Gli 'atti politici' all'epoca delle privatizzazioni: il banco di prova della Direttiva *Data Retention*[*]

di Maria Francesca De Tullio **
(25 maggio 2015)

1. Introduzione

La ricerca si interrogherà sui limiti entro i quali è legittimo che lo Stato deleghi ai privati le intercettazioni a scopi di sicurezza. L'occasione è data dall'annullamento della Direttiva cd. *Data Retention* da parte della Corte di Giustizia: oggi il Legislatore ha carta bianca in materia, e deve rispondere alle sollecitazioni portate dall'inasprimento del terrorismo islamico. Occorre quindi studiare una disciplina che sia efficace e rispettosa dei principi democratici.

Si partirà dal quadro normativo disegnato dai Trattati sull'Unione Europea e dalla *Convenzione Europea dei Diritti dell'Uomo* (CEDU). Lo scopo sarà indagare su come l'ordinamento concilia i diritti fondamentali con le esigenze investigative. Apparentemente le due istanze sono opposte: le garanzie penalistiche impongono di non perdere il contatto con l'azione illecita, mentre gli addetti ai lavori chiedono di poter intervenire in largo anticipo rispetto al reato. Le stesse fonti evidenzieranno come l'intervento delle imprese si può inserire nell'assetto costituzionale dei poteri.

Attraverso i parametri ricostruiti si verificherà la legittimità della Direttiva cd. *Data Retention*, che privatizza in molti punti la raccolta su vasta scala di metadati. L'esame sarà ripetuto nell'ordinamento del Regno Unito, rispetto al quale saranno osservati gli effetti concreti delle leggi di recepimento e la loro corrispondenza ai principi fondamentali.

Allora, si potrà accertare se l'*outsourcing* ha lasciato dei vuoti di tutela, e, in caso di esito positivo, proporre come il legislatore interno e comunitario possano regolare l'attività esternalizzata.

2. Titolarità e ragionevolezza dei nuovi poteri emergenziali: il principio di precauzione

Per incardinare correttamente la questione della privatizzazione, che sarà oggetto di trattazione nel prosieguo, sembra opportuno approfondire i principi fondamentali che regolano l'emergenza. Non si pretende qui di sostituire le tante e autorevoli

[*] Scritto sottoposto a *referee*.

elaborazioni sul tema[1], ma solo di riprenderne alcuni aspetti. Si vedrà cioè come i canoni di ragionevolezza possono ancora aderire alla realtà attuale.

Lo stato d'emergenza non è più un insieme di misure straordinarie provvisorie. Lo sviluppo tecnologico migliora le capacità delle organizzazioni criminali, e quindi costringe le autorità a uno stato di perenne allerta: l'unica strategia utile di sorveglianza sembra un controllo totale, che ha luogo a prescindere da specifici sospetti[2]. Vi è ormai poco di 'eccezionale' nelle deroghe: esse fanno parte di un'ordinaria «amministrazione del rischio»[3], che viene affidata ai privati per motivi di efficacia ed efficienza.

L'esternalizzazione non porrebbe problemi se la sicurezza fosse l'unico obiettivo dell'ordinamento: in questo caso non rileverebbe la natura del soggetto, ma solo la sua competenza. Nel diritto costituzionale, però, l'*outsourcing* deve fare i conti con i principi fondamentali. L'intercettazione, nella fattispecie, incide sulla riservatezza, sancita dall'articolo 8 della CEDU[4] e dall'articolo 8 della *Carta dei Diritti Fondamentali dell'Unione Europea*[5] (cd. 'Carta di Nizza').

Secondo le due fonti citate, le deroghe non possono mai vanificare il contenuto essenziale delle libertà inviolabili, e devono perseguire un valore di rango pari a quello della posizione lesa[6]. Nell'*an*, la misura deve essere attuata solo se non si può ottenere lo stesso risultato con mezzi meno invasivi; nel *quantum*, essa deve essere limitata allo stretto necessario per il perseguimento del fine[7]. Dal punto di vista

---

[1] Agli specifici fini di questo scritto sono risultati preziosi, in particolare: E. CHELI, *Stato costituzionale e ragionevolezza*, Editoriale Scientifica, Napoli, 2011, pp. 19-35; A. MORRONE, *Il custode della ragionevolezza*, Giuffré, Milano, 2001, pp. 3-30; G. SCACCIA, *Gli "strumenti" della ragionevolezza nel giudizio costituzionale*, Giuffré, Milano, 2000, pp. 182-354; A.S. AGRÒ, *Commento all'art. 3*, in G. BRANCA (fondato da) – A. PIZZORUSSO (continuato da), *Commentario alla Costituzione*, Zanichelli – Foro Italiano, Bologna – Roma, 1975, p. 126, pp. 142-145.

[2] J. YOO, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, UC Berkeley Public Law Research Paper No. 2369192, anche in *http://ssrn.com/abstract=2369192*, pp. 7-8; P.L. PETRILLO, *Forma di governo e legislazione anti-terrorismo in Canada. Spunti di riflessione comparata sul ruolo dei Parlamenti al tempo dell'emergenza permanente*, in *http://www.forumcostituzionale.it/site/index3.php?option=content&task=view&id=941*, p. 16.

[3] L'espressione è in: M.C. CABIDDU, *Necessità ed emergenza: ai confini dell'ordinamento*, in *Amministrare*, fasc. 2/2010, p. 172. La stessa tendenza viene rilevata anche in: D. CHIAVIELLO, *L'amministrazione dell'"ordinaria" emergenza*, in *Federalismi.it*, n. 12/2010, p. 13-23; A. BENAZZO, *L'emergenza nel conflitto tra libertà e sicurezza*, Giappichelli, Torino, 2004, pp. 4-5; G. MICCIARELLI, *Emergenza ed eccezione nel diritto contemporaneo*, in A. TUCCI (a cura di), *Disaggregazioni. Forme e spazi di* governance, Mimesis edizioni, Milano, 2013, pp. 58-60; T.E. FROSINI – C. BASSU, *La libertà personale nell'emergenza costituzionale*, in *http://archivio.rivistaaic.it/materiali/anticipazioni/liberta_personale/index.html*, p. 3; P. MINDUS, *Emergenza, Costituzione, diritti fondamentali: una guida critica*, *Working paper* n. 9/2007, Dipartimento di studi politici dell'Università di Torino, Torino, 2007, pp. 37.

[4] Convenzione Europea dei Diritti dell'Uomo, in *http://www.echr.coe.int/Documents/Convention_ITA.pdf*, Articolo 8.

[5] Carta dei Diritti Fondamentali dell'Unione Europea, in *http://www.europarl.europa.eu/charter/pdf/text_it.pdf*, Articolo 8.

[6] Convenzione Europea dei Diritti dell'Uomo, Articolo 8; Carta dei Diritti Fondamentali dell'Unione Europea, Articolo 52.

[7] European Court of Human Rights – Court (Plenary), *Case of Klass and Others v. Germany*, Application no. 5029/71, 6/9/1978, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510*, punti 42, 50; Corte di Giustizia dell'Unione Europea – Grande Sezione, *Digital Rights Ireland Ltd c. Ireland*, cause riunite C−293/12 e C-594/12, 8 aprile 2014, in *http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dbcd805c70edfe45d48ed4fd48d0b7d*

formale, è requisito vitale che la compressione sia disposta dal potere legislativo, il quale deve predisporre un sistema di controlli «adeguato ed effettivo» contro gli abusi[8]. Tale obbligo trova fondamento nell'istituto della riserva di Legge, proprio della nostra Costituzione, e comunque nella *rule of law*, che regge il sistema dell'Unione Europea e della CEDU. Lo spirito di tali norme è la tutela delle minoranze: nella discussione parlamentare, la maggioranza decide solo a seguito di un confronto con le opposizioni. Perché la *ratio* di tali regole sia effettivamente garantita, la Legge deve essere abbastanza chiara e precisa da rendere prevedibili al cittadino le conseguenze della sua condotta[9].

Non si condivide qui l'idea che l'emergenza possa sospendere o indebolire tali canoni: questi ultimi sono connaturati alla sovranità popolare, al punto che normalmente negli ordinamenti democratici resistono alla revisione costituzionale[10]. Rinunciarvi vorrebbe dire probabilmente aprire una fase nuova, lontana dalle regole dello Stato sociale di diritto.

Il reale *impasse* oggi è che la sorveglianza – come sopra descritta – procede anche quando non si hanno nemmeno delle ipotesi circa l'*an*, il tempo e il luogo del futuro attentato. Sicché il giudizio di proporzionalità, che è un giudizio prognostico, deve immedesimarsi in un'autorità che non è in grado di prevedere esattamente se il provvedimento è necessario e se avrà un effetto utile. In tali condizioni vi è un pericolo maggiore che l'esito sarà irragionevole, ma l'ordinamento è in parte costretto ad accettare questo azzardo: se la polizia si attivasse solo su dati sicuri, rischierebbe di agire troppo tardi, con conseguenze irrimediabili per i diritti. In simili situazioni la limitazione della riservatezza può essere accettabile, in quanto viene in rilievo «un'altra sfera attinente alla sicurezza, quella collegata alla tutela di esigenze collettive di tutela, derivante dalla promozione del sistema delle libertà costituzionali in via positiva, più che dalla garanzia delle tradizionali libertà negative, potenzialmente svincolata dall'ambito penale e dalla funzione repressiva dello Stato»[11].

Nel campo ambientale si è cercato di ricondurre a razionalità simili decisioni mediante il principio di precauzione, recepito dall'articolo 191 del *Trattato sul Funzionamento dell'Unione Europea*[12]. Il canone, però, non è limitato a quell'ambito,

---

d70.e34KaxiLc3qMb40Rch0SaxuNaNf0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=205128 (d'ora in poi: *Digital Rights Ireland Ltd c. Ireland*), punto 38.

[8] European Court of Human Rights – Court (Plenary), *Case of Klass and Others v. Germany*, Application no. 5029/71, 6/9/1978, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510*, punto 50.

[9] European Court of Human Rights – Court (Plenary), *Case of the Sunday Times v. The United Kingdom*, Application no. 6538/74, 26/4/1979, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57584*, punto 49; Corte di Giustizia dell'Unione Europea – Seconda Camera, *Knauf Gips KG c. Commissione europea*, C−407/08 P, 1/7/2010, in *http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0407&lang1=en&type=TXT&ancre=*, punto 91.

[10] P. PINNA, *L'emergenza nell'ordinamento costituzionale italiano*, La Commerciale, Sassari, 1988, pp. 165-185.

[11] T.F. GIUPPONI, *Sicurezza personale, sicurezza collettiva e misure di prevenzione. La tutela dei diritti fondamentali e l'attività di* intelligence, in *http://www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0043_giupponi.pdf*, p. 5. Tanto la sorveglianza quanto le misure di prevenzione – discusse dall'Autore citato – trovano la loro *ratio* nella necessità di garantire la 'sicurezza dei diritti', e a tale scopo vanno commisurate: *ibidem*, pp. 2-14.

[12] La politica ambientale «è fondata sui principi della precauzione e dell'azione preventiva, sul principio della correzione, in via prioritaria alla fonte, dei danni causati all'ambiente, nonché sul principio 'chi inquina paga'»: *Trattato sul Funzionamento dell'Unione Europea*, in *http://www.csm.it/Eurojust/CD/25.pdf*, Articolo 191.

perché secondo la Commissione Europea può essere esteso «a qualunque misura di gestione dei rischi»[13].

Secondo la più comune definizione del principio, «dove vi è la minaccia di un pericolo serio e irreversibile la mancanza di piena certezza scientifica non deve essere utilizzata come una ragione per posporre misure» volte a sventare il pregiudizio[14]. La commercializzazione di un prodotto potenzialmente dannoso, ad esempio, può essere vietata anche quando non si hanno sicurezze sulla sua nocività. Ciò in quanto il diritto alla salute può essere ritenuto più importante rispetto alle libertà economiche. Allo stesso modo, un cittadino può essere sorvegliato in base a un mero sospetto, anche se non si è certi che stia materialmente tentando o organizzando un delitto.

Il rovescio della medaglia è che vi sono dei limiti: il Legislatore non può bendarsi gli occhi volontariamente, né trascurare del tutto uno dei valori in gioco. Prima e dopo l'emanazione, deve condurre un'analisi rispettosa degli standard accettati dalla comunità scientifica: la misura precauzionale è consentita se l'esame evidenzia che vi sono ragioni fondate per temere un pregiudizio e che la residua incertezza è oggettivamente ineliminabile, perché la disciplina specialistica non è giunta a un sufficiente stato di avanzamento. In caso contrario, si legittimerebbe l'ignoranza colpevole del Legislatore che agisse senza essersi curato di studiare adeguatamente la materia. Il passaggio successivo è quello con cui si stima la proporzionalità dei provvedimenti. Ancora una volta, serve il contributo dei saperi extra-giuridici: questi ultimi traducono in grandezze misurabili e confrontabili i costi e i benefici per i beni giuridici coinvolti[15].

La scelta pubblica è costretta ad avvalersi della tecnica, ma al contempo si emancipa da una supina adesione alla stessa[16]. Dove gli esperti danno certezze obiettive, chi decide deve conformarsi a tali responsi, perché la norma è vincolata al fatto; tuttavia esistono questioni opinabili, e su queste ultime il principio non leva spazio alla discrezionalità degli organi legittimati dal voto popolare[17]. Quando esiste un margine di errore, il decidente deve pur sempre scegliere secondo opportunità

---

[13] COMMISSIONE EUROPEA, *Comunicazione COM(2000) 1, 2000, sul tema 'principio di precauzione'*, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:it:PDF*, § 6.3. L'applicazione di tale canone per l'applicazione del principio di ragionevolezza al «terrorismo del tempo ordinario» si deve a: G. DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, in *Federalismi.it*, n. 10/2015, in *http://www.federalismi.it/ApplOpenFilePDF.cfm?artid=29517&dpath=document&dfile=18052015224734.pdf&content=Le+libert%C3%A0+fondamentali+in+tempo+di+ordinario+terrorismo+-+stato+-+dottrina+-+*, pp. 2-7.

[14] «In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation»: Principio 15, *Rio Declaration on Environment and Development*, in *http://www.unep.org/Documents.Multilingual/Default.asp?DocumentID=78&ArticleID=1163*. Molte delle riflessioni presentate sono nate dagli spunti critici di Sunstein: vd. C. SUNSTEIN, *Laws of fear: beyond the precautionary principle*, Cambridge University Press, 2005, pp. 13-149, pp. 224-227.

[15] Qui si è interpretato il principio di precauzione a partire dalle indicazioni della Commissione: COMMISSIONE EUROPEA, *Comunicazione COM(2000) 1, 2000, sul tema 'principio di precauzione'*, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:it:PDF*, §§ 5, 6.

[16] N. SACHS, *Rescuing the Strong Precautionary Principle from its Critics*, in *University of Illinois Law Review*, 2011, vol. 2011, pp. 1316-1317; G.N. MANDEL – J.T. GATHII, *Cost-Benefit Analysis Versus the Precautionary Principle: Beyond Cass Sunstein's Laws of Fear*, in *University of Illinois Law Review*, 2006, anche in *http://ssrn.com/abstract=822186*, pp. 1069-1071.

[17] R. ALEXY, *Teoria dei diritti fondamentali*, Il Mulino, Bologna, 2012, pp. 646-649.

quale sbaglio costituisce il male minore[18]. Nel campo dell'*intelligence*, ad esempio, si possono correre due opposti rischi: fermare un innocente o lasciare agire un terrorista. L'opzione sull'uno o sull'altro dipende dall'importanza data al bene sicurezza, e quindi presuppone un bilanciamento tra valori costituzionali che lo scienziato non è autorizzato a svolgere.

Il principio di legalità deve essere rispettato in modo sostanziale: dove c'è oggettiva incertezza c'è una scelta di merito, e quindi la decisione spetta all'organo eletto[19]. In caso contrario, si spezzerebbe il legame tra il popolo sovrano e lo Stato apparato.

Resta il problema di comprenderne i limiti di necessità e proporzionalità. Qui l'ignoranza sul fatto potenzialmente dannoso non cambia le carte in tavola, ma semplicemente impone di considerare il profilo probabilistico dei rispettivi vantaggi e svantaggi. Un sacrificio sicuro, infatti, non può 'pesare' nella ponderazione quanto uno eventuale, e quindi «quanto più gravemente pesa l'intervento in un diritto fondamentale, tanto maggiore deve essere la certezza delle premesse a supporto dell'intervento»[20].

---

[18] D.E. ADELMAN, *Harmonizing Methods of Scientific Inference with the Precautionary Principle: Opportunities and Constraints*, in *Environmental Law Reporter*, 2004, vol. 34, pp. 10133-10134, p. 10137; M. GEISTFELD, *Implementing the Precautionary Principle*, in *Environmental Law Reporter*, 2001, vol. 31, pp. 11332-11333; N. SACHS, *Rescuing the Strong Precautionary Principle from its Critics*, in *University of Illinois Law Review*, 2011, vol. 2011, pp. 1303-1304, 1320; I. CARMASSI, *Emissioni elettromagnetiche: tutela della persona e principio di precauzione*, in *Danno e responsabilità*, n. 7/2008, pp. 729 ss..

[19] È qui che viene in rilievo il cd. 'atto politico', insindacabile all'autorità giudiziaria in quanto espressione della funzione di indirizzo. Sul tema cfr. T. MARTINES, *Indirizzo politico*, in *Enciclopedia del diritto*, vol. XXI, Milano, 1971, pp. 134 ss.; G.B. GARRONE, *Atto politico*, in *Digesto delle discipline pubblicistiche*, vol. I, Torino, 1987, pp. 544 ss.; G. GROTTANELLI DE' SANTI, *Indirizzo politico*, in *Enciclopedia giuridica*, vol. XVI, Roma, 1989, pp. 1 ss.; V. CRISAFULLI, *Per una teoria giuridica dell'indirizzo politico*, in *Studi urbinati*, 1939; V. CHELI, *Atto politico e funzione di indirizzo politico*, Milano, 1961, pp. 93 ss.; ID., *Funzione di governo, indirizzo politico, sovranità popolare*, in G. AMATO – A. BARBERA (a cura di), *Manuale di diritto pubblico*, Bologna, 1994, pp. 297 ss.; A. MANNINO, *Indirizzo politico e fiducia nei rapporti tra il Governo e il Parlamento*, Milano, 1973; F. FERRARA, *Problemi attuali dell'indirizzo politico nei sistemi di governo parlamentari: il caso italiano*, in *Politica del diritto*, 1981, p. 413; M. DOGLIANI, *Indirizzo politico. Riflessioni su regole e regolarità nel diritto costituzionale*, Napoli, 1985, pp. 201 ss.; P. CIARLO, *Mitologia dell'indirizzo politico e identificazione partitica*, Napoli, 1988. Per una comparazione con l'ordinamento francese cfr. G. DI GASPARE, *Considerazioni sugli atti di governo e sull'atto politico. L'esperienza italiana e francese nello stato liberale*, Milano, 1984. Oggi tuttavia la funzione di indirizzo deve confrontarsi con l'evoluzione dell'istituto della rappresentanza, su cui cfr. A. CIANCIO, *I gruppi parlamentari: studio intorno a una manifestazione del pluralismo politico*, Giuffrè, Milano, 2008, pp. 103-194; S. CURRERI, *Democrazia e rappresentanza politica: dal divieto di mandato al mandato di partito*, Firenze University Press, Firenze, 2004, pp. 35-128.

[20] La citazione è in: R. ALEXY, *Teoria dei diritti fondamentali*, Il Mulino, Bologna, 2012, p. 651. Lo stesso concetto è stato sostenuto dalla Corte suprema degli Stati Uniti: «In each case [courts] must ask whether the gravity of the "evil," discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger» [«in ciascun caso [le Corti] devono chiedersi se la gravità del "male", scontata in proporzione alla sua improbabilità, giustifica una tale invasione della libertà [...] in quanto necessaria a evitare il danno»]: Supreme Court of United States, *D. Ennis et al. v. United States*, No. 336, 4/6/1951, in *http://law.justia.com/cases/federal/districtcourts/oklahoma/okndce/4:2007cv00436/25229/63*. La sentenza è commentata in: R. SERRA CRISTÓBAL, *The Impact of Counter-terrorism Security Measures on Fundamental Rights: The Need for Supranational Common Standards of Rights Protection to respond to terrorism risk*, Relazione tenuta al IX Congresso internazionale della IACL, *Constitutional Challenges: Global and Local*, Oslo, 16-20 giugno 2014, in *http://www.jus.uio.no/english/research/news-andevents/events/conferences/2014/wccl-.cmdc/wccl/papers/ws1/w1-crist%C3%B3bal.pdf*, p. 4. Analogamente, la Corte costituzionale tedesca ha fissato anche una regola per cui «la probabilità che il pericolo paventato si

L'imperscrutabilità della minaccia nulla toglie dunque al portato dei principi di legalità e ragionevolezza: a quanto è parso di comprendere, quel che attiene al bilanciamento dei diritti fondamentali è prerogativa del potere pubblico, in particolare degli organi politici, e deve essere stabilito secondo stretta proporzionalità. Nel paragrafo seguente si spiegherà cosa succede a tale equilibrio costituzionale quando le funzioni di *intelligence*, e in particolare la sorveglianza delle comunicazioni, vengono privatizzate.

3. La funzione di indirizzo nell'*intelligence* privatizzata: la *data retention* in Europa

Alla luce dei principi ricostruiti, bisogna chiedersi quali aspetti della raccolta su vasta scala di metadati possano essere privatizzati e quali caratteristiche debbano presentare le aziende che svolgono l'attività[21]. L'esternalizzazione, infatti, non può tradursi in una scelta irragionevole o elusiva dei diritti.

Con l'*outsourcing* il privato è incaricato di funzioni che incidono coercitivamente sui diritti altrui; sicché le regole che egli si dà sono valide *erga omnes*, e non solo nei confronti di chi partecipa alla loro produzione o si vincola ad esse volontariamente. Di conseguenza il regime di tali atti si distanzia da quello dell'autonomia negoziale: non è più consentito all'azienda tutto quanto non sia espressamente vietato, come invece il principio di legalità imporrebbe all'autonomia negoziale. L'impresa, al contrario, deve rispettare i canoni pubblicistici, e quindi può attuare i soli poteri che le sono esplicitamente attribuiti dalla Legge, perché il principio di legalità sull'attività di imperio opera nella accezione positiva[22]. L'esternalizzazione avviene dunque mediante un atto formale simile a una delega: il Legislatore demanda l'esercizio di competenze proprie a un *contractor*, dettando criteri direttivi sull'oggetto del mandato e sui requisiti strutturali del mandatario[23].

Quanto al primo punto, si deve rilevare che ai privati non può essere affidata la ponderazione tra i valori dell'ordinamento: secondo la Commissione Europea, la decisione su tale ambito spetta in via esclusiva agli organi eletti[24]. Essenziale alla delega infatti è che «il delegato resta sempre responsabile dell'atto emanato»[25], ma

realizzi deve essere tanto più elevata, quanto più incisivo risulti l'intervento limitativo e quanto più importante sia il bene giuridico minacciato»: G. SCACCIA, *Gli "strumenti" della ragionevolezza nel giudizio costituzionale*, Giuffré, Milano, 2000, pp. 237-238.

[21] Rispetto a entrambi i profili della delega ai privati di decisioni vincolanti *erga omnes*, nonché all'impostazione complessiva del tema, si è accolto lo schema proposto in: G. DE MINICO, *Regole. Comando e consenso*, Giappichelli, Torino, 2005, pp. 151-169.

[22] Tra i tanti che hanno trattato il tema, cfr. G.U. RESCIGNO, *Sul principio di legalità*, in *Diritto Pubblico*, n. 19/1995, pp. 262-263.

[23] C. DE FIORES, *Trasformazioni della delega legislativa e crisi delle categorie normative*, Cedam, Padova, 2001, pp. 68-76; A.A. CERVATI, *La delega legislativa*, Giuffré, Milano, 1972, pp. 126-135. Vd. anche *supra*, nota 8.

[24] Così la Commissione ha stabilito nella *Comunicazione della Commissione al Parlamento Europeo e al Consiglio*. *Il futuro delle agenzie europee*, COM (2008) 135 definitivo, 11/3/2008, in *http://www.parlamento.it/web/docuorc2004.nsf/8fc228fe50daa42bc12576900058cada/5b5cba9f3297c495c125741f002f9a49/$FILE/COM2008_0135_IT.pdf*, § 2. Il documento riguarda le Autorità Indipendenti, ma la regola *a fortiori* è applicabile ai privati. Un approfondimento sul punto si deve a: G. DE MINICO, *Indipendenza delle autorità o indipendenza dei regolamenti? Lettura in parallelo all'esperienza comunitaria*, in *Alle frontiere del diritto costituzionale. Scritti in onore di Valerio Onida*, Giuffrè, Milano, 2011, pp. 730-740.

[25] G. MIELE, voce *Delega (diritto amministrativo)*, in *Enciclopedia del diritto*, vol. XI, Giuffré, Milano, 1971, p. 916. Nel diritto amministrativo, infatti, l'atto delegato è un atto definitivo: P. SACCO, *Il profilo della delega e*

ciò sarebbe impossibile nell'*outsourcing*: l'azienda è un soggetto politicamente irresponsabile, che non potrebbe mai rispondere di una funzione di governo. Questo vale a maggior ragione in materia di deroga alle libertà inviolabili, dove solo la fonte primaria può stabilire limiti, condizioni e controlli.

Il primo confine dell'esternalizzazione sembra essere dunque che i *contractors* possono esercitare solo compiti meramente attuativi, nell'ambito di un equilibrio tra principi che deve essere stato già stabilito dall'atto legislativo. «Se [, invece,] eteronomia e autonomia si collocassero sullo stesso piano, il rispetto dei valori dell'ordinamento superiore dipenderebbe da una mera eventualità: la loro coincidenza con i principi sostenuti dalle autorità private»[26].

In secondo luogo, la delega deve disciplinare l'organizzazione dell'azienda. Quanto meno, occorre che essa vincoli l'impresa a dotarsi di un organo deliberativo distinto da quello esecutivo, e prescriva controlli statali sull'attuazione delle regole interne ed eteronome. Queste eccezioni alla libertà associativa paiono giustificate e imposte dall'attività del privato, stante in questo caso la sua natura pubblicistica. Analogamente la nostra Costituzione, ad esempio, interviene sulla struttura dei partiti e dei sindacati, appunto in quanto essi hanno un ruolo rilevante nella realizzazione dell'interesse generale[27].

Vincoli di questo tipo servono verosimilmente a salvaguardare anche la razionalità intrinseca dell'esternalizzazione, cioè la coerenza con i suoi stessi scopi[28].

L'*outsourcing* è motivato da almeno tre fondamentali ragioni: la maggiore competenza tecnica delle imprese, la loro capacità di operare a costi inferiori e la loro neutralità[29]. Tuttavia tali vantaggi non sono scontati, ma sono assicurati solo se la delega prescrive specifiche garanzie in tal senso[30].

---

subdelega di funzioni amministrative, Giuffrè, Milano, 1984, p. 79.

[26] G. DE MINICO, *Regole. Comando e consenso*, Giappichelli, Torino, 2005, p. 167.

[27] *Ibidem*, pp. 156-157.

[28] C. DE FIORES, *Trasformazioni della delega legislativa e crisi delle categorie normative*, Cedam, Padova, 2001, pp. 73-77.

[29] D. RUMSFELD, *DOD Acquisition and Logistics Excellence Week Kickoff – Bureaucracy to Battlefield*, Discorso al Pentagono del 10/9/2001, in *http://www.defense.gov/speeches/speech.aspx?speechid=430*; S. BUTT, *Outsourcing Intelligence: the Relationship between the State and Private Intelligence in Post-apartheid South Africa*, A minor dissertation submitted in partial fulfilment of the requirements for the award of the degree of Master of Social Science in International Relations, 2010, in *https://open.uct.ac.za/handle/11427/3796*; A. LUCARELLI, *La democrazia dei beni comuni*, Laterza, Roma, 2013, pp. 21-25; S.A. SHAPIRO – E.C. FISHER – W.E. WAGNER, *The Enlightenment of Administrative Law: Looking inside the Agency for Legitimacy*, in *Wake Forest Law Review*, n.3/2012, vol. 47, anche in *http://ssrn.com/abstract=2173015*, pp. 464-471.

[30] S. BUTT, *Outsourcing Intelligence: the Relationship between the State and Private Intelligence in Post-apartheid South Africa*, A minor dissertation submitted in partial fulfilment of the requirements for the award of the degree of Master of Social Science in International Relations, 2010, in *https://open.uct.ac.za/handle/11427/3796*, pp. 19-24, pp. 61-78; S. ACKERMAN, *Senior NSA official moonlighting for private cybersecurity firm*, in *theguardian.com*, 17/10/2014, in *http://www.theguardian.com/us-news/2014/oct/17/senior-nsa-official-moonlighting-private-cybersecurity-firm*; T. BURGHARDT, *Private Spies: The Secret World of Intelligence Outsourcing*, in *Global Research*, 2/8/2008, anche in *http://www.globalresearch.ca/private-spies-the-secret-world-of-intelligence-outsourcing/9729*; J. MAYER, *The C.I.A.'s Travel Agent*, in *The New Yorker*, 30/8/2006, anche in *http://www.newyorker.com/magazine/2006/10/30/the-c-i-a-s-travel-agentt*; N. TZIFAKIS, *Contracting Out to Private Military and Security Companies*, Brussels: Centre for European Studies (CES) Research Paper, luglio 2012, anche in *http://ssrn.com/abstract=2117664*, pp. 30-48; Z. CHESTERMAN, *'We Can't Spy… If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'*, in *The European Journal of International Law*, n. 5/2008, vol. 19, pp. 1058-1064, pp. 1066-1069.

A monte, la Legge deve ovviare alla scarsa concorrenzialità che connota il settore, la quale mina l'efficacia e l'economicità. I requisiti tecnici e i regimi di autorizzazione richiesti dalle autorità costituiscono infatti una barriera all'entrata che genera difficoltà croniche per la libera competizione. Le norme stabilite dal mandato devono però anche penetrare nella *governance* interna della compagnia. Allo Stato spetta di introdurre controlli amministrativi sulla *performance* dell'impresa e di imporre norme sulla scelta dei soci e dei vertici che realizzino nei fatti l'imparzialità. In particolare, occorre evitare – o comunque regolamentare – lo scambio di personale tra Agenzie di *intelligence* e *contractors*, che alimenta i conflitti di interesse e la reciproca concessione di vantaggi abusivi o illeciti.

Il Parlamento, in altre parole, non pare liberarsi delle proprie responsabilità quando delega la sorveglianza ai privati. Esso deve quanto meno assicurare un bilanciamento proporzionato tra i valori, nonché aumentare i vincoli eteronomi sul mandatario in maniera proporzionale al peso dell'interesse pubblico coinvolto[31].

L'azienda, a sua volta, risponde in proprio delle violazioni che compie a danno dei diritti fondamentali, pure se riceve un mandato 'in bianco'[32]. In primo luogo, le libertà inviolabili elencate nella 'Carta di Nizza' sono obblighi 'orizzontali' immediatamente vincolanti anche per tutti i privati[33]. In secondo luogo, i *contractors* si mostrano ormai equiparabili all'autorità governativa: sempre più l'ordinamento dell'Unione costruisce la nozione di Pubblica Amministrazione in base al tipo di attività svolta, più che alla natura del soggetto incaricato[34]. Ciò ha conseguenze anche sull'effettività della tutela

---

[31] G. De Minico, *A Hard Look at Self-Regulation in the UK*, in *European Business Law Review*, n. 1/2006, vol. 17, anche in *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1347348*, pp. 186-191, p. 210.

[32] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, Human Rights Council - Seventeenth session, A/HRC/17/27, 16/5/2011, in *http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*, punto 45.

[33] *Walrave*, C-36/74, Corte di Giustizia dell'Unione Europea, 12/12/1974, in *http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30d69549abea206a4a67885291a6cc0eeb0c.e34KaxiLc3qMb40Rch0SaxuOaNf0?text=&docid=88848&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=263383*, §§ 16-19. Questo vale per le norme chiare, precise e incondizionate, ma la Corte di Giustizia ha dato un'interpretazione ampia di tale nozione: G. Strozzi – R. Mastroianni, *Diritto dell'Unione Europea. Parte istituzionale* (VI edizione), Giappichelli, Torino, 2013, pp. 208-209; G. Tesauro, *Diritto comunitario* (V edizione), Cedam, Padova, 2008, p. 94.

[34] Sempre più l'ordinamento dell'Unione Europea tende a definire l'Amministrazione non in base al soggetto che esercita l'autorità, bensì in base alla natura del potere: F. Caringella, *Manuale di diritto amministrativo* (VII edizione), DIKE Giuridica Editrice, Roma, 2014, pp. 585-586; F.G. Scoca, *Capitolo 1 - La pubblica amministrazione e la sua evoluzione*, in F.G. Scoca (a cura di), *Diritto amministrativo* (II edizione), Giappichelli, Torino, 2011, p. 17. Ciò accade, ad esempio, in materia ambientale: ci si riferisce alla *Convenzione sull'accesso alle informazioni, la partecipazione dei cittadini e l'accesso alla giustizia in materia ambientale*, Aahrus, 25/6/1998, in *http://www.isprambiente.gov.it/it/garante_aia_ilva/normativa/Normativa-sull-accesso-alle-informazioni/normativa-sovranazionale/convenzione_aarhus_25_06_1998.pdf*, articolo 2, commentata in J. Ebbesson, *Public Participation and Privatisation in Environmental Matters: An Assessment of the Aarhus Convention*, in *Erasmus Law Review*, n. 2/2011, vol. 4, anche in *http://ssrn.com/abstract=1971694*, pp. 78-81. Lo stesso avviene in materia di responsabilità per la violazione di norme comunitarie: Corte di Giustizia dell'Unione Europea, *Commissione c. Irlanda*, C-249/81, 27/11/1982, in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:61981CJ0249*, punto 15 (questo aspetto è anche rilevato in: G. Strozzi – R. Mastroianni, *Diritto dell'Unione Europea. Parte istituzionale* (VI edizione), Giappichelli, Torino, 2013, p. 326). L'ordinamento italiano riceve di riflesso tale orientamento: così, ad esempio, nelle norme sul procedimento amministrativo e sulle procedure di evidenza pubblica in materia di contratti (in quest'ultimo caso, su impulso della stessa Unione Europea): L. 241/1990, *Nuove norme in materia di procedimento amministrativo e di diritto*

per il cittadino: come ha stabilito il nostro Consiglio di Stato, gli atti del privato che esercita una pubblica funzione sono equiparati ai provvedimenti di imperio, qualora «incidano sulle posizioni soggettive di privati che vi entrino in contatto»[35]. Ne deriva che i comportamenti delle compagnie sono soggetti agli stessi rimedi opponibili agli enti pubblici, anche senza alcuna specifica previsione legislativa in tal senso.

Ora tali ragionamenti sui vincoli soggettivi e oggettivi che deve porre il Legislatore saranno applicati alla Direttiva dell'Unione Europea sulla *data retention*. Il fine è quello di verificare come l'esternalizzazione sia avvenuta e come dovrebbe avvenire secondo i canoni individuati.

3.1 La Direttiva *Data Retention*

La Direttiva 2006/24/CE del 15 marzo 2006 (cd. *Data Retention*)[36], finalizzata all'utilizzo dei tabulati per finalità di lotta al crimine, è un buon esempio del comportamento che il Legislatore comunitario non avrebbe dovuto tenere. Ai privati sono stati imposti poteri ampi, senza vincoli che garantissero la tutela della riservatezza.

L'Atto aveva l'obiettivo di armonizzare le disposizioni nazionali che in deroga alla Direttiva 2002/58/CE[37] imponevano la conservazione dei dati «allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi»[38]. Nella pratica, poi, è stata inserita tra le finalità anche quella preventiva[39].

La disciplina si imperniava su due obblighi disposti nei confronti dei *providers*: uno di archiviazione e l'altro di consegna alle autorità. I «fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione» dovevano conservare per un periodo da sei a ventiquattro mesi tutti i dati di traffico trattati[40]. Oggetto della prestazione imposta non erano i contenuti, ma

---

di accesso ai documenti amministrativi, 18/8/1990, in *http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990-08-07;241*, articolo 29(1); D. Lgs. n. 163/2006, *Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE*, 12/4/2006, in *http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2006-04-12;163*, articolo 32(f).

[35] Consiglio di Stato – Sezione IV, sent. 918/1998, 5/6/1998. La ripresa di questa giurisprudenza alla luce della nuova nozione comunitaria di Pubblica Amministrazione si deve a F. CARINGELLA, *Manuale di diritto amministrativo* (VII edizione), DIKE Giuridica Editrice, Roma, 2014, p. 632.

[36] *Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:IT:PDF.*

[37] La Direttiva 2002/58/CE è l'Atto che traduce in norme specifiche per il settore delle comunicazioni elettroniche i principi enunciati nella Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali. La norma prevede in via generale che i dati possano essere conservati dai *providers* solo finché necessari per la prestazione del servizio (articolo 6); sono ammesse tuttavia delle deroghe in materia di sicurezza (articoli 1 e 15): *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*, Gazzetta ufficiale n. L 201 del 31/7/2002, in *http://www.interlex.it/testi/02_58ce.htm*.

[38] Articolo 1, Direttiva 2006/24/CE.

[39] La stessa Corte di Giustizia l'ha interpretata in questo senso, valutandone la ragionevolezza anche in rapporto allo scopo preventivo: *Digital Rights Ireland Ltd c. Ireland*, punti 59 ss..

[40] Non si trattava di un dovere di raccolta: oggetto della normativa erano solo i dati che sarebbero stati comunque «generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati»: Direttiva 2006/24/CE, Articolo 3. Per il periodo di conservazione, vd. *Ibidem*, Articoli 8 e 12.

solo le informazioni estrinseche: l'ubicazione, gli identificativi del chiamante e del chiamato e la data e l'ora di inizio e fine della conversazione, nonché i loro analoghi informatici, segnatamente l'indirizzo IP e i momenti di inizio e fine della connessione[41].

Questo rappresentava una duplice interferenza nel diritto alla riservatezza sancito dalla 'Carta di Nizza'. La raccolta è di per sé un'ingerenza nella sfera personale, perché «crea le condizioni per un controllo che, seppur esercitato soltanto *a posteriori* in occasione del loro impiego, minaccia tuttavia in modo permanente, per tutto il periodo della loro conservazione, il diritto dei cittadini [...] alla riservatezza della loro vita privata»[42]. L'accesso delle autorità, poi, costituiva un'ulteriore compressione, anche se riguardava solo i metadati[43]: anche i dati estrinseci danno una certa visuale sulla sfera personale dell'individuo.

Nonostante ciò non si garantiva che l'intrusione fosse limitata allo stretto necessario: non si imponevano norme adeguate sulla sicurezza dei *databases* e non si vietava né all'Esecutivo né ai *providers* di farne un uso diverso da quello di indagine. Né si poteva contare sul regime che l'Unione dispone in via generale per la tutela dei dati personali: le Direttive 95/46/CE[44] e 2002/58/CE[45] non si applicano infatti in materia di sicurezza.

La *Data Retention* disponeva quindi un sacrificio sicuro e rilevante della riservatezza. Il corrispettivo vantaggio era invece doppiamente incerto.

In primo luogo, la sorveglianza era indiscriminata, e colpiva anche chi non era minimamente considerato pericoloso; pertanto non si può dire che la misura fosse giustificata dal timore fondato di un pregiudizio serio e irreversibile. In secondo luogo, non è stato tuttora mai dimostrato che la *data retention* serva realmente a sventare le trame criminose. Sono poche le prove addotte[46], e per di più la cronaca ha riferito di casi in cui gli attentatori sono riusciti a colpire nonostante fossero sotto specifico

---

[41] *Ibidem*, Articolo 5.

[42] *Conclusioni dell'Avvocato Generale*, *Digital Rights Ireland Ltd c. Ireland*, C 293/12, 12/12/2013, in *http://curia.europa.eu/juris/document/document_print.jsf?doclang=IT&text=&pageIndex=0&part=1&mode=lst&docid=145562&occ=first&dir=&cid=15124*.

[43]European Court of Human Rights – Court (Plenary), *Case of Malone v. The United Kingdom*, Application no. 8691/79, 2/8/1984, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533*, punto 64; *Digital Rights Ireland Ltd c. Ireland*, punti 29, 34, 35. Così anche la Corte costituzionale tedesca e la Corte suprema degli Stati Uniti: Bundesverfassungsgericht,1 BvR 370/07, 27/2/2008, in *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html* (la traduzione in lingua inglese è sul sito ufficiale del *Bundesverfassungsgericht*, in *http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html*); Supreme Court of the United States, *United States v. Jones*, No. 10-1259, 23/1/2012, in *http://www.law.cornell.edu/supremecourt/text/10-1259*.

[44] *Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31995L0046&from=IT*, articolo 3.

[45] Direttiva 2002/58/CE, articolo 1.

[46] Un *ex*-vicedirettore della FBI ha ammesso davanti all'*Intelligence and Security Committee* del Senato che vi è un solo caso in cui è stata scoperta in anticipo una trama terroristica grazie all'esame dei dati sulle comunicazioni. Vd. S. ACKERMAN, *US privacy board dissenters defend balancing act of NSA surveillance*, in *theguardian.com*, 23/1/2014, in *http://www.theguardian.com/world/2014/jan/23/us-privacy-boards-dissenters-nsa-surveillance-balance*; S. ACKERMAN – P. LEWIS, *US senators rail against intelligence disclosures over NSA practices*, in *The Guardian*, 31/7/2013, anche in *http://www.theguardian.com/world/2013/jul/31/us-senate-intelligence-officials-nsa*.

controllo di polizia[47]. Sarebbe stato forse più equilibrato un approccio meno invasivo, come quello della *data preservation*. Tale modello appare più mirato, perché impedisce la distruzione dei dati solo in presenza di un indizio e permette l'accesso solo in presenza di prove solide[48].

Rilievi simili di irragionevolezza sono stati mossi dalla Corte di Giustizia, che con la sentenza *Digital Rights Ireland v. Ireland* ha annullato l'intera Direttiva 2006/24/CE.

Il Giudice comunitario ha statuito a chiare lettere che il Legislatore ha lo specifico obbligo di adottare «norme chiare e precise che [regolino] la portata dell'ingerenza»[49]. Ciò è importante ai fini di questo studio, perché conferma che non tutto è delegabile: il Legislativo deve prevedere limiti, condizioni e controlli alla compressione dei diritti. La decisione specifica anche che il sacrificio delle libertà fondamentali deve seguire parametri di necessità e proporzionalità.

La sentenza tuttavia è solo tangente al discorso che si sta svolgendo. Qui si vuole analizzare il ruolo dei privati nella raccolta e analisi dei dati, sottolineando che essi sono stati illegittimamente autorizzati a influire sul bilanciamento tra i diritti fondamentali.

a) La conservazione dei dati da parte dei *providers*

La Direttiva *Data Retention* consegnava ai fornitori di servizi di comunicazione un potere-dovere di incidere in maniera sproporzionata sui diritti. La raccolta riguardava infatti tutti gli utenti, senza che si discriminasse in base alla presenza di un indizio o di un qualsiasi nesso con un fatto di reato[50]. L'imposizione era accompagnata dalla concessione di ampie libertà nella decisione sul bilanciamento. Sicché il Legislatore affidava la ponderazione a soggetti privi di legittimazione; in più, generava sacrifici non necessari della *privacy*, che sarebbero stati prevedibili ed evitabili senza danno per la sicurezza.

L'unico obbligo di trattamento che gravava sui *providers* era quello di mettere in atto «adeguate misure tecniche e organizzative» contro l'abuso, l'alterazione o la diffusione accidentale dei dati[51]. Non veniva prescritto che le informazioni fossero conservate nel territorio dell'Unione, con la conseguenza che esse potevano essere

---

[47] J. BURKE, *Charlie Hebdo suspects on US terrorist watchlist 'for years'*, in *The Guardian*, 9/1/2015, anche in *http://www.theguardian.com/world/2015/jan/09/charlie-hebdo-suspects-us-terrorist-watchlist-cherif-said-kouachi*.

[48] *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE* (2005/C 298/01), in *http://www.privacy.it/gepd20050926.html*, punto 20; COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Relazione sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE* (COM(2005)0438 – C6 0293/2005 – 2005/0182(COD)), in http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+WORD+V0//IT, Parere della Commissione per il mercato interno e la protezione dei consumatori; E. GUILD – S. CARRERA, *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*, CEPS Liberty and Security in Europe Papers No. 65, 29/5/2014, anche in *http://ssrn.com/abstract=2445901*, pp. 2-3; C. WALKER, *Data retention in the UK: Pragmatic and proportionate, or a step too far?*, in *Computer Law & Security Review*, n. 4/2009, vol. 25, p. 326.

[49] *Digital Rights Ireland Ltd c. Ireland*, punto 65.

[50] *Ibidem*, punti 48-59.

[51] Direttiva 2006/24/CE, Articolo 7.

trasferite in Paesi che non avrebbero garantito un regime di controlli equivalente a quello comunitario. Infine, nessun diritto era accordato al titolare. In concreto, come ha rilevato la stessa Corte di Giustizia, la disposizione autorizzava «i [suddetti] fornitori a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato»[52].

Questo rappresenta una negligenza del Legislatore, perché la raccolta creava rischi per la riservatezza che nulla aggiungevano alla qualità delle indagini. Difficilmente invero i *providers* si sarebbero onerati di spese improduttive per tutelare la riservatezza; per di più la Direttiva non imponeva alle imprese vincoli e controlli sull'uso delle informazioni, e con questo consentiva loro di vendere le masse di dati o sfruttarle per fini pubblicitari[53].

In ultima analisi, veniva attribuito ai fornitori il potere discrezionale di creare danni sproporzionati rispetto al fine. Tali pregiudizi sarebbero stati verosimilmente prevedibili ed evitabili: era chiaro che le aziende avrebbero agito soltanto in vista di interessi propri e senza attenzione all'equilibrio del sistema giuridico.

La possibilità per le compagnie di comprimere la riservatezza a proprio vantaggio avrebbe avuto un significato peculiare dove gli Stati avessero scelto di restituire ai *providers* i costi della conservazione. In contrasto con l'utilità sociale, i privati avrebbero potuto arricchirsi ingiustificatamente a spese dell'erario, giacché avrebbero tratto profitto dai *databases* senza aver nulla investito sulla raccolta. Si sarebbero dovuti adottare quindi specifici accorgimenti quanto alla determinazione del rimborso; invece la *Data Retention* ha preferito tacere del tutto sul finanziamento, lasciando liberi gli ordinamenti interni[54].

Peraltro, anche in presenza di un indennizzo integrale gli oneri imposti sarebbero stati una barriera insormontabile per l'ingresso delle piccole e medie imprese nel mercato delle comunicazioni. Esse «sarebbero [state] costrett[e] non solo a modificare la tecnica del sistema ma anche ad un costante trattamento di richieste emananti dalle autorità»[55]; pure i danni di immagine avrebbero gravato sui bilanci,

---

[52] *Digital Rights Ireland Ltd c. Ireland*, punto 67

[53] Recentemente nel Regno Unito Google è stata condannata da una Corte d'Appello proprio perché tramite la raccolta dei *cookies* memorizzava dati personali (tale era considerata la cronologia delle pagine visitate) senza il consenso dell'utente, al fine di alienarli ai pubblicitari perché potessero fornire servizi mirati: Court of Appeal – Civil Division, *Google v. Vidal-Hall*, [2015] EWCA Civ 311, 27/3/2015, in *https://www.judiciary.gov.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf*, punti 2, 138. Per una visuale più ampia sul fenomeno: R. BEHAR, *Never Heard Of Acxiom? Chances Are It's Heard Of You. How a little-known Little Rock company – the world's largest processor of consumer data – found itself at the center of a very big national security debate*, in *Fortune Magazine*, 23/2/2004, in *http://archive.fortune.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm*; E. MOROZOV, *The Real Privacy Problem*, in *http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/*.

[54] E. KOSTA – P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Review*, n. 5/2006, vol. 22, anche in *http://www.sciencedirect.com/science/article/pii/S0267364906000689*, p. 377; J. RAUHOFER, *Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union*, in *SCRIPT-ed*, n. 4/2006, Vol. 3, anche in *http://ssrn.com/abstract=2257469*, pp. 336-339.

[55] COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Relazione sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE* (COM(2005)0438 – C6 0293/2005 – 2005/0182(COD)), in *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+WORD+V0//IT*, *Parere della Commissione per l'industria, la ricerca e l'energia*.

perché sarebbe diminuita la fiducia dell'utenza verso le aziende[56]. La distorsione della concorrenza non sarebbe stata uno svantaggio meramente economico. Sul *web* – come nel settore audiovisivo – i monopoli sono un 'male in sé', perché anche in assenza di comportamenti abusivi mettono in pericolo il pluralismo informativo; d'altra parte le concentrazioni nel settore delle comunicazioni fanno alzare i costi e rendono difficile l'accesso a servizi necessari per l'esercizio dei diritti[57].

Vi è da chiedersi se tutti questi danni collaterali apportati dalla delega ai privati sono stati compensati da adeguati benefici. Qui sembra addirittura che l'esternalizzazione sia andata contro le proprie stesse finalità: alterando la competizione, probabilmente ha impedito che il mercato adempisse alla sua promessa di efficienza.

In conclusione, gli obblighi di raccolta configurati dalla *Data Retention* avrebbero causato danni alla riservatezza aggiuntivi rispetto a quelli strettamente necessari allo scopo. Secondo la Corte di Giustizia invece si sarebbero dovuti impedire tali effetti imponendo la conservazione nell'Unione e la predisposizione di misure per la sicurezza dei dati adeguate alla massa di informazioni. La delega di scelte politiche a soggetti non legittimati pure era giuridicamente impraticabile, e per giunta ha creato specifici svantaggi ai diritti fondamentali: essa ha influito sulla concorrenza in un settore sensibile e ha consentito l'utilizzo dei dati a soli scopi privati.

b) La sinergia pubblico-privato nell'analisi dei metadati

Il secondo compito attribuito ai *providers* era quello di trasmettere i dati alle autorità competenti. L'articolo 4 limitava questo dovere a «specifici casi», ma tale unico vincolo probabilmente era più apparente che sostanziale: se nell'esperienza statunitense si sono considerati «rilevanti per un'investigazione» tutte le informazioni in possesso delle compagnie, non si vede perché ciò non potesse avvenire in Europa, dove tra l'altro non era imposto alcun mandato giurisdizionale[58]. In ogni caso, vista la profondità del pregiudizio che interessava il diritto alla riservatezza, ci si sarebbero attese garanzie particolari circa i soggetti legittimati al trattamento, le condizioni, i limiti e i controlli.

---

[56] L. PADILLA, *Four ways the N.S.A. revelations are changing businesses*, in *Guardian Professional*, 9/6/2014, in *http://www.theguardian.com/media-network/media-network-blog/2014/jun/09/edward-snowden-nsa-changing-business*; E. KOSTA – P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Review*, n. 5/2006, vol. 22, anche in *http://www.sciencedirect.com/science/article/pii/S0267364906000689*, p. 379.

[57] M. VILLONE, *Conclusioni. La Costituzione e il "diritto alla tecnologia"*, in G. DE MINICO (a cura di), *Dalla tecnologia ai diritti. Banda larga e servizi di rete*, Jovene, Napoli, 2010, pp. 260-267; G. DE MINICO, *Towards an Internet Bill of Rights*, in corso di pubblicazione in *International Comparative Law Review*, n. 1/2015, § 2: *The Available Alternative: Self-regulations or Binding Rules?*, dove l'Autrice riflette sugli effetti negativi dell'autoregolazione sia sulle libertà economiche che su quelle fondamentali, proponendo un regime inedito di combinazione di fonti.

[58] Si dice infatti che l'analisi di determinati dati è necessaria alla singola investigazione, ma che le informazioni a loro volta possono essere ottenute solo con l'esame indiscriminate di tutte le comunicazioni. Quindi tutti i registri sulle chiamate sarebbero rilevanti per le investigazioni governative: DEPARTMENT OF JUSTICE, *Obama Administration White Paper on N.S.A. Bulk Collection of Telephony Metadata*, 10/8/2013, in *http://publicintelligence.net/doj-bulk-telephony-collection/*, p. 13; J. YOO, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, UC Berkeley Public Law Research Paper No. 2369192, anche in *http://ssrn.com/abstract=2369192*, pp. 8-9. *Contra*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Report on the Telephone Records Program Conducted under Section 215 of the U.S.A. PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 23/1/2014 in *http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf*, p. 61.

Oggi non si può più ritenere che i tabulati siano uno strumento poco invasivo. I metadati sono più che mai eloquenti: i dati di traffico Internet sono in realtà densi di contenuto – basti pensare all'indirizzo delle singole pagine visitate – e le stesse tecnologie della comunicazione sono sempre più presenti nella vita di ognuno. D'altro canto, le indagini automatizzate sono in grado di supportare l'intuito e l'esperienza degli agenti con strumenti inediti: l'incrocio delle relazioni e degli spostamenti di ciascuno rivela molto della sfera personale[59]. Considerati anche questi fattori, la Corte di Giustizia ha mosso precise censure alla *Data Retention*: l'accesso alle informazioni sarebbe stato accettabile solo se confinato alle finalità di sicurezza, e comunque mai senza la supervisione di un'autorità giurisdizionale o indipendente[60].

Ai fini del presente discorso, però, interessa approfondire un profilo che la sentenza *Digital Rights Ireland* non ha isolato, e cioè i metodi di indagine: anche su questo punto la Direttiva non disponeva nulla, e quindi non impediva che il bilanciamento sfuggisse in buona parte al controllo delle istituzioni, con gravi e prevedibili danni per i principi democratici.

Normalmente i sistemi informatici per l'analisi dei dati non vengono prodotti *in house* dallo Stato, bensì acquistati dall'esterno[61]. Anche qui, vengono esternalizzate attività non neutrali: quando si incide sui diritti con decisioni automatizzate, molte scelte politiche sono incorporate nelle tecnologie adoperate, e quindi vengono effettuate in sede di progettazione. Non potrebbe avere altra *ratio* il principio della cd. *privacy by design*, secondo cui è sin dal «momento di determinare i mezzi del trattamento» che «il responsabile del trattamento [...] mette in atto adeguate misure e procedure tecniche e organizzative» di tutela[62].

La constatazione è valida soprattutto per il cd. *data mining*, che è uno strumento particolarmente sofisticato, utile perché permette di elaborare nuove ipotesi investigative anche in mancanza di previ sospetti. Mediante alcune formule statistiche, il sistema individua alcune correlazioni ricorrenti tra i dati, le quali indicano i rapporti, le circostanze e le caratteristiche personali che sono più frequentemente associati a una minaccia o a un evento criminoso[63]; in questo modo, l'agente è in grado di capire quali 'profili' e quali situazioni debbano essere posti sotto ulteriore osservazione. Ad esempio, il meccanismo potrebbe rilevare che i criminali

---

[59] U.S. District & Bankruptcy Courts for the District of Columbia, *Klayman et alii v. Obama et alii,* Civil Action No. 13-0851 (RJL), 16/12/2013, in *http://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf*, pp. 47-55 (*Analysis*, § II(B)(ii)); Court of Appeal – Civil Division, *Google v. Vidal-Hall*, [2015] EWCA Civ 311, 27/3/2015, in *https://www.judiciary.gov.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf*, punti 111-132.

[60] *Digital Rights Ireland Ltd c. Ireland*, punti 61, 62.

[61] WIKILEAKS, *Spy Files 3 Documents: Surveillance Industry Documents*, *https://wikileaks.org/spyfiles3*.

[62] «Al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, il responsabile del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, mette in atto adeguate misure e procedure tecniche e organizzative»: *Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)* (2012/0011 (COD)), 25/1/2012, in *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282012%290011_/com_com%282012%290011_it.pdf*, articolo 23. Lo stesso principio è contenuto nella *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico*, COM/2007/0096, 15/3/2007, in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52007DC0096*, § 3.6.

[63] M. HILDEBRANDT, *Profiling and the Rule of Law*, in *Identity in the Information Society (IDIS)*, n. 1/2008, pp. 58-59; F. BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, in *Boston College Law Review*, 2007, vol. 48, pp. 614-615.

provengono prevalentemente dalla periferia cittadina, e quindi suggerire alla polizia che gli abitanti di quella zona devono essere controllati con speciale attenzione.

Ebbene, l'utilizzo di simili sistemi include almeno due scelte di bilanciamento, che tuttavia erano lasciate 'in bianco' dalla Direttiva.

In primo luogo, il Legislatore comunitario avrebbe dovuto chiarire che il risultato del processo automatizzato non potesse dare luogo a una presunzione neanche relativa di colpevolezza[64]. La mera ricorrenza statistica può giustificare, ad esempio, che nella ricerca del reo si indaghi prima sui quartieri 'a rischio'; non sembra tuttavia che essa possa legittimare la polizia a considerare ciascun abitante un potenziale criminale. Ciò sarebbe infatti contrario alla presunzione di innocenza.

In secondo luogo, la politica avrebbe dovuto dettare delle regole sull'impostazione dell'algoritmo con cui avrebbero lavorato i sistemi, cioè sulla selezione del metodo che il programma avrebbe utilizzato per trarre i risultati dal materiale grezzo. L'esito del *data mining*, anche dove non è assunto come decisivo, dà luogo a una compressione dei diritti, perché il fatto stesso di sottoporre qualcuno a particolare osservazione è un'interferenza con la sua sfera individuale[65]. D'altra parte può capitare, ad esempio, che il procedimento informatico più efficace sia poco controllabile, in quanto basato sulla probabilità più che sulla logica comune[66]; oppure, le formule possono finire per operare discriminazioni che però non sono giustificabili per la Costituzione in vigore[67]. In tutti i casi, pare, la scelta progettuale entra nel merito del bilanciamento tra la sicurezza e una serie di altri valori, e quindi non è neutrale.

Sicché lo Stato non può limitarsi a commissionare la fabbricazione dello strumento più accurato possibile, perché questo potrebbe risultare sproporzionato; né può lasciare 'carta bianca' al produttore, giacché ciò vorrebbe dire affidare delle valutazioni sui principi fondamentali a un soggetto privo di legittimazione elettorale. Tutte queste preoccupazioni erano abbandonate dalla Direttiva alla contrattazione segreta tra il Governo e i privati[68].

Il coinvolgimento delle imprese può creare anche danni collaterali all'*accountability*. Il contatto tra agenti pubblici e dipendenti dell'azienda è tale che a chi guarda dall'esterno diventa «impossibile dire dove finisca l'apparato governativo e dove inizi [la compagnia]»[69]. Tale indistinzione rende ancora meno controllabile un settore – quello della sicurezza nazionale – che di per sé è connotato da scarsa

---

[64] P.M. SHANE, *The Bureaucratic Due Process of Government Watch Lists*, *Ohio State Public Law Working Paper No. 55*, 2006, p. 22.

[65] *Ibidem*, pp. 2-4.

[66] T. ZARSKY, *Transparent Predictions*, in *University of Illinois Law Review*, n. 4/2013, anche in *http://ssrn.com/abstract=2324240*, p. 1517-1520.

[67] F. BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, in *Boston College Law Review*, 2007, vol. 48, p. 637; B. GOOLD, *Privacy, Identity And Security*, in B. GOOLD – L. LAZARUS (a cura di), *Security and Human Rights*, Hart Publishing, 2007, pp. 21-22; D. BIGO – S. CARRERA – N. HERNANZ – J. JEANDESBOZ – J. PARKIN – F. RAGAZZI – A. SCHERRER, *Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law*, CEPS Paper in Liberty and Security in Europe Papers No. 61, 6/11/2013, anche in *http://ssrn.com/abstract=2360473*, p. 31.

[68] N. TZIFAKIS, *Contracting Out to Private Military and Security Companies*, Brussels: Centre for European Studies (CES) Research Paper, luglio 2012, anche in *http://ssrn.com/abstract=2117664*, pp. 34-42.

[69] «It's impossible to tell where the government ends and Lockheed begins»: Danielle Brian, di *Project on Government Oversight*, in T. WEINER, *Lockheed and the Future of Warfare*, in *The New York Times*, 28/11/2004, anche in *http://www.nytimes.com/2004/11/28/business/yourmoney/28lock.html?_r=2&oref=slogin&*. L'osservazione è svolta anche in: R.J. HILLHOUSE, *Outsourcing Intelligence* in *The Nation*, 30/7/2007, anche in *http://www.thenation.com/article/outsourcing-intelligence*.

trasparenza: le autorità possono attribuire ad altri le proprie colpe, o al limite esternalizzare il 'lavoro sporco' in capo a *contractors* che non sono politicamente responsabili[70]. Questo in nome di un'efficienza che per il pubblico è difficile accertare, perché naturalmente nel campo di cui si parla gli appalti non seguono un regime di evidenza pubblica.

D'altra parte anche a livello legislativo, attraverso il *lobbying*, si dà adito a una vera e propria commistione tra autorità e poteri economici. Le *corporations* hanno forza sufficiente per influire nei processi normativi dell'Unione[71], e non si vede perché non dovrebbero usarla per far approvare le leggi sulla sicurezza che alimentano la domanda delle loro merci[72].

Il Giudice comunitario ha statuito che il Legislatore avrebbe dovuto prevedere e impedire gli esiti sproporzionati dell'accesso ai dati: sarebbe stato necessario imporre requisiti, condizioni e controlli indipendenti. Qui sembra opportuno aggiungere che l'esternalizzazione assumeva forme illegittime, perché attribuiva una funzione di indirizzo a soggetti politicamente irresponsabili, che avevano tutto l'interesse a utilizzare la forza pubblica per fini propri. L'*outsourcing* sregolato delle indagini generava autonome preoccupazioni di irragionevolezza. L'assenza di un'idonea supervisione pubblica non solo creava svantaggi per l'*accountability*, ma minava anche il fine stesso dell'esternalizzazione: dove il pubblico non può controllare l'adempimento del contratto, le imprese sono incentivate a non usare la dovuta diligenza.

3.2 Il futuro dell'esternalizzazione dopo la sentenza della Corte di Giustizia *Digital Rights Ireland v. Ireland*

L'attuale scenario sulle intercettazioni a fini di *intelligence* è una materia malleabile: a livello comunitario vi è un vuoto normativo in cui restano validi solo i principi tradotti nella decisione della Corte di Giustizia e alcune norme settoriali[73]. In questo spazio tuttavia si discute poco di come conformarsi alla sentenza, perché dall'estate 2014, dopo la nascita dell'*Islamic State of Iraq and Syria*, sembra più urgente rafforzare la lotta al terrorismo. L'attenzione si è concentrata in particolare – oltre che sulle comunicazioni – sul controllo dei passeggeri nei voli e dei contenuti *online* incitanti all'estremismo[74].

---

[70] S. CHESTERMAN, *'We Can't Spy… If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'*, in *The European Journal of International Law*, n. 5/2008, vol. 19, pp. 1060-1061.

[71] Le grandi imprese hanno mostrato di avere forza contrattuale sufficiente a influire sui processi legislativi: F. ROBINSON, *Copy, Paste, Legislate…*, in *Real Time Brussels*, 11/2/2013, in *http://blogs.wsj.com/brussels/2013/02/11/copy-paste-legislate/*; *New data protection rules at risk, EU watchdog warns*, in *Euractive.com*, 30/5/2013, in *http://www.euractiv.com/infosociety/eu-watchdog-warns-lobbyists-parl-news-528128*.

[72] N. TZIFAKIS, *Contracting Out to Private Military and Security Companies*, Brussels: Centre for European Studies (CES) Research Paper, luglio 2012, anche in *http://ssrn.com/abstract=2117664*, pp. 32-33.

[73] La Direttiva 95/46/CE sulla protezione dei dati non si applica alla sicurezza, mentre la Decisione Quadro 2008/977/GAI del Consiglio si applica solo agli scambi transnazionali di dati: Direttiva 95/46/CE, articolo 3; *Decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale*, in *http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32008F0977&from=IT*, Articolo 1, Considerando 9.

[74] Consiglio dei Ministri della Giustizia e degli Affari Interni dell'Unione Europea, 9 e 10 ottobre 2014: PRESS OFFICE – GENERAL SECRETARIAT OF THE COUNCIL, *Press Release*, 3336th Council meeting Justice and Home

Sul primo punto si auspica la ripresa del progetto di cd. *PNR (Passengers Name Records) Directive*, che ha subito un percorso travagliato e attualmente è in fase di stallo[75]: lo spirito è quello di creare sistema armonizzato per l'acquisizione e lo scambio tra le forze di polizia di quelle «informazioni non verificate fornite dai passeggeri, che vengono raccolt[e] e conservat[e] nei sistemi di prenotazione e di controllo delle partenze dei vettori aerei a fini commerciali»[76].

L'attuale *draft*[77] dovrebbe subire ancora delle modifiche per conformarsi al giudicato dell'aprile 2014: la raccolta dei dati è concepita come totale e indiscriminata[78], e non sarebbe assistita da un mandato. Tuttavia il progetto appare interessante perché in parte restaura la fiducia nel settore pubblico. I dati PNR, infatti, non sarebbero conservati dalle compagnie aeree: i vettori fungerebbero solo da tramite, perché acquisirebbero i dati dai clienti e li trasmetterebbero a un'Unità di

---

Affairs (Luxembourg, 9-10/10/2014), 14044/14, in *http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/145033.pdf*; PRESS OFFICE – GENERAL SECRETARIAT OF THE COUNCIL, *Background note*, 3336th Council meeting Justice and Home Affairs (Luxembourg, 9-10/10/2014), 8/10/2014, in *http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/145004.pdf*; Consiglio dei Ministri dell'Interno, 11 gennaio 2015: PRESS OFFICE – EMBASSY OF FRANCE IN LONDON, *Joint Statement Issued Following a Meeting of the Ministers of the Interior in Paris* (11/1/2015), 21/1/2015, in *http://www.ambafrance-uk.org/Charlie-Hebdo-joint-statement-of*; Riunione informale del Consiglio Europeo, 12 febbraio 2015: EUROPEAN COUNCIL – PRESS OFFICE, *Press Statement by the members of the European Council*, Informal meeting of the Heads of State or Government (Brussels, 12/2/2015), 12/02/2015, in *http://www.consilium.europa.eu/en/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/*; FOREIGN AFFAIRS COUNCIL – PRESS OFFICE, *Council conclusions on counter-terrorism, press release*, 9/2/2015, in *http://www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-counter-terrorism/*.

[75] La proposta risale a due decisioni del 2004, del Consiglio e della Commissione. In seguito all'annullamento di tali atti da parte della Corte di Giustizia, il progetto è stato ripresentato nel 2007 e rimodernato nel 2011 perché è intervenuto il Trattato di Lisbona. Cfr. *Decisione del Consiglio del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (*Passenger Name Record*, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti*, 2004/496/CE, in *http://www.privacy.it/com2004-496.html*; *Decisione della Commissione, del 14 maggio 2004, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti*, C(2004) 1914, in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32004D0535*; Corte di Giustizia dell'Unione Europea – Grande sezione, *Parlamento Europeo c. Consiglio dell'Unione Europea e Commissione delle Comunità Europee*, cause riunite C-317/04 e C-318/04, 30 maggio 2006, in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62004CJ0317*; *Proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) nelle attività di contrasto*, 2007/0237 (CNS), 6/11/2007, in *http://www.garanteprivacy.it/documents/10160/10704/1531454*.

[76] COMMISSIONE EUROPEA, *Relazione alla Proposta di Direttiva del Parlamento Europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi* (2011/0023 (COD)), in *http://www.garanteprivacy.it/c/document_library/get_file?uuid=060163a3-6726-4687-aeaa-7aa331cb9438&groupId=10160*, § 1.

[77] *Proposta di direttiva del Parlamento Europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi* (2011/0023 (COD)), 2/2/2011, in *http://www.garanteprivacy.it/c/document_library/get_file?uuid=060163a3-6726-4687-aeaa-7aa331cb9438&groupId=10160*.

[78] Proposta di direttiva sull'uso dei dati del codice di prenotazione, 2011/0023 (COD), Articolo 6.

informazione sui passeggeri istituita in ciascuno Stato[79]. In fase di analisi il *data mining* è espressamente autorizzato[80], ma con una certa sensibilità sulle implicazioni che potrebbe avere il trattamento automatizzato. Quanto meno, è imposto alle autorità competenti di non utilizzare criteri irragionevolmente discriminatori[81].

Si tratta di timidi accenni, che non eliminerebbero i rapporti di collaborazione e di delega tra *intelligence* e *corporations*. I dati sarebbero pur sempre raccolti dalle compagnie aeree, e quindi la loro accuratezza deriverebbe dalle scelte gestionali delle aziende[82]; in fase di accesso, poi, gli Stati potrebbero continuare ad avvalersi dei *contractors* per l'analisi delle informazioni. Del resto, guardando al più ampio panorama delle misure dibattute, l'affievolimento dell'esternalizzazione pare un'isolata eccezione, più che una nuova regola.

Già a gennaio, è stato messo in discussione il principio sancito nella Direttiva *E-commerce* secondo cui gli *Internet Service Providers* non rispondono dei contenuti pubblicati dagli utenti[83]. Il Consiglio dei Ministri dell'Interno dell'Unione Europea, riunitosi a Parigi, ha manifestato l'intenzione di imporre ai fornitori l'individuazione, segnalazione o rimozione dei materiali che incitano all'odio e al terrore.

La traduzione in diritto positivo di questi progetti dovrà tener conto di almeno due *caveat*. Il primo è che la responsabilità della censura non potrebbe passare dallo Stato alle compagnie[84]. Eppure questo obiettivo è difficile da raggiungere: vista la mole di materiale da esaminare, le imprese dovrebbero progettare un controllo automatizzato, e non sarebbe agevole per le istituzioni intervenire in questo procedimento. Il secondo imperativo è che l'interferenza con i diritti sia posta in connessione con uno specifico fatto di reato: l'espressione del pensiero dovrebbe poter essere repressa solo quando presenta un certo grado di materialità, cioè quando è in grado di attivare un comportamento criminoso[85]. Per la verità, tuttavia, il clima complessivo e il tenore delle dichiarazioni rese non sembra favorevole al rispetto di tali requisiti.

Lo stesso atteggiamento si ritrova anche negli Stati membri, che stanno dettando norme sempre più sbilanciate a favore della sicurezza[86]. In Italia, ad esempio, sono

[79] *Ibidem*, Articolo 9.

[80] *Ibidem*, Considerando 7.

[81] *Ibidem*, Articoli 4, 5.

[82] *Risoluzione del Parlamento europeo del 20 novembre 2008 sulla proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto*, in *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0561+0+DOC+XML+V0//IT*, punto 33.

[83] *Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*, 8/6/2000, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:IT:HTML*, Articolo 14.

[84] E. Hickok, *Intermediary liability and state surveillance*, in Association for Progressive Communications – Humanist Institute for Cooperation with Developing Countries, *Communications surveillance in the digital age*, Global Information Society Watch 2014, in *http://www.giswatch.org/2014-communications-surveillance-digital-age*, p. 46.

[85] Corte costituzionale, sent. 87/1966, in *http://www.giurcost.org/decisioni/1966/0087s-66.html*, punti 3-5; Corte costituzionale, sent. n. 65/1970, in *http://www.giurcost.org/decisioni/1970/0065s-70.html*; Corte costituzionale, sent. 108/1974, in *http://www.giurcost.org/decisioni/1974/0108s-74.html*, punto 4.

[86] G. De Minico, *Le libertà fondamentali in tempo di ordinario terrorismo*, in *Federalismi.it*, n. 10/2015, in *http://www.federalismi.it/ApplOpenFilePDF.cfm?artid=29517&dpath=document&dfile=18052015224734.pdf&content=Le+libert%C3%A0+fondamentali+in+tempo+di+ordinario+terrorismo+-+stato+-+dottrina+-+*, pp. 8-23.

state ridotte le tutele per la riservatezza[87] e sono state emanate misure sul filtraggio dei siti Internet[88]. In alcuni casi, la tendenza si accompagna alla richiesta di soccorso ai privati, che dovrebbero aiutare a superare le difficoltà tecniche. Le autorità di Parigi stanno già programmando dei vertici con gli *over the top* per mettere in atto protocolli in vista della lotta ai messaggi eversivi[89]. Inoltre, proprio in materia di raccolta dei dati, un disegno di Legge del medesimo Stato pianifica di costringere i *providers* a introdurre nelle loro reti sistemi di analisi del traffico[90].

A queste prospettive la Corte di Giustizia ha opposto l'argine del principio di proporzionalità; resta ora da vedere se la legislazione futura recepirà questo giudicato o le tendenze repressive alimentate dalla nascita dell'*Islamic State of Iraq and Syria*. Oggi le aspettative confluiscono nel pacchetto di riforme sulla *privacy* in cantiere dal 2011, che comprende anche una proposta di Direttiva, 2012/0010 (COD)[91], recante la normativa speciale sulla *privacy* in materia di prevenzione e repressione del crimine. Invero, non sembra di poter concentrare molte speranze su questo sforzo innovatore: il *draft* 2012/0010 è quello in fase meno avanzata di approvazione, e comunque dovrebbe essere significativamente modificato perché possa risultare conforme alla sentenza.

La proposta prevede regole più puntuali di quelle contenute nella *Data Retention*, specie sulla finalità del trattamento, sulla sua liceità e sull'esercizio dei diritti da parte dell'interessato[92]; tuttavia alcuni punti che hanno causato l'annullamento della

---

[87] D.L. 7/2015, *Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione*, 18/2/2015, in *http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-02-18;7!vig=*, convertito con L. 43/2015 del 17/4/2015, in *http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-04-17;43*, Articoli 4-*bis*, 7.

[88] *Ibidem*, Articolo 2.

[89] C. LESNES, *Djihadisme en ligne: Cazeneuve invite les géants du Net à plus de vigilance*, in *Le Monde.fr*, 21/2/2015, anche in *http://www.lemonde.fr/politique/article/2015/02/21/djihadisme-en-ligne-cazeneuve-invite-les-geants-du-net-a-plus-de-vigilance_4580897_823448.html#S4CB5uet6eWOEipr.99*; LEMONDE.FR, *Discours de haine sur Internet: ce que prévoit le gouvernement*, in *Le Monde.fr*, 24/2/2015, in *http://www.lemonde.fr/pixels/article/2015/02/24/discours-de-haine-sur-internet-ce-que-prevoit-le-gouvernement_4581660_4408996.html#Zz0PHOoFCklZFjLy.99*. sulle misure ha manifestato la propria perplessità la *Commission Nationale Consultative des Droits de l'Homme*: COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, *Avis sur la lutte contre les discours de haine sur internet*, 12/2/2015, in *http://www.cncdh.fr/sites/default/files/15.02.12_avis_lutte_discours_de_haine_internet_cncdh_0.pdf*, punto 18.

[90] *Projet de loi relatif au renseignement, adopté par l'Assemblée Nationale en première lecture*, texte adopté n° 511, 5/5/2015, in *http://www.assemblee-nationale.fr/14/ta/ta0511.asp*, Articolo 2 del progetto, nuovo art. L. 851-3 del *Code de la Sécurité Intérieure*.

[91] *Proposta di direttiva del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati* (2012/0010 (COD)), 25/1/2012, in *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282012%290010_/com_com%282012%290010_it.pdf*. Accanto ad essa vi è una proposta di Regolamento Generale sulla Protezione dei Dati: *Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)* (2012/0011 (COD)), 25/1/2012, in *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282012%290011_/com_com%282012%290011_it.pdf*.

[92] Proposta di Direttiva 2012/0010 (COD), Articoli 10-17.

2006/24/CE restano intatti nell'attuale testo. Gli obblighi sulla sicurezza dei dati appaiono meglio precisati, anche con riferimento alla *privacy by design*, ma continuano a lasciare spazio a considerazioni economiche: essi si sostanziano nella prescrizione di misure «adeguate», «tenuto conto dell'evoluzione tecnica e dei costi di attuazione»[93]. Inoltre le condizioni del trasferimento sono ammorbidite rispetto a quelle sollecitate dalla Corte: il progetto richiede l'adeguatezza delle tutele fornite nel Paese di destinazione, e non l'equivalenza[94]. Sono infine trascurati nodi cardinali quali lo sfruttamento economico delle informazioni da parte dei *providers* e la raccolta di dati a prescindere da qualsiasi nesso con un fatto di reato, almeno futuro o probabile. Quanto all'accesso, il *draft* prevede che i 'dati sensibili' non possano fondare discriminazioni[95], ma per il resto non detta scopi e requisiti tassativi, né impone controlli indipendenti.

Non da ultimo, è esclusa la «sicurezza nazionale» dal campo applicativo[96]. La vaghezza dell'espressione utilizzata fa sì che l'intero sistema di tutele possa essere vanificato senza troppi sforzi in situazioni di emergenza come quella attuale.

In conclusione, la strada fin qui intrapresa dall'Unione Europea non pare convergere con i principi dettati dalla sentenza *Digital Rights Ireland v. Ireland*, e quindi non resta che constatare come si stia volgendo verso una situazione di sempre maggiore illegittimità. Il paragrafo seguente sarà volto ad esaminare meglio, in concreto, le dinamiche della delega 'in bianco' che il Legislatore comunitario ha conferito e sta conferendo ai privati: si assumerà come caso di studio il Regno Unito, dove la *Data Retention* è stata attuata senza ulteriori vincoli e la privatizzazione ha inciso sulla realizzazione dei fini costituzionali.

4. Le falle dell'*outsourcing* nell'attuazione della *Data Retention*: il caso del Regno Unito

Il Regno Unito ha attuato la *Data Retention* senza aggiungervi limiti a tutela della *privacy*, e invero non è stato neanche l'unico Stato membro che ha agito in tal senso. Sicché in buona parte dei Paesi europei i rischi presagiti dalla Corte di Giustizia si sono mostrati concreti: gli spazi lasciati liberi dal Legislatore hanno portato alla diffusa violazione della riservatezza, perpetrata in vere e proprie zone d'ombra dei controlli democratici.

La Gran Bretagna, come è noto, non ha una Costituzione scritta, ma riconosce comunque la *privacy* come un diritto fondamentale ben radicato nel proprio ordinamento. La CEDU contempla infatti tale garanzia all'articolo 8, ed è pacifico che la Convenzione sia ormai parte del diritto nazionale: nel 1998 lo *Human Rights Act*[97] ne ha recepito il contenuto, dando anche un'efficacia di precedente alle sentenze della Corte Europea dei Diritti Umani[98]. Il sistema è stato consolidato con l'ottemperanza agli obblighi comunitari, quando – in esecuzione della Direttiva

[93] «Tenuto conto dell'evoluzione tecnica e dei costi di attuazione, metta in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme alle disposizioni adottate ai sensi della presente direttiva e assicuri la tutela dei diritti dell'interessato»: *Ibidem*, Articolo 19.

[94] *Ibidem*, Articoli 34-35.

[95] *Ibidem*, Articoli 8-9.

[96] *Ibidem*, Articolo 2.

[97] *Human Rights Act 1998*, *An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes*, 1998 Chapter 42, 9/11/1998, in *http://www.legislation.gov.uk/ukpga/1998/42*.

95/46/CE – il *Data Protection Act 1998*[99] ha consentito il trattamento dei dati personali solo in presenza di specifiche condizioni[100]; anche la giurisprudenza della *House of Lords* ha ritenuto esistente un diritto all'uso corretto e legale dei dati, a prescindere dalla segretezza delle informazioni in questione[101].

La normativa sulle telecomunicazioni non potrebbe che essere colata nello stesso calco: i *Telecommunications (Data Protection and Privacy) Regulations 1999*[102] ammettono la conservazione dei metadati solo se necessaria per la prestazione del servizio[103]. I servizi segreti però hanno premuto sul Governo per chiedere una diversa regolamentazione: essi lamentavano che l'immediata cancellazione delle informazioni personali avrebbe sottratto materia prima alle indagini[104].

Non bastava il fatto che i *Regulations* del 1999 si ritraessero in materia di sicurezza[105], perché sarebbe servita una deroga espressa per dispensare le imprese dall'obbligo di distruggere i dati[106]. Un primo tentativo esperito nel 2001 ha rivelato che le sorti della lotta al terrorismo nel Regno Unito erano ormai inevitabilmente legate alla disciplina sovranazionale. L'*Anti-Terrorism, Crime and Security Act*[107] ha creato un quadro di collaborazione volontaria tra fornitori e Governo[108], ma il timore di sanzioni comunitarie scoraggiava le imprese dall'adesione; sicché l'unica via d'uscita è stata chiedere il consenso dell'Unione alla Direttiva *Data Retention*[109], che infine ha reso obbligatoria l'archiviazione dei metadati.

---

[98] F. Abbondante, *Riservatezza e telecomunicazioni: l'ordinamento anglosassone*, in A. Pace – R. Zaccaria – G. De Minico (a cura di), *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008, pp. 184-187; L. Donohue, *Anglo-American Privacy and Surveillance, in Journal of Criminal Law and Criminology*, Vol. 96, 2006, anche in *http://ssrn.com/abstract=2020411*, p. 1153-1154. Il percorso che ha portato a tale esito è tratteggiato dalla giurisprudenza in: *Ash & Anor v McKennitt & Ors*, [2006] EWCA Civ 1714, England and Wales Court of Appeal – Civil Division, 14/12/2006, in *http://www.bailii.org/ew/cases/EWCA/Civ/2006/1714.html*, punto 8.

[99] *Data Protection Act 1998*, *An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information*, 1998 Chapter 29, 16/7/1998, in *http://www.legislation.gov.uk/ukpga/1998/29/introduction*.

[100] *Data Protection Act 1998*, *Schedule 2*.

[101] House of Lords of Appeal, *Campbell v. MGN Limited*, [2004] UKHL 22, 6/5/2004, in *http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm*, punto 15. Il carattere sensibile della problematica è sottolineato in: M. Hildebrandt, *Profiling and the Rule of Law*, in *Identity in the Information Society (IDIS)*, n. 1/2008, p. 62.

[102] *The Telecommunications (Data Protection and Privacy) Regulations 1999*, Statutory Instrument n. 1999 No. 2093, in *http://www.legislation.gov.uk/uksi/1999/2093/made*.

[103] *Ibidem*, *Section 7*.

[104] National Criminal Intelligence Service, *Looking to the Future. Clarity on Communications Data Retention Law,* Submission to the Home Office for Legislation on Data Retention, 21/8/2000, in *http://cryptome.org/ncis-carnivore.htm*, §§ 3, 6.

[105] *The Telecommunications (Data Protection and Privacy) Regulations 1999*, *Regulations 32* e *33*.

[106] C. Walker – Y. Akdeniz, *Anti-terrorism Laws and Data Retention: War Is Over?*, in *Northern Ireland Legal Quarterly*, n. 2/2003, vol. 54, pp. 162-164); L. Donohue, *Anglo-American Privacy and Surveillance, in Journal of Criminal Law and Criminology*, Vol. 96, 2006, anche in *http://ssrn.com/abstract=2020411*, p. 1181.

[107] *Anti-Terrorism, Crime and Security Act 2001*, *An Act to amend the Terrorism Act 2000; to make further provision about terrorism and security; to provide for the freezing of assets; to make provision about immigration and asylum; to amend or extend the criminal law and powers for preventing crime and enforcing that law; to make provision about the control of pathogens and toxins; to provide for the retention of communications data; to provide for implementation of Title VI of the Treaty on European Union; and for connected purposes*, 2001 Chapter 24, 14/12/2001, in *http://www.legislation.gov.uk/ukpga/2001/24.*

[108] *Anti-terrorism, Crime and Security Act 2001*, *Sections 102(1)-(3), 103*.

I *Data Retention (EC Directive) Regulations* del 2007[110] e del 2009[111] – attuativi della Direttiva – ne hanno riprodotto lo schema: essi hanno imposto la raccolta indiscriminata dei dati senza specificare le garanzie del trattamento e i limiti all'uso da parte delle compagnie[112]. Gli ordini esecutivi del *Secretary of State* non hanno migliorato lo squilibrio, e anzi hanno rammentato ai *providers* che l'informativa al titolare è vietata quando pregiudica le finalità di sicurezza, di polizia e di *intelligence*[113]. Neanche sull'accesso ai dati il recepimento della Direttiva ha guarito le pecche dell'atto comunitario: i *Regulations* ripetono, senza aggiungere altro, che i dati devono essere forniti all'autorità in specifici casi e nei modi stabiliti dal Parlamento[114]. Le fonti primarie, dal canto loro, costruiscono il potere di intrusione come la regola, e la tutela della riservatezza come un'eccezione.

In questo il sistema risente di una secolare tradizione che considera la sicurezza una prerogativa propria della Corona (*Royal Prerogative*), quindi del Governo[115]: i limiti legali e i controlli indipendenti sono stati vissuti dall'ordinamento come una concessione ai ripetuti interventi della Corte Europea dei Diritti dell'Uomo[116], e quindi risultano improntati a un'ottica minimalistica[117]. Ancora adesso il *Regulation of*

---

[109] I. BROWN, *Government Access to Private-Sector Data in the United Kingdom*, in *International Data Privacy Law*, 1/6/2012, in *http://ssrn.com/abstract=1026974*, p. 13.

[110] *The Data Retention (EC Directive) Regulations 2007*, Statutory Instrument 2007 n. 2199, in *http://www.legislation.gov.uk/uksi/2007/2199/contents*.

[111] *The Data Retention (EC Directive) Regulations 2009*, Statutory Instrument 2009 n. 859, in *http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents*.

[112] *The Data Retention (EC Directive) Regulations 2007*, *Regulation 4, 6*; *The Data Retention (EC Directive) Regulations 2009*, *Regulation 4, 6*. La norma è commentata in: C. WALKER, *Data retention in the UK: Pragmatic and proportionate, or a step too far?*, in *Computer Law & Security Review*, n. 4/2009, vol. 25, p. 328.

[113] *Acquisition and Disclosure of Communications Data Code of Practice*, Pursuant to Section 71 of the *Regulation of Investigatory Powers Act 2000*, in *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf*, *Sections 7.4-7.7*.

[114] *The Data Retention (EC Directive) Regulations 2007*, *Regulation 7*; *The Data Retention (EC Directive) Regulations 2009*, *Regulation 7*.

[115] Cfr. G. GROTTANELLI DE' SANTI, voce *Atto politico e atto di governo*, in *Enciclopedia giuridica*, Treccani, Roma, 1988, vol. IV, p. 3; O. GROSS, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, in *Minnesota Public Law Research Paper No. 03-2*, anche in *http://ssrn.com/abstract=370800 or http://dx.doi.org/10.2139/ssrn.370800*, 1102-1104; A.J. MCADAMS, *Internet Surveillance after September 11. Is the United States Becoming Great Britain?*, in *Comparative Politics*, n. 4/2005, vol. 37, pp. 479-498, anche in *http://www.jstor.org/discover/10.2307/20072905?sid=21105519435183&uid=2&uid=4&uid=3738296*, p. 486. Di tale mentalità si trova traccia anche nella giurisprudenza: «Any regulation of so complex a matter as telephone tapping is essentially a matter for Parliament, not the courts» [«qualsiasi regolamentazione di una materia complicata come le intercettazioni telefoniche è essenzialmente una materia per il Parlamento, non per le Corti»]: High Court of Justice – Chancery Division, *Malone v. Commissioner for the Metropolitan Police (no.2)*, [1979] Chancery Division 344 [1979], in *http://www.leeds.ac.uk/law/hamlyn/malone-case.htm*, Ch. 380.

[116] European Court of Human Rights – Court (Plenary), *Case of Malone v. The United Kingdom*, Application no. 8691/79, 2/8/1984, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533*; European Court of Human Rights – Court (Chamber), *Case of Halford v. the United Kingdom*, Application no. 20605/92, 25/6/1997, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58039*; European Court of Human Rights – Third Section, *Case of Khan v. The United Kingdom*, Application no. 35394/97, 12/5/2000, in *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58841*.

[117] F. ABBONDANTE, *Riservatezza e telecomunicazioni: l'ordinamento anglosassone*, in A. PACE – R. ZACCARIA – G. DE MINICO, *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008, pp. 188-194; L. DONOHUE, *Anglo-American Privacy and Surveillance*, in *Journal of Criminal Law*

Investigatory Powers Act (RIPA) *2000*[118] configura l'accesso ai metadati come dominio dell'Esecutivo: un'autorità designata (*designated person*), tra quelle elencate nella Legge[119], può imporre ai *providers* di telefonia e di Internet la consegna dei metadati e i relativi obblighi strumentali[120]. Non è previsto, cioè, un mandato giurisdizionale preventivo.

I diritti dell'interessato ricevono una tutela debole, perché egli può solo ricorrere *ex post* a un Giudice speciale, l'*Investigatory Powers Tribunal*[121]. Peraltro il cittadino può agire solo se viene a sapere della lesione, il che non è affatto scontato dove manca una notifica e comunque è imposto un generale segreto[122]. Il giudizio in ogni caso si svolge davanti a un Tribunale speciale, in cui si deroga alla piena pubblicità del processo e alle norme sul contraddittorio e sull'inutilizzabilità delle prove[123]. Sull'applicazione del RIPA vigila anche l'*Interception of Communications Commissioner*, ma egli svolge un controllo che di fatto è solo collaborativo, perché ha come proprio esito solo la presentazione di un *report* al Primo Ministro[124].

Sarebbe comunque difficile accertare un'illegalità, perché la Legge lascia 'in bianco' numerosi aspetti sostanziali, e presenta pochi contenuti realmente vincolanti per le autorità esecutive. Gli obiettivi che giustificano l'accesso ai dati sono indicati in clausole di grande elasticità, come «sicurezza», «ordine pubblico» o addirittura «interesse al benessere economico dello UK, nella misura in cui sia anche rilevante agli interessi di sicurezza nazionale»[125]. D'altra parte la proporzionalità tra mezzi e fini viene solo enunciata nella *section* 22[126]: la possibilità di comprimere i diritti non è graduata in base ai reati addebitati o alle prove in possesso dell'autorità.

Globalmente, quindi, il quadro legislativo britannico sembra presentare vizi analoghi a quelli della Direttiva 2006/24/CE. Esso predispone mezzi che paiono eccessivi rispetto al fine: il danno alla riservatezza è danno sicuro e vasto, mentre i vantaggi sono incerti. L'elasticità *in peius* della Legge è tale che dal 2000 a oggi le tecniche di sorveglianza hanno potuto rinnovarsi senza sfociare nell'illegalità. L'unica difficoltà è stata quella di tenere il passo con lo sviluppo di Internet, che ha aumentato i volumi delle comunicazioni e talvolta le ha rese più sfuggenti.

Dal 2009 il Regno Unito ha avviato due grandi progetti per l'acquisizione di metadati su vasta scala, con la costruzione dei macro-sistemi *Global Telecoms*

---

and Criminology, Vol. 96, 2006, anche in *http://ssrn.com/abstract=2020411*, pp. 1155-1168.

[118] *Regulation of Investigatory Powers Act 2000*, *An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes*, 28/7/2000, 2000 Chapter 23, in *http://www.legislation.gov.uk/ukpga/2000/23/contents*.

[119] *Regulation of Investigatory Powers Act 2000*, *Section 25(1)*, *(2)*.

[120] *Ibidem*, *Section 22(1)*, *(4)*.

[121] *Ibidem*, *Section 65*.

[122] I. BROWN, *Government Access to Private-Sector Data in the United Kingdom*, in *International Data Privacy Law*, 1/6/2012, in *http://ssrn.com/abstract=1026974*, p. 11.

[123] *The Investigatory Powers Tribunal Rules 2000*, Statutory Instrument 2000 n. 2665, in *http://www.legislation.gov.uk/uksi/2000/2665/made*, *Sections 6, 9, 11*.

[124] *Regulation of Investigatory Powers Act 2000*, *Section 58(2)*.

[125] *Ibidem*, *Section 22(2)*, in particolare *(a)-(d)*.

[126] *Ibidem*, *Section 22(5)*.

Exploitation, per la telefonia, e *Mastering the Internet*, per i *web*[127]. In particolare, con il programma *Tempora*, lo Stato si è accordato segretamente con i *providers* perché questi ultimi installassero nei cavi sottomarini di Internet dei dispositivi che avrebbero deviato tutto il traffico interno e internazionale verso le strutture dei *Government Communications Headquarters* (GCHQ). Con questi mezzi, i servizi segreti riescono a ottenere un flusso di dati stimato pari a quello che si otterrebbe inviando le informazioni contenute in tutti i libri della *British Library* per centonovantadue volte al giorno.

L'impresa è resa possibile anche dal supporto finanziario e logistico degli Stati Uniti[128], prestato secondo un accordo, cd. *Five Eyes*, stretto nel 1946 insieme ad altre tre Nazioni, cioè l'Australia, il Canada, e la Nuova Zelanda. In esecuzione di questo Trattato la *National Security Agency* (NSA) degli USA e i GCHQ britannici operano a stretto contatto: ad esempio, lavorano congiuntamente al programma *PRISM*, con cui si fanno consegnare i dati dagli *Internet Service Providers*, o a *Quantum*[129], che consente loro di introdursi abusivamente nelle reti interne delle compagnie telefoniche e di Internet per acquisire i contenuti non protetti da crittografia. Ciò significa pure che i dati raccolti dal Regno Unito vengono diffusi senza filtri anche presso le autorità d'oltreoceano, che non osservano garanzie equivalenti a quelle previste dall'Unione. Per altri versi, gli Stati Uniti sono famosi per la libertà – e talvolta la leggerezza – con cui esternalizzano la compressione dei diritti fondamentali[130].

Tutto questo non viola il RIPA, ma ne sfrutta le zone d'ombra: recentemente tanto l'*Investigatory Powers Tribunal* quanto l'*Intelligence and Security Committee of Parliament* hanno assolto l'Esecutivo e i *contractors* perché hanno agito in conformità alla fonte primaria. Gli stessi organi di supervisione hanno visto nella Legge la principale responsabile degli aspetti controversi, e infatti ne hanno messo in evidenza i punti critici.

---

[127] Per la documentazione su questi due sistemi si è fatto riferimento essenzialmente a: I. BROWN, *Witness Statement on behalf of the applicants in Big Brother Watch – Open Rights Group – English Pen – dr Constanze Kurz v. United Kingdom*, Application No. 58170/13, European Court Of Human Rights, 27/9/2013, in *https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN_BROWN-FINAL_WITNESS_STATEMENT.pdf*; E. MACASKILL – J. BORGER – N. HOPKINS – N. DAVIES – J. BALL, *Mastering the internet: how GCHQ set out to spy on the world wide web*, in *The Guardian*, 21/6/2013, anche in *http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet*; E. MACASKILL – J. BORGER – N. HOPKINS – N. DAVIES – J. BALL, *Mastering the internet: how GCHQ set out to spy on the world wide web*, in *The Guardian*, 21/6/2013, anche in *http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet*; E. MACASKILL – J. BORGER – N. HOPKINS – N. DAVIES – J. BALL, *The legal loopholes that allow GCHQ to spy on the world*, in *The Guardian*, 21/6/2013, anche in *http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world*; E. MACASKILL – J. BORGER – N. HOPKINS – N. DAVIES – J. BALL, *GCHQ taps fibre-optic cables for secret access to world's communications*, in *The Guardian*, 21/6/2013, anche in *http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*; C. WILLIAMS, *UK.gov to spend £2bn on ISP tracking – Uberdatabase ditched, but IMP is go*, in *The Register*, 27/4/2009, anche in *http://www.theregister.co.uk/2009/04/27/imp_consultation/*; C. WILLIAMS, J*acqui's secret plan to 'Master the Internet'*, in *The Register*, 3/5/2009, anche in *http://www.theregister.co.uk/2009/05/03/gchq_mti/*.

[128] N. HOPKINS – J. BORGER, *Exclusive: NSA pays £100m in secret funding for GCHQ*, in *The Guardian*, 1/8/2013, anche in *http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden*.

[129] SPIEGEL STAFF, *Quantum Spying. GCHQ Used Fake LinkedIn Pages to Target Engineers*, in *Spiegel Online International*, 11/11/2013, in *http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html*.

[130] N. KLEIN, *The shock doctrine: The rise of disaster capitalism*, MacMillan, New York, 2007, trad. it. *Shock Economy. L'ascesa del capitalismo dei disastri*, Rizzoli, Milano, 2012, pp. 323-351.

L'*Intelligence and Security Committee of Parliament* ha sollecitato l'emanazione di un atto parlamentare unitario e accessibile: gli equilibri tra sicurezza e *privacy* devono risultare da un quadro chiaro e completo[131]. L'*Investigatory Powers Tribunal*, invece, ha chiesto maggiore trasparenza: secondo la sentenza le intercettazioni non erano legali prima che fosse adito lo stesso Tribunale, ma lo sono diventate durante il procedimento, in quanto solo allora l'Esecutivo è stato costretto a svelare al pubblico le regole interne[132].

Probabilmente non sarebbero mancati gli strumenti giuridici per condannare la sorveglianza in modo più incisivo. Chi svolge una funzione di interesse generale deve rispondere a titolo di pubblica autorità per le violazioni dei diritti fondamentali contenuti nella CEDU e nella 'Carta di Nizza'. Questo vale anche nella frequente ipotesi in cui l'incaricato è un *contractor* privato, anche e soprattutto se è il Parlamento ad autorizzarlo all'esecuzione del compito.

Una portavoce dei servizi segreti ha confidato a *The Register* che nel sistema *Mastering the Internet* «i GCHQ lavorano con un'ampia gamma di *partners* dal mondo dell'industria per avere un complesso portfolio di progetti tecnici»[133]. Probabilmente, vista la capacità e la velocità di calcolo richieste per elaborare e classificare le informazioni, si ritiene che sia più efficiente e produttivo decentrare i relativi servizi in *outsourcing*: gli *Internet Service Providers* vengono finanziati per occuparsi «non solo di raccogliere e conservare i dati» mentre corrono lungo le reti «ma anche di organizzarli, collegando i dati di terzi ai propri dove hanno caratteristiche in comune»[134].

La scelta di onerare i *providers* è stata presentata come una concessione alle libertà: la necessità di chiedere i dati alle imprese rappresenterebbe un momento di controllo, perché le compagnie possono denunciare gli abusi. La barriera però è più apparente che reale, se il Governo ha comunque piena potestà di accesso alle informazioni. D'altra parte la compagnia coinvolta non è un supervisore affidabile, perché tendenzialmente reagisce all'ordine di consegna solo se teme danni economici. Le aziende fornitrici di reti e servizi non difendono sempre la *privacy*, e anzi di solito la avversano perché impone dei costi[135]; esse hanno iniziato a contestare gli ordini segreti delle autorità solo quando il sistema di sorveglianza è

---

[131] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, *Privacy and Security: A modern and transparent legal framework*, in *https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7craQ0lD9NHPYjy3VH-FiHCDIzBdAdCjP2i9wGoV1OYF-0RK3oLYGfAmw2bmeL3DaM7CBKIDSkt9YA-MlO8MQFtO8GAOj09V2TwMumFrkNUTrB4WkuTkLQeh708NDR0QXv1MLC7_iV666wOe7SN8gfJHEjbV9d6eyUr4zyG6LikS4Et7OVFBfy8wyA7s708rEXf6RLayTgVGv9qRMNlaS5B2G5-H8UiWU0hVod5igtGK3QtFLh91Sqy4IISWnOluDXLSsgV7&attredirects=0*, punti MM, NN, UU.

[132] *Investigatory Powers Tribunal*, *Liberty v. GCHQ*, [2015] UKIPTrib 13 77-H, 6/2/2015, in *http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf*.

[133] «GCHQ works with a broad range of industry partners to deliver a complex portfolio of technical projects»: C. WILLIAMS, J*acqui's secret plan to 'Master the Internet'*, in *The Register*, 3/5/2009, anche in *http://www.theregister.co.uk/2009/05/03/gchq_mti/*.

[134] «Not only to collect and store data but to organise it, matching third party data to their own data where it had features in common»: C. WILLIAMS, *UK.gov to spend £2bn on ISP tracking – Uberdatabase ditched, but IMP is go*, in *The Register*, 27/4/2009, anche in *http://www.theregister.co.uk/2009/04/27/imp_consultation/*.

[135] Si sono già citati i tentativi di *lobbying* nell'UE. Da ultimo, anche i recenti progetti di Obama per tutelare la *privacy* degli studenti nelle scuole subiscono analoghe pressioni: B. HEROLD, *Draft of President Obama's Student-Data-Privacy Bill Raises Questions*, in *Education Week*, 29/1/2015, anche in *http://blogs.edweek.org/edweek/DigitalEducation/2015/01/federal_student-data-privacy_draft_bill.html*.

divenuto di dominio pubblico e lo scandalo rischiava di causare loro danni all'immagine[136].

Emergeva infatti il dubbio che i *providers* collaborassero volontariamente con lo Stato, e tali voci trovavano la conferma dello stesso Snowden e di un importante avvocato della NSA[137]. Le *corporations* affermavano invece di essere state raggirate o costrette[138], e chiedevano limiti, controlli e trasparenza per poter provare al pubblico la loro estraneità alle intrusioni[139]. Mai però sono arrivate a chiedere una tutela sostanziale ed *erga omnes* della riservatezza, che quindi imponesse vincoli anche alle imprese stesse.

Per questo il Legislatore diligente non può confidare sul fatto che il mercato produca da sé garanzie efficaci, come se costituisse una 'mano invisibile' anche contro gli abusi dell'Esecutivo. Anzi, il Parlamento avrebbe potuto ragionevolmente prevedere che il coinvolgimento dei privati avrebbe creato lesioni collaterali: come si è detto nel paragrafo precedente, tale scelta è suscettibile di permettere ulteriori diffusioni dei dati e di rendere più difficili i controlli pubblici. La stessa circostanza che non esistano notizie certe sul ruolo delle imprese spiega bene la problematica: non è chiaro se le *corporations* siano state vittime o complici, ma vi è di certo solo che è stata lesa la *privacy* di chiunque, che i dati sono stati trasferiti in luoghi dove sono scarsamente tutelati, che l'accesso alle informazioni è stato deciso arbitrariamente e segretamente dall'Esecutivo e, infine, che rispetto a tutto questo è quanto meno non agevole l'individuazione dei responsabili.

Per queste ragioni dal presente lavoro di ricerca sembra potersi trarre la conclusione per cui l'*intelligence* ha un esteso nucleo politico che è 'intrinsecamente di governo', e non può essere affidato alle compagnie. Dal punto di vista oggettivo, chiunque decida sulla materia deve rispettare i vincoli dettati dal principio di precauzione e individuati dalla Corte di Giustizia. In caso di violazione, l'ordinamento prevede che il responsabile risponda con i mezzi disponibili per il ricorso contro la pubblica autorità, anche se si tratta di un privato.

---

[136] J. GARSIDE, *Deutsche Telekom to follow Vodafone in revealing surveillance*, in *The Guardian*, 6/6/2014, in *http://www.theguardian.com/world/2014/jun/06/deutsche-telekom-to-also-reveal-surveillance-data*.

[137] J. BALL – J. BORGER – G. GREENWALD, *Revealed: how US and UK spy agencies defeat internet privacy and security*, in *Guardian Weekly*, 6/9/2013, in *http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*; A. POUCHARD, *Microsoft aurait permis l'accès de la N.S.A. à Outlook et Skype*, in *Le Monde.fr*, 12/07/2013, in *http://www.lemonde.fr/technologies/article/2013/07/12/microsoft-aurait-permis-l-acces-de-la-nsa-a-outlook-et-skype_3446801_651865.html*; J. APPELBAUM – L. POITRAS, *Edward Snowden Interview: The N.S.A. and Its Willing Helpers*, in *Spiegel Online International*, 8/7/2013, in *http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html*; S. ACKERMAN, *US tech giants knew of N.S.A. data collection, agency's top lawyer insists*, in *theguardian.com*, 19/3/2014, anche in *http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de*.

[138] B. GELLMAN – L. POITRAS, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, in *Washington Post*, 6/6/2013, *updated* 7/6/2013, anche in *http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html*; J. BALL – J. BORGER – G. GREENWALD, *Revealed: how US and UK spy agencies defeat internet privacy and security*, in *Guardian Weekly*, 6/9/2013, in *http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security*.

[139] AOL – APPLE – GOOGLE – MICROSOFT – FACEBOOK – YAHOO, Lettera alle Camere del Congresso degli U.S.A., 31/10/2013, in *http://9to5mac.com/2013/11/01/apple-and-other-leading-tech-companies-support-usafreedom-act-to-limit-nsa-powers/*; AOL – APPLE – DROPBOX – GOOGLE – LINKEDIN – MICROSOFT – FACEBOOK – TWITTER – YAHOO, *An open letter to Washington*, in *https://www.reformgovernmentsurveillance.com/*.

4.1 Le occasioni mancate dopo l'annullamento della *Data Retention*

Dopo la sentenza *Digital Rights Ireland v. Ireland* non vi è certezza sulle sorti delle normative interne già in vigore alla data della pronuncia. Sembra chiaro invece che il giudicato pone dei paletti a tutte le discipline approvate dopo la sua pubblicazione. Gli Stati possono ancora derogare all'obbligo di immediata distruzione dei dati, perché ciò è consentito dall'articolo 15 della Direttiva 2002/58/CE; tuttavia a tali eccezioni è imposto un limite di proporzionalità, e quest'ultimo deve essere letto secondo i crismi individuati dalla Corte di Giustizia[140].

Invero nel Regno Unito la dialettica con il potere giurisdizionale sembra l'unico motore di un cambiamento virtuoso, ancorché limitato, del sistema. Nell'aprile 2015 l'*Investigatory Powers Tribunal* ha dichiarato illegali le intercettazioni a carico dell'imputato Belhadj in quanto colpivano le conversazioni con il difensore[141]. Il Giudice ha dovuto anche riaffermare le garanzie più basilari del processo[142]: l'Esecutivo infatti adduceva la tenuità della lesione per chiedere al Tribunale di non rivelare al ricorrente che erano stati violati i suoi diritti[143]. La decisione finale ha rigettato questo argomento; inoltre, anche se non ha affermato il principio di legalità nei confronti del Parlamento, ha quanto meno imposto un rinnovamento a livello di fonti secondarie[144].

L'adeguamento dei Codici interni è già stato avviato dallo *Home Office*: la bozza del futuro *Interception of Communications Code of Practice* è attualmente sottoposto a consultazioni. Il *draft* però non vieta le intercettazioni coperte da privilegio legale: esso impone solo che siano presentate specifiche motivazioni, e neanche puntella tale requisito con la previsione di garanzie aggravate[145].

Più in generale, sembra potersi dire che la strada verso il mutamento richiesto dalla Corte di Giustizia non sia stata ancora imboccata.

---

[140] J. RAUHOFER – D. MAC SÍTHIGH, *The Data Retention Directive Never Existed*, University of Edinburgh School of Law Research Paper Series No. 2014/34, anche in in *SCRIPTed-A Journal of Law, Technology and Society*, n. 1/2014, vol. 11, in *http://script-ed.org/?p=1480*, pp. 7-9.

[141] *Investigatory Powers Tribunal*, *Belhadj v. Security Service*, [2015] UKIPTrib 13_132-H, 29/4/2015, in *https://www.judiciary.gov.uk/judgments/investigatory-powers-tribunal-belhadj-and-others-v-security-service-and-others-judgment-and-determination/*

[142] *Ibidem*, punti 16,17.

[143] *Ibidem*, Punto 7(i),(ii).

[144] *Ibidem*, punto 26.

[145] HOME OFFICE, *Draft Interception of Communications Code of Practice. Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000*, february 2015, in *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf*, punto 4.1.

Appena a luglio 2014, il *Data Retention and Investigatory Powers Act*[146] ha riportato in vita la *Data Retention* – cioè i regolamenti interni attuativi – fino a nuovo ordine del *Secretary of State*[147]; esso ha anche consolidato i poteri previsti nel RIPA, e addirittura ne ha espanso la portata territoriale. Oggi la Legge esplicita che gli ordini di consegna possono essere emessi anche verso imprese situate fuori dalla giurisdizione del Regno Unito[148].

Il divario tra le norme britanniche e la sentenza del Giudice comunitario si sta allargando dopo la nascita dell'*Islamic State of Iraq and Syria*. Gli obblighi degli *Internet Service Providers* sono stati ampliati: per effetto del *Counter-Terrorism and Security Act 2015*[149] i fornitori devono anche consentire all'autorità designata di identificare gli utenti[150]. Questo fa parte di un impianto complessivo della riforma, che introduce misure indiscriminate e in alcune ipotesi neanche assistite da controlli indipendenti.

Si cerca in primo luogo di tenere sotto controllo il flusso di persone che entrano ed escono dal Paese. Il Segretario di Stato può vietare a taluni soggetti l'uscita dal territorio nazionale o, con un'autorizzazione giudiziaria, ritirare i passaporti per impedire il rientro ai cittadini sospettati di essere partiti per unirsi al *jihad*[151]. La medesima autorità ha il compito di emanare dei protocolli generali in base ai quali le compagnie aeree, ferroviarie e di navigazione possono di volta in volta ottenere l'autorizzazione per far viaggiare i passeggeri e i membri dell'equipaggio da e verso il Regno Unito[152].

Alle istituzioni che sono più a contatto con i cittadini – come le scuole, le forze di polizia e le unità sanitarie – si attribuisce un generico dovere di «evitare che gli individui siano portati al terrorismo» (*prevent individuals being drawn into terrorism*). La specificazione degli strumenti e dei mezzi con cui tale fine dovrebbe essere perseguito è lasciata alla discrezionalità degli stessi enti, fatta salva la possibilità per il *Secretary of State* di emanare direttive esecutive con uno *Statutory Instrument* approvato dalle due Camere[153]. L'impatto della norma sembra difficilmente contenibile: basti pensare che i docenti – secondo l'Unione Nazionale degli

---

[146] *Data Retention and Investigatory Powers Act 2014*, *An Act to make provision, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data; to amend the grounds for issuing interception warrants, or granting or giving certain authorisations or notices, under Part 1 of the Regulation of Investigatory Powers Act 2000; to make provision about the extra-territorial application of that Part and about the meaning of "telecommunications service" for the purposes of that Act; to make provision about additional reports by the Interception of Communications Commissioner; to make provision about a review of the operation and regulation of investigatory powers; and for connected purposes*, 2014 Chapter 27, 17/7/2014, in *http://www.legislation.gov.uk/ukpga/2014/27/introduction/enacted*.

[147] *Data Retention and Investigatory Powers Act 2014*, *Section 1(1), Section 1(4)(h)*.

[148] *Ibidem*, *Section 4*. La norma è commentata in: N. PANTLIN – M. EVERETT, *New data retention law in the UK*, in N. PANTLIN, *European national news*, in *Computer Law & Security Review*, n. 8/2014, vol. 30, p. 603.

[149] *Counter-Terrorism and Security Act 2015*, *An Act to make provision in relation to terrorism; to make provision about retention of communications data, about information, authority to carry and security in relation to air, sea and rail transport and about reviews by the Special Immigration Appeals Commission against refusals to issue certificates of naturalisation; and for connected purposes*, 2015 Chapter 6, 12/2/2015, in *http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted/data.htm*.

[150] *Counter-Terrorism and Security Act 2015*, *Section 21*.

[151] *Ibidem*, *Sections 1*, *2*.

[152] *Ibidem*, *Section 22*.

[153] *Ibidem*, *Sections 26, 29(1)*.

Insegnanti – sono restii a instaurare dibattiti in classe per timore di dover denunciare i propri studenti per le loro posizioni[154].

Complessivamente, le Leggi emanate dopo l'intervento della Corte di Giustizia continuano a privilegiare il bene sicurezza in modo contrario ai principi di legalità e di precauzione: si accetta un danno sicuro e vasto ai diritti in cambio di un vantaggio dalla consistenza aleatoria. Fatte salve le norme sul ritiro dei passaporti, si prefigura una compressione delle libertà fondamentali non esattamente definita dalla fonte primaria e non preceduta da un mandato giurisdizionale; in particolare, non si prevede quale livello minimo di prova possa supportare i provvedimenti, né si stabilisce che nel *quantum* vi sia una correlazione tra l'invasione della sfera personale e la finalità preventiva.

Nella stessa ottica, i discorsi che enunciano gli intenti futuri attaccano la riservatezza e la libertà di espressione: il rieletto *premier*, ad esempio, aveva dichiarato che se fosse stato confermato alla carica avrebbe tentato di vietare le comunicazioni crittografate[155]. Le sfere che restano segrete al potere sono viste come 'aree oscure', piuttosto che come valori necessari alla democrazia; esse vengono considerate sempre meno in quanto limite giuridico e sempre più come un limite tecnico da oltrepassare. Così si invoca l'intervento dei privati, che dovrebbero fornire le competenze mancanti allo Stato.

Il Direttore dei GCHQ ha affermato che le compagnie dominanti sul *web* sono diventate «la rete di comando e controllo di prima scelta per terroristi e criminali»; quindi ha chiesto loro di svolgere la propria attività in maniera «sostenibile», cioè di collaborare con le forze di sicurezza e di polizia[156]. Gli ha fatto eco il Primo Ministro Cameron, che ha esortato le imprese a mostrarsi all'altezza della loro «responsabilità sociale»[157]. Nello stesso mese, il Presidente del *Parliamentary Intelligence and Security Committee* ha accusato le *corporations* di fornire un «paradiso sicuro» agli attentatori.

Tale narrativa trasmette un'idea contraria ai principi dello Stato di diritto: se la rete è un luogo criminale, gli utenti del *web* si presumono colpevoli, non innocenti. I discorsi suggeriscono anche che i privati possano essere resi responsabili della lotta al crimine; come si è già detto, però, questo è giuridicamente inammissibile, perché il bilanciamento dei valori è un dovere inderogabile degli organi eletti.

Anche a livello interno, dunque, come a livello comunitario, la via per l'attuazione dei principi di legalità e di precauzione pare ancora lontana. Per il momento al cittadino non resta che azionare gli strumenti a sua disposizione, primo tra tutti quello del controllo politico sui propri rappresentanti. Dal punto di vista strettamente

---

[154] PRESS ASSOCIATION, *Teachers 'fear having to report pupils' for expressing views about extremism*, in *The Guardian*, 6/4/2015, anche in *http://www.theguardian.com/education/2015/apr/06/teachers-fear-having-to-report-pupils-for-expressing-views-about-extremism*.

[155] N. WATT – R. MASON – I. TRAYNOR, *David Cameron pledges anti-terror law for internet after Paris attacks*, in *The Guardian*, 12/1/2015, anche in *http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg*.

[156] «They aspire to be neutral conduits of data and to sit outside or above politics. But increasingly their services not only host the material of violent extremism or child exploitation, but are the routes for the facilitation of crime and terrorism. However much they may dislike it, they have become the command-and-control networks of choice for terrorists and criminals»: R. HANNIGAN, *The web is a terrorist's command-and-control network of choice*, in *Financial Times*, 3/11/2014, anche in *http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3JFRumFr6*

[157] V. DODD – E. MACASKILL – P. WINTOUR, *Lee Rigby murder: Facebook could have picked up killer's message – report*, in *The Guardian*, 26/11/2014, anche in *http://www.theguardian.com/uk-news/2014/nov/25/lee-rigby-murder-internet-firm-could-have-picked-up-killers-message-report-says*.

giuridico, il Parlamento può essere chiamato a rispondere delle violazioni in sede di *judicial review*, mentre contro i privati si possono esercitare i ricorsi che il RIPA e le norme comunitarie e CEDU ammettono contro le decisioni d'autorità.

5. Conclusioni

In questa analisi, si è inteso tratteggiare in che misura un ordinamento democratico può ammettere la privatizzazione nella raccolta e analisi dei metadati a fini di sicurezza. Certamente la scelta è confortata da finalità legittime quali l'efficacia, l'efficienza e l'imparzialità della lotta al crimine; qui ci si è chiesti, però, se la strategia è compatibile con l'assetto dei poteri e i diritti fondamentali stabiliti dall'ordinamento dell'Unione Europea. La questione è stata esaminata partendo da un caso di studio con cui anche il Legislatore comunitario sarà costretto a confrontarsi. Si è preso ad esempio il modello avviato con la Direttiva *Data Retention*, approvata nel 2006 mentre si affacciava in Europa il terrorismo di matrice islamica.

Il primo passo è stato la ricostruzione della cornice normativa. È sembrato pacifico che nel sistema giuridico preso come riferimento le deroghe alla riservatezza devono rispettare i principi di legalità e di proporzionalità. Controverso è come tali regole affrontino i problemi nuovi: oggi i dispositivi di prevenzione e repressione agiscono per lo più prima e a prescindere dalla singola minaccia, e richiedono scelte dal complesso contenuto tecnico.

Il principio di precauzione è stato un'utile chiave di lettura, perché disciplina secondo ragionevolezza la decisione di chi intende agire con anticipo, quando il danno è ancora incerto. Tale canone in primo luogo obbliga a tener conto anche dei diritti fondamentali contrapposti alla sicurezza, perché impone per ciascuna opzione una stima di tutti i costi e benefici. Esso specifica parimenti che la tecnica non esaurisce la decisione. La corretta analisi del fatto è un imprescindibile requisito di ragionevolezza, ma dove la scienza non elimina tutti i margini di dubbio è necessaria una scelta discrezionale dell'organo eletto. Questi deve rispettare criteri di proporzionalità e, vista la situazione di parziale ignoranza, deve ponderare anche il fattore probabilistico: a parità di intensità, una lesione certa 'pesa' più di un danno incerto.

I principi di legalità e ragionevolezza non perdono il loro significato: le deroghe ai diritti devono essere disposte dal Legislativo, che deve stabilire condizioni, limiti e controlli secondo necessità e proporzionalità. Spetta poi all'Esecutivo dare attuazione a queste prescrizioni, e quindi scegliere, predisporre e mettere in atto i mezzi concreti. Tutti questi compiti attengono alla funzione di indirizzo, e quindi non possono essere delegati a soggetti politicamente irresponsabili. Ai fini di questo scritto, ciò significa che la raccolta e l'analisi dei dati di traffico non possono essere esternalizzate se e nella misura in cui implicano valutazioni di merito sul bilanciamento dei valori.

Secondo la Corte di Giustizia, la Legge deve imporre almeno che la raccolta sia collegata a un fatto di reato e che i dati siano conservati nel territorio dell'Unione, protetti con misure adeguate e sottoposti al controllo di un'Autorità Indipendente. La stessa fonte deve anche definire finalità, requisiti, condizioni e controlli per l'accesso delle autorità alle informazioni; in particolare, deve imporre un mandato giurisdizionale. All'interno di tale perimetro si apre il legittimo margine discrezionale del Governo e dell'Amministrazione, e solo un'eventuale residua attività materiale, priva però di contenuto politico, può essere lasciata ai privati.

È pur vero che in ambiti così sensibili probabilmente non vi sono aspetti solo pratici, perché qualsiasi dettaglio della raccolta e dell'analisi incide su diritti della massima rilevanza. La stessa tecnica non è necessariamente neutrale: la scelta di un determinato strumento presuppone una scelta di valore a monte, e la progettazione di tale mezzo incorpora tali opzioni.

Per mettere alla prova queste conclusioni si è seguito l'*iter* applicativo della Direttiva *Data Retention*, anche attraverso il suo recepimento nel Regno Unito: in questi due casi le norme sono state tanto carenti da lasciare ai privati decisioni nevralgiche nel bilanciamento. Questo ha dato luogo a esiti lesivi delle libertà inviolabili, perché le imprese non si sono auto-imposte dei costi a tutela della riservatezza e anzi hanno avuto la possibilità di sfruttare esse stesse i dati per ottenere vantaggi economici.

D'altra parte vi sono buone ragioni per dubitare che l'esternalizzazione sia stata uno strumento idoneo ai propri scopi. Probabilmente l'*outsourcing* non ha abbassato i costi, perché non si è rivolto a un mercato concorrenziale: servizi tanto dispendiosi erano alla portata soltanto di poche grandi imprese. Inoltre, in assenza di vincoli e controlli specifici non vi era alcuna garanzia di efficacia e neutralità, perché nulla assicurava che le imprese eseguissero correttamente i loro obblighi e non intrattenessero rapporti di reciproci scambi con le autorità governative.

Tutte queste motivazioni sembrano mostrare che un intervento dello Stato è necessario, e deve seguire i precisi crismi sopra elencati. Tuttavia dopo la pronuncia della Corte di Giustizia nulla si è mosso, e la recrudescenza dei fenomeni terroristici dopo la nascita dell'ISIS ha favorito un approccio repressivo che rema in senso contrario. Se i Trattati europei esigono un cambiamento, il Legislatore interno e quello europeo sono i primi obbligati, e rispondono davanti alla giustizia costituzionale anche per le azioni dei privati: essi devono assicurare le garanzie per le libertà inviolabili, e non possono liberarsi di tale responsabilità mediante una delega illegittima.

Questa strada è ricca di incognite, ma il cittadino può comunque ottenere soddisfazione rivolgendosi nel singolo caso a un secondo obbligato, cioè chi materialmente compie la violazione. Il rispetto dei diritti fondamentali può essere preteso contro chiunque; i privati che esercitano una funzione di interesse generale non sono immuni, ma, anzi, sono sottoposti agli stessi vincoli, principi e controlli pubblicistici che graverebbero sul soggetto statale.

Queste sono le conclusioni che è sembrato di poter trarre dall'approfondimento svolto. Ci si è avventurati su questo delicato terreno perché la domanda è sembrata ineludibile; non si ha però altra pretesa che quella di porre un problema e contribuire per quanto possibile alla sua evoluzione.

** Laureata in Giurisprudenza presso l'Università degli Studi di Napoli Federico II.