protezione dati nonché rispetto alla sua capacità di incidere in modo sproporzionato sulla libertà d'impresa dei produttori di *device* e di sistemi operativi.

[33] V. par. 5 in diritto della sentenza della Corte costituzionale n. 115 del 2011. La decisione della Corte riprende la precedente giurisprudenza di cui alla sentenza n. 4 del 1957, 190 del 2007 e, in riferimento agli obblighi coattivi, della sentenza n. 290 del 1987. Quest'ultima decisione è di particolare interesse, anche nel caso di specie, perché offre una lettura congiunta del divieto di imporre prestazioni personali o patrimoniali, di cui all'art. 23 Cost., e dei limiti alla proprietà privata di cui all'art. 42, comma 3, Cost.

[34] Corte giust., sent. 24-11-2011, c-70/10, *Scarlet v. Sabam*.

[35] V. in proposito F. Pizzetti, *Il caso del diritto d'autore*, Torino, 2ed. 2013, ed ivi in particolare i saggi di L. Ferola, O. Pollicino e M. Siano.