RIVISTA AIC ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI

Rivista N°: 3/2016
DATA PUBBLICAZIONE: 28/09/2016

AUTORE: Monica 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 **

Sommario: 1. La tecnologia, nuova frontiera della sicurezza. – 1.a) "Dopo l'11 settembre", il volto della paura. – 2. USA vs. Apple*: il mondo capovolto. – 3. Principi liberali, diritti e garanzie costituzionali: a rischio, in nome della sicurezza? – 3.a) Sulla separazione dei poteri:* Pim vs. Orenstein*. - 3.a.1) Per evitare il confronto democratico, il potere esecutivo ricorre a quello giudiziario. – 3.b) Sul sacrificio dei diritti:* United States vs. New York Tel. Co*., fra riserva di giurisdizione e di legge, e* due process of law*. – 3.c) Variazione sulla tesi di Orenstein: a lezione dall'FBI sui principi liberali e le garanzie costituzionali. - 4. Dal* Safe Harbour *al* Privacy Shield*. Il diritto alla vita privata dall'Unione europea agli Stati Uniti d'America. – 4.a)* Facebook USA e National Security Electronic Surveillance Programme*: i dati personali europei negli Stati Uniti, senza la protezione della Carta dei Diritti. – 5. Dopo Edward Snowden: il rispetto della vita privata e dei dati personali "alla luce della Carta dei Diritti", o … – 6. … la garanzia della sicurezza nazionale "alla luce dei legittimi interessi d'ordine superiore" del pubblico potere statunitense? – 7. Cittadini europei e Governo federale degli Stati Uniti d'America: come proteggere le libertà nell'era della tecnologia? – 8.* Microsoft vs. USA*: "molto rumore per nulla" … le democrazie sono imperfette, ma restano pur sempre democrazie.*

1. La tecnologia, nuova frontiera della sicurezza.

"La libertà è qualcosa che si fabbrica in ogni istante. […] Quale sarà, allora, il criterio per calcolare il costo della produzione della libertà? Sarà, naturalmente, la cosiddetta sicurezza"[1].

---

* Associato di Istituzioni di Diritto Pubblico nell'Università degli Studi di Milano-Bicocca.

** Il saggio è dedicato alla prof.ssa Maria Paola Viviani Schlein. L'A. ringrazia, per la lettura e la valutazione del manoscritto, i proff. Jacques Ziller, Francesco Rigano, Barbara Randazzo e Diana U. Galetta, ricordando che nel lavoro convergono parte dei risultati della ricerca svolta per il PRIN 2012 *La codificazione dei procedimenti dell'Unione europea*, di cui è responsabile il prof. Jacques Ziller.

[1] M. FOUCAULT, *Nascita della biopolitica. Corso al Collège de France (1978 – 1979)*, Feltrinelli, Milano, 2012, pp. 67-68: per il più ampio brano da cui è tratta la citazione, e le riflessioni sul nesso fra sicurezza e tecnologia che discendono dallo stesso passaggio, v. F. PIZZOLATO, P. COSTA, *Introduzione*, in Id., (a cura di), *Sicurezza, Stato e mercato*, Giuffré, Milano, 2015, VII e ss.

L'Associazione Italiana Costituzionalisti è iscritta al Registro Operatori della Comunicazione dal 9.10.2013 col n. 23897
La Rivista AIC è registrata presso il Tribunale di Roma col n. 339 del 5.8.2010 — Codice ISSN: 2039-8298 (on-line)
Rivista sottoposta a referaggio — Rivista inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche
Direttore Responsabile: Prof. Massimo Luciani — Direttori: Prof. Ginevra Cerrina Feroni, Prof. Emanuele Rossi

Nell'opera dalla quale è tratto questo passaggio, *Michel Foucalt* traccia il nesso fra libertà e sicurezza individuando nel liberalismo – nella relativa "arte di governo, che manipola soprattutto gli interessi" – l'arbitro dell'una e dell'altra, capace di garantire, "agli individui e alla collettività, che saranno esposti il meno possibile ai pericoli."[2]

Difficile, oggi, affermare lo stesso: dall'attuale momento storico emerge infatti un intreccio di questioni che, spesso, disegna in misura differente proprio le fattezze dell'arbitro chiamato a proteggere dalle più diverse insidie i consociati. Questo, perché il suo peculiare ruolo fa ormai perno su ciò che *evidente non è più*: la nozione di pericolo.

Se, come scrive Camilla Buzzacchi, sembra "ormai metabolizzata l'epoca della 'globalizzazionÈ, polarizzata intorno alla categoria dello spazio fisico, e ora l'interesse del mondo scientifico e delle istituzioni – nazionali e sovranazionali – è ampiamente rivolto all'impatto della tecnologia sulla società, interpretando la medesima tecnologia come parametro strategico, responsabile di una nuova forma di complessità"[3], anche il ragionamento intorno a quella nozione e, addirittura, la nozione stessa, possono soltanto cambiare.

Nel momento in cui la tecnologia[4] è "responsabile di una nuova forma di complessità", il (più generico) concetto di pericolo fa riflettere, anzitutto, sul contesto al quale, fino a tempo addietro, è stato ricondotto: un alveo, nel passato relativamente recente, di *un* liberalismo e di *molte* "arti di governo" - a seconda del Paese che quel liberalismo faceva proprio, declinandolo in modo necessariamente unico e irripetibile[5] - divenuto, da nazionale, pure inter- e sovranazionale.

---

[2] Di nuovo M. FOUCAULT, *Nascita della biopolitica*, *cit.*, pp. 67-68; per una disamina del suo pensiero, M. SCHUILENBURG, (en. trans. G. Hall, intr. by D. Garland), *The Securitization of Society: Crime, Risk and Social Order*, New York University Press, New York and London, 2015, spec. 70 ss.; per un'analisi del più ampio tema come trattato dalla dottrina europea e americana sempre M. SCHUILENBURG, *The Securitization of Society: On the Rise of Quasi-Criminal Law and Selective Exclusion*, in *Soc. Justice, vol. 38, no.s 1-2,* 71 ss., spec. 73 per la posizione di M. FOUCAULT su questioni di salute pubblica, 74 per la distinzione fra *safety* e *security* fatta da diversi studiosi (ad es. Z. BAUMAN, L. ZEDNER e M. FOUCAULT), 76 per il nesso fra *securitization* e Stato di diritto, 83 ss. per la rielaborazione proposta da M. SCHUILENBURG dell'opera di M. FOUCAULT '*Sécurité, territoire, population'* and '*Naissance de la biopolitique*' *into a process of securitization*.

[3] C. BUZZACCHI, *Tecnologia e protezione dei dati personali nella società dei "big data". Problemi della profilazione e della garanzia della sicurezza pubblica*, 1. *La tutela della riservatezza come una delle questioni aperte dai* big data, in corso di pubblicazione negli *Studi della Sezione di Diritto pubblico dell'Economia del DiSeaDe*, Università di Milano Bicocca, Giuffré, Milano, 2016; per le tematiche che emergeranno nel corso del testo v., sul più ampio tema delle telecomunicazioni alla luce dei principi costituzionali e sulla disciplina di *Internet*, G. GARDINI, *Le regole dell'informazione. Dal cartaceo al bit*, Giappichelli, Torino, 2014, rispettivamente 239 ss. e 269 ss.; sul nesso fra diritti fondamentali e nuovi mezzi AA.VV., *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Cedam, Padova, 2003, e *A. Valastro*, *Libertà di comunicazione e nuove tecnologie*, Giuffrè, Milano, 2001; sempre attuale poi S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995.

[4] Per i profili qui trattati, S. GURTWIRTH, R. LEENES, P. DE HERT, Y. POULLET, (*Ed.s*), *European Data Protection: in Good Health?*, Springer, Berlin, 2012.

[5] Per tutti le riflessioni di B. CROCE, *Storia d'Europa nel secolo XIX*, Laterza, Bari, 1932, spec. 41 ss.; ID., *Liberismo e liberalismo*, in Id., *Etica e politica*, 1956, Laterza, Roma-Bari, spec. 356 ss.; G. BEDESCHI, *Tra Croce ed Einaudi*, in Id., (a cura di), *Storia del pensiero liberale*, Laterza, Roma-Bari, 1992, 272 ss.; G. SARTORI, *Liberalismo*, in Id., *Elementi di teoria politica*, il Mulino, Bologna, 1996, 139 ss. Sullo Stato di derivazione liberale e sulle relative forme di governo G. DE VERGOTTINI, *Diritto costituzionale comparato*, Cedam, Padova, 4ª ed., 1996, 233 ss. e 542 ss.; per i più diversi profili storico-giuridici che chiariscono l'affermazione del testo, non solo nella prospettiva nazionale, C. MARTINELLI, *Diritto e diritti oltre la Manica*, il Mulino, Bologna, 2014; A. CARDINI, *Storia del liberalismo. Stato e mercato dal liberalismo alla democrazia*, ESI, Napoli, 2009.

L'era del superamento[6] della categoria di spazio fisico[7] sottrae la concezione di pericolo (anche se in misura *solo parziale*, come dimostra la tragica vicenda dell'immigrazione dalla Siria e da zone geopolitiche, non solo limitrofe, altrettanto martoriate) al riferimento rappresentato dalle frontiere nazionali, intese come fisico-politiche, interne ed esterne[8]. Dunque, se queste, da sempre manifestazione, fra l'altro, del binomio amico(-sicurezza)/nemico(-pericolo)[9] – e della relativa percezione, che è cosa di gran lunga differente[10] – non sono più l'unico riferimento della nozione, anche i suoi contorni teorici e concreti mutano.

Il pericolo che, un tempo, affrancato dal "vecchio sistema politico della sovranità", dava origine, "fra il sovrano e il suddito", a "[…] rapporti giuridici [ed …] economici che impegnavano" il primo a proteggere il secondo, "permettendo al suddito di chiedere al sovrano "di essere protetto contro il nemico esterno, o contro il nemico interno", nel "liberalismo [diventano] tutt'altra cosa"[11].

Ai giorni nostri, altra ancora.

Separare la sicurezza, intesa come "costo della produzione della libertà", dalle frontiere, per il mondo occidentale (ma non solo) è la conseguenza del profilarsi di *insidie nuove*, da sommare a quelle risalenti.

Del resto, come osservato in dottrina[12], proprio i fenomeni di inter- e sovranazionalizzazione recenti mettono in discussione alcune certezze: fra queste, la piena integrità della sovranità statale – *che non comporta il superamento della forma-Stato*[13] - e, quindi, il "legame strutturale fra [questa] e le funzioni di ordine e di sicurezza"[14]. Se, da un lato, ciò fa da

---

[6] Più che attuale in quest'ottica Z. BAUMAN, *Modernità e globalizzazione*, (intervista di G. Battiston), Ed. dell'Asino, Roma, 2009. Per le riflessioni sulla separazione fra lo Stato e il territorio, inteso come suo elemento costitutivo, così come acuita dalle specificità dell'*Internet*, e sul relativo riverbero sulla regolamentazione giuridica di quello e altri fenomeni, M.P. VIVIANI SCHLEIN, *Internet e i confini del diritto*, in AA. VV., *Percorsi di diritto dell'informazione*, Giappichelli, Torino, 3ª ed., 2011, 333 ss.

[7] Il riferimento è alla *cit.* poco sopra fatta di C. BUZZACCHI, *Tecnologia e protezione dei dati personali …*, *cit*. Per le questioni di cui ai pgff. 3 ss. C. DE GIACOMO, *Diritto, libertà e* privacy *nel mondo della comunicazione globale*, Giuffrè, Milano, 1999.

[8] Per il nesso fra la nozione delle "frontiere di mare e terra" e gli sviluppi geopolitici recenti E. RICCI, *Il dramma del Mediterraneo: frontiere liquide, confini solidi*, Mimesis, Milano, 2015; per la cornice giuridica alla quale ricondurre questo nesso M. ARCARI, T. SCOVAZZI, *Corso di diritto internazionale*, spec. vol. I, *Caratteri fondamentali ed evoluzione storica del diritto internazionale*, Giuffrè, Milano, 2014.

[9] Per approfondire l'accenno nel testo C. SCHMITT, *Terra e mare*, Adelphi, Milano, 3ª ed., 2006, senza dimenticare il passato inquietante dello studioso, così come emerge in H. QUARITSCH, (a cura di), *Carl Schmitt. Risposte a Norimberga*, Laterza, Roma-Bari, 2006, spec. al cap. 2, *Carl Schmitt: criminale di guerra o esperto?*, 61 ss.

[10] M. DOGLIANI, *Il volto costituzionale della sicurezza*, in G. Cocco, (a cura di), *I diversi volti della sicurezza*, Giuffré, Milano, 2012, spec. 9 (e ss.).

[11] Di nuovo M. FOUCAULT, *Nascita della biopolitica*, *cit.*, pp. 67-68, nel richiamo fatto da F. PIZZOLATO, P. COSTA, *Introduzione*, *cit.*, p. VII.

[12] F. PIZZOLATO, *Mercati e politiche della sicurezza nell'ordinamento dello Stato moderno*, in F. PIZZOLATO, P. COSTA, (a cura di), *Sicurezza, Stato e mercato*, *cit.*, 2.

[13] Per tutti sul punto A. MATTIONI, voce *Sovranità*, in *Digesto delle Discipline Pubblicistiche*, (Aggior.), UTET, Torino, 2013, 665 ss.

[14] Sempre F. PIZZOLATO, *Mercati e politiche della sicurezza …*, *cit.*, 2, e di nuovo M.P. VIVIANI SCHLEIN, *cit.*, 333 ss., spec. 334, che, pur riconoscendo all'*Internet* potenzialità straordinarie, ne coglie "il problema dei problemi", ossia il suo essere una "realtà del tutto a-territoriale": questo profilo emergerà trattando il caso *Schrems*, ai pgff. 4 ss.

cornice a uno sviluppo positivo (ossia a "quel complesso insieme di informazioni che va sotto il nome di *big data* […] straordinario perché consistenti appaiono le prospettive favorevoli per il contesto economico e sociale degli Stati membri e dell'Unione"[15]), da un altro sembra pure capace di disegnare scenari differenti[16].

Può, infatti, mettere a rischio l'equilibrio di alcuni assetti (specificamente, il rapporto fra potere pubblico e poteri privati[17]) e l'inviolabilità di specifici beni e libertà costituzionali[18] finora protetti, anche, dall'equilibrio di quegli assetti[19]. Quali e come, è cosa che emergerà nel corso del testo, con le anticipazioni che qui si fanno.

1.a) "Dopo l'11 settembre", il volto della paura.

Ricorda Alessandro Pace[20] come, "dopo gli avvenimenti – purtroppo non rimasti isolati - dell'11 settembre 2001, la percezione della sicurezza sia profondamente cambiata", senza però per questo far ritenere che il suo bisogno "costituisca ormai il contenuto di un vero e proprio diritto dei cittadini"[21].

Così intesa, la sicurezza[22] è dunque "uno stato psicologico collettivo da cui promana un interesse diffuso, la cui tutela è di competenza esclusiva dello Stato", e l'ordine pubblico, di conseguenza, consisterebbe nel "mero ordine materiale ("*l'ordre dans la rue*" di *Marcel*

---

[15] Di nuovo C. BUZZACCHI, *Tecnologia e protezione dei dati personali …*, *cit.*

[16] Per una posizione opposta a quella di C. BUZZACCHI, *Tecnologia e protezione dei dati personali …*, *cit.*, ossia che evidenzia le irrinunciabili precondizioni di utilizzo dei *big data* per rispettare i principi democratici, F. CHIUSI, *Grazie mr Snowden #Datagate #NSA*, articolo del 17 febbraio 2014 reperibile all'indirizzo *Internet* www.valigiablu.it/grazie-mr-snowden-datagate-nsa/.

[17] Per il profilo pubblico-privato come uno dei problemi caratterizzanti quello della sicurezza M. SCHUILENBURG, *The Securitization of Society …*, *cit.*, 15.

[18] A tutt'oggi fondamentali le riflessioni di N. CHOMSKY, *La democrazia del grande fratello*, Piemme, Casale Monferrato, 2005; v. anche M. AINIS, (a cura di), *Informazione, potere, libertà*, Giappichelli, Torino, 2005, e G. DE MINICO, *Regole: comando e consenso*, Giappichelli, Torino, 2004.

[19] Per approfondire questo accenno D. DONATI, *Società dell'informazione, principio di pubblicità e diritti*, in P. Leyland, D. Donati, G. Gardini, (a cura di), *Freedom of Information in the United Kingdom and Italy – L'accesso alle informazioni nel Regno Unito e in Italia,* (*Center for Constitutional Studies and Democratic Devolopement Lecture Series*), Libreria Bonomo Editrice, Bologna, vol. 8, 2003.

[20] A. PACE, *La sicurezza pubblica nella legalità costituzionale*, in *Riv. tel. AIC*, n. 1, 2015. L'A. sottolinea immediatamente come il cambiamento della percezione della sicurezza pubblica sia mutato due generazioni dopo la II[a] Guerra mondiale, e richiama in questa prospettiva, articolata sull'esperienza italiana, la sua opera, *Libertà e sicurezza. Cinquant'anni dopo*, in *Dir. e soc.*, 2013, 203 ss., e le suggestioni di Z. BAUMANN, *Dallo Stato sociale allo Stato di sicurezza*, in Id., *L'Europa è un'avventura* (*Europe. An Unfinished Adventure*, 2004, trad. it. M. Cupellaro), Laterza, Roma-Bari, 2006, 109 ss.

[21] Ossia, sempre nelle parole di A. PACE, *La sicurezza pubblica …*, *cit.*, pgf. 1., *Perché è inesatto e fuorviante parlare di un diritto alla sicurezza*, *"*non è possibile sostenere né che si tratti di un diritto ad esercitare arbitrariamente le proprie ragioni (artt. 392 c.p.) al di là, quindi, dei limiti consentiti dall'autodifesa (art. 52 c.p.), né che costituisca un preteso diritto a prestazioni positive della polizia e dei carabinieri a semplice richiesta del cittadino, senza alcun margine di discrezionalità da parte delle forze dell'ordine".

[22] Da non confondere, ammonisce A. PACE, sempre in Id., *La sicurezza pubblica …*, *cit.*, pgf. 1., con il "generico bisogno di sicurezza che investe i settori più svariati quali la sicurezza economica, la sicurezza della propria salute ecc.". Per questa considerazione l'A. stesso rinvia a P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in R. Nania, P. Ridola, (a cura di), *I diritti costituzionali*, vol. I, Giappichelli, Torino, 2[a] ed., 2006, 138 ss.

Hauriou)", a rischio[23] solo in presenza di "comportamenti umani violenti o di fatti naturali […] pregiudizievoli per la pubblica incolumità"[24].

Il nesso fra la prima e il secondo[25] starebbe nel fatto che la sicurezza esiste quando l'ordine pubblico viene mantenuto "grazie alla funzione di pubblica sicurezza" e, in particolare, in ragione di quelle misure capaci di "eliminare a monte le cause dei potenziali disordini"[26]. Questo stesso nesso consentirebbe di individuare i limiti imposti dalla legalità costituzionale alla (funzione della) sicurezza, e le disposizioni costituzionali che permettono interventi di natura preventiva[27]; *ma non* l'esercizio di "un ipotetico potere generale di prevenzione"[28].

Ora, gli attentati dell'11 settembre e quelli recenti[29] hanno però reso ancor più necessarie modalità di investigazione estranee a questa cornice (sebbene riconducibili alla seconda metà degli anni Ottanta[30]), perché parte del loro "spazio" è nuova: l'*electronic data processing*[31].

La società dell'informazione[32] pare aver creato l'*humus* più fertile per quel potere di prevenzione, che si esprime fra l'altro in attività d'indagine (uno fra i molti volti della funzione della pubblica sicurezza, qui decisivo) articolate su "*the possibilities of automatic data processing and its capacity of handling and connecting items*"[33].

---

[23] Di nuovo M. SCHUILENBURG, *The Securitization of Society: Crime, Risk and Social Order*, *cit.*, 60 ss., 286 ss.

[24] A. PACE, sempre in ID., *La sicurezza pubblica …*, *cit.*, pgf. 2., evidenzia come quella concezione della sicurezza pubblica sia stata individuata dalla Corte costituzionale: v. Corte cost., sent. 14 giugno 1956, n. 2, e le osservazioni sull'equilibrio fra sicurezza e pericolo di Z. BAUMANN, *Community. Seeking Safety in an Insecure World,* Polity Press, Cambridge-Maiden, 2008.

[25] Importanti le riflessioni in tema di Z. BAUMANN, *Community: Seeking Safety …*, *cit.*

[26] Di nuovo A. PACE, in Id., *La sicurezza pubblica …*, *cit.*, pgf. 2., facendo propria la posizione di W.I. JENNINGS, *Public Order*, in *Pol. Qu.*, vol. 8, 1937, 7 ss.

[27] Ossia le misure "di sicurezza sociale ed altri servizi pubblici", adottate per i soli motivi di ordine e di sicurezza pubblica: A. PACE, *La sicurezza pubblica …*, *cit.*, pgf. 2, e M. SCHUILENBURG, *The Securitization of Society: Crime, Risk and Social Order*, *cit.*, 29 ss.

[28] A. PACE, in Id., *La sicurezza pubblica …*, *cit.*, pgf. 2., laddove critica J. ISENSEE, *Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates*, Duncker&Humboldt, Berlin-New York, 1983, spec. 34 ss., e G. CERRINA, G. MORBIDELLI, *La sicurezza come valore superprimario*, in *Percorsi cost.*, n. 1, 2008, 41.

[29] Dopo l'attentato di Parigi del 2015 alla redazione della testata satirica *Charlie Hebdo*, Z. BAUMAN svolge una lezione in Italia sui temi dell'integrazione, del multiculturalismo e dei pericoli recenti, poi raccolta in ID., L. Noseda, (a cura di), *La convivenza. Un intervento dopo gli attentati di Parigi*, Casagrande, Bellinzona, 2015.

[30] Ci si riferisce, fra l'altro, alle questioni e agli accadimenti collegati alla legge federale *Computer Fraud Act Abuse* (o CFAA), del 1986, adottata per modificare la preesistente normativa sulla stessa materia (18 U.S.C. §1030), e poi emendata a sua volta numerose volte, fino allo *Theft Enforcement and Restitution Act* del 2008: per i fatti legati a questa, impossibili qui da ricostruire, v. l'indirizzo *Internet* https://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. Per la proposta di ulteriori revisioni dell'atto normativo fatta dall'amministrazione *Obama* nel gennaio 2015 v. invece https://www.usa.gov/.

[31] W. ACHELPÖHLER, H. NIEHAUS, *Data Screening as a Means of Preventing Islamist Terrorist Attacks on Germany*, in *GLJ*, n. 5, vol. 5, 495 ss.

[32] A completamento dell'approccio suggerito R. ZACCARIA, voce *Informazione e telecomunicazioni*, in G. Santaniello, (diretto da), *Trattato di diritto amministrativo*, Cedam, Padova, 1999.

[33] W. ACHELPÖHLER, H. NIEHAUS, *cit.*, 496.

Lo sviluppo delle tecnologie dell'informazione alimenta il cortocircuito fra legalità costituzionale, diritti fondamentali[34] e potere generale di prevenzione[35]. In particolare, la raccolta di dati anche non sensibili e l'accesso indiscriminato agli stessi (tramite l'attività di *data screening*, pure quando esercitata da articolazioni del pubblico potere per proteggere i consociati), incide, soprattutto, sul diritto al rispetto della vita privata[36]. Per questo, alcune giurisdizioni costituzionali, convinte del fatto che, in virtù delle tecniche menzionate, non sia più possibile operare la distinzione fra dati sensibili e altri, ritengono che "*there is no 'insignificant' data left in times of automatic data processing*"[37]. Se così è, la conseguenza è una soltanto: "*any poll, storage or passing on of personal data, even the fact that the state simply takes note of them, means an intrusion into the right to data privacy*"[38].

Da qui, in particolare in Germania, dopo l'11 settembre, le pronunce costituzionali sul principio della riservatezza dei dati[39]. Sulla presunzione, infatti, che nella Repubblica federale risiedessero terroristi in attesa di compiere attentati, in ogni *Land* le autorità di pubblica sicurezza richiedevano a tutte le università tedesche di fornire i dati in loro possesso degli studenti. Nascevano così il dibattito sull'intrusione nel privato da parte del pubblico potere (in nome di un pericolo *forse* attuale), e i tanti ricorsi che soltanto nello *Hessen*, nel *Nordrhein-Westfalen* e a Berlino hanno avuto esito favorevole agli studenti interessati, ma non solo. La consapevolezza che, come avvenuto in relazione al terrorismo interno negli anni Settanta, la polizia giudiziaria federale avrebbe conservato i dati di decine di migliaia di persone ha iniziato a far temere molti per il rispetto della vita privata[40].

---

[34] Per le tematiche che emergeranno di seguito v. A. CERRI, voce *Riservatezza, (diritto alla)*, II, *Diritto comparato e straniero*, in *Enc. giur. Treccani*, vol. XXVI, Roma, 1991; A. CLEMENTE, (a cura di), *Privacy*, Cedam, Padova, 1999; M.G. LOSANO, (a cura di), *La legge italiana sulla* privacy*. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001.

[35] In questa luce il quadro fornito dal Commissario delle Nazioni Unite sul tema: *The Right to Privacy in the Digital Age*. *Report of the Office of the United Nations High Commissioner for Human Rights*, *30th June 2014*, spec. la lett. *A. The Right to Protection Against Arbitrary or Unlawful Interference with Privacy, Family, Home or Correspondence*, pgff. 15-27, 6 ss., e la lett. *C. Who Is Protected, and Where?*, pgff. 31-36, 11 ss.; per il testo integrale v. l'indirizzo *Internet* www.ohchr.org/EN/.../A.HRC.27.37_en.pdf.

[36] Particolarmente attuale in questa luce J. WELP, *Zur Legalisierung der Rasterfahndung,* in H.U. Erichsen, H. Kollhosser, J. Welp, (*Hg.*)*, Recht der Persönlichkeit*, Bd. 389, Duncker&Humboldt, Berlin, 1996, 389 ss. Come noto, il diritto alla *privacy* è stato sviluppato proprio negli Stati Uniti: fra tutti, sempre attuali E. BLOUSTEIN, *Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser*, in *New York Univ. Law Rev.*, n. 39, 1964, 962 ss.; H. GROSS, *The Concept of Privacy,* in *New York Univ. Law Rev.*, n. 42, 1967, 34 ss.; R. GAVISON, *Privacy and the Limits of Law,* in *Yale Law Journal*, n. 89, 1980, 421 ss., e J. HIRSCHLEIFER, *Privacy: its Origin, Function and Future*, in *Journal of Legal Studies*, n. 9, 1980, 649 ss.

[37] I giudici costituzionali tedeschi, ad esempio, derivano il diritto all'autodeterminazione inerente i dati personali dalla lettura congiunta degli artt. 2, primo comma e 1, primo comma della Legge fondamentale (*Grundgesetz* o GG): così BVerfG 65, 1 <43-45>, nella ricostruzione di W. ACHELPÖHLER, H. NIEHAUS, *cit.*, 497.

[38] Di nuovo W. ACHELPÖHLER, H. NIEHAUS, *cit.*, 497. A fondamento di questa posizione U. DI FABIO, voce *Art. 2*, Rn. 176, in T. Maunz, G. Dürig, (Hg.), *Grundgesetz*, (39. EgLf), Beck, München, 2001.

[39] La più significativa sul principio resta BVerfG 65, 1 (<43>. Sempre attuale poi in questa prospettiva A. ETZIONI, *The Limits of Privacy*, Basic Books, New York, 1999.

[40] Per la vicenda, la nozione di pericolo attuale e concreto, e i profili giuridici legati, W. ACHELPÖHLER, H. NIEHAUS, *cit.*, 497 ss., spec. 504, dove gli Aa. ricordano che i dati richiesti dalle autorità solo nella maggior parte delle università riguardavano gli studenti "*male, 18 years old at least, 41 at most, Islamic, student or former student, valid permit of residence without any local restriction, unknown to the police, no children of his own, financially independent ([…] irregular deposits in the bank account)*"; in altre, venivano chieste pure differenti informazioni.

Nell'arco di poco, le dimensioni di questo fenomeno sono enormemente cresciute[41].

Di seguito si analizzeranno i casi *Apple*, *Schrems* e *Microsoft* per approfondire il forte impatto del *data screening* sulla sicurezza collettiva e la sfera individuale privata[42] (che ha inciso addirittura sulle relazioni diplomatico-commerciali fra Unione europea e Stati Uniti d'America), alla luce della tesi al fondo di questo lavoro.

Soltanto le Costituzioni e i principi che le reggono possono garantire, attraverso il pubblico potere, l'equilibrio fra sicurezza e diritti; troppe le insidie celate da scelte diverse, affidate a poteri privati, che perseguono interessi di parte.

2. USA vs. Apple: il mondo capovolto.

I modelli di relazione tra sicurezza e Stato, ai quali (sulla spinta dell'esperienza sovranazionale), si è aggiunto il cd. mercato[43], sono stati classificati in letteratura distinguendoli fra premoderno, moderno e postmoderno[44], indicando le novità correlate di cui recenti sviluppi sarebbero portatori. Attraverso la cd. " 'privatizzazione della sicurezza' ", infatti, "il modello liberale classico e, con ciò, la sua legittimità", oggi (più che mai) potrebbero essere messi in dubbio, con un effetto.

Per quanto lenta, l'erosione del "legame strutturale fra la sovranità statale e le funzioni di ordine e di sicurezza" non condurrebbe solo al perseguimento di obiettivi differenti (ossia, nel cd. premoderno, a "un progetto teso a realizzare il bene" e, nella modernità, a un mezzo "per limitare il male"[45]), ma inciderebbe sugli equilibri che reggono il binomio ordinamento giuridico statuale-ente a fini generali/ordinamenti giuridici minori-enti a fini particolari - o, con una formula imprecisa ma efficace nella sua semplicità, Stato/soggetti privati.

Sottrarre le funzioni dell'ordine e della sicurezza, in tutto o in parte, alla sovranità statale o allo Stato e alle sue istituzioni *tout court*, concretizza all'orizzonte un rischio: abbandonare la connotazione *costituzionale* della sicurezza.

Come discusso nel volume che raccoglie la prima parte di questa ricerca[46], la sicurezza è difatti – oltre a quanto sopra già affermato - un bene costituzionale che *può inserirsi*

---

[41] Sui profili legati alle questioni toccate G. GARDINI, *Per un'etica dell'informazione e della comunicazione*, FrancoAngeli, Milano, 2009, e, di nuovo, M.P. VIVIANI SCHLEIN, *cit.*, 335 e 337-338, per la violazione della *privacy* così come emersa nel caso *Google-Vividown*. Per la tutela della *privacy* assicurata nell'ordinamento giuridico italiano, M. CUNIBERTI, *Riservatezza e identità personale*, in AA. VV., *Percorsi di diritto dell'informazione*, Giappichelli, Torino, 3ª ed., 2011, spec. 115, laddove invoca una riflessione giuridica rinnovata sull'evoluzione tecnologica, perché ha aumentato "le possibilità di attacco alla sfera privata, di manipolazione e di controllo dei dati personali".

[42] Osservano il tema della sorveglianza come tipico della società contemporanea, evidenziando come siano i "sorvegliati" a fornire spesso informazioni personali (ad es. tramite i *social network*) Z. BAUMAN, D. LYON, *Sesto potere: la sorveglianza nella modernità liquida*, GLF ed. Laterza, Bari, 2014.

[43] Per le tematiche già affrontate che ruotano intorno a questo nuovo soggetto della relazione sempre F. PIZZOLATO, P. COSTA, *Sicurezza, Stato e mercato*, *cit.*

[44] F. PIZZOLATO, P. COSTA, *Introduzione*, *cit.*, VIII-IX ss.

[45] F. PIZZOLATO, *Mercati e politiche della sicurezza …*, *cit.*, 2-3; per l'approfondimento bibliografico a sostegno del ragionamento dello stesso A. v., in particolare, le note da (7) fino a (10) compresa, sempre 2-3.

[46] F. PIZZOLATO, P. COSTA, *Sicurezza, Stato e mercato*, *cit.*

nel bilanciamento con altri beni e/o diritti costituzionali, ma *non* al punto da *essere posta sul loro stesso, identico piano*[47].

Non al punto, di certo, da far sì che, in nome della sua garanzia, lo Stato possa violare diritti costituzionalmente protetti - peraltro, garantiti pure da atti normativi e non, inter- e sovranazionali[48], alcuni dei quali vincolanti una parte almeno degli attori della comunità internazionale ed europea[49]. Nemmeno al punto, però, da far immaginare che lo Stato abdichi al suo ruolo (e alle garanzie che questo comporta) a favore di soggetti privati.

Quest'ultimo è il pericolo di fronte al quale ci troviamo (fra molti altri, beninteso) proprio quando, nella discussione intorno alla sicurezza, irrompe una nuova attrice: la tecnologia[50].

Chiarisce quanto affermato la più che nota attualità: fra le stragi terroristiche conosciute, quella della cittadina statunitense di San Bernardino ha attirato ovunque attenzione, non solo per la perdita di vite umane, ma per il confronto nato fra il *Federal Bureau of Investigation* (FBI) degli Stati Uniti (o USA) e la *Apple Inc.*[51]. Un breve riepilogo dei fatti (al di là della – *parrebbe* - conclusione recente della vicenda) aiuta a capire meglio il nesso fra quest'ultima, altri casi d'oltreoceano e i temi qui trattati. Il tutto, per leggere in chiave nazionale ed europea[52] un accadimento che per sua natura può solo superare i tradizionali confini fisici.

Per svolgere le indagini, gli investigatori federali avevano necessità di acquisire, fra l'altro, i dati contenuti nell'*iPhone* di uno degli attentatori di San Bernardino, *Rizwan Farouk*. Indispensabile allo scopo conoscere la *password* a protezione del telefono cellulare: superato il decimo tentativo per accedere alla memoria del congegno, sempre digitando una parola-chiave errata, tutte le informazioni custodite sarebbero state altrimenti distrutte da un meccanismo di sicurezza automatico. Di conseguenza, alla *Apple*, la società produttrice, era stato chiesto di creare un *software* in grado di lasciar inserire agli investigatori federali tutte le

---

[47] In questa luce T.F. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali*, in S. Vida, (a cura di), *Diritti umani. Teorie, analisi, applicazi*oni, Bononia University Press, Bologna, 2008, 1 ss., e C. BUZZACCHI, *Sicurezza e* Securitization *tra Stati, Unione europea e mercato: prerogativa dei pubblici poteri o attività economica?*, in F. PIZZOLATO, P. COSTA, *Sicurezza, Stato e mercato*, *cit.*, 87 ss.

[48] Sulle libertà e i diritti, dalle origini sino alla internazionalizzazione, e sulla loro dimensione regionale, A. RINELLA, *Diritti e libertà fondamentali*, in G. Morbidelli, L. Pegoraro, A. Rinella, M. Volpi, (a cura di), *Diritto pubblico comparato*, Giappichelli, Torino, 5ª ed., 2016, rispettivamente 305 ss. e 325-334.

[49] L'affermazione va compresa nel senso che, come noto, non tutti gli Stati parte delle Nazioni Unite hanno ratificato atti a tutela di diritti e libertà della persona umana, e che, per ovvie ragioni geopolitiche, quelli europei ideati allo stesso scopo non vincolano chi non è parte o dell'UE o del Consiglio d'Europa. Sul carattere vincolante della Carta dei diritti dell'UE, K. STERN, *La Carta europea dei Diritti fondamentali. La forza vincolante e l'ambito di applicazione dei diritti codificati nella Carta*, in *RIDPC*, n. 6, 2014, 1235 ss.

[50] Il termine "tecnologia" è qui usato nel senso più lato possibile per introdurre le problematiche di seguito approfondite, relative ai mezzi tecnici a protezione della *privacy*.

[51] Lo hanno immediatamente affrontato G. VIGEVANI e C. MELZI nell'articolo pubblicato sul *Sole 24h* dello scorso 19 febbraio 2016, 28, intitolato *In gioco c'è la libertà dei singoli*.

[52] Per approfondire, invece, il *common law*, L. PEGORARO, A. RINELLA, *Le fonti di legittimazione*, in G. Morbidelli, L. Pegoraro, A. Rinella, M. Volpi, (a cura di), *Diritto pubblico comparato*, *cit.*, 63 ss.

possibili *passwords* senza correre alcun rischio, compreso quello di attivare altri strumenti di protezione collegati allo *hardware* (in nota le necessarie precisazioni tecniche[53]).

Avendo la società rifiutato di collaborare, l'unica via per costringerla a farlo è stata quella giudiziaria: il magistrato adito dal Governo federale USA – *Shery Pim*, *U.S. Magistrate Judge* della *U.S. District Court* del *Central District* della California (in breve MJ)[54] – ha dunque emesso un *order*[55] con il quale ha ingiunto alla multinazionale di fornire agli inquirenti il *software* richiesto e/o ogni utile intervento tecnico alternativo. Per la portata delle questioni

---

[53] Probabile che l'aiuto alla *Apple Inc.* sia stato richiesto anche in ragione di alcuni errori compiuti dagli agenti federali, allo scopo indicato nel testo, nella primissima fase dell'indagine.

Precisa F. CHIUSI, FBI-Apple*: la battaglia sulla crittografia. E perché* Apple *ha ragione*, articolo del 18 febbraio 2016 reperibile all'indirizzo *Internet* http://www.valigiablu.it/fbi-apple-iphone-terrorismo/, che il MJ chiede a *Apple* di "Consentire all'FBI di provare a inserire la *password* corretta (in sostanza, abilitare tentativi infiniti di trovarla, una tecnica detta "*brute force*"); 3. Garantire che non ci siano le attese (*delay*) tra un tentativo e l'altro attualmente previste da iOS, a meno di quelle necessarie al funzionamento dell'*hardware*. Il tutto deve essere fatto tramite un programma – SIF, *Software Image File* – dotato di un identificativo unico *Apple*, e in grado di funzionare solo sul telefonino dell'attentatore. Il programma deve essere messo in funzione o in una struttura dell'FBI o in una di Apple". La richiesta di "aiutare l'FBI a decifrare i messaggi sui suoi *device iOS*", "nota il *Washington Post*, non sarebbe in ogni caso riassumibile con l'idea che l'FBI abbia più genericamente chiesto ad *Apple* di 'violare' la sua crittografia".

[54] Come noto, il sistema giudiziario statunitense è costruito su una complessa articolazione (per la quale, oltre alla bibliografia qui indicata, si rinvia al sito del Dipartimento di Giustizia USA, all'indirizzo https://www.justice.gov/usao/justice-101/federal-courts). Istituiti a norma del 28 U.S.C. § 631, i cd. *United States Magistrate Judges* sono giudici federali monocratici delle *U.S. District Courts* (ossia delle corti federali ubicate nei distretti giudiziari federali – i *Federal Iudicial Districts* - presenti negli Stati federati); vengono designati da un comitato, il cd. *Citizen's Merit Screening Committee*, ed eletti a maggioranza dai *District Court Judges* non a riposo. Le decisioni degli MJ, la cui competenza è fissata per legge o loro delegata dai *District Judges* (che, per questo, può variare molto da Stato a Stato), possono essere impugnate dinanzi ai *District Judges*, la cui composizione è collegiale. Avverso le decisioni federali di primo grado (cioè quelle delle *District Courts*) si può ricorrere di fronte alle *U.S. Courts of Appeal*, ossia il collegio, presieduto da un giudice nominato dal *Chief Justice* della Corte Suprema, la cui giurisdizione si estende su uno dei *circuits* in cui è suddiviso il territorio federale. Tutte le decisioni definitive dei giudici federali possono essere impugnate dinanzi la Corte Suprema, anche se, come spesso sostenuto, quest'ultima opera come Corte costituzionale e non, "semplicemente", come giudice di ultima istanza: per questa ricostruzione A.T. VON MEHREN, *U.S. Legal System: Between the Common Law and Civil Law Legal Tradition*, Centro di studi e ricerche di diritto comparato e straniero, Roma, 2000; sul potere giudiziario anglosassone e nordamericano G. MORBIDELLI, *L'organizzazione giudiziaria in Gran Bretagna e negli Stati Uniti*, in G. Morbidelli, L. Pegoraro, A. Reposo, M. Volpi, (a cura di), *Diritto costituzionale italiano e comparato*, *cit.*, 708 ss.; per ogni approfondimento sulla forma di governo degli USA di nuovo G. DE VERGOTTINI, *cit.,* 557 ss., e spec. 564 per le considerazioni sulla Corte Suprema. Per una critica, invece, della distinzione netta fra sindacato di costituzionalità accentrato e diffuso, L. PEGORARO, *Giustizia costituzionale comparata: dai modelli ai sistemi*, Giappichelli, Torino, 2015, e, per la disamina del sindacato di costituzionalità negli USA, ID., *Il controllo giurisdizionale: genesi della* judicial review of legislation *negli Stati Uniti d'America e controllo di costituzionalità*, in G. Morbidelli, L. Pegoraro, A. Rinella, M. Volpi, (a cura di), *Diritto pubblico comparato*, *cit.*, 554-557.

[55] *Order Compelling Apple, Inc. to Assist Agents in Search*, *in the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, 35KGD203*, (*15-0451M*), *U.S. District Court for the Central District of California*, *February 16th, 2016*, il cui testo è reperibile all'indirizzo *Internet* https://www.cacd.uscourts.gov/.

che l'*order* comporta, l'amministratore delegato di *Apple*, *Tim Cook*, ha scritto una lettera aperta[56], i cui passaggi rilevanti per quanto qui interessa sono i seguenti.

Nella lettera, *Cook* sottolineava che, alla richiesta di collaborazione dell'FBI, *Apple* non si era opposta, anzi[57]. Il problema, però, nasceva nell'istante in cui l'FBI chiedeva di creare una *backdoor*[58] capace di aggirare il meccanismo di protezione dei dati sopra ricordato. *Apple* avrebbe potuto sviluppare un simile *software* – ma, in quel momento, non voleva farlo, per la seguente ragione. Secondo *Cook*, chi conosce i fondamentali della sicurezza digitale può facilmente intuire le conseguenze abnormi della richiesta del Governo federale. Infatti, nessuno può garantire che, una volta ideato, un simile *software* possa essere utilizzato solo nelle indagini in corso, anzi: "*in the physical world",* quel *software* potrebbe essere "*the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable*."

Da qui, il rifiuto della *Apple* di rispettare l'*order* del MJ californiano, che avrebbe messo a rischio gli stessi cittadini americani dalle azioni criminali[59] compiute nel cyberspazio[60] o da *hackers* [61].

Ora, se la vicenda da un lato ricalca schemi noti, per i quali la garanzia della sicurezza si trasforma nel sacrificio, imposto al singolo consociato, dell'inviolabilità della sua sfera privata (intesa come l'alveo "naturale" dei diritti intangibili[62]), dall'altro, evidenzia come l'ampia tematica della "tecnologia" funga da punto di scontro non soltanto, come ovvio, fra

---

[56] Il testo integrale della lettera, rivolta ai clienti di *Apple*, si trova al seguente indirizzo *Internet*: http://www.apple.com/customer-letter/. Per il testo dell'*order* v. anche www.scpr.org/news/2016/02/16/57621/judge-orders-apple-to-help-hack-san-bernardino-kil/.

[57] Al contrario, sostiene *T. Cook*, quando "*the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal*".

[58] Continua *T. Cook*: "*the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession. The FBI may use different words to describe this tool, but make no mistake: building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control*."

[59] Per i nessi in tema di *privacy* e problematiche di natura penalistica v. la collettanea curata da E. CLAES, A. DUFF, S. GUTWIRTH, (*Ed.s*), *Privacy and the Criminal Law*, Intersentia, Antwerpen-Oxford, 2006, spec. il cap. di P. DE HERT, S. GUTWIRTH, *Privacy, Data Protection and Law Enforcement. Opacy of the Individual and Transparency of the Power*, 61 ss.

[60] Per questo specifico profilo E. CATELANI, R. FILACI, *Libertà di espressione,* Internet *e* cyber crime*: quali forme di cooperazione?*, in P. Caretti, (a cura di), *L'informazione, il percorso di una libertà*, Passigli, Milano, 2012, vol. II, 34 ss.

[61] Conclude quindi *T. Cook* che la risposta fattiva alla richiesta dell'FBI comprometterebbe "*decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe*."

[62] Diritti esercitati, fra l'altro, nel segno di una cittadinanza consapevole e attiva: sul punto, anche per la ricca bibliografia, J. E. COHEN, *What is Privacy for?*, in *Harvard Law Rev.*, n. 126, 2012, 1904 ss., spec. 1912-1915 sul tema della sorveglianza, e 1918-1927 su quello dei *big data*, e D. KLITOU, *Privacy-inventing Technologies and Privacy by Design: Safeguarding Privacy, Liberty & Security in the 21st Century*, T.M.C. Asser Press, The Hague, 2014.

sicurezza e libertà (o autorità e singoli individui, non necessariamente cittadini), ma, il che pare ben più grave, fra potere pubblico e poteri privati.

Rispondendo alla richiesta del Governo USA, e dando seguito all'*order* di un magistrato federale, *Apple* avrebbe dovuto sviluppare lo strumento capace di decrittare tutto ciò (o molto di quello che) ruota intorno alla vita privata dei suoi "*customers*" e, per questa via, di quella di "*tens of millions of American citizens*"[63].

Ha però scelto, *in quel momento almeno*, di non farlo, ergendosi a difensore di un bene giuridico (la sicurezza dei dati, anche non sensibili), da ritenere inviolabile se si vuole proteggere la sfera delle libertà dell'individuo da aggressioni e interferenze alle quali nemmeno un governo dalle radici democratiche come quello statunitense è legittimato.

Detto altrimenti: siamo di fronte a una conquista, o a una nuova minaccia?

3. Principi liberali, diritti e garanzie costituzionali: a rischio, in nome della sicurezza?

Come immaginabile, il caso è diventato una battaglia di principio[64]. Non appena l'*order* dello scorso 16 febbraio 2016 è divenuto noto alla pubblica opinione, *Edward Snowden*, conosciuto per avere rivelato i programmi di sorveglianza massiccia e indiscriminata degli Esecutivi statunitense e britannico[65], ha sintetizzato questa chiave di lettura dell'accaduto, affidandola a un *tweet* suggestivo: *"The @FBI is creating a world where citizens rely on #Apple to defend their rights, rather than the other way round".*

L'erosione del "legame strutturale fra la sovranità statale e le funzioni di ordine e di sicurezza" può dunque non solo condurre al perseguimento di obiettivi differenti – realizzare il bene o limitare il male[66]: addirittura, può delegittimare lo Stato, il pubblico potere, al punto da metterne in discussione il ruolo di difensore delle libertà costituzionalmente protette. Quando la sicurezza pare meglio garantita da un soggetto privato – da una multinazionale attrice di punta del mercato dell'informatica e delle comunicazioni – questo è quello che succede.

C'è quindi da chiedersi se abbia ragione, fra i tanti, *Edward Snowden*, o se altre siano le letture *costituzionalmente obbligate o possibili* dell'accaduto. Fermo restando che l'FBI ha

---

[63] Sempre la lettera *cit.* di *T. Cook*.

[64] Di notevole interesse il dibattito e le posizioni riportate nel sito della *American Civil Liberties Union*, all'indirizzo *Internet* www.aclu.org., e, sulla *privacy* intesa come un tema di "etica pubblica", da disciplinare grazie a norme condivise, data la complessità dell'architettura sociale e istituzionale odierna, M. BOCCHIOLA, Privacy*: filosofia e politica di un concetto inesistente*, (con prefazione di S. Rodotà), Luiss University Press, Roma, 2014.

[65] Fondamentali le riflessioni di F. CHIUSI sul punto, sviluppate nell'articolo *Grazie mr Snowden #Datagate #NSA*, *cit.*

[66] Il riferimento è di nuovo a F. PIZZOLATO, *Mercati e politiche della sicurezza …*, *cit.*, per l'approfondimento bibliografico a sostegno del ragionamento dello stesso A. v., in particolare, le note a piè di pagina (7) fino a (10) compresa, 2-3. Affronta invece numerosi casi concreti, utili per integrare quelli qui trattati, G. FINOCCHIARO, Privacy *e protezione dei dati personali: disciplina e strumenti operativi*, Zanichelli, Bologna, 2012.

trovato il modo di agire grazie a un terzo la cui identità non è nota[67], questo il ragionamento qui proposto.

Il MJ *Pim* emette l'*order* sulla base giuridica dell'*All Writs Act* (o AWA)[68], e sul precedente *search warrant* relativo allo stesso caso, ingiungendo[69] alla *Apple* di aggirare o disabilitare il sistema di sicurezza di cancellazione dei dati; di permettere agli agenti federali di inserire, mediante ogni possibile protocollo in uso sull'*iPhone*, un numero imprecisato di *passwords* per accedere ai dati protetti; di garantire che, all'immissione delle *passwords*, il *software* dell'*iPhone* non faccia scattare meccanismi difensivi capaci di superare quelli propri dall'*hardware*[70].

Pim aggiunge, infine, che *Apple* non deve tenere copia dei dati scoperti, perché la custodia delle prove cade sotto l'esclusiva responsabilità degli agenti federali[71]. Di fondamentale importanza per comprendere il comportamento dell'FBI successivo all'*order* la richiesta del MJ di non far attivare automatismi di protezione dell'*hardware*, sulla quale si tornerà dopo, al pgf. 3.c).

Le questioni sulle quali soffermarsi consistono nel chiedersi anzitutto se l'*order* così scritto *(a)* rientri nella cornice di un ordinamento giuridico fondato sulla separazione dei poteri e la garanzia dei diritti fondamentali: quello statunitense, nel caso di specie, ma anche altri, le cui radici politico-giuridiche affondano nell'art. 16 della Dichiarazione dei Diritti dell'Uomo e del Cittadino del 1789[72]. Poi, è necessario capire se *(b)* il sacrificio individuale che un simile atto comporta (che ha un duplice volto: da un lato, conduce alla violazione, da parte dello Stato, della sfera privata di un singolo individuo, dall'altro, impone a un soggetto privato di adoperarsi per far raggiungere a un corpo di sicurezza dello stesso Stato questo scopo) rientri nei limiti costituzionalmente legittimi[73] posti a garanzia della *public safety* e *national security*, o della sicurezza *tout court*.

---

[67] Diverse le ipotesi formulate sulla stampa europea e statunitense, nessuna delle quali è significativa per il ragionamento esposto nel testo.

[68] Sull'*All Writs Act*, 28 United States Code (U.S.C.) § 1651, 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, 293 ss., 296 ss., anche per la bibliografia che ricostruisce l'applicazione fatta dell'atto, nel corso dei decenni, in sede giudiziaria.

[69] Si indicano qui quelli previsti espressamente al punto 2. dell'*order*, non soffermandosi su quelli ulteriori, di cui ai punti 3. e 4., di non immediato rilievo.

[70] Per i profili squisitamente tecnici si rimanda alle osservazioni di B. SCHNEIER, all'indirizzo *Internet* www.schneier.com/blog/archives/2016/02/decrypting_an_i.html; e www.schneier.com/blog/archives/2016/02/the_importance_.html;www.schneier.com/blog/archives/2016/03/lots_more_writi.html; per i più recenti risultati del *Workshop on the Economics of Information Security (WEIS)*, sempre B. SCHNEIER, (*Ed.*), *Economics of Information Security and Privacy, III*, Springer, New York, 2013.

[71] Per queste importanti indicazioni v. il punto 6. dell'*order*.

[72] Ossia al noto testo "Ogni società in cui la garanzia dei diritti non è assicurata, né la separazione dei poteri stabilita, non ha una costituzione", per il quale P. BISCARETTI DI RUFFIA, *Le Costituzioni di dieci Stati di "democrazia stabilizzata",* Giuffrè, Milano, 1994, 169.

[73] Per quanto si chiarisce di seguito nel testo, la questione indicata *sub* b) può essere inizialmente analizzata articolandola sul caso americano, perché le riflessioni relative, per i principi sui quali sono fondate, valgono, come si vedrà, anche per ordinamenti giuridici diversi.

All'ombra di questi profili legati a un caso concreto, si delinea un problema teorico[74] che qui si approfondisce perché interessa non soltanto l'ordinamento giuridico statunitense: dal principio di separazione dei poteri alla riserva di legge e di giurisdizione (per indicare solo gli istituti di garanzia più significativi e diffusi nelle aree geopolitiche almeno occidentali), ogni ordinamento giuridico a fini generali appronta diversi strumenti per proteggere le libertà[75]. È fin troppo noto, come dimostra la storia passata e recente qui da non indagare, che, a volte o spesso, proprio i soggetti istituzionali non rispettino quelle tutele.

C'è da chiedersi allora – *con urgenza* – se, quando questo accade, la soluzione stia nel rinunciare alle garanzie conquistate grazie ai principi liberali delle due Rivoluzioni settecentesche, custoditi dalle Costituzioni contemporanee, per sostituirle con altre, difese da nuovi attori[76].

3.a) Sulla separazione dei poteri: Pim vs. Orenstein.

Le questioni appena accennate ottengono una risposta implicita da parte del MJ californiano *Shery Pim*, che porta a ordinare alla *Apple* di aiutare come descritto l'FBI, e una esplicita, del tutto diversa, formulata pochi giorni dopo da *James Orenstein*, MJ di *New York*. Premesso che, solo nel secondo caso, la vicenda non si è ancora conclusa, facile è immaginare come, al di là delle intenzioni di *Apple* o del Governo USA, prima o poi si arriverà a una pronuncia della Corte Suprema, oppure all'istituzione di una commissione d'inchiesta o sulla sicurezza digitale in seno al Congresso[77] (anche in ragione del *plaintiff* presentato lo scorso 14 aprile dalla *Microsoft* dinanzi al magistrato di *Seattle*, per il quale *infra*, al pgf. 8)[78]; queste comunque le considerazioni qui rilevanti.

James Orenstein, *Magistrate Judge* della *U.S. D.C.* dello *Eastern District* di *New York*, il 29 febbraio 2016, a nemmeno due settimane di distanza dall'*order* del 16 febbraio

---

[74] Per ogni approfondimento necessario S. RODOTÀ, Privacy *e costruzioni della sfera privata. Ipotesi e prospettive*, in *Pol. Dir.*, 1991, 521 ss.

[75] In particolare, sulla possibilità che, nell'ordinamento giuridico nordamericano, la *privacy* possa configurare il contenuto di un diritto fondamentale della persona umana, E. CLAES, *Does Privacy Deserve to be Accorded the Status of a Human Right?*, in E. Claes, A. Duff, S. Gutwirth, (*Ed.s*), *Privacy and the Criminal Law*, *cit.*, 183 ss. Si v. inoltre S. RODOTÀ, *Data Protection as Fundamental Right*, in S. Gurtwirth, Y. Poullet, P. de Hert, C. de Terwangne, S. Nouwt, (*Ed.s*), *Reinventing Data Protection?*, Springer, Berlin (New York), 2009, 77 ss.

[76] Ossia e di nuovo il principio di separazione dei poteri e quello relativo alla garanzia dei diritti. Sulla più ampia tematica che ruota intorno (anche) a questi L. ZEDNER, *Privacy Implications of New Penal Technologies*, in E. Claes, A. Duff, S. Gutwirth, (*Ed.s*), *Privacy and the Criminal Law*, *cit.*, 175 ss.

[77] È intenzione del senatore democratico *M. Warner* e del deputato repubblicano *M. McCaul* istituire quantomeno una commissione parlamentare che affronti il tema della sicurezza digitale: fcw.com/articles/2016/02/29/mccaul-warner-encryption.aspx; sul *Digital Commission Act* presentato alla camera dei Rappresentanti del Congresso USA il 29 febbraio 2016 v. invece homeland.house.gov/mccaul-warner-commission-2/.

[78] *U.S. D.C.* dello *Western District* di *Washington, Seattle, Microsoft Co. v. The United States Department of Justice*, *Complaint for Declaratory Judgement* del 14 aprile 2016, reperibile all'indirizzo *Internet* https://dockets.justia.com/browse/state-washington/noscat-13/nos-890.

2016, redige un *Memorandum and Order*[79] che affronta in modo diametralmente opposto le tematiche in gioco, con la conseguenza di rigettare un'istanza del Governo federale relativa a un caso differente, ma del tutto identica all'altro per quanto richiesto. È bene procedere in ordine cronologico e per tematiche.

Con l'*order* del 16 febbraio, il MJ della California *Shery Pim* decide nella convinzione di non violare il principio di separazione dei poteri, per due ragioni. Il magistrato fa propria la posizione del Governo USA che chiede che, sulla base della legge federale *All Writs Act* (o AWA), sia possibile emettere l'*order*.

In origine, l'AWA costituiva il §14 del *Judiciary Act* del 1789[80], che stabiliva che le corti federali potessero "*issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law*"[81]. Sarà la Corte Suprema a chiarire quando, in assenza di una previsione espressa, disciplinata per legge, i magistrati federali possano adottare simili atti[82], stabilendo che l'AWA ha natura di fonte residuale di attribuzione della competenza (a emanare *writs*)[83].

In altri termini, la Corte Suprema concepisce la possibilità di emettere i *writs* discussi come uno strumento per concorrere all'esercizio delle competenze già attribuite per legge alle corti federali - così come si evince dal primo Congresso federale e dalla Costituzione[84]. Per questo motivo delinea la precondizione insuperabile che un simile *order* contribuisca a realizzare concretamente i fini razionali perseguiti dal diritto, e gli obiettivi di giustizia a quest'ultimo intrinsecamente affidati[85]. La discrezionalità del magistrato chiamato a pronunciarsi non si potrà mai trasformare in un ampliamento costituzionalmente illegittimo delle competenze conferite per Costituzione e per legge alle corti federali[86].

Il principio di separazione dei poteri, quindi, regge il ragionamento della Corte Suprema: se così è, il magistrato federale che emette un atto di quella natura nel pieno rispetto dei limiti chiariti dalla giurisprudenza della Corte, non viola lo stesso principio e la più ampia

---

[79] *Memorandum and Order, in Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* (*15-MC-1902)*, *U.S. District Court Eastern District of New York*, del 29 febbraio 2016, il cui testo è reperibile all'indirizzo *Internet* www.nyed.uscourts.gov.

[80] Per questo v. 1 Stat. 81-82: l'AWA è così richiamato e spiegato da *Gabriel Gorenstein*, *Magistrate Judge della U.S.D.C, Southern D. New York*, nell'*Opinion and Order* del 31 ottobre 2014 (*No. 14 Mag. 2258*), reperibile all'indirizzo *Internet* www.nyed.uscourts.gov.

[81] Così il 28 U.S.C.§ 1651(a).

[82] A titolo esplicativo, e secondo l'atto come redatto al tempo del Primo Congresso statunitense, i *writs* di *scire facias*, *habeas corpus* ecc.: per il passaggio relativo all'indicazione di questi *writs* v. la lettera *B. The All Writs Act* del *Memorandum* del MJ *James Orenstein*, *cit.*

[83] "*All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute*", così la Corte Suprema in *Pa. Bureau of Corr. V. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985).

[84] Ossia nell'esercizio della "*existing statutory jurisdiction*" (per cui *Acman v. Kirby, Mc Inerney & Squire, LLP*, 464 F.3d 328, 333-34 (2d Circ. 2006)), e "*as prescribed by the Congress and the Constitution*" (così *Harris v. Nelson*, 394 U.S. 286, 300 (1969), come, peraltro, già affermato in *Price v. Johnston*, 334 U.S. 266, 282 (1948)).

[85] " […] *to achieve the rational ends of law*", e "*the ends of justice entrusted in it*": *United States v. New York Telephone Co.*, 434 U.S.159, 172-173 (1977).

[86] "*Flexibly in conformity with these principles*": di nuovo *United States v. New York Telephone Co.*, *cit.*, 173.

cornice dell'ordinamento giuridico di riferimento, le cui radici politico-giuridiche affondano nell'art. 16 della Dichiarazione dei Diritti dell'Uomo e del Cittadino del 1789.

In linea puramente teorica, stando nei limiti descritti, il magistrato (federale) non potrebbe mai (*infra*, al pgf. seguente) comprimere in modo arbitrario l'alveo di libertà di singoli individui o delle relative forme di associazione: solo restando nella sfera dei poteri attribuiti per Costituzione e per legge (federale) l'azione giurisdizionale si colloca infatti nel contesto più ampio di tutti i principi e diritti costituzionali che fanno sistema fra loro. Di stretta conseguenza, la sicurezza, agganciata a questa catena logica, *mai potrebbe diventare un bene costituzionale inserito nel bilanciamento perfetto con i diritti fondamentali* perché posto sul loro stesso, identico piano.

Fin qui quanto si può dedurre dal primo caso; il secondo affronta le stesse questioni in una luce diversa.

James Orenstein non accoglie la richiesta dell'Esecutivo USA di ordinare alla *Apple* di fornire ogni aiuto tecnico per aggirare il meccanismo di sicurezza del telefono cellulare di *Jun Feng*, sospettato di traffico di stupefacenti. Nel *Memorandum*, peraltro, il MJ sottolinea che altri dodici casi simili sono ancora pendenti, tutti accomunati dalle posizioni opposte di *Apple* e del Governo federale in merito alla possibilità che una corte federale, sulla base dell'AWA, possa ordinare alla multinazionale di dare agli agenti federali l'assistenza tecnica per violare i *security passcodes*. Contrariamente al caso precedente, però, è proprio l'interpretazione dell'AWA a portare stavolta il MJ adito a non dar seguito all'istanza governativa.

Per come ricostruite da *Orenstein*, le (poche) modifiche apportate al testo originario del 1789 sarebbero state adottate per accentuare le garanzie caratterizzanti l'AWA[87], mirate a non ampliare le competenze delle corti federali. Dopo un ragionamento articolato su tutto il testo della legge in questione, e la puntualizzazione dei requisiti in assenza dei quali il magistrato federale non ha la competenza necessaria per emanare un *order*[88]*,* il MJ afferma che il Governo USA suggerisce un'interpretazione troppo ampia dell'AWA, tale da rendere la legge costituzionalmente illegittima se sindacata alla luce del principio di separazione dei poteri, ma non solo.

Anche laddove il magistrato federale potesse adottare un *order* come quello richiesto, non va dimenticato che la decisione sarebbe ancorata a una doppia base: la prima, *giuridica e astratta*, fornita dall'AWA, la seconda, *discrezionale e concreta*, data dal margine decisionale che la stessa lascia al magistrato federale rispetto ad ogni caso. Se, però, il principio di separazione dei poteri resta sempre il riferimento insuperabile del giudizio sulla costituzionalità dell'AWA, a cascata la "*discretionary action*" del MJ non *amplierà il potere spettante al magistrato*, *tutelando così il destinatario dell'atto*, e i suoi diritti *tout court*.

---

[87] Di nuovo la lettera *B. The All Writs Act* del *Memorandum* del MJ *James Orenstein*, *cit.*

[88] Sempre la lettera *B. The All Writs Act* del *Memorandum* del MJ *James Orenstein*, *cit*, all'elenco delle sei condizioni.

Infatti, come già chiarito dalla giurisprudenza della Corte Suprema[89], l'*order* può essere emesso se ricorrono contemporaneamente tre condizioni: ci deve essere una stretta relazione fra il destinatario dell'atto e le materie di competenza della corte; il sacrificio da imporre deve essere ragionevole; l'*order* da emanare deve concorrere al miglior esercizio delle competenze della corte[90].

Questo approccio logico porta alle due conclusioni che danno a questo caso una svolta del tutto diversa. Valutando la sussistenza contestuale delle tre condizioni sopra ricordate, *Orenstein* può solo autolimitare la discrezionalità che la legge gli attribuisce, e affermare quindi in modo lapidario: "*I further conclude that even if the statute does apply, all three discretionary factors weigh against issuance of the requested writ, and that the Application should therefore be denied as a matter of discretion even if it is available as a matter of law*"[91].

Spontaneo chiedersi per quale motivo il Governo federale si sia esposto alla possibilità di una simile decisione: partendo dalla sentenza *N.Y. Tel. Co.* della Corte Suprema[92], *Orenstein* individua una risposta al quesito. Quella, differente, sulla quale ragionare per la gravità che la caratterizza, verrà trattata ai pgff. seguenti, spec. al 3.c).

3.a.1) Per evitare il confronto democratico, il potere esecutivo ricorre a quello giudiziario.

Nella sentenza del 1977 *N.Y. Tel. Co.*, il tema della separazione dei poteri porta la Corte Suprema a stabilire che nessun magistrato federale, richiamando l'AWA, possa emanare un *order* la cui adozione sia vietata da un'altra legge federale (in via esplicita o implicita)[93]. In questa luce, la tesi della *Apple*, articolata sulla legge federale CALEA, per *Orenstein* è corretta, e fa comprendere le ragioni ultime che spingono il Governo USA ad agire come finora fatto.

CALEA, ossia la legge federale *Communications Assistance for Law Enforcement Act*[94], va inquadrata nel disegno del Congresso volto a impedire che, a soggetti privati (quali ad es. la *Apple*), possano essere rivolte richieste non previste espressamente dalla stessa fonte. CALEA entra in vigore nel 1994, quando il legislatore statunitense deve individuare la

---

[89] Il precedente è ancora una volta *United States v. New York Telephone Co.*, *cit.*, 172-174-178.

[90] V. lettera *B. The All Writs Act* del *Memorandum* del MJ *James Orenstein*, *cit.*, laddove afferma che "*A court deciding whether to take such a discretionary action should consider three additional factors: 1. The closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction; 2. the reasonableness of the burden to be imposed on the writ's subject; and 3. the necessity of the requested writ to aid the court's jurisdiction (which does replicate the second statutory element, despite the overlappimg language)*".

[91] Così l'ultimo periodo di cui alla lettera *B. The All Writs Act* del *Memorandum* del MJ *James Orenstein*, *cit.*

[92] Ossia la più volte richiamata *United States v. New York Telephone Co.*, *cit.*

[93] V. la lettera *C. Statutory Requirement,* punto 3. *Agreeable to the Usages and Principle of Law* sempre del *Memorandum* del MJ *James Orenstein*, *cit.*

[94] *Communications Assistance for Law Enforcement Act*, CALEA, *Pub.L.No. 103-414, 108 Stat. 4279*, di cui al 47 U.S.C. §§1001-1010.

misura del sacrificio che può patire la *privacy* nell'era delle sempre più avanzate tecnologie delle comunicazioni. Gli istituti della riserva di legge e di giurisdizione rispondono alle esigenze di garanzia: la CALEA verrà intesa come mezzo "*to preserve the government's ability"*, ma soltanto se *"pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies* […]"[95]. In seguito, sottolinea *Orenstein*, la stessa fonte diverrà anche la base giuridica per delineare le "*responsabilities of private companies to preserve and allow access to records relating to wire and electronic communications*"[96].

Le due garanzie sono importanti anche perché è chiaro che, da quel momento in poi, i casi concreti che coinvolgeranno le agenzie e i corpi di sicurezza federali e i sospettati di atti penalmente rilevanti finiranno con l'interessare anche soggetti terzi: e, come stabilito dalla giurisprudenza della Corte Suprema, "*the power of federal courts to impose duties upon third parties is not without limits*"[97].

Qui, il ragionamento[98] di *Orenstein* sposa l'interpretazione di *Apple* dell'ultima parte del testo della CALEA sulla decrittazione dei dati: "*Encryption. A telecommunication carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer,* unless the encryption was provided by the carrier *and the carrier* possesses the information necessary to decrypt *the communication*"[99].

Quell' "a meno che" ("*unless*") viene interpretato dal MJ in omaggio a una lettura garantista della legge federale, e, anche, di una convinzione: "*It is also clear that the government has made considered decision that it is better off securing such crypto-legislative authority from the courts (in proceedings that had always been, at the time it filed the instant Application, shielded from public scrutiny)* rather than taking the chance that open legislative debate might produce a result less to its liking"[100].

La posizione del magistrato è fondata su un fatto: il giorno stesso in cui il Governo USA si è rivolto ai MJ di due diversi distretti della Corte di *New York*, *James B. Comey* (già *U.S. Deputy Attorney General* durante l'amministrazione *George W. Bush*, e ora a capo

---

[95] Fra le quali, ad es., come ricostruito da *James Orenstein* citando la giurisprudenza precedente il suo *Memorandum and Order*, "*digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling*": così *U.S. Telecom Ass'n v. F.C.C.,* 227 F.3d 450, 454 (D.C. Circ. 2000), richiamando espressamente il *CALEA House Report, rep. No.* 103-287, pt.1, at 14 (1994).

[96] Così la nota (12) del *Memorandum and Order* più volte richiamato: per il passaggio citato nel testo v. il 47 U.S.C. §1028(2)-(4), relativo alle cd. "*responsabilities concerning 'call-identifying information' "*.

[97] Per la cit. sempre il precedente della *United States v. New York Telephone Co.*, *cit.*, 172. Lo richiama nell'ottica proposta nel testo *Gabriel Gorenstein*, nell'*Opinion and Order* già *cit*.

[98] L'intenzione del legislatore federale sembra dunque essere quella di precludere "*the government from requiring carriers to build into the encryption measures they make available to their subscribers as a 'back door' that enables law enforcement access to encrypted communications. It does no more provide that law enforcement is entitled to have carriers assist in securing acces to encrypted information where the carrier in making such encryption available, has also retained a decryption key for its own purposes that would allow such access*"; così la nota (13) del *Memorandum and Order* di *James Orenstein.*

[99] Le evidenziazioni del testo *cit.* (anche in seguito) sono di chi scrive. V. la lettera *C. Statutory Requirement,* punto 3. *Agreeable to the Usages and Principle of Law* sempre del *Memorandum* del MJ *James Orenstein*, *cit.*, spec. lett. *a) CALEA, i) The Statute's Purpose and Text*.

[100] *Memorandum* del MJ *James Orenstein*, lettera *C.,* punto *b. Statutory Construction, cit.*

dell'FBI) ha annunciato che, nonostante la necessità di modificare la CALEA per attribuire al Governo i poteri per obbligare *Apple* (come altri) a fare quanto richiesto con l'*order*, l'amministrazione *Obama* non avrebbe avviato l'*iter* legislativo indispensabile[101].

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 costituzionali, *in modo solo limitato può limitarli*) può essere garantita esclusivamente nel rispetto della separazione dei poteri. Qualsivoglia legge federale che, in nome della nozione di sicurezza sostenuta dal Governo USA, attribuisca al potere giurisdizionale competenze costituzionalmente illegittime se sindacate alla luce dello stesso principio, può infatti, a cascata, solo disconoscere il ruolo del potere legislativo, attribuendo "*to the First Congress an anomalous diminishment of its own authority (to deny a request to increase the executivÈs investigative powers it deemed inadvisable simply by declining to enact it)*[,] *as well as an equally implausible intention to confer essentially unlimited legislative powers on the judiciary*"[102].

Là dove la tecnologia del futuro si impone, i principi liberali settecenteschi emergono dal passato, più attuali che mai, col rischio di essere travolti: un magistrato, però, pare averli difesi.

3.b) Sul sacrificio dei diritti: United States v. New York Tel. Co., fra riserva di giurisdizione e di legge, e due process of law.

Come anticipato, è bene riflettere ora sul sacrificio individuale frutto dell'*order*, ricordando anzitutto che l'atto non solo autorizza lo Stato a violare la sfera privata di un singolo individuo, ma impone a un soggetto privato (terzo, rispetto alla vicenda complessiva), di collaborare a questo scopo. C'è dunque da chiedersi per quale ragione, per uno almeno dei due MJ, un *order* simile non configuri una compressione costituzionalmente illegittima dei diritti in nome della sicurezza.

Per *Shery Pim*, la tutela che il suo *order* garantisce a un soggetto terzo (*Apple*) rispetto all'inchiesta federale e, indirettamente, a quello interessato dalla violazione della sua *privacy* (l'attentatore deceduto, che qui diventa riferimento per futuri casi più o meno analoghi), sta nelle valutazioni affidate ai punti 6. e 7. del suo atto. *Pim* stabilisce che la richiesta di col-

---

[101] In questo senso lo *statement* di *James B. Comey* (diverso, dunque, da quanto sostenuto da *Barack Obama* nel gennaio 2015; *supra*, alla nota 29), "*Statement Before the Senate Committee on Homeland Security and Governmental Affairs*", dell'8 ottobre 2015, per il quale www.fbi.gov/news/testimony/threats-to-the-homeland: "*The United States Government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time*."

[102] Quindi, per *James Orenstein*, adottare una simile prospettiva interpretativa dell'AWA "*would fly in the face of the doctrine of constitutional avoidance, which 'allows court to avoid the decision of constitutional questions' by providing 'a tool for choosing between competing plausible interpretation of statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises seroius constitutional doubts*": per le cit. *Am. Civil Liberties Union v. Clapper,* 785 F.ed 787, 808 (2d Circ. 2015), per la quale il precedente *Clark v. Martinez,* 543 U.S. 371, 380-381 (2005): così di nuovo il *Memorandum* del MJ *James Orenstein*, *cit.*

laborazione rivolta alla multinazionale anzitutto non obbliga *Apple* a custodire copia dei dati, e che, laddove la collaborazione voluta sia irragionevolmente onerosa, la multinazionale possa ottenere un *relief* dalla corte. Il MJ stabilisce poi che le prove (cioè i dati contenuti nell'*iPhone*) dovranno rimanere sotto la sola responsabilità degli agenti federali. Pare evidente come, nell'ottica del MJ, l'atto poggi su precise garanzie a tutela del terzo coinvolto nell'inchiesta federale, e di quello che ha compiuto l'attentato.

A favore di questa lettura dell'*order* deporrebbero l'*Opinion and Order* dell'ottobre 2014 del MJ *Gabriel Gorenstein*[103] in un caso simile, e i precedenti *United States v. New York Tel. Co.* e *United States v. Mountain States Tel. & Tel. Co.*[104]. *Gorenstein* chiarisce come, di fronte ad *order* come quelli discussi, il soggetto terzo rispetto all'inchiesta federale debba poterli impugnare. Nel rispetto del *due process of law*, proprio le corti federali infatti, in casi della stessa natura, hanno seguito una linea decisionale univoca, stabilendo che "*due process requires that a third party subject to an order under the All Writs Act should be afford a hearing on the issue of burdensomeness prior to compelling it to provide such assistance to the Government […] the manufacturer should be given clear notice that it has the opportunity to object the Order*"[105].

Queste, dunque, le garanzie concatenate: il principio di separazione dei poteri precede e comporta quelli della riserva di legge, di giurisdizione, e del *due process of law*. Ciò significa che il sacrificio dei diritti costituzionalmente protetti va inquadrato nella cornice dei principi di ogni Costituzione delle forme di Stato democratiche, occidentali. In quest'ottica, il sacrificio può essere imposto "in concreto" solo da chi è articolazione dell'ordinamento giuridico democratico, ossia i corpi di sicurezza pubblici, sui quali grava la responsabilità delle prove ottenute grazie al soggetto terzo.

La sicurezza è dunque un *bene giuridico degno di protezione*, ma inserito *in un bilanciamento imperfetto* con i *diritti* dell'individuo: questo, anche quando in gioco ci sono le libertà di chi ha compiuto atti odiosi contro la persona umana.

Resta soltanto un dubbio: la realizzazione della catena di garanzie esposte è più facile in un ordinamento giuridico che mette al centro della sua architettura costituzionale i diritti di libertà, come quello statunitense, oppure in uno europeo occidentale, il cui perno ruota sulla tenuta dell'ordinamento giuridico nel suo complesso?[106] La riflessione seguente non risolve il quesito, ma prova a coglierne i complessi risvolti.

---

[103] Sempre (come già *cit. supra*) *Gabriel Gorenstein*, nell'*Opinion and Order* del 31 ottobre 2014, spec. il ragionamento al terz'ultimo pgf. dell'atto.

[104] Di nuovo fondamentale il precedente *United States v. New York Telephone Co.*, *cit.*, al quale va aggiunto *United States v. Mountain States Tel. & Tel. Co.,* 616 F.2d 1122, 1132-33 (9th Circ. 1980).

[105] *Gabriel Gorenstein*, *Opinion and Order*, *cit.*, al terz'ultimo paragrafo dell'atto.

[106] Sul punto G. GONZALÉS FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Berlin, 2014, 21 ss., spec. 27 per l'esperienza degli USA, e 37 per quella sovranazionale.

3.c) Variazione sulla tesi di Orenstein: a lezione dall'FBI sui principi liberali e le garanzie costituzionali.

Nel caso californiano, l'FBI supera il meccanismo di protezione dell'*iPhone* con l'aiuto di un soggetto la cui identità è segreta[107]. Sempre *Edward Snowden,* nei giorni successivi all'*order* del 16 febbraio, aveva affermato che l'FBI poteva agire senza *Apple*: visto quanto accaduto, difficile pensare che avesse torto; facile chiedersi per quale motivo il Governo USA abbia comunque scelto la via giudiziaria.

Quanto segue è sola congettura di chi scrive; è chiaro, però, come questa sia una ipotesi che, *proprio attraverso l'esposizione di quella contraria*, permette di non abbandonare la tesi qui proposta: il rischio che beni e diritti costituzionalmente protetti corrono è maggiore quando la loro protezione è offerta dal potere privato. Attenzione, però*:* un pericolo simile sussiste *comunque, anche se in misura minore*, quando è il potere pubblico ad agire.

Come già accennato, il giorno in cui il Governo federale si è rivolto ai MJ di due diversi distretti della Corte di *New York*, *James B. Comey* (ora a capo dell'FBI) ha annunciato che l'amministrazione *Obama* non avrebbe avviato l'*iter* legislativo per modificare la CALEA, così da attribuire per legge federale al Governo USA i poteri richiesti con l'istanza al MJ[108].

Forte 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. L'Esecutivo federale lo ha fatto, forse, anche per ragioni diverse, ma servite a raggiungere lo scopo perseguito sin dall'inizio.

Ora, evidente è che adottare una legge federale è cosa laboriosa, inadatta ai tempi di un'indagine su un attentato terroristico. Inoltre, comporta una visione d'insieme (propria del legislatore) che di necessità va oltre la fattispecie penalmente rilevante relativa all'inchiesta in corso: di conseguenza, prima ancora che sulla garanzia della sicurezza, un atto normativo simile è articolato sulla protezione delle libertà e sui limiti che i poteri dello Stato devono rispettare quando si confrontano con la tutela della sicurezza. Al contrario, la discrezionalità del magistrato adito, secondo un calcolo nemmeno tanto azzardato delle probabilità, offriva maggiori garanzie al Governo USA di ottenere quanto richiesto, almeno in uno, o addirittura in diversi Stati federati: lo dimostrano, del resto, i due *order* così differenti, a firma *Pim* e *Orenstein*.

In un ordinamento giuridico di *common law* come quello nordamericano, poi, fondato sui "precedenti", la possibilità che anche un solo MJ, per ogni Stato federato in cui fosse stato adito, desse applicazione all'AWA sposando la tesi degli avvocati del Governo USA, avrebbe risolto il problema legato a più indagini. Se, inoltre, in qualche - pure in uno soltanto – *federal circuit* si fosse arrivati a una *U.S. Court of Appeal*, il dibattito parlamentare a venire

---

[107] Le stesse fonti, nei giorni in cui si scrive, rendono noto che anche in altri casi l'FBI sarebbe riuscita a fare lo stesso con i cellulari di sospettati: fra questi, due minorenni accusati di omicidio.

[108] In questo senso sempre lo *Statement* di *James B. Comey*, "*Statement Before the Senate Committee on Homeland Security and Governmental Affairs*", *cit.*

non avrebbe potuto del tutto trascurare le osservazioni sulla legittimità costituzionale dell'atto fatte in sede giurisdizionale.

In ogni caso, resta il fatto che anche un solo *order* in grado di obbligare *Apple* a creare una *backdoor* avrebbe dato all'FBI, per il futuro, quella chiave universale di accesso ai dati personali capace di consentire ogni possibile indagine in ogni possibile caso, non necessariamente legato ad atti di terrorismo.

C'è poi di più. Per come articolata, la serie di rimedi giurisdizionali ha dato all'FBI una risorsa irrinunciabile: il tempo.

L'*order* – nei casi *Feng* e *Farouk* - è infatti logicamente collegato ad un primo *search warrant* ottenuto dall'FBI sempre con un provvedimento giurisdizionale; un primo magistrato autorizza le perquisizioni per trovare l'*iPhone*, un secondo le attività per aggirarne il sistema di sicurezza. I tempi per realizzare il *search warrant* sono però per legge brevi (14 giorni, ricorda *Orenstein*). Se, quindi, gli inquirenti hanno bisogno di più tempo per essere sicuri di riuscire a decrittare con i loro soli mezzi il *device*, e se il destinatario dell'*order* non lo esegue, permettendo così al Governo di presentare un'istanza ulteriore per ottenerne il rispetto, allora nel complesso i termini si allungano.

Si trattava solo di una questione di tempo; in ogni caso l'FBI avrebbe aggirato il sistema di protezione: lo avrebbe fatto prima, a seguito di un provvedimento giurisdizionale immediato e favorevole al Governo, o un poco dopo, grazie ai tempi dell'azione giudiziaria.

Tradotta nell'ottica che qui interessa, la vicenda svela un paradosso.

Proprio nel momento in cui sono stati utilizzati per proteggere i cittadini da futuri atti terroristici, *i rimedi giurisdizionali a tutela dei diritti* costituzionalmente protetti *hanno spezzato l'equilibrio fra sicurezza e libertà*.

O, forse, lo hanno *"solo" gravemente incrinato*, se il Congresso istituirà una commissione d'inchiesta o sulla sicurezza digitale, oppure entrambe, facendo rientrare dalla finestra ciò che era uscito dalla porta: la separazione dei poteri e la garanzia dei diritti.

4. Dal Safe Harbour al Privacy Shield. Il diritto alla vita privata dall'Unione europea agli Stati Uniti d'America.

Il caso *Apple* fa capire quanto la tecnologia impatti sulla relazione fra la sicurezza e i diritti. Per come emerso da quell'esperienza, il tema della protezione dei dati, anche non sensibili[109], consente di osservare ora le scelte del legislatore europeo[110] (nonché gli obblighi gravanti sugli Stati membri) e le relazioni in tema proprio con gli USA.

---

[109] Approfondiscono la cornice alla quale ricondurre quanto trattato di seguito R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione: con riferimento alla tutela della* privacy*, alla diffamazione e all'editoria* on-line, Cedam, Padova, 2003; A. PACE, R. ZACCARIA, G. DE MINICO, (a cura di), *Mezzi di comunicazione e riservatezza: ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008.

[110] Tematica da ricondurre anche a un ambito più esteso: R. MAZZESCHI, A. DEL VECCHIO, M. MANETTI, P. PUSTORINO, (a cura di), *Il diritto al pluralismo nell'informazione in Europa e in Italia*, Rai Eri, Roma, 2012; G. GARDINI, *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Mondadori, Milano, 2009; G. MORBIDELLI, F. DONATI, (a cura di), *L'evoluzione del sistema delle comunicazioni tra diritto interno e comunitario*, Giappichelli,

Aiuta ad approfondire questi profili la giurisprudenza sovranazionale *Schrems*[111], che ha portato a rinegoziare il cd. *Safe Harbour* sul trasferimento dei dati oltreoceano, ideando il *Privacy Shield*[112]. È bene ricordare la cornice giuridica in cui si inserisce la pronuncia[113].

Nella Comunicazione del novembre 2013[114], la Commissione europea ricordava come i "trasferimenti di dati personali [fossero] un importante e necessario elemento delle relazioni transatlantiche", essendo "parte integrante degli scambi commerciali fra le due sponde dell'Oceano, anche per i nuovi settori emergenti del digitale, come i media sociali o il *cloud computing*, che vedono grosse quantità di dati viaggiare dall'Unione europea agli Stati Uniti"[115]. L'istituzione stabiliva così un nesso indissolubile fra dati personali trasferiti dall'UE, relazioni UE-USA e scambi commerciali[116], con una novità.

Se, fino a quel momento, solo in astratto si poteva temere per la protezione dei dati, dopo le rivelazioni di *Edward Snowden* sui programmi di sorveglianza (il cd. PRISM[117]), il pericolo diventa attuale[118].

Ora, il trasferimento dei dati personali verso gli USA[119] era già stato oggetto della decisione della Commissione 2000/520/CE[120], adottata a norma della direttiva 95/46/CE[121]. Va-

---

Torino, 2005; S. AMOROSINO, A. ALESSI, *Le regole europee per la comunicazione: materiali per la Costituzione dell'Unione*, Giuffré, Milano, 2003; F. BASSAN, *Concorrenza e regolazione nel diritto comunitario delle comunicazioni elettroniche*, Giappichelli, Torino, 2002.

[111] Corte di Giustizia dell'Unione Europea, Grande sezione, sent. 6 ottobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, in C-362/14, in *RIDPC*, n. 6, 2015, 1793 ss., con nota di R. DE SIMONE; per un approfondito ragionamento sulla più ampia tematica F. BALDUCCI ROMANO, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *RIDPC*, n. 6, 2015, 1619 ss. Interessante inoltre sul più ampio tema G. GONZALÉS FUSTER, *The Emergence of Personal Data Protection …*, *cit.*, 55 ss. per la disamina della normativa in alcuni Stati UE, 111 ss. per quella sovranazionale, e p. 264 ss. per la configurazione del diritto fondamentale alla tutela dei dati personali.

[112] La rinegoziazione, al momento in cui si scrive, non è ancora stata perfezionata.

La direttiva n. 95/46/CE, del 24 ottobre 1995, del *Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro*, è relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e alla disciplina del trasferimento degli stessi dagli Stati membri dell'UE ad altri paesi al di fuori dell'UE; gli artt. 25 e 26 della direttiva stabiliscono il quadro giuridico per il trasferimento dall'UE a paesi terzi al di fuori del SEE: di nuovo G. GONZALÉS FUSTER, *The Emergence of Personal Data Protection …*, *cit.*, 124-156. La decisione della Commissione (*infra*) che riteneva il trasferimento /justice/newsroom/data-protection/news/160229_en.htm.

[113] Affrontano profili verso gli USA fosse conforme a questa disciplina è stata superata, nel febbraio 2016, dal nuovo accordo noto come *Privacy Shield*: per il testo e gli allegati http://ec.europa.eu inerenti la cornice non solo giuridica della questione trattata S. GURTWIRTH, R. LEENES, P. DE HERT, Y. POULLET, (*Ed.s*), *European Data Protection. Coming of Age*, Springer, Berlin, 2013; si sofferma invece su quelli sollevati dalla sentenza, relativi all'equilibrio fra esigenze (sociali, individuali, economiche) di circolazione dei dati e protezione del diritto al rispetto della vita privata S. SILEONI, *La tutela della riservatezza negli Stati uniti e le nuove frontiere per la circolazione dei dati personali*, in *Quad. cost.*, n. 4, dicembre 2015, 1027 ss.

[114] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM(2013) 846 def., d'ora in poi semplicemente "la Comunicazione del 2013" o anche "la Comunicazione".

[115] La Comunicazione del 2013, 2.

[116] Sul punto di nuovo S. SILEONI, *cit.*, 1028.

[117] Ossia il *National Security Electronic Surveillance Programm* della NSA, utilizzato probabilmente dal 2007 in poi per l'accesso e la raccolta indiscriminata di informazioni, relative anche ai cittadini europei, attraverso *Internet* e altri fornitori di servizi elettronici e telematici.

[118] Sul punto per tutti S. GURTWIRTH, Y. POULLET, P. DE HERT, R. LEENES, (*Ed.s*), *Computers, Privacy and Data Protection: an Element of Choice*, Springer, Berlin, 2011.

lutando positivamente la tutela dei dati offerta negli USA, la decisione permetteva il trasferimento di dati dall'UE alle società, stabilite negli Stati Uniti, che avevano accettato il cd. "approdo sicuro", ossia i principi a protezione del diritto alla vita privata come garantito dalle norme UE.

L' "approdo sicuro" agevolava gli scambi commerciali[122]: alle imprese statunitensi[123] che desideravano aderire al regime era infatti richiesta solo una autocertificazione relativa al rispetto dell' "approdo", da fornire al Dipartimento del Commercio USA[124]. Diversi erano poi gli strumenti di controllo successivo (rimedi extragiudiziali, la cooperazione con il *panel*

---

[119] Come ricorda l'Avvocato generale: *conclusioni* dell'Avv. Gen. *Yves Bot*, 23 settembre 2015, *Maximilian Schrems c. Data Protection Commissioner*, in C-326/14, in relazione alla domanda di pronuncia pregiudiziale proposta dalla *High Court* dell'Irlanda, al p.to 2.) (in seguito indicate anche soltanto come *conclusioni*).

[120] Decisione della Commissione del 26 luglio 2000, n. 2000/520/CE.

[121] E delle relative *Domande più frequenti* (o FAQ) *in materia di riservatezza* elaborate dal Dipartimento del Commercio degli Stati Uniti per gli atti menzionati nel testo, europei e statunitensi: GUCE del 25 agosto 2000, L215, 7, e (per le modifiche successive) GUCE del 25 aprile 2001, L115, 14.

[122] Come spiega l'Avv. gen. alle *conclusioni* al punto 14. Secondo la decisione 2000/520, spec. l'Allegato I, "*Garanzie d'applicazione*", i principi consistono in: un obbligo di informazione in forza del quale "le organizzazioni devono informare i singoli individui in merito alle finalità per cui vengono raccolte e utilizzate le informazioni su di essi, alle modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, alla tipologia dei terzi a cui vengono fornite le informazioni, e infine ad opzioni e mezzi che le organizzazioni mettono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni. Queste indicazioni vanno formulate (…) quando si tratti del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte" (v. Allegato I, "*Notifica*").

Un obbligo per le organizzazioni di offrire agli individui la possibilità di scegliere se le informazioni personali che li riguardano verranno rivelate a terzi ovvero utilizzate per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati dall'interessato. Nel caso di dati di carattere delicato, "va data la possibilità di scelta affermativa o esplicita (facoltà di consenso) per quanto riguarda la possibilità che le informazioni in questione vengano rivelate a terzi od utilizzate per scopi diversi da quelli per cui esse erano state originariamente raccolte o da quelli successivamente autorizzati dagli interessati con l'esercizio della facoltà di consenso" (v. Allegato I, "*Scelta*").

In materia, invece, di trasferimento successivo dei dati, la decisione stabilisce che le "organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta" (v. Allegato I, "*Trasferimento successivo*").

In tema di sicurezza dei dati, viene fissato un obbligo per le "organizzazioni che detengono, aggiornano, utilizzano o diffondono informazioni personali (…) [di] prendere ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati" (v. Allegato I, "*Sicurezza*").

Infine, per quanto concerne l'integrità dei dati, si configura un obbligo per le organizzazioni di "prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati" (v. Allegato I, "*Integrità dei dati*").

La decisione chiarisce poi che gli individui i cui dati sono in possesso di un'organizzazione devono "poter accedere alle informazioni personali che li riguardano (…) ed altresì poterle correggere, emendare o cancellare se ed in quanto esse risultino inesatte" (v. Allegato I, "*Accesso*"), e individua l'obbligo di prevedere "meccanismi volti a garantire il rispetto dei principi [dell'approdo sicuro], la possibilità di ricorso, per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi" (sempre l'Allegato I, "*Garanzie d'applicazione*").

[123] In questo senso la decisione 2000/520/CE, Allegato I, secondo comma.

[124] Per queste indicazioni l'Allegato I, terzo comma.

dell'UE sulla protezione dei dati[125] e le istanze alla *Federal Trade Commission* (FTC)[126] e al *Department of Transportation*[127]).

La sorveglianza elettronica, in teoria giustificabile per preservare la sicurezza nazionale da condotte criminali, in particolare di natura terroristica, ha però svelato come il Governo USA e le sue agenzie e corpi di sicurezza[128] abbiano avuto accesso *massiccio e indiscriminato* ai dati europei[129].

Questa consapevolezza ha dato un peso straordinario alle affermazioni di *Snowden*[130] e al caso *Schrems*[131], dimostrando che, negli Stati Uniti, la protezione dei dati personali dei cittadini europei era limitata. Di seguito il caso che ha originato la vicenda, e portato a scrivere le nuove regole affidate al cd. *Privacy Shield*.

4.a) Facebook USA e National Security Electronic Surveillance Programme: i dati personali europei negli Stati Uniti, senza la protezione della Carta dei Diritti.

Grazie al rinvio pregiudiziale alla Corte di Giustizia dell'UE originato dalla vicenda *Schrems*, la decisione 2000/520/CE della Commissione, per la quale, fino al 2007 almeno, il trattamento dei dati negli Stati Uniti godeva di tutele paragonabili a quelle del diritto UE, è stata dichiarata invalida, in ragione della scarsa protezione offerta negli USA agli stessi dati[132].

---

[125] Di rilievo dunque l'attività del WORKING GROUP 29, istituito sulla base dell'art. 29 della direttiva 95/46/CE: su questa di nuovo G. GONZALÉS FUSTER, *The Emergence of Personal Data Protection …*, *cit.*, 124 ss., anche per la direttiva n. 97/66/EC.

[126] Le cui competenze necessarie allo scopo sono stabilite dalla quinta sezione del *Federal Trade Commission Act*.

[127] Il quale è competente ad esaminare le denunce ricevute in ragione del 49 U.S.C. §41712.

[128] Peraltro, a poco sarebbero serviti i poteri esercitati dalla *Foreign Surveillance Court* (FISC) in base al *Foreign Surveillance Act* (FSA) del 1978, che non è riuscita ad impedire alcuna violazione di diritti. Anzi, proprio l'art. 702 dell'FSA (per come modificato nel 2008) avrebbe offerto alla *National Security Agency* la base giuridica per sviluppare il programma PRISM sulla sorveglianza elettronica. L'eventuale procedimento dinanzi alla FISC si svolge inoltre senza alcuna garanzia di pubblicità e trasparenza, e *inaudita altera parte*; dunque, i cittadini dell'UE mai avrebbero potuto essere ascoltati sulla sorveglianza e l'intercettazione dei loro dati, perché le decisioni sul relativo accesso poggiano sul solo diritto statunitense: la ricostruzione proposta è sempre quella dell'Avv. Gen. *Y. Bot*; per la banca dati relativa al PRISM v. invece il *Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection* del 27 novembre 2013*,* all'indirizzo *Internet ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.* Questo *Report* accompagna il *Parere del Garante europeo della protezione dei dati* "*Sulla comunicazione della Commissione al Parlamento europeo e al Consiglio 'Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA' e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'UE e delle aziende ivi stabilite"* (il testo completo del parere 2014/C 116/04 è reperibile in francese, inglese e tedesco sul sito *web* del Garante, all'indirizzo *Internet* www.edps.europa.eu.

[129] Come ricorda la *High Court* irlandese nel rinvio pregiudiziale che origina la sentenza *Schrems, cit.*

[130] Più volte richiamate da *Y. Bot, cit.*

[131] Nel rinvio pregiudiziale, la *High Court* irlandese ribadisce che, di fatto, il pubblico potere USA si è spinto ben oltre lo scopo legittimo della tutela della sicurezza nazionale: per il quesito del rinvio pregiudiziale v. curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=EN.

[132] S. SILEONI, *La tutela della riservatezza negli Stati uniti …*, *cit.*, 1029-1030, riassume in due ordini di questioni gli effetti della sentenza: il primo, di natura generale, relativo all'interpretazione dell'art. 25 della direttiva

Maximilian Schrems, cittadino austriaco residente in Austria, dal 2008 era iscritto alla rete sociale *Facebook*. Chi risiede nel territorio dell'UE e desidera utilizzare *Facebook*, al momento dell'iscrizione, accettando le condizioni di utilizzo della piattaforma, in sostanza sottoscrive un contratto con *Facebook Ireland*, società controllata di *Facebook Inc.*, situata negli USA. I dati personali degli utenti di *Facebook* residenti nel territorio UE vengono poi trasferiti su un *server* ubicato negli Stati Uniti, dove sono oggetto di trattamento.

Nel 2013 *Schrems*, preoccupato per i programmi di sorveglianza elettronica (in particolare, della NSA)[133], si rivolgeva al *Data Protection Commissioner* irlandese - gli Stati membri devono creare autorità indipendenti di settore[134] - chiedendo di vietare a *Facebook Ireland* di trasferire negli USA i suoi dati personali[135]. Il *Data Commissioner*, ritenendo che ogni questione sull'adeguatezza della protezione dei dati negli Stati Uniti andasse risolta nel rispetto della decisione 2000/520/CE, negava però il provvedimento.

Schrems impugnava allora il diniego dinanzi alla *High Court* irlandese: la Corte, pur riconoscendo che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'UE verso gli USA rispondevano ad esigenze di pubblico interesse, affermava che le rivelazioni di *Snowden* dimostravano come la NSA ed altre articolazioni federali avessero commesso "eccessi considerevoli"; ribadiva che il diritto irlandese non vieta il trasferimento dei dati personali al di fuori del territorio nazionale se il paese terzo che li accoglie assicura un elevato livello di protezione dei diritti fondamentali, della vita privata e dell'inviolabilità del domicilio, nel rispetto della Costituzione irlandese, della riserva di legge e del principio di proporzionalità. Alla luce delle attività scoperte, per il diritto irlandese gli USA non assicuravano dunque un elevato livello di tutela dei dati personali; per questa ragione, secondo la *High Court*, il Commissario avrebbe dovuto accogliere l'istanza di *Schrems* e fare le verifiche del caso.

Dato che la questione riguardava l'attuazione, ai sensi dell'articolo 51 della Carta dei diritti[136], del diritto UE, per la Corte irlandese la decisione 2000/520 andava sindacata alla

---

95/46 alla luce degli artt. 7 e 8 della Carta dei diritti; il secondo, inerente la legittimità del trasferimento dei dati negli USA, che passerà attraverso la revisione delle deroghe al pieno rispetto di quel diritto e la più attenta definizione dei poteri di sorveglianza statunitensi sui dati provenienti dall'UE.

[133] Sui rischi legati all'accettazione dei termini di utilizzo di servizi evocati nel testo F. CHIUSI, *Grazie mr Snowden #Datagate #NSA, cit.*

[134] Come voluto dalla direttiva 95/46/CE.

[135] La questione è dunque in parte diversa da quelle che hanno caratterizzato la giurisprudenza europea e sovranazionale sul diritto all'oblio: per questa v. M. BASSINI, Google *davanti alla Corte di giustizia: il diritto all'oblio,* in *Quad. cost.*, n. 3, 2014, 730 ss.; D. LINDSAY, *The 'Right to Be Forgotten' in European Data Protection Law*, in N. Witzleb, D. Lindsay**,** M. Paterson, Sh. Rodrick, (*Eds.*), *Emerging Challenges in Privacy Law*, Cambridge Intellectual Property and Information Law, No. 23, 2014, Cambridge University Press, Cambridge, spec. 290-337, (disponibile anche in rete: Cambridge Books Online dx.doi.org/10.1017/CBO9781107300491.019); G. VIGEVANI, *La Corte di Strasburgo non riconosce il diritto di rimuovere da un archivio telematico un articolo diffamatorio*, in *Quad. cost.*, n. 4, 2013, 1011 ss.; F. PIZZETTI, (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013.

[136] Sull'interpretazione dell'art. 51 della Carta K. STERN, *cit.*, p. 1235 ss., e PARLAMENTO EUROPEO, (*Policy Department C*, *Citizen's Rights and Constitutional Affairs*), *The Interpretation of the EU Charter of Fundamental Rights: The Dilemma of Stricter or Broader Application of The Charta to National Measures*, PE 556.930, il cui testo, nella sola lingua inglese, è reperibile all'indirizzo *Internet* www.europarl.europa.eu/supporting-analyses.

luce degli articoli 7 (sul diritto al rispetto della vita privata) e 8 (sulla protezione dei dati personali) della Carta e dei principi elaborati nella sentenza *Digital Rights Ireland e a.* [137].

Con il PRISM, poi, la NSA avrebbe potuto accedere ai dati personali di *Schrems*, trasferiti a *Facebook USA*: la decisione 2000/520 andava quindi anche del tutto rivalutata; in questo senso il *Data Commissioner* avrebbe dovuto attivarsi, perché così stabilito dalla legge irlandese sulla protezione dei dati, e per un secondo motivo[138].

Il tema del bilanciamento fra sicurezza nazionale e protezione dei dati[139], intesi come articolazione del diritto alla vita privata, emerge fin dalla giurisprudenza UE in materia di asilo[140], per la quale gli Stati membri *devono adottare* misure a salvaguardia dei diritti fondamentali di cui agli artt. 7 e 8 della Carta, proprio quando i paesi terzi non li garantiscono altrettanto. La direttiva 95/46 persegue questa logica, dalla quale la decisione 2000/520/CE[141] non doveva distaccarsi[142], anzi.

L'art. 8 disciplina espressamente il diritto alla protezione dei dati personali. In particolare, i pgf. 2 e 3 di quest'ultimo stabiliscono che i dati devono essere trattati secondo il principio di lealtà, per finalità determinate, in base al consenso della persona interessata o ad altro fondamento previsto per legge, e che ogni individuo ha il diritto di accedere e/o rettificare quelli raccolti che lo riguardino.

Per la direttiva 95/46, il rispetto di queste previsioni è affidato a un'autorità indipendente, per garantire "un elevato grado di tutela delle libertà e dei diritti fondamentali con riguardo al trattamento dei dati personali"[143]. Non sbaglia quindi la *High Court* irlandese quando sostiene che le "autorità di controllo previste" dall'articolo "28 della direttiva 95/46[144] sono le custodi dei menzionati diritti e libertà fondamentali"[145].

---

[137] Corte di Giustizia UE, Grande Sezione, sent. 8 aprile 2014, *Digital Rights Ireland e a.*, in C-293/12 e C-594/12.

[138] Il Commissario nazionale deve verificare il livello di protezione dei dati in uno Stato terzo rispetto all'UE, come da articolo 25, pgf. 6, della direttiva 95/46: *Data Protection Law* del 1988, come emendata dalla *Data Protection (Amendment) Act* del 2003, art. 11, pgf. 2, lett.a) ("*The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof*"; per il testo completo v. www.irishstatutebook.ie/eli/2003/act/6/section/11/enacted/en/html#sec11 oppure www.dataprotection.ie/docs/Law-On-Data-Protection/m/795.htm).

[139] Sul tema importante B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. UE*, n. 2, 2013, p. 313 ss., spec. p. 315 ss.

[140] Questa la posizione di *Y. Bot*: per la giurisprudenza significativa sul punto Corte di Giustizia UE, Grande Sezione, sent. 21 dicembre 2011, *N. S. (M. E., A. S. M., M. T., K. P., E. H.) (C-411/10) c. Secretary of State for the Home Department*, e *M. E. e a. (C-493/10) c. Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform*, in C-411/10 e C-493/10.

[141] Ossia quelle di cui all'articolo 3, pgf. 1, lettera b), della decisione stessa.

[142] Di cui all'articolo 28, pgf. 3 della direttiva *cit.*

[143] Spec. il *considerando* n. 10 e l'art. 1 della direttiva 95/46/CE.

[144] "Inoltre, ai sensi dell'articolo 28, pgf. 4, primo comma, della direttiva 95/46/CE, «[q]ualsiasi persona (…) può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali». L'articolo 28, pgf. 4, secondo comma, di tale direttiva, precisa che «[q]ualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 [di detta] direttiva». […] quest'ultima disposizione consente agli Stati membri di adottare misure di legge intese a limitare la portata di diversi obblighi e diritti previsti nella direttiva 95/46, qualora tale restrizione costituisca una misura necessaria alla salvaguardia, segna-

La Corte, però, ragiona in punto di diritto. Non è detto che la Commissione, nel 2000 e dopo, potesse fare lo stesso.

Per l'Avv. gen. *Bot*[146], l'istituzione *temeva* l'interferenza del *Data Commissioner* : la sua competenza a sospendere il trasferimento dei dati là dove non avrebbero ricevuto protezione uguale a quella europea rischiava infatti di mettere *in pericolo la rinegoziazione con gli USA* della decisione n. 520[147].

5. Dopo Edward Snowden: il rispetto della vita privata e la protezione dei dati personali "alla luce della Carta dei Diritti", o …

In questa cornice, la Corte di Giustizia UE ha dovuto chiarire il ruolo delle autorità nazionali con riguardo al trattamento dei dati personali[148], e le competenze della Commissione discendenti dall'articolo 25, pgf. 6, della direttiva, volte a valutare la protezione offerta da un paese terzo. Per la Corte, "le disposizioni della direttiva 95/46, disciplinando il trattamento dei dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono *necessariamente essere interpretate alla luce dei diritti fondamentali garantiti dalla Carta*"[149].

La direttiva[150] persegue difatti "una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche e, segnatamente, del diritto fondamentale del rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di

---

tamente, della sicurezza dello Stato, della difesa, della pubblica sicurezza, nonché della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali": così le *conclusioni* dell'Avv. gen. *Y. Bot*, al p.to 66.

[145] Per questa posizione Corte di Giustizia UE, sentt. 8 aprile 2014, *Commissione/Ungheria*, in C-288/12, p.to 48, e p.to 51 per la giurisprudenza citata, e, infine, p.to 53; *Digital Rights Ireland e a.*, *cit.*, p.to 68, e la giurisprudenza citata; 9 marzo 2010, *Commissione/Germania*, in C-518/07, p.to 25.

[146] V. il pgf. 60 delle *conclusioni* dell'Avv. gen. *Y. Bot*.

[147] Indipendentemente dalla valutazione della Commissione, le autorità nazionali di controllo, *in ragione del loro ruolo fondamentale in materia di protezione dei dati personali*, devono poter indagare quando investite di una istanza che indica elementi capaci di rimettere in discussione la protezione assicurata da un paese terzo. Questo, incluso il caso in cui la Commissione abbia constatato, in una decisione basata sull'art. 25, pgf. 6, della direttiva 95/46, che il paese terzo interessato assicura invece un livello di tutela adeguato: per il ragionamento sempre le *conclusioni* dal pgf. 66 al pgf. 80.

[148] Interessante ricordare proprio qui la posizione adottata dal Garante italiano sui dati contenuti in fascicoli di cause civili o atti di processi penali, che chiarisce quanto preoccupa, sotto i profili più diversi, diverse autorità di controllo nazionali: per questo G. VIGEVANI, *Il "decalogo" del garante sulla sicurezza dei dati raccolti nelle intercettazioni*, in *Quad. cost.*, n. 3, 2014, 681 ss. Sul potere di controllo esercitato dal Garante sulla magistratura nell'esercizio della funzione giurisdizionale, come ricordato dallo stesso G. VIGEVANI, v. F. SORRENTINO, *È arrivato il "Codice della privacy" (con molti dubbi di costituzionalità). Limiti e problemi nel controllo sull'autorità giudiziaria*, in *Dir. e giust.*, n. 41, 2003, 101 ss.

[149] Il corsivo è di chi scrive: sent. *Schrems*, *cit.*, p.to 38., e, per la giurisprudenza precedente a sostegno di questa posizione, Corte di Giustizia UE, sentt. *Österreichischer Rundfunk e a.*, in C-465/00, C-138/01 e C-139/01, p.to 68.; Grande sezione, 13 maggio 2014, *Google Spain e Google*, in C-131/12, p.to 68.; Quarta Sezione, 11 dicembre 2014, *Reyneš*, in C-212/13, p.to 29.

[150] Sent. *Schrems*, *cit.*, par. 39, fa riferimento all'art. 1 della direttiva 95/46 e al secondo e decimo *considerando*.

protezione di tali libertà e diritti fondamentali"[151]. Questa garanzia, prevista dal diritto primario UE – ossia dalla Carta[152] - passa attraverso l'obbligo che incombe sugli Stati membri di istituire autorità "incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relativa alla tutela delle persone fisiche con riguardo al trattamento" dei dati[153].

Importante chiarire l'entità della protezione in gioco: agganciata al fondamentale requisito dell'indipendenza delle autorità nazionali, essa deve essere "efficace e affidabile, e deve essere interpretata alla luce di tale finalità"[154].

Come deducibile dal *considerando* n. 62 della direttiva, questo approccio comporta due garanzie: la prima, ancorata appunto all'indipendenza delle autorità interne, "elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali"[155]; la seconda, data dall'efficacia e dall'affidabilità delle loro attività, tali da rafforzare la protezione "delle persone e degli organismi interessati"[156].

Questi due aspetti, peraltro, non coprono soltanto le violazioni che possono verificarsi sul territorio nazionale dove opera l'autorità indipendente, ma anche quelle che si verificano altrove[157]: il "trasferimento" va dunque compreso come un "trattamento" dei dati ai sensi dell'art. 2, lett. b), della direttiva 95/46[158], e il relativo controllo come complementare rispetto alle "condizioni generali di liceità dei trattamenti di dati personali" di cui alla stessa fonte[159].

Inoltre, gli obblighi che discendono dalla direttiva incombono tanto sulla Commissione, quanto sugli Stati membri. Entrambi sono chiamati a garantire "un livello di protezione adeguato", la prima adottando una decisione sul rispetto di quest'ultimo da parte di un paese terzo[160], i secondi in altro modo. Fino alla pronuncia di invalidità di ogni decisione della Commissione, le autorità nazionali e gli Stati membri non potranno adottare atti contrari alla decisione di adeguatezza[161], ma, le prime almeno, potranno verificare se il trasferimento ri-

---

[151] Come sostenuto nella giurisprudenza della Corte UE sui diritti di cui agli artt. 7 e 8 della Carta: v. sentt. *Schrems*, *cit.*, p.to 39.; *Digital Records Irelands e a.*, *cit.*, p.to 68; Corte di Giustizia UE, Terza Sezione, 7 marzo 2009, *Rijkeboer*, in C-553/07, p.to 47.

[152] Sent. *Schrems*, *cit.*, p.to 40.

[153] In questa luce Corte di Giustizia UE, Grande Sezione, sentt. 16 ottobre 2012, *Commissione/Austria*, in C-614/10, p.to 36, e 8 aprile 2014, *Commissione/Ungheria*, in C-288/12, p.to 47.

[154] Sent. *Schrems*, *cit.*, p.to 41.

[155] Sent. *Schrems*, *cit.*, al p.to 41, e Corte di Giustizia UE, Grande sezione, sentt. 22 novembre 2007, *Commissione/Germania*, in C-518/07, p.to 25, e, di nuovo, 8 aprile 2014, *Commissione/Ungheria*, in C-288/12, p.to 48 (nonché la giurisprudenza richiamata in quest'ultima pronuncia).

[156] Valgono le indicazioni giurisprudenziali della nota immediatamente precedente.

[157] Sent. *Schrems*, *cit.*, dal p.to 42 al 50 compreso.

[158] Corte di Giustizia UE, sent. 30 maggio 2006, *Parlamento/Consiglio e Commissione*, in C-317/04 e C-318/04, p.to 56.

[159] Corte di Giustizia UE, 6 novembre 2003, sent. *Lindqvist*, in C-101/01, p.to 63: per questa e sulla tematica G.F. FERRARI, *La tutela dei dati personali in Italia 15 anni dopo: tempo di bilanci e di bilanciamenti*, Egea, Milano, 2012, 27 ss.; S. NIGER, *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006; R. PARDOLESI, (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffré, Milano, 2003; e ancora C. DE GIACOMO, *Diritto, libertà e* privacy *nel mondo della comunicazione globale: il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Giuffré, Milano, 1999.

[160] Sent. *Schrems*, *cit.*, p.ti 50 e 52.

[161] Di nuovo sent. *Schrems*, *cit.*, p.to 52.

spetti i requisiti della direttiva. Solo questa configurazione degli obblighi gravanti sul livello nazionale ed europeo permetterà una protezione effettiva, altrimenti "le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi [verrebbero] private del diritto, garantito all'articolo 8, pgff. 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali"[162].

Le decisioni della Commissione di cui alla direttiva 95/46, al fondo, toccano dunque la garanzia dei diritti fondamentali della persona come previsti dalla Carta, ossia dal diritto primario UE[163]: per questo è decisivo che le tutele degli Stati terzi in tema di dati, lette "alla luce della Carta", diano "una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione"[164].

6. … la garanzia della sicurezza nazionale "alla luce dei legittimi interessi d'ordine superiore" del pubblico potere statunitense?

Anche in ragione del caso *Apple*, resta da chiedersi come un simile livello di protezione possa coniugarsi con le ben diverse esigenze dettate (negli USA[165], e non solo[166]) dalla sicurezza nazionale. La Corte UE risponde con un dato che, in apparenza quantitativo, tocca nel merito la dimensione potenziale del fenomeno.

Le decisioni in materia della Commissione devono tener conto non soltanto di un livello "adeguato" di tutela (ossia conforme a quello della Carta dei diritti UE), ma dello stesso alla luce del "*numero significativo di persone* i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non" lo assicuri[167]. Quindi, "il potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da un paese terzo" dovrebbe realizzare "un *controllo stretto* dei requisiti risultanti dall'art. 25 della direttiva 95/46, *letto alla luce della Carta*"[168].

Il perno di questo approccio ruota intorno a una ulteriore preoccupazione. In un regime ancorato all'autocertificazione[169], il rispetto dei diritti fondamentali, della vita privata non-

---

[162] Qui la Corte UE ragiona sul precedente tracciato dalla sent. *Digital Rights Ireland e a.*, *cit.*, p.to 68.

[163] Sent. *Schrems*, *cit.*, p.to 60.

[164] Sent. *Schrems*, *cit.*, p.to 74.

[165] S. SILEONI, *La tutela della riservatezza negli Stati uniti …*, *cit.*, 1030, ritiene possibile che l'UE, nei rapporti con gli USA, possa sforzarsi per porre in equilibrio sicurezza e riservatezza: dato, però, quanto chiaramente affermato da *James B. Comey* (ora a capo dell'FBI) a proposito dell'intenzione dell'amministrazione *Obama* di non esercitare alcuna iniziativa per una nuova legge federale sulla questione, *supra*, al pgf. 3.a.1), sembra difficile che gli Stati Uniti siano un valido interlocutore, al momento almeno.

[166] Per la più ampia cornice disegnata dall'art. 24 della direttiva 2004/83/CE e le problematiche connesse F. BIONDI DAL MONTE, *Terrorismo, ordine pubblico e sicurezza nazionale nell'Unione europea*, in *Quad. cost.*, n. 3, 2015, 788 ss., spec. p. 790 per la nozione di pubblica sicurezza interna ed esterna degli Stati membri, e quella di ordine pubblico individuata dalla giurisprudenza sovranazionale; v. inoltre Corte di Giustizia UE, Prima Sezione, sent. 24 giugno 2015, *H.T. c. Land Baden-Wűrttemberg*, in C-373/13.

[167] Il corsivo è di chi scrive.

[168] Il corsivo è di chi scrive; il riferimento è sempre sent. *Schrems*, *cit.*, p.to 78, in analogia a quanto già stabilito nella sent. *Digital Rights Ireland e a.*, *cit.*, p.ti 47 e 48.

[169] *Supr*a, al pgf. dedicato alla descrizione del regime cd. di "approdo sicuro" negli Stati Uniti: la Commissione, all'art. 1, pgf. 1, della decisione 2000/520/CE, aveva infatti considerato che i principi di cui all'Allegato I

ché dei dati personali, dipende nono solo dai meccanismi "di accertamento e controllo" delle relative violazioni[170], ma, pure, dalle deroghe o eccezioni alla loro protezione.

La decisione del 2000[171] stabiliva difatti che le organizzazioni statunitensi, *aderenti o meno all'approdo sicuro*, dovevano osservare la legge del paese di appartenenza anche quando confliggente con quel regime. Per la Corte UE, questo porta a un solo risultato: la garanzia del *primato delle "esigenze di sicurezza nazionale*, interesse pubblico o amministrazione della giustizia" degli USA, "in forza del quale le organizzazioni americane sono tenute a disapplicare senza limiti tali principi" se "interferiscono con tali esigenze e risultano dunque incompatibili con le medesime"[172].

Detto altrimenti: proprio l'atto di un'istituzione sovranazionale, in virtù di una deroga di carattere generale prevista dallo stesso, ha esposto *i diritti fondamentali dei cittadini europei*, i cui dati personali sono stati trasferiti negli USA, a *una compressione fondata sulle esigenze statunitensi di sicurezza nazionale*[173]. Questo, oltretutto, nonostante la legislazione USA non conosca norme volte a limitare interferenze intense utili alla *national security*[174]*.* C'è però anche di più.

7. Cittadini europei e Governo federale degli Stati Uniti d'America: come proteggere le libertà nell'era della tecnologia?

Per la Corte UE[175] la normativa che non preveda "alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardino, oppure di ottenere la rettifica o la soppressione di tali dati, "non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'art. 47 della Carta. Infatti, l'art. 47, primo comma, della Carta esige che ogni individuo i cui diritti e le libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. […] l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto"[176].

Questo l'ultimo anello della catena logica che porta a dichiarare invalida la decisione del 2000, dando una lettura dell'art. 25 della dir. 95/46 conforme alla Carta dei diritti, e tale

---

della stessa, laddove applicati nel rispetto delle FAQ previste dall'Allegato II, offrivano il livello adeguato richiesto dall'UE (va ricordato che i principi e le FAQ erano stati pubblicati dal Dipartimento del commercio USA sul relativo sito).

[170] Sent. *Schrems*, *cit.*, p.to 81.

[171] Specificamente il *Titolo B* dell'Allegato IV, spec. quarto comma.

[172] Sent. *Schrems*, *cit.*, p.to 87.

[173] Non ha particolare importanza che i dati in questioni siano sensibili, oppure che l'ingerenza che li interessa abbia causato inconvenienti: di nuovo per queste osservazioni sent. *Digital Rights Ireland e a.*, *cit.*, p.to 33.

[174] Sent. *Schrems*, *cit.*, p.to 88.

[175] Sent. *Schrems*, *cit.*, p.to 95.

[176] Sent. *Schrems*, *cit.*, p.to 95, e, come ricordate dalla stessa Corte, sentt. 23 aprile 1986, *Les Verts/Parlamento*, in C-294/83, p.to 23; 15 maggio 1986, *Johnston*, in C-222/84, p.ti 18 e 19; 15 ottobre 1987, *Heylens e a.*, in C-222/86, p.to 14; Terza Sezione, 11 settembre 2008, *UGT-Rijo e a.*, in cause riunite da C-428/06 a C-434/06, p.to 80.

da valorizzare i poteri delle autorità nazionali *anche rispetto alla Commissione*. L'istituzione, infatti, mai potrebbe impedire alle autorità indipendenti nazionali l'esame di ogni istanza[177] relativa alla protezione dei diritti e delle libertà di un individuo, in relazione al trattamento di dati personali che lo riguardino.

Che i poteri delle autorità indipendenti possano mettere in discussione una decisione di adeguatezza della Commissione[178], o rendere difficile la rinegoziazione di accordi in materia, non è decisivo, perché se questa fosse la logica sposata dalla Corte, una soltanto sarebbe la conseguenza: mettere a rischio i diritti fondamentali, primo fra tutti quello al rispetto della vita privata[179].

8. Microsoft vs. USA: "molto rumore per nulla" … le democrazie sono imperfette, ma restano pur sempre democrazie.

Julie E. Cohen, interrogandosi sulle conseguenze di una intensa compressione dell'inviolabilità della *privacy*, arriva a sostenere che "[a] *society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy*"[180].

Una posizione simile, per motivi forse diversi, è quella della *Microsoft*, che, lo scorso 14 aprile, si è rivolta alla *U.S. District Court* di *Seattle*[181] per ottenere una pronuncia di illegittimità costituzionale relativa all'*Electronic Communication Privacy Act* (o ECPA), la cui sezione 2705(b)[182] violerebbe, secondo la multinazionale, il Primo e il Quarto emendamento[183] della Costituzione federale americana.

Microsoft avvia l'azione in ragione di due diritti che ritiene siano stati lesi: il primo, posto in capo ai consumatori, che sempre dovrebbero sapere se e quando il Governo federale ha ottenuto un *warrant* che gli permetta di accedere alla loro posta elettronica; il secondo, della multinazionale, che dovrebbe poter comunicare agli stessi che il Governo USA pretende, in assoluta segretezza, la sua collaborazione per conoscere le loro *e-mail*[184].

Le lesioni lamentate deriverebbero dall'applicazione della sezione 2705(b) dell'ECPA, che, per salvaguardare eventuali indagini, permette alle corti federali di obbligare *Microsoft* a

---

[177] In ultimo fondata sull'art. 28 della direttiva 95/46CE, da cui le autorità nazionali derivano i loro poteri.

[178] Ancorata all'art. 25 della dir. 95/46/CE.

[179] Sent. *Schrems*, *cit.*, dal p.to 100 al p.to 103 compreso.

[180] J. E. COHEN, *What Privacy is For?*, *cit.*, 1912.

[181] Per la precisione, alla *U.S. D.C.* dello *Western District* di *Washington,* a *Seattle*, come indicato *supra*, alla nota (78).

[182] 18 U.S.C. §2075(b).

[183] Come noto, i primi dieci Emendamenti della Costituzione federale, approvati nel 1791, rappresentano il cd. *Bill of Rights* americano. Stabiliscono, rispettivamente, il Primo e il Quarto emendamento: (I) *Freedom of Religion, Press, Expression,* "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*"; (IV) *Search and Seizure*, "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized*".

[184] Di nuovo *Microsoft Co. v. The United States Department of Justice*, *Complaint for Declaratory Judgement* del 14 aprile 2016, *Introduction*, *cit.*

tenere i suoi clienti all'oscuro del fatto che il Governo USA sta investigando sul contenuto e le informazioni personali di cui alle loro *e-mail*. In particolare, la sezione 2705(b) non prevede che il rischio di vanificare le inchieste vada valutato in relazione a singole indagini, e non stabilisce un limite di tempo oltre il quale il rispetto della segretezza imposta a *Microsoft* (con il cd. *secrecy order*) possa venir meno[185].

Nel tempo, i *secrecy orders* ottenuti dal Governo grazie alla sezione 2705(b) dell'ECPA sarebbero aumentati tanto quanto l'abitudine dei consumatori ad affidare dati sensibili e personali al *cloud*. Per questa via, secondo *Microsoft*, sarebbero stati violati il Quarto emendamento, che, vietando perquisizioni e sequestri ingiustificati, garantisce che i cittadini (e, per *Microsoft*, le imprese) siano "*secure in their persons, houses, papers and effects*", e il Primo emendamento, dal quale discenderebbe il diritto di *Microsoft* a comunicare liberamente con i suoi clienti e a discutere altrettanto liberamente delle modalità governative di svolgimento delle indagini federali[186].

Ora, per la multinazionale: "*People do not give up their rights when they move their private information from physical storage to the cloud*"[187].

Per *Microsoft*, questo approccio regge la tesi di incostituzionalità proposta: l'evoluzione tecnologica recente incide di certo sui mezzi prescelti per conservare informazioni e dati personali, ma non sull'obbligo costituzionale posto a carico dell'Esecutivo federale di rendere note le indagini avviate sulle informazioni e sui dati in questione, escluse alcune circostanze di natura del tutto eccezionale[188]. Il Governo USA, al contrario, avrebbe utilizzato la transizione al *cloud computing* come occasione per trasformare il requisito della segretezza delle indagini da eccezionale ad ordinario, costringendo gli *online cloud providers* come *Microsoft*, fra i tanti, ad adempiere a un obbligo imposto in via giudiziaria. Nei 18 mesi che precedono l'aprile 2016, le corti federali avrebbero adottato circa 2600 *secrecy orders*, impedendo alla multinazionale di rendere noti i *warrants*; nel solo Distretto di *Washington*, poi, ben venticinque di questi non avrebbero previsto alcun limite temporale per il segreto richiesto[189].

In sintesi, sempre con le parole di *Julie E. Cohen*, *"[F]reedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems*"[190].

Con questa azione *Microsoft* imbocca la via che probabilmente porterà alla Corte Suprema, per vedere infine riconosciuti, nell'era della tecnologia, la più piena inviolabilità del diritto alla sfera privata (inteso come libertà negativa), e il nuovo volto del diritto a manifesta-

---

[185] Sempre il *plaintiff* di *Microsoft*, *Introduction*, p.to 1., *cit.*
[186] Così di nuovo il *plaintiff* di *Microsoft*, *Introduction*, p.to 1., *cit.*
[187] Il *plaintiff* di *Microsoft*, *Introduction*, p.to 1., *cit.*, ultimo periodo.
[188] Il *plaintiff* di *Microsoft*, *Introduction*, p.to 2., *cit.*
[189] Il *plaintiff* di *Microsoft*, *Introduction*, p.to 5., *cit.*
[190] J. E. COHEN, *What Privacy is For?*, *cit.*, 1905, al quale si rinvia anche per i riferimenti bibliografici sul punto all'opera di M. FOUCAULT e M. WEBER.

re il proprio pensiero, di cui sarebbero titolari anche le imprese. Passando attraverso il potere giudiziario per conseguire questo obiettivo, ciò dimostrerebbe la tesi di questo scritto.

Le democrazie sono imperfette[191] perché la realizzazione dei principi liberali settecenteschi sui quali si reggono avviene all'ombra del fattore umano, per definizione fallace.

Proprio perché imperfette, però, l'unico modo di salvaguardarle sta, quando in gioco ci sono la sicurezza, la tecnologia e i diritti, nel riportare alla luce, in modo fedele al modello astratto, la separazione dei poteri e la tutela dei diritti (in questo caso delle libertà negative). Se così è, solo chi persegue l'interesse dell'intera collettività può riuscire in questo; sostituire allo Stato di diritto i poteri privati può sembrare una conquista, ma non lo è.

Al momento almeno, utenti e consumatori non eleggono gli amministratori delegati o i membri dei Consigli di amministrazione delle multinazionali che, nei secoli, non risulta abbiano scritto Carte dei Diritti.

I cittadini, al contrario[192], come singoli o associazioni (ai più diversi fini), possono esercitare gli strumenti di democrazia diretta e ricorrere ai rimedi giuridici a protezione delle loro libertà, grazie alle Costituzioni che dovrebbero affrancarli dalla versione contemporanea della condizione di suddito: essere una semplice pedina, nella sostanza, di *stakeholders* di fama mondiale.

Much ado about nothing?

---

[191] A. DI GIOVINE, S. SICARDI, (a cura di), *Democrazie imperfette: atti del Convegno dell'Associazione di diritto pubblico comparato ed europeo*, *Torino, Università degli Studi, 29 marzo 2002*, Giappichelli, Torino, 2005.

[192] In relazione alle tesi proposta v. anche F. CHIUSI, *Grazie mr Snowden #Datagate #NSA, cit.*, spec. laddove individua i fenomeni del "determinismo tecnologico" (che fa temere per la sopravvivenza della politica intesa come rappresentanza delle libere scelte dei cittadini), e del "riduzionismo tecnologico" (capace di trasformare la politica in "algoritmo, [in] scelta obbligata").