Costituzionalismo.it

Fascicolo 2 | 2017
MEDIAZIONE POLITICA E COMPROMESSO PARLAMENTARE

Data retention e diritti della persona

di LUCIA SCAFFARDI

Costituzionalismo.it

DATA RETENTION E DIRITTI DELLA PERSONA

di *Lucia Scaffardi*
Professoressa associata di Diritto pubblico comparato
Università degli Studi di Parma

ABSTRACT

ITA

Come è possibile tenere in equilibrio esigenze securitarie collettive e privacy individuale in materia di mantenimento dei dati relativi alle comunicazioni elettroniche? Partendo dal quadro normativo europeo e con la successiva analisi dei *leading case*s *Digital Rights Ireland* e *Tele2 Sverige/Watson*, che hanno segnato una svolta sul fronte della *Data retention*, il contributo affronta l'analisi delle legislazioni di Regno Unito, Svizzera e Italia, alla ricerca di una soluzione a questo non semplice e delicato interrogativo.

EN

How can we balance collective security issues and privacy in the realm of electronic communication data retention? Starting from the European normative framework and with the subsequent analysis of the leading cases Digital Rights Ireland e Tele2 Sverige/Watson, which marked a turning point on the matter of data retention, this paper analyses the legislations of the United Kingdom, Switzerland and Italy, searching for an answer to this delicate and intricate question.

DATA RETENTION E DIRITTI DELLA PERSONA

di *Lucia Scaffardi*

SOMMARIO: *1. Introduzione; 2. Il diritto alla protezione dei dati personali e la riservatezza in Europa: cenni; 3. Il caso* Digital Rights Ireland*: la svolta sulla* Data retention*; 4. L'*Investigatory Powers Act *2016 e la sentenza Tele2 Sverige/Watson; 5. E gli altri Paesi stanno a guardare? I casi della Svizzera e dell'Italia; 6. Il precario equilibrio tra prevalenti ragioni securitarie e difficili scelte legislative.*

1. Introduzione

«Se gli uomini fossero angeli, non occorrerebbe alcun governo. Se fossero gli angeli a governare gli uomini, ogni controllo esterno o interno sul governo diverrebbe superfluo. Ma nell'organizzare un governo di uomini che dovranno reggere altri uomini, qui sorge la grande difficoltà: prima si dovrà mettere il governo in grado di controllare i propri governati, e quindi obbligarlo ad autocontrollarsi»[1]. Queste mirabili righe, tratte dal *The Federalist*, hanno ispirato l'avvocato generale Saugmandsgaard nelle conclusioni[2] della recente causa *Tele2 Sverige-Watson*[3] e riassumono quanto mai lucidamente un complesso problema che le Corti europee (e nazionali) si sono trovate ad affrontare negli ultimi anni. Ovvero, fino a che punto i Parlamenti possono approvare normative sulla *Data retention* in tempi di "ordinario terro-

* Il presente lavoro costituisce la completa rielaborazione di una relazione presentata al *II° Observatorio Internacional de Derechos Humano* dal titolo "*Los derechos humanos en situaciones de crisis*" organizzata dall'Accademia Interamericana de Derechos Humanos (AIDH) di Saltillo (Coauhila), che ha avuto luogo presso l'Università degli Studi di Siena il 27 e 28 ottobre 2016, curato dai Professori Luis Efrén Ríos Vega, Tania Groppi e Irene Spigno.

[1] A. HAMILTON O J. MADISON, *Il Federalista n. 51*, in A. HAMILTON, J. JAY, J. MADISON, *The Federalist*, 1787, edizione italiana: Bologna, Il Mulino, 1997, p. 458.

[2] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe, 19 luglio 2016, consultabile at *www.curia.europa.eu*.

[3] Corte di giustizia UE, 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.

rismo"[4], per permettere "al governo di controllare i governati", ma contemporaneamente obbligare il governo a controllare se stesso e cioè fare in modo che l'attività scaturente da tali controlli non esondi la necessaria operatività per quanto attiene la conservazione e l'accesso ai dati, così da non ledere aprioristicamente il diritto alla privacy dei cittadini garantendone al tempo stesso la sicurezza?

In altri termini, quali sono gli obblighi imposti dai Parlamenti (composti di uomini e non sempre di angeli) ai fornitori di comunicazioni elettroniche per rendere conoscibili – per un periodo di tempo definito – determinati dati di traffico nonché l'ubicazione degli utenti stessi che questi dati generano? E ancora, quali sono i limiti normativi di utilizzo di questi metadati?

La Corte di giustizia ha cercato di tracciare una strada maestra che tentasse di rispondere a tale intricato quesito nel 2014, anno in cui, con la sentenza *Digital Rights Ireland*[5], ha dichiarato invalida la Direttiva 2006/24/EC sulla *Data retention* (cd Direttiva Frattini), la quale prevedeva un obbligo indiscriminato di mantenimento di dati per i *providers* di comunicazione elettronica. La Corte di giustizia ha in questo modo affermato come la conservazione dei dati per fini legati alla lotta al terrorismo e alla protezione dell'ordine pubblico previsto nella Direttiva fosse eccessivo e non proporzionato al fine che si intendeva raggiungere, vista anche l'indeterminatezza delle previsioni che si riferivano alla raccolta dei dati. A questo *leading case* va oggi ad aggiungersi un nuovo, fondamentale momento. Infatti, con la sentenza del 21 dicembre 2016 *Tele2 Sverige/Watson*, sono state apportate ulteriori indicazioni in materia, spostando l'attenzione sul tema dal piano legislativo europeo a quello nazionale e determinando così una complessiva lettura della questione in senso garantistico. Il tema, d'altra parte, continua a manifestarsi in tutta la sua problematicità, riscontrabile oggi nell'iter di approvazione di alcune specifiche legislazioni nazionali di cui si tratterà nella parte finale di questo lavoro per

[4] Per una lettura comparata di testi recenti che si interrogano sulle misure adottate in Europa ed America in tempi di terrorismo si consultino: L. MAYALI, J. YOO, *A Comparative Examination of Counter-Terrorism Law and Policy*, in *UC Berkeley Public Law Research*, Paper No. 2949078/2016; G. DE MINICO, *Costituzione emergenza e terrorismo*, Napoli, Iovene, 2016.

[5] Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a.*

cercare di comprendere quale (e se vi) sia un nuovo punto di equilibrio tra privacy digitale e ragioni securitarie[6].

2. Il diritto alla protezione dei dati personali e la riservatezza in Europa: cenni

Prima di affrontare l'analisi delle sentenze appena richiamate, pare utile una breve ricostruzione del diritto alla protezione dei dati personali e alla riservatezza in Europa. Nel diritto comunitario, infatti, essa ha ricevuto puntuale disciplina fin dal 1995, con la Direttiva 95/46/CE, tesa appunto a tutelare le persone fisiche riguardo al trattamento dei dati personali. Con la Direttiva 2002/58/CE è stata ampliata la tutela della protezione dei dati anche al settore delle comunicazioni elettroniche, ma il vero punto di svolta in tema di conservazione dei dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica si è registrato con la Direttiva 2006/24/CE. Già da diverso tempo si osservava, infatti, come tali dati costituissero «uno strumento particolarmente importante e valido nella prevenzione, indagine, accertamento e perseguimento dei reati, in particolare della criminalità organizzata»[7]. Tuttavia, solo a seguito degli attacchi terroristici di Madrid (2004) e di Londra (2005), si comprese appieno la portata e l'importanza della conoscenza e dell'acquisizione, per periodi significativi, di questi dati[8]. La Direttiva 2006/24/CE[9] diveniva

[6] Fra i più recenti contributi che si occupano di questo tema si vedano gli interessanti lavori di M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, n. 23/2016 e V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *Federalismi.it*, n. 15/2017.

[7] Conclusioni del Consiglio "Giustizia e affari interni" del 19 dicembre 2002.

[8] Negli Stati Uniti questa esigenza, che si era palesata già dopo gli attacchi alle Torri gemelle, aveva prodotto una legislazione fin dal 2001 assai permissiva relativamente al possibile mantenimento di dati di traffico (*Patriot Act 2001*) attraverso l'utilizzo di programmi come ad esempio *Echelon*. Questa legge è stata oggetto di forti critiche in quanto incidente sulle stesse garanzie costituzionali. Sul punto si leggano: M. F. DOWLEY, *Government Surveillance Powers Under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, in *Suffolk University Law Rev.*, 2002, p. 165; K. J. LAWNER, *Post-Sept. 11th International Surveillance Activity: A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe*, in *Pace International Law Rev.*, 2002, p. 435; L. T. LEE, *The USA Patriot*

dunque espressione concreta di questa necessità e del come essa potesse essere raggiunta:

> «Data l'importanza dei dati relativi al traffico e dei dati relativi all'ubicazione per l'indagine, l'accertamento e il perseguimento dei reati, come dimostrato da lavori di ricerca e dall'esperienza pratica di diversi Stati membri, è necessario garantire a livello europeo la conservazione, per un certo periodo di tempo, alle condizioni previste dalla presente Direttiva, dei dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione» [10].

Fra le diverse previsioni, questa Direttiva introduceva un obbligo per i fornitori di servizi di comunicazioni elettroniche di conservare certi dati e di garantire che essi fossero disponibili a fini di indagine, accertamento e perseguimento di reati gravi quali definiti da ciascuno Stato membro nella propria legislazione nazionale. Il fine generale di tale normativa era rappresentato dall'intento di poter giungere ad un'armonizzazione delle diverse legislazioni nazionali europee in tema di conservazione di dati, così da rendere efficaci questi strumenti non solo sul piano nazionale, ma anche su quello internazionale, di fronte alla possibilità virtuosa di "scambi" transfrontalieri di informazioni.

Per completare la ricostruzione del quadro normativo europeo, vanno accennate alcune prospettive *de iure condendo*: nel gennaio

---

Act and Telecommunications: Privacy Under Attack, in *Rutgers Computer & Technology Law Journal*, 2003, p. 371. Per una lettura in combinato disposto fra norme europee e quelle americane si veda: F. BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Mining*, in *Boston College Law Rev.*, 2007, p. 614. Sul tema nella vasta dottrina anche in lingua italiana si vedano T. FROSINI, C. BASSU, *La libertà personale nell'emergenza costituzionale*, in A. DI GIOVINE, *Democrazie protette e protezione della democrazia* (a cura), Torino, Giappichelli, 2005, 75 ss.; T. FROSINI, *Lo stato di diritto si è fermato a Guantanamo*, in *DPCE*, 4/2005, 1645 ss.; ma anche più di recente C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, Giappichelli, 2010 a cui si rinvia anche per ulteriore bibliografia.

[9] 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 *GUUE L* 105 del 13 aprile 2006, p. 54.

[10] Considerando 11 della Direttiva 2006/24/CE, cit., p. 55.

2017 è stata avanzata dalla Commissione una *Proposta di Regolamento relativa al rispetto alla vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche*, che andrebbe ad abrogare la vigente Direttiva, già citata, 2002/58/CE. Al momento la proposta si trova in fase di discussione presso il Consiglio europeo e in Parlamento è stata nominata quale relatrice Marju Lauristin della Commissione Libertà Civili, Giustizia e Affari Interni (LIBE); quest'ultima commissione voterà, secondo lo scadenziario fissato, in ottobre 2017[11]. Va sottolineato come tale proposta miri ad aggiornare, alla luce dei più recenti avanzamenti in materia tecnologica, la normativa sulla riservatezza nel campo delle comunicazioni elettroniche, allo scopo di garantire, da una parte, un più elevato livello di tutela della privacy, armonizzato in tutta l'Unione europea e, dall'altro, nuove opportunità di innovazione alle imprese[12]. Inoltre, tra gli scopi della proposta vi è quello di creare un sistema normativo solido ed aggiornato, in linea con il recente Regolamento Generale dell'UE sulla protezione dei dati[13].

[11] Per ulteriori informazioni riguardo lo stato di avanzamento della proposta, si legga *Relazione del Consiglio sull'avanzamento dei lavori*, aggiornata al 19 maggio 2017, disponibile at ***www.interlex.it***.

[12] Sulle finalità e gli obiettivi perseguiti dalla proposta in esame, si veda il *Press Release Database* della Commissione europea, all'indirizzo ***www.europa.eu***.

[13] Non a caso, il termine assegnato dalla Commissione per la conclusione dell'iter legislativo è il 2018, anno in cui entreranno in vigore le nuove disposizioni in tema di protezione dei dati. Si fa qui riferimento al pacchetto di riforme sulla protezione dei dati composto dal Regolamento 2016/679, cosiddetto GDPR (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation), O.J. L 119/1 (2016)) e dalla Direttiva 2016/680 (Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J. L 119/89 (2016)) che diventerà operativo, appunto, dal 2018 (il Regolamento sarà applicabile a decorrere dal 25 maggio 2018, mentre la Direttiva dovrà essere recepita a livello nazionale entro il 6 maggio 2018). Su questo fondamentale Regolamento si consulti: L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy Europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016 e F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al Nuovo Regolamento europeo*, Torino, Giappichelli,2016.

3. Il caso *Digital Rights Ireland*: la svolta sulla *Data retention*

La sentenza *Digital Rights Ireland*[14] attiene, come cennato nella parte introduttiva di questo lavoro, la validità della Direttiva 2006/24, relativamente alla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico, con esclusione però del contenuto delle comunicazioni.

La decisione riunisce due distinte richieste pregiudiziali. La prima era proveniente dall'*High Court* irlandese, nell'ambito di una controversia che vedeva la *Digital Rights Ireland* contestare la legittimità di misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche e, in particolare, chiedeva al giudice del rinvio di dichiarare la nullità della Direttiva 2006/24 e della conseguente normativa di recepimento irlandese[15]. La *High Court* aveva sottoposto alla Corte di giustizia la questione pregiudiziale, interrogandosi se la limitazione dei diritti alla protezione dei dati personali e alla riservatezza del ricorrente fossero compatibili o meno con il Trattato in quanto non proporzionati, non necessari e/o non adeguati agli obiettivi legittimi perseguiti (garantire la disponibilità di determinati dati a fini di indagine, accertamento e perseguimento di reati gravi).

La seconda richiesta, proveniente dal *Verfassungsgerichtshof* austriaco sulla base dei ricorsi in materia costituzionale proposti dal *Land* della Carinzia e da oltre 11.000 cittadini, aveva ad oggetto la compatibilità della legge di recepimento della Direttiva 2006/24 con la Costituzione austriaca. In particolare, il giudice si interrogava sulla Direttiva «in quanto permette di immagazzinare una massa di dati relativi ad un numero illimitato di persone per un lungo tempo. La conservazione dei dati riguarderebbe quasi esclusivamente persone il cui comportamento non giustifica affatto la conservazione dei dati che le

[14] Per una lettura commentata a questa importante sentenza si consultino: S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Democrazia e Sicurezza*, n. 3/2014; M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione Europea da parte della Corte di giustizia UE: Prospettive ed evoluzioni future del sistema europeo di* Data Retention, in *Il Diritto dell'Unione Europea*, Anno XIX, fasc. 4, 2014, pp. 803 ss.; C. M. CASCIONE, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della corte di giustizia e gli echi del datagate*, in *Nuova Giur. Civ.*, 11/2014, p. 11039.

[15] Criminal Justice (Terrorist Offences) Act 2005, no. 2/2005.

riguardano. Tali persone sarebbero esposte ad un rischio elevato di vedere le autorità ricercare i loro dati, venire a conoscenza del relativo contenuto, informarsi sulla loro vita privata e utilizzare tali dati per molteplici fini, tenuto conto, segnatamente, del numero incalcolabile di persone che hanno accesso ai dati per un periodo di almeno sei mesi». Dunque, secondo il giudice del rinvio, vi sarebbero stati dubbi, da un lato circa il fatto che la Direttiva fosse idonea al raggiungimento degli obiettivi da essa perseguiti e, dall'altro, riguardo la proporzionalità dell'ingerenza nei diritti fondamentali interessati.

Seguendo l'iter logico-argomentativo della Corte, possiamo individuare tre momenti attraverso cui si è sviluppato il *reasoning*: 1. la rilevanza degli artt. 7 (Rispetto della vita privata) e 8 (Protezione dei dati di carattere personale) della Carta UE per ciò che attiene la questione di validità della Direttiva; 2. l'esistenza di "ingerenze" sui diritti appena richiamati e, 3., la legittimità di queste "ingerenze" e della loro eventuale giustificabilità, con conseguente valutazione della correttezza del bilanciamento dei valori in gioco.

Quanto al primo aspetto, è opportuno specificare come la sentenza, pur evocando anche l'articolo 11 della Carta relativo alla libertà d'espressione[16] , non affronta in realtà tale questione di validità, dal momento che l'analisi svolta sulla base degli artt. 7 e 8 della Carta è stata ritenuta di per sé sufficiente ai fini dell'accertamento dell'invalidità. Viene da subito rilevato come l'obbligo di raccolta di determinati dati attinenti le telecomunicazioni[17] mostri una serie di

[16] In particolare si vedano i par. 25 e 28 della sentenza in commento.

[17] Così come veniva previsto dagli articoli 3 e 5 della Direttiva: art. 3 inerente l'obbligo di conservazione dei dati afferma « 1. In deroga agli articoli 5, 6 e 9della direttiva 2002/58/CE, gli Stati membri adottano misure per garantire che i dati di cui all'articolo 5 della presente direttiva, qualora siano generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati, da fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione nell'ambito della loro giurisdizione, siano conservati conformemente alle disposizioni della presente direttiva. 2. L'obbligo di conservazione stabilito al paragrafo 1 comprende la conservazione dei dati specificati all'articolo 5 relativi ai tentativi di chiamata non riusciti dove tali dati vengono generati o trattati e immagazzinati (per quanto riguarda i dati telefonici) oppure trasmessi (per quanto riguarda i dati Internet) da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione nell'ambito della giurisdizione dello Stato membro interessato nel processo di fornire i servizi di comunicazione interessati. La presente direttiva non richiede la conservazione dei dati per quanto riguarda le chiamate non collegate»; l'art. 5, in tema di categorie di dati da conservare, stabilisce « 1. Gli Stati membri provvedono affinché in applicazione della presente

importanti problematiche che incidono sul diritto alla vita privata e su quello alla protezione dei dati, così come sanciti dagli articoli 7 e 8 della Carta UE. Queste considerazioni vengono messe in risalto attra-

direttiva siano conservate le seguenti categorie di dati: a) i dati necessari per rintracciare e identificare la fonte di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero telefonico chiamante; ii) nome e indirizzo dell'abbonato o dell'utente registrato; 2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet: i) identificativo/i dell'utente; ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica; iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i; 13.4.2006 IT Gazzetta ufficiale dell'Unione europea L 105/57 2) per la posta elettronica su Internet e la telefonia via Internet: i) identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione; 2) per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet: i) data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato; ii) data e ora del log-in e del log-off del servizio di posta elettronica su Internet o del servizio di telefonia via Internet sulla base di un determinato fuso orario; d) i dati necessari per determinare il tipo di comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato; 2) per la posta elettronica Internet e la telefonia Internet: il servizio Internet utilizzato; e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature: 1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati; 2) per la telefonia mobile: i) numeri telefonici chiamanti e chiamati; ii) International Mobile Subscriber Identity (IMSI) del chiamante; iii) International Mobile Equipment Identity (IMEI) del chiamante; iv) l'IMSI del chiamato; v) l'IMEI del chiamato; vi) nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione; 3) per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet: i) numero telefonico chiamante per l'accesso commutato (dial-up access); ii) digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione; f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: 1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione; 2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni. 2. A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione».

verso un'analisi puntuale dei dati sottoposti alla conservazione, secondo quanto previsto dalla Direttiva, che portano la Corte ad affermare come tale tipo di raccolta arrivi a coprire «le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati»[18]. Da qui, «È giocoforza constatare che l'ingerenza che la Direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta si rivela essere (…) di vasta portata e va considerata particolarmente grave»[19].

Stabilita dunque la rilevanza primaria degli articoli 7 e 8 della Carta, la Corte si è chiesta se vi fosse una giustificazione possibile per l'ingerenza nei diritti garantiti. Al proposito, i Giudici hanno rilevato come il sistema di *Data retention* previsto nella Direttiva debba essere letto alla luce dell'art. 52 par. 1 della Carta[20], che prevede come siano possibili eventuali limitazioni all'esercizio dei diritti e delle libertà, ma queste debbano essere previste per legge ed in modo che venga rispettato il contenuto essenziale dei diritti, nel rispetto del principio di proporzionalità[21] e necessità. Relativamente al contenuto essenziale del diritto alla riservatezza, la Corte sostiene che questo non sia stato intaccato in quanto i temi delle comunicazioni sono esclusi dalla conservazione. Tuttavia, il punto mostra un elemento di contraddittorietà nello sviluppo argomentativo[22]. Infatti, non si può affermare come si

[18] Paragrafo 27.

[19] Paragrafo 37.

[20] L'articolo nel suo paragrafo 1 così dispone: «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà».

[21] Sul cosiddetto test di proporzionalità applicabile nel giudizio ai diritti si vedano i fondamentali contributi di R. ALEXY, *Teoria dei diritti fondamentali*, Bologna, Il Mulino, 2012 e A. BARAK, *Proportionality*, Cambridge, Cambridge University Press, 2012.

[22] Si legga al proposito quanto affermato da Nino, il quale sostiene appunto come la Corte «avrebbe potuto precisare meglio entro quali limiti e a quali condizioni un'ingerenza qualificata come grave non sia in grado di incidere sul contenuto essenziale delle comunicazioni, non limitandosi a considerare semplicisticamente che l'esclusione del contenuto delle comunicazioni è di per sé tale da non pregiudicare il contenuto essenziale dei diritti tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali. Ciò è tanto più vero se si considera che precedentemente la Corte ha messo in rilievo che anche la sola conservazione dei dati, senza che ne sia raccolto il contenuto, è in grado di rilevare le abitudini di vita dei soggetti i cui dati siano sottoposti a sorveglianza, incidendo in maniera significativa

stia trattando di «intrusione grave» alla riservatezza, come viene fatto successivamente e più precisamente in sede di valutazione della proporzionalità dell'ingerenza, perché la Direttiva non prevede garanzie atte a proteggere i dati da abusi e da accessi illeciti[23], senza arrivare a sancire che la Direttiva stessa è illegittima quanto «al rispetto del contenuto essenziale del diritto alla riservatezza»[24].

Sorvolando su questo aspetto che comunque si ritiene particolarmente rilevante, la Corte si interroga invece se l'ingerenza su tali diritti risponda a finalità di interesse generale e sia strettamente necessaria. Dal momento che l'obiettivo della Direttiva è quello della lotta al terrorismo e alla criminalità organizzata, la Corte ritiene che questi siano obiettivi di interesse generale dell'Unione, dato che le raccolte di dati rappresentano uno strumento particolarmente utile nella prevenzione e nella lotta a questi reati. Tuttavia, per quanto questo obiettivo sia di fondamentale importanza «non può di per sé giustificare il fatto che una misura di conservazione, come quella istituita dalla Direttiva 2006/24, sia considerata necessaria ai fini della suddetta lotta»[25]. Quello allora su cui si deve interrogare la Corte è il *quomodo* attraverso cui viene ad essere sviluppata la raccolta e se esso sia proporzionale rispetto al fine che si prefigge di raggiungere la Direttiva stessa.

Al proposito, la Corte introduce un interessante punto laddove, in analogia con quanto previsto dall'articolo 8 della CEDU, decide di citare la sentenza Marper[26]. La Corte EDU con questo pronunciamento era intervenuta per la prima volta sullo spinoso problema dell'utilizzo, del mantenimento e della distruzione dei campioni di DNA e delle

---

sull'esercizio dei loro diritti. Inoltre, circa l'idoneità delle disposizioni della direttiva a creare le condizioni per l'adozione di adeguate misure tecniche ed organizzative a tutela dei dati oggetto di sorveglianza, sarebbe stata necessaria un'analisi più precisa di questa qualità, anche e soprattutto alla luce della circostanza che, in sede di valutazione della proporzionalità dell'ingerenza, la Corte è poi giunta — come vedremo — a mettere in rilievo che la direttiva stessa non contiene garanzie sufficienti, che assicurino una effettiva protezione dei dati contro i rischi di abuso ed eventuali accessi ed usi illeciti di suddetti dati». M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione Europea da parte della Corte di giustizia UE: Prospettive ed evoluzioni future del sistema europeo di* Data Retention, Giuffrè, Milano, op. cit., p. 821.

[23] Vedi al proposito i paragrafi 61 e 62.

[24] G. DE MINICO, *Costituzione emergenza e terrorismo*, op. cit., p.221.

[25] Paragrafo 51.

[26] EUROPEAN COURT OF HUMAN RIGHTS, *S. and Marper v. United Kingdom decision*, Grand Chamber, *Application* n. 30562/04 and 30566/04, Judgment 4 December 2008.

impronte digitali[27]. Il giudice di Strasburgo, pur riconoscendo la positività di questi mezzi di indagine, sottolineava come l'utilizzo e il mantenimento degli stessi, in quanto incidenti sulla vita privata e sulla privacy individuale, debbano essere attentamente valutati e vi debba essere un bilanciamento che non sia foriero di un possibile uso indiscriminato di questi mezzi di indagine[28], arrivando a dichiarare l'interferenza delle norme sottoposte alla sua valutazione con il diritto al rispetto della vita privata delle persone interessate e questo proprio a causa della natura indiscriminata della conservazione dei campioni cellulari e dei relativi profili del DNA in ragione della natura e della qualità delle informazioni personali contenuti in questi dati.

La Corte di giustizia, con questa citazione in analogia, ha in certo qual modo tratteggiato una linea ideale e complessiva sulla «*blanket data retention*», sia essa di derivazione da computer, digitale o di DNA, tutte raccolte di dati che in diverso modo vanno ad incidere sulla protezione dei dati personali sotto il profilo del diritto al rispetto della vita privata. Ne deriva come sia necessario valutare la gravità di questa incidenza attraverso uno scrutinio assai stretto.

Questo scrutinio, nel caso in commento, ha portato la Corte a ritenere che non sia giustificabile una tale raccolta di dati – per quanto importante sia la lotta alla criminalità – perché andrebbe ad introdurre un sistema di sorveglianza di massa senza limiti di oggetto (i dati vengono confusamente individuati senza alcun riferimento alle diverse possibili tipologie come ad es. quelli personali e sensibili), senza

[27] Per un commento a questo importante *leading case* si veda L. HEFFERNAN, *DNA and Fingerprint Data Retention: S and Marper v. United Kingdom*, in *European Law Rev.*, 2009, p. 491. Sia poi consentito il riferimento a L. SCAFFARDI, *L'uso del DNA in ambito investigativo penale nell'Unione Europea: tutti per uno o ognuno per sé?*, in *Rivista dell'Associazione Italiana dei Costituzionalisti (AIC)*, 4/2012, pp. 6 ss.

[28] «Il carattere generale ed indifferenziato con cui opera il meccanismo di conservazione delle impronte digitali, dei campioni di cellule e dei profili di DNA di individui sospettati della commissione di determinati reati che però non sono poi condannati, così come esso è stato applicato nel caso di specie ai ricorrenti, non garantisce un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco; agli occhi della Corte, dunque, lo Stato convenuto ha oltrepassato qualsiasi margine di apprezzamento accettabile in proposito. Ne segue che la conservazione dei dati personali oggetto della presente controversia costituisce una ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata; tale ingerenza non può essere considerata come necessaria in una società democratica», EUROPEAN COURT OF HUMAN RIGHTS, *S. and Marper v. United Kingdom decision*, *cit*, Par. 125

l'indicazioni di reati la cui gravità rendesse proporzionale la limitazione e senza l'indicazione di necessarie garanzie [29].

Conseguentemente, la Corte ha dichiarato illegittimo il regime della *Data retention* previsto dalla Direttiva in quanto contrario ai principi di tutela della privacy e dei dati personali risultanti dalla Carta europea dei diritti fondamentali della UE. Questo perché la Direttiva 2006/24 non prevede norme chiare e precise sull'ingerenza nei diritti fondamentali e l'ingerenza stessa non è limitata allo stretto necessario. Inoltre non sono previste garanzie sufficienti sulla modalità di conservazione dei dati contro i rischi di abuso o di usi illeciti degli stessi. Gli effetti della sentenza, per scelta della Corte stessa, sono divenuti immediati. Non ha infatti ritenuto di sospenderne gli effetti, come suggerito dall'Avvocato generale[30]. Questa determinazione è stata assunta senza dubbio riflettendo sull'importante *vulnus* che andava ad incidere su di un diritto fondamentale, ma anche con l'auspicio che il legislatore europeo intervenisse quanto prima sulla materia, cosa ad oggi non ancora avvenuta[31]. Anzi, si è aperto un vuoto normativo in Europa e

[29] Si legga al proposito il Paragrafo 59: «Pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta Direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi».

[30] Conclusioni dell'Avvocato generale P. Cruz De Villalon, presentate il 12 dicembre 2013, punti 154-158: «157. (..) Nel caso di specie, da un lato, non vi sono dubbi circa la rilevanza e anche l'urgenza degli obiettivi ultimi della restrizione dei diritti fondamentali di cui trattasi. Dall'altro, i motivi di invalidità constatati sono di natura particolare. Da una parte, la direttiva 2006/24 è invalida per effetto della mancanza di inquadramento sufficiente delle garanzie disciplinanti l'accesso ai dati raccolti e conservati e il loro impiego (qualità della legge), a cui tuttavia può essere stato posto rimedio nell'ambito delle misure di trasposizione adottate dagli Stati membri. Dall'altro, come risulta dagli elementi forniti alla Corte, gli Stati membri si sono generalmente avvalsi con moderazione delle loro competenze per quanto attiene alla durata massima del periodo di conservazione dei dati. 158. In tali circostanze, occorre sospendere gli effetti della constatazione dell'invalidità della direttiva 2006/24 per dar tempo al legislatore dell'Unione di adottare le misure necessarie per porre rimedio all'invalidità accertata, restando inteso che tali misure devono essere adottate entro un lasso di tempo ragionevole».

[31] Al proposito si ricorda che né il ricordato Regolamento 2016/679, né tantomeno la Direttiva 2016/680 (su cui più ampiamente si legga la nota 13), hanno affrontato la questione del trattamento dei dati personali con finalità di prevenzione di reati legati al terrorismo o più generalmente ai reati gravi.

mentre le legislazioni nazionali attuative della Direttiva 2006/24 sono divenute contrarie al diritto dell'Unione Europea, ai cittadini non rimane che rivolgersi al giudice nazionale per vedere garantita la piena efficacia alla tutela giuridica del proprio diritto[32]. Ovviamente rimane salva l'autonomia statuale di approvare nuove leggi in tema, nel pieno rispetto del principio di proporzionalità e alla luce della precedente Direttiva 2002/58/CE che consente, al suo articolo 15, par. 1, deroghe al generale divieto di conservazione dei dati per la salvaguardia della sicurezza nazionale o l'accertamento di reati[33].

[32] Sul punto vedi F. FABBRINI, *The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harv. Hum. Rts. Journal*, 28/2015, che ricorda appunto come: «the ECJ decision does not automatically remove national implementing acts from the legal order (...). However, because national data retention laws are technically exceptions to the Data Protection Directive, they are subject to review for compatibility with EU human rights law».

[33] L'art. 15 della citata normativa, così come modificata dalla Direttiva 2009/136/CE, recita: « 1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea. (..) 1 ter. I fornitori istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti sulla base delle disposizioni nazionali adottate a norma del paragrafo 1. Su richiesta, forniscono alla competente autorità nazionale informazioni su dette procedure, sul numero di richieste ricevute, sui motivi legali addotti e sulla loro risposta. 2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa. 3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.»

4. L'*Investigatory Powers Act 2016* e la sentenza *Tele2 Sverige/Watson*

La recente entrata in vigore dell'*Investigatory Powers Act 2016*[34] rappresenta un nuovo, importante tassello nel mosaico legislativo del Regno Unito dedicato alle misure di sicurezza contro criminalità e terrorismo che proietterà la sua luce (ma anche le sue ombre) su altri Paesi europei attenti agli sviluppi legislativi intorno a questi temi, la cui definizione come è stato evidenziato alla fine del paragrafo precedente, è sempre più controversa e complessa nella sua realizzazione.

Il percorso che ha portato all'approvazione della legge nel Regno Unito è stato tutt'altro che semplice, costellato di ricorsi, pronunce e sentenze che hanno evidenziato come il tema del trattamento dei dati personali nelle comunicazioni elettroniche rappresenti, come si diceva, una materia alla ricerca di un punto di equilibrio fra sempre più pressanti necessità investigative e diritti individuali.

Ripercorrere quelle tappe è essenziale per comprendere le scelte inglesi e le possibili opzioni validate dal legislatore in *dis-continuità* con il passato. Il 17 luglio 2014, a soli tre mesi dalla sentenza *Digital Rights Ireland* di cui si è scritto precedentemente, nel Regno Unito veniva emanato il *Data Retention and Investigatory Powers Act 2014*[35]. Questa legislazione appariva come una sorta di risposta politica, prima ancora che giuridica, alla decisione del giudice europeo. Si trattava, infatti, di un testo incentrato sulla pervasiva possibilità di accesso nelle comunicazioni degli individui e il conseguente utilizzo dei dati ottenuti. Fin dalla *section* 1, il DRIPA stabiliva che il Segretario di Stato potesse chiedere ad un fornitore di telecomunicazioni il mantenimento e l'accesso a dati considerati potenzialmente rilevanti, se riteneva che tale richiesta fosse necessaria e proporzionata in virtù del raggiungimento di determinate finalità da parte del Governo quali, ad esempio, gli interessi di sicurezza nazionale o più generalmente di sicurezza pubblica o prevenzione di reati non ulteriormente qualificati. Si veniva dunque a far riferimento ad un catalogo generico e di estrema ampiezza[36], al quale il Segretario di Stato avrebbe potuto far rife-

[34] D'ora in poi, IPA.

[35] D'ora in poi, DRIPA.

[36] Si vedano al proposito i punti da a) a h) dell'articolo 22 (2) del *Regulation of Investigatory Powers Act 2000* a cui il DRIPA rinviava: « It is necessary on grounds falling within this subsection to obtain communications data if it is necessary— (a) in the interests of

rimento per le sue richieste di accesso. La norma prevedeva una clausola temporale secondo cui i dati potevano essere conservati per un massimo di 12 mesi.

Il 17 luglio 2015 la *High Court of Justice* si pronunciava sul ricorso proposto da due cittadini, Peter Brice e Geoffrey Lewis, unitamente a due parlamentari inglesi, David Davis (conservatore) e Tom Watson (laburista), audite anche le associazioni civili *Open Rights Group* e *Privacy International*, dichiarando la sezione 1 del DRIPA incompatibile col diritto comunitario, in particolare con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Le conclusioni dell'*High Court,* che facevano aperto riferimento al citato precedente *Digital Rights Ireland*, sottolineavano come il DRIPA non prevedesse regole chiare e precise affinché l'accesso e l'utilizzo dei metadati sulle comunicazioni, conservati a seguito di una *retention notice*, fossero strettamente limitati allo scopo di prevenire e perseguire gravi reati specificamente determinati. In tal senso, ai punti 94 e 95 del dispositivo, l'Alta Corte stabiliva che l'accesso e l'uso dei metadati dovesse essere circoscritto all'obiettivo di prevenire e punire «*precisely defined serious offences*»[37]. Era considerato possibile che i dati di persone non sospette potessero essere utilizzati per supportare le indagini, qualora queste però fossero rivolte all'individuazione di eventuali *serious crimes* e non per perseguire reati bagatellari. Inoltre, alla Corte appariva ulteriormente improprio che la richiesta per l'accesso ai dati non fosse sottoposta all'esame preliminare di un tribunale o di un organo amministrativo indipendente, la cui decisione potesse limitare l'accesso e l'utilizzo dei dati a quanto strettamente necessario per il conseguimento dello scopo perseguito. La *High Court,* in aperta con-

national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the United Kingdom; (d) in the interests of public safety; (e) for the purpose of protecting public health; (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.».

[37] Sentenza High Court Of Justice, Case No: Co/3665/2014, Co/3667/2014, Co/3794/2014, *Secretary Of State For The Home Department V Tom Watson, Peter Brice, Geoffrey Lewis*.

tinuità con il pronunciamento di Lussemburgo, aveva dunque enucleato una serie di indicazioni attraverso le quali era possibile sviluppare una attività di raccolta dati, anche massiva, ma a determinate condizioni, tali da tutelare gli individui da un uso improprio delle informazioni, con relativa possibile lesione al diritto alla privacy.

Questa giurisprudenza apriva nel Regno Unito una serie di interrogativi di non relativa portata, stante anche il fatto che il DRIPA conteneva al suo interno una c.d. *sunset clause*[38] che determinava la fine della sua vigenza al 31 dicembre 2016 [39]. Diveniva allora imprescindibile, per il governo *in primis* e per lo stesso Parlamento che stava discutendo un nuovo disegno di legge complessivo sulla materia, comprendere fino a dove la legge parlamentare britannica si potesse spingere sulla base dell'art. 15, paragrafo 1, della Direttiva 2002/58[40], che prevede, come noto, la possibilità per gli Stati membri di adottare disposizioni legislative limitative dei diritti fondamentali, ma solo qualora la restrizione costituisca «una misura necessaria, opportuna e proporzionata all'interno di una società democratica» al fine di salvaguardare la sicurezza e la difesa dello Stato nonché la prevenzione, l'accertamento e il perseguimento di reati, senza portare però ad una lesione dei diritti dei cittadini europei (tutelati agli artt. 7, 8, 52 paragrafo 1).

La neo premier Theresa May decise, attraverso il *Secretary of State for the Home Department*, di proporre appello contro detta sentenza dinanzi alla *Court of Appeal* [41]. Quest'ultima pose a sua volta una domanda pregiudiziale alla Corte di giustizia, riguardante l'interpretazione dell'articolo 15, paragrafo 1, della Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in merito alla conformità dell'articolo 1 del *Data Retention and Investigatory Powers Act 2014* al diritto Ue [42].

La Corte si è pronunciata in merito il 21 dicembre 2016. Il caso *Tele2 Sverige/Watson* ha trattato due rinvii pregiudiziali presentati ri-

[38] S. RANCHORDAS, in *Statute Law Review*, 1/2015.

[39] *Final Provisions* sec. 8 (3): « Sections 1 to 7 (and the provisions inserted into the Regulation of Investigatory Powers Act 2000 by sections 3 to 6) are repealed on 31 December 2016».

[40] Così come modificata dalla Direttiva 2009/136, si veda nota 33.

[41] C-698/15 *Secretary of State for the Home Department v Tom Watson and Others*.

[42] L. WOODS, in *Eur. Data Prot. L. Rev.*, 1/2015.

spettivamente dai giudici svedesi e, come detto, da quello britannico (C-203/15 e C-698/15) che sono stati successivamente riuniti e contiene una serie di rilevanti indicazioni in tema[43]. Descriverne alcuni passaggi aiuta a ben comprendere come, secondo il giudice di Lussemburgo, le legislazioni nazionali debbano trattare i dati inerenti le comunicazioni elettroniche per non essere in contrasto con la normativa europea. Innanzitutto, gli obiettivi idonei a portare alla deroga al principio di riservatezza sono contenuti esaustivamente nell'art. 15, paragrafo 1, prima frase, della Direttiva 2002/58, ma questi devono essere «correlati alla gravità dell'ingerenza nei diritti fondamentali», determinando così che solo la lotta alla criminalità grave può giustificare una simile lesione (punto 115). Reati gravi come potrebbero essere quelli legati alla lotta al terrorismo o alla criminalità organizzata. La conservazione dei dati deve essere «strettamente necessaria» per combattere questi gravi crimini e l'accesso ai dati va comunque sottoposto a preventiva valutazione di una Corte o di un'autorità indipendente a seguito della richiesta delle autorità nazionali preposte. I soggetti che vedono «scandagliati» i propri dati devono essere informati il più presto possibile, introducendo così una sorta di obbligo di informativa – nel momento ovviamente in cui queste notificazioni non siano più suscettibili di danneggiare l'inchiesta giudiziaria – e dando in questo modo la possibilità ai singoli individui di agire nel caso si verifichi una lesione dei propri diritti fondamentali (punti 119 e 121). C'è poi un ulteriore tema di grande importanza riguardo la distruzione dei dati. La Corte specifica, infatti, come la normativa nazionale debba determinare la durata della conservazione dei dati e come questi debbano essere conservati nel territorio dell'Unione e distrutti irreversibilmente al termine del periodo prescritto dalla norma, in analogia con quanto già previsto nella sentenza *Digital Rights Ireland* (punti 66 e 68).

Nelle more del giudizio, considerando anche l'avvicinarsi della *sunset clause*, il Parlamento di Westminster calendarizzava appositamente l'iter legislativo della nuova legge ed arrivava, il 16 novembre

[43] Per un'attenta analisi della recente sentenza si vedano: G. TIBERI, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla Data retention*, in *Quad. Cost.*, 2/2017, pagg. 434-437; O. POLLICINO, G.E. VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza Tele2 Sverige della Corte di giustizia UE*, in *Forum* di *Quad. Cost*, 1/2017; O. POLLICINO, M. BASSINI, *La Corte di giustizia e una trama ormai nota: la sentenza tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Contemp.*, 9 gennaio 2017.

2016, all'approvazione dell'*Investigatory Power Act 2016*. La legge otteneva l'assenso regio il successivo 29 novembre per entrare in vigore, in tempo utile, il 30 dicembre 2016. L'IPA è un testo particolarmente dettagliato, composto di ben 272 articoli per una lunghezza di 300 pagine[44]. Riassuntivamente, esso si occupa di riformare il regime attraverso il quale la polizia e i servizi di *intelligence* possono essere autorizzati a condurre intercettazioni e/o ad acquisire dati relativi a comunicazione di massa. Ciò che rileva ai fini del nostro lavoro, è comprendere se l'attuale *Investigatory Powers Act 2016* sia in linea con le prescrizioni derivanti dalla giurisprudenza europea (*Digital Rights Ireland* e *Tele2 Sverige/Watson*) ed interna (*High Court*). Certamente il fattore temporale non ha permesso al legislatore di conoscere il dispositivo della sentenza *Tele2 Sverige/Watson,* pur tuttavia questa pronuncia appare in continuità con quanto già previsto e ben conosciuto nel Regno Unito fin dal 2014, in *Digital Rights Ireland,* così come note erano le considerazioni a cui era pervenuta la stessa *High Court* avverso cui si era opposto ricorso. Eppure la nuova legge, seppure introduca interessanti e innovative figure di coordinamento e supervisione come l'*Investigatory Powers Commissioner* (*sections* 227-240), sicuro portato delle maggiori garanzie richieste in questi processi di sorveglianza massiva, dall'altro presenta alcune disposizioni che non soddisfano i criteri posti dalla Corte di giustizia, prefigurando possibili nuovi ricorsi.

Si può da subito notare, infatti, come l'IPA non limiti gli scopi del mantenimento dei dati ai cd. *serious crimes*. Secondo la nuova normativa inglese, le richieste dei dati possono essere concesse per motivi diversi da quelli inerenti reati gravi (ad esempio per motivi fiscali o di salute pubblica), continuando a far riferimento ad un generico interesse alla sicurezza pubblica, ma anche ad aspetti attinenti la regolamentazione dei mercati o alla stabilità finanziaria (*Section* 61(7)), finendo così per dilatare in modo praticamente universale i motivi sulla base dei quali sia possibile accedere ai dati conservati e non discostandosi significativamente in questo dal precedente DRIPA. Quanto alle autorizzazioni (*warrants*), queste devono seguire un procedimento che vede la richiesta da parte, ad esempio, di un capo di un servizio di

[44] Su questo provvedimento e lo scenario britannico in tema sia consentito il rimando a L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato*, in *Quad. Cost.*, 2/2017, p. 412.

intelligence (o un funzionario designato da questo) al Segretario di Stato. Quest'ultimo può emanare tale mandato di *mass surveillance* dopo aver vagliato la proporzionalità della richiesta pervenuta. Detta autorizzazione deve comunque essere ulteriormente esaminata prima del suo definitivo via libera anche da un giudice (*Judicial Commissioner, Sections 23, 89, 108, 146*), attuando così un meccanismo di doppio controllo esecutivo-giudiziario da leggersi positivamente rispetto al passato.

A quella che potrebbe apparire una norma garantista e in linea con le richieste espresse dal Giudice europeo, si contrappone però una nuova incertezza, rappresentata dall'elemento temporale. Esso, infatti, viene sì modificato rispetto al passato e ridotto ad un massimo di sei mesi (*Section* 32), ma con la previsione che si possa attuarne il rinnovo sulla base della procedura descritta, rendendo così possibile il dilatarsi del tempo senza un limite preciso e facendo venir meno uno degli elementi sempre richiesti dalla giurisprudenza, vale a dire la definizione temporale del mantenimento dei dati. Non esistono infine, all'interno dell'IPA, norme che prevedano come in momenti successivi alla fase investigativa gli interessati vengano portati a conoscenza che i dati che li riguardano siano stati utilizzati, come invece viene auspicato dai diversi giudici.

Al termine di questa riflessione risulta dunque pienamente intellegibile come il Regno Unito, da sempre attento alle esigenze securitarie, cerchi di opporre una sorta di resistenza statuale che mira ad ampliare i margini di discrezionalità nelle operazioni di raccolta, conservazione ed analisi dei dati relativi alle comunicazioni elettroniche. Tendenza che oggi, alla luce della preventivata uscita del Regno Unito dalla Ue, apre ulteriori elementi di riflessione.

5. E gli altri Paesi stanno a guardare? I casi della Svizzera e dell'Italia

A questo punto dell'analisi, si può sottolineare come il quadro scaturente dalle sentenze della Corte di giustizia in tema di *Data retention*, nonché alcune pronunce rese dalle Corti statali[45] negli ultimi an-

[45] «Nel panorama europeo possiamo quindi registrare la presenza di ordinamenti che già prima della sentenza 2014 avevano seguito un'interpretazione di maggior tutela della

ni, sembrano tendere in Europa a riequilibrare il difficile rapporto tra sicurezza e diritto alla protezione dei dati in favore di questi ultimi, nel segno dell'applicazione di un pieno criterio di proporzionalità e di gravità dei reati.

Questa interessante giurisprudenza evidenzia ad esempio come sia possibile riscontrare oggi nella regolamentazione del diritto alla privacy europea una discordante lettura giuridica del tema rispetto agli Stati Uniti d'America[46]. Difatti, mentre in Europa si è generalmente cercato di assicurare una piena ed effettiva tutela al diritto alla privacy nei suoi multiformi significati, negli USA esso viene tutelato non in quanto diritto fondamentale dell'individuo, ma come diritto del consumatore, in continuo bilanciamento con esigenze economiche e securitarie tali da determinarne il possibile affievolimento nella tutela dello stesso[47]. Anche nel tema più specifico del trattamento e della conser-

riservatezza per mezzo delle proprie corti costituzionali, il che ha portato al recepimento del livello di tutela oggi accolto in materia anche dall'Unione (Germania, Repubblica Ceca, Romania, Bulgaria e Cipro). D'altra parte, altri Stati membri hanno annullato le norme sulla *Data retention* successivamente dalla sentenza *Digital Rights* del 2014, recependo il nuovo orientamento della Corte di Giustizia, come avvenuto ad esempio per l'Austria o la Slovacchia, operando talvolta in via legislativa, talaltra per l'azione diretta della magistratura che ha proceduto a disapplicare od annullare la normativa interna, dando prevalenza al nuovo diritto dell'Unione (come nel caso dei Paesi Bassi, dell'Irlanda, del Belgio e della Slovenia)», così F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolta alla disciplina UE, al giudizio della Corte di giustizia rivolto alle discipline nazionali,* in *DPCE online*, n. 2/2017, pag. 356. Tra alcune sentenze di grande importanza, si ricorda: sentenza della Corte Costituzionale tedesca del 2 marzo 2010 n.11 (1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08), sentenza n. 13627 del 11 dicembre 2008 della Corte Costituzionale bulgara e sentenza n. 1-258/2009 della Corte Costitutionale rumena, datata 8 ottobre 2009.

[46] Sulle diverse concezioni attribuite alla privacy in Europa ed in America si vedano i lavori di: WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in *Yale Law Journal*, 2003-2004 e BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis Of Antiterrorism Data Mining*, in *Boston College Law Review*, 48, 2007, 609 ss. e da ultimo P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems*, in *Forum Quad. Cost.*, 14 giugno 2017.

[47] Si fa qui riferimento, ad esempio, ai noti fatti che vanno sotto il nome di *Datagate* che hanno visto coinvolto Edward Snowden, che ha fornito alla stampa documenti segreti che hanno reso evidente i programmi di *mass sourveillance* attuati negli USA dalla National Security Agency. Su questi aspetti si leggano F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *federalismi.it*, n.13/2013 e il recente contruibuto di L.P.VANONI, *Balancing privacy and national security*

vazione dei dati nell'ambito della fornitura di servizi di comunicazione accessibili al pubblico, qui assunto come fulcro centrale di ragionamento, l'Europa sembra distinguersi per la sua differente disciplina, ritenuta *omnibus*[48]. Ma, a fronte di un'Europa certamente rivolta allo sviluppo di un quadro normativo di carattere generale e armonizzato[49], va sottolineato come si assista ad una resistenza statuale che mira ad ampliare i margini di discrezionalità nelle operazioni di raccolta, conservazione ed analisi di dati personali, come evidenziato nel caso inglese. Appare allora lecito chiedersi se non si stia assistendo ad un surrettizio avvicinamento, fra le due sponde dell'Atlantico, di modelli pur così distanti nei loro presupposti.

Ritornando al piano europeo, assunto ora in senso geografico, può essere utile ampliare ulteriormente le considerazioni svolte finora, soprattutto per quanto riguarda le ultime evoluzioni in materia e proponendo dunque alcune considerazioni *de iure condendo* su due Paesi tanto vicini geograficamente quanto distanti sul piano dell'approccio e delle soluzioni individuate per garantire sicurezza da un lato e diritti individuali dall'altro. Ci riferiamo, nello specifico, a Svizzera ed Italia.

Il 25 settembre 2016 si sono tenuti in Svizzera alcuni referendum. Ma mentre l'opinione pubblica italiana era attratta dall'esito di quello cantonale in Ticino sui lavoratori transfrontalieri, il risultato del ben più importante referendum nazionale [50], riguardante il tema

---

in the global digital era: a comparative perspective of EU and US constitutional systems, in *forumcostituzionale.it*, 14 giugno 2017.

[48] Sul tema, tra gli altri, si veda J.R. REIDENBERG, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, in *FCLJ*, 195/1992, p. 208 ss, in cui è chiara la contrapposizione tra l'approccio americano definito *ad hoc* e quello europeo definito invece *omnibus*. Sul tema si veda anche R. LATTANZI, *Diritto alla protezione dei dati di carattere personale: appunti di viaggio*, in F. PRIOLO E ALTRI, *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, in *I quaderni europei*, n. 63/2014.

[49] Così come previsto dalla Direttiva 95/46/CE, rivista alla luce della pronuncia *Digital Rights Ireland*.

[50] Tale Referendum verteva anche su *Iniziativa Economia Verde* e *Iniziativa AVS plus: per un'AVS forte*. Per quanto qui ci interessa, relativamente alla Legge federale sulle Attività Informative, bisogna precisare che la Legge oggetto di referendum era stata approvata il 25 settembre 2015 dal Consiglio Nazionale con 145 voti, contro 41 contrari ed 8 astenuti, e dal Consiglio degli Stati con 35 voti a favore contro 5 voti negativi e 3 astensioni. Sia il Consiglio Federale che l'Assemblea Federale hanno dunque raccomandato di adotta-

dell'adozione della nuova Legge federale sulle Attività Informative[51], è passato – non solo da noi – quasi totalmente inosservato. Il testo di legge sottoposto a referendum è stato validato da parte di una larga maggioranza dei cittadini svizzeri (il 65,5%)[52]: gli abitanti della Confederazione hanno scelto di rinunciare a parte delle loro libertà, "concedendo" al Servizio delle attività informative della Confederazione (il cosiddetto Sic[53]), di intercettare conversazioni telefoniche, controllare la posta elettronica ed i sistemi informatici attraverso veri e propri "virus di Stato", i cd *spywares*.

La forte innovazione, ed anche il più grande timore degli oppositori di questa legge, consiste proprio nell'ampliamento dei poteri di sorveglianza ed acquisizione di informazioni del Sic, ora più pervasivi ed invasivi della sfera privata: mentre prima di questo intervento legisla-

---

re tale Legge, appoggiata principalmente da partiti di centro e di destra. Il referendum contro tale progetto invece è stato lanciato e sostenuto da un'alleanza formata essenzialmente da partiti di sinistra e da alcune organizzazioni quali dirittifondamentali.ch e Digitale Gesellschaft. Tali informazioni sono tratte dal sito istituzionale del Dipartimento federale della Difesa, ***www.vbs.admin.ch***.

[51] D'ora in poi LAIn.

[52] Il valore della partecipazione complessiva alle urne è compreso tra il 42,6% e il 43,1%, riscontrando così un coinvolgimento di poco inferiore rispetto alla media degli ultimi 20 anni. Le percentuali più alte sono state quelle dei cantoni di Vaud (74,2%) e Nidvaldo (70,1%). In Ticino e nei Grigioni il fronte del sì ha raggiunto rispettivamente il 66,1 e il 63,6%. Per ulteriori interessanti approfondimenti sui dati statistici relativi al referendum in questione, si veda T. MILIC, D. KUBLER, *Studio VOTO relativo alla votazione federale del 25 settembre 2016*, 2016, disponibile at ***www.newsd.admin.ch***.

[53] Il Sic è un servizio di intelligence che, sulla base di quanto previsto nella LAIn, svolgerà attività di prevenzione ed individuazione tempestiva di quelle minacce alla sicurezza, interna ed esterna, elencate all'art. 6: attacchi terroristici, spionaggio, diffusione di armi nucleari, biologiche o chimiche, commercio illegale di sostanze radioattive, materiale bellico e altri beni d'armamento, attacchi a infrastrutture indispensabili per il funzionamento della società, dell'economia e dello Stato (infrastrutture critiche), estremismo violento. Altre funzioni ad esso attribuite sono: l'accertamento e valutazione di fatti avvenuti all'estero che hanno però rilievo per la politica di sicurezza interna; salvaguardia della capacità d'azione della Svizzera; più ampiamente la tutela di interessi nazionali. Una volta rilevate situazioni di pericolo e minaccia, il Sic ha il dovere di informarne e, se necessario allertare, le autorità politiche federali e dei vari Cantoni, al fine di mettere tali soggetti in condizione di prendere le decisioni più opportune. Il Sic, pur essendo sottoposto a svariati controlli, di cui si parlerà più ampiamente nel prosieguo di questa disamina, è essenzialmente al «servizio del Consiglio federale, degli organi di sicurezza cantonali, dei Dipartimenti e della condotta militare. Il SIC svolge tutti i suoi compiti in modo conforme al diritto e nel rispetto del principio della proporzionalità» (così si legge sul sito istituzionale del Dipartimento federale della Difesa, in ***www.vbs.admin.ch***).

tivo il Servizio informativo aveva accesso solo a dati pubblici liberamente accessibili (quelli che oggi sono denominati misure di acquisizione per le quali non è necessaria alcuna autorizzazione), dall'entrata in vigore della LAIn questo organo garante della sicurezza potrà, nel rispetto di precise regole e limiti, sorvegliare fonti di informazioni strettamente private quali corrispondenza postale e traffico delle telecomunicazioni, potrà impiegare apparecchi di localizzazione e di sorveglianza per intercettare o registrare comunicazioni o conversazioni private oppure per osservare o registrare fatti in luoghi privati o non accessibili al pubblico ed infine potrà infiltrarsi in sistemi e reti informatiche[54]. Tutte queste misure, che vengono eseguite segretamente, senza cioè che i soggetti interessati ne vagano informati se non eventualmente solo in un momento successivo[55], riducono fortemente lo spazio di tutela della riservatezza e della privacy del singolo cittadino.

Per mitigare questo intervento così invasivo e per evitare abusi, il legislatore ha previsto una serie di limitazioni e di controlli. Innanzitutto, il Sic potrà ricorrere all'acquisizione di tali informazioni solo in situazioni di concreta e grave minaccia e potrà agire solo previa autorizzazione da parte di tre diversi soggetti, mediante una procedura «a cascata»: a seguito dell'ottenimento dell'autorizzazione da parte del Tribunale Amministrativo Federale (comunque limitata nel tempo, per una durata di tre mesi), il Sic dovrà ottenere il nullaosta dal capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), il quale decide previa consultazione del capo del Dipartimento federale degli affari esteri (DFAE) e del capo del Dipartimento federale di giustizia e polizia (DFGP)[56]. Ulteriore forma di garanzia di legittimità dell'operato del Sic è l'istituzione di un'autorità di vigilanza indipendente[57].

Secondo i sostenitori della LAIn, grazie a questa severa condizionalità imposta dal legislatore nei confronti del Sic, nonostante i suoi

[54] Si veda più ampiamente l'art. 26, LAIn, disponibile in formato pdf all'indirizzo *www.admin.ch*.

[55] «Entro un mese dalla conclusione dell'operazione, il SIC comunica alla persona sorvegliata il motivo, il genere e la durata della sorveglianza cui è stata sottoposta mediante misure di acquisizione soggette ad autorizzazione»: così recita l'art. 33, LAIn, che elenca anche casi eccezionali in cui è possibile differire o addirittura rinunciare a tale informativa.

[56] Così gli artt. 29 e 30 LAIn; merita una menzione l'art. 31, che permette di evitare la procedura di autorizzazione in casi di particolare urgenza.

[57] Sul tema si vedano più ampiamente gli artt. 76 e ss. della legge LAIn.

ampliati confini di intervento, l'equilibrio tra sicurezza da una parte e riservatezza e libertà individuali dall'altra risulta pienamente garantito. Forse è presto per valutare se sia realmente così: molto dipenderà dalle ordinanze attuative[58], nonché dal funzionamento dell'organismo di vigilanza posto a controllo del Sic e da come quest'ultimo utilizzerà concretamente i suoi nuovi poteri; non si può tuttavia fare a meno di notare alcuni aspetti per lo meno potenzialmente problematici: l'articolo 5 della LAIn[59], pur "pianificando" nel dettaglio le attività che, grazie alla nuova normativa, sono considerate legali, vi include il mantenimento delle informazioni senza una specifica motivazione fino alla durata di un anno[60]. Proprio da disposizioni come questa sono nati i timori che hanno portato alla votazione del 25 settembre 2016: il referendum è infatti stato promosso da un eterogeneo gruppo di partiti

[58] Vedi *infra*.

[59] Il testo prevede come: «La presente legge ha lo scopo di tutelare interessi nazionali importanti e intende: - contribuire a garantire i fondamenti della democrazia e dello Stato di diritto della Svizzera e a proteggere i diritti di libertà della sua popolazione; - accrescere la sicurezza della popolazione della Svizzera e degli Svizzeri all'estero; - sostenere la capacità d'azione della Svizzera; - contribuire a tutelare gli interessi internazionali in materia di sicurezza».

[60] Si veda l'art 5: «Principi dell'acquisizione di informazioni:

1 Per adempiere i suoi compiti, il SIC acquisisce informazioni tanto da fonti accessibili al pubblico quanto da fonti non accessibili al pubblico.

2 A tale scopo il SIC ricorre sia a misure di acquisizione non soggette ad autorizzazione sia a misure di acquisizione soggette ad autorizzazione.

3 Il SIC sceglie di volta in volta la misura di acquisizione che:

a) è più idonea ed è necessaria per raggiungere un determinato obiettivo in materia di acquisizione; e

b) incide il meno possibile sui diritti fondamentali delle persone interessate.

4 Il SIC può acquisire dati personali all'insaputa delle persone interessate.

5 Il SIC non acquisisce e non tratta informazioni sull'attività politica e sull'esercizio della libertà di opinione, di riunione o di associazione in Svizzera.

6 Il SIC può eccezionalmente acquisire le informazioni di cui al capoverso 5 relative a un'organizzazione o a una persona e registrarle con riferimento alle persone se sussistono indizi concreti che tale organizzazione o tale persona esercita i propri diritti per preparare o eseguire attività terroristiche, di spionaggio o di estremismo violento.

7 Il SIC cancella i dati registrati con riferimento alle persone non appena possono essere escluse attività secondo il capoverso 6, ma al più tardi dopo un anno dalla registrazione, se fino a tale momento dette attività non sono confermate.

8 Il SIC può acquisire e trattare anche le informazioni di cui al capoverso 5 relative a organizzazioni e gruppi della lista d'osservazione di cui all'articolo 72 o a loro esponenti se, in tal modo, è possibile valutare la minaccia rappresentata da tali organizzazioni e gruppi.»

che avevano dato vita alla cosiddetta «Alleanza contro lo Stato ficcanaso»[61] e che ritenevano ingiustificato e del tutto sproporzionato l'ampliamento del campo di azione del Sic. Per contro, invece, i sostenitori della legge denunciavano che di fronte al moltiplicarsi delle forme di minaccia, sempre più complesse e difficili da individuare preventivamente, i poteri del Servizio delle attività informative della Confederazione, così come previsti prima della LAIn, non fossero più sufficienti a consentirgli di compiere adeguatamente ed efficacemente la propria missione[62].

La nuova legislazione dovrebbe entrare in vigore nel settembre 2017, entro quella data, infatti, il Governo dovrà elaborare, secondo un scadenzario da lui stesso definito, le disposizioni applicative richieste dalla norma[63]: solo a quel punto e a seguito della sua concreta ap-

[61] Nel sito dell'associazione (***www.stato-ficcanaso.ch***) erano dettagliate le motivazioni del ricorso alla volontà popolare contro la nuova legge: «Tutti vengono sorvegliati, non solo criminali, come spesso viene sostenuto. Intercettazione telefonica, lettura delle mail, dei messaggi whatsapp e sms, come pure la sorveglianza d'internet attraverso ricerca di parole chiavi, sono tutti mezzi della sorveglianza di massa indipendente da sospetti. Siamo tutti colpiti da queste misure! Innumerevoli nostri dati personali vengono registrati e analizzati – senza che abbiamo commesso alcuna colpa. Il servizio informativo si espande da un ente di difesa da pericoli a un apparato poliziesco offensivo al di fuori dello Stato di diritto. Non è previsto né controllo democratico da parte del popolo, né trasparenza. Gli scandali delle schedature del passato, nei quali centinaia di migliaia di cittadini sono stati sorvegliati, ci devono fungere da insegnamento. Non possiamo creare un altro mostro raccoglitore di dati all'interno dello Stato. (…) Dell'inchiesta su attività terroristiche e criminalità organizzata – così come delle rispettive attività di pianificazione – sono già oggi responsabili il Ministero pubblico della Confederazione e le varie autorità di polizia cantonale. Essi dispongono dei mezzi necessari e di una supervisione legislativa. La sorveglianza statale più ampia e non sulla base di sospetti fondati mina lo Stato di diritto e la democrazia!».

[62] Per il governo e la maggioranza di destra in Parlamento, che aveva approvato la legge nel settembre 2015, si è trattato dunque di una vittoria, salutata dal ministro della Difesa con parole enfatiche nella conferenza stampa che ha seguito l'esito del referendum: «La nuova legge sulle attività informative darà dei mezzi moderni al SIC. Prevede anche dei controlli supplementari per rispondere ai timori di numerosi cittadini».

[63] In particolare «lo scadenziario prevede l'inizio della consultazione per le tre ordinanze – quella sul Servizio delle attività informative della Confederazione (O-SIC), quella sui sistemi di informazione e di archiviazione e quella sull'autorità di vigilanza indipendente – a metà ottobre del 2016. In seguito, da gennaio ad aprile del 2017, le ordinanze passeranno in consultazione presso i Cantoni, le organizzazioni coinvolte, le Commissioni della politica di sicurezza e la Delegazione delle Commissioni della gestione. Nel mese di giugno del 2017 è prevista la seconda consultazione e ad agosto la decisione finale del Consiglio federale»: così si legge sul sito istituzionale del Dipartimento federale della difesa. Per questo e più ampiamente per verificare lo stato di avanzamento della procedura (al momento, pur ter-

plicazione potremo comprendere se l'estensione dei poteri del Sic siano ben controbilanciati dalle severe condizioni normative, dal sistema autorizzativo multilivello e dall'autorità di vigilanza o se invece il governo elvetico abbia posto in essere, pur con il consenso del popolo svizzero stesso, misure che comprimono riservatezza e libertà del singolo a favore di una, più o meno giustificabile, maggiore sicurezza entro i propri confini.

In Italia, invece, un intervento legislativo complessivo pare purtroppo di là da venire. Come noto, il nostro Paese prevede, dal 2003, un'apposita disciplina in materia, contenuta nell'art. 132 del «Codice della privacy» (D. Lgs. 196/2003). Detto articolo è stato però derogato svariate volte[64], a riprova di quanto sia difficile e controverso il bilanciamento tra diritto alla riservatezza[65] e interesse collettivo alla sicu-

minata la fase di consultazione, non sono ancora disponibili i pareri delle parti chiamate ad esprimersi in merito alle ordinanze) si legga ***www.vbs.admin.ch***.

[64] I numerosi interventi in deroga che si sono succeduti sono i seguenti: decreto-legge 24 dicembre 2003, n. 354, convertito con modificazioni dalla legge di conversione 26 febbraio 2004, n. 45, recante interventi per l'amministrazione della giustizia; decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge di conversione 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale; legge 18 marzo 2008, n. 48, recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, siglata a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno, testi questi citati anche nel prosieguo del paragrafo. Ancora, il decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei 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. Infine, decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, come modificato dal decreto legge 30 dicembre 2015, n. 210, convertito con modificazioni dalla legge 25 febbraio 2016, n. 21.

[65] Sulla vastissima produzione italiana in tema di diritto alla riservatezza si segnalano tra i molti: L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016; ID., *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO , C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014; G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA - P. RIDOLA (a cura di), *I diritti fondamentali*, vol. II, Torino, Giappichelli, 2006; U. DE SIERVO, *Tutela dei dati personali e riservatezza*, in AA. VV., *Diritti, nuove tecnologie, trasformazioni sociali: scritti in memoria di Paolo Barile*, Padova, Cedam, 2003; G. BUTTARELLI, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, Giuffrè, 1997; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1997 e ID, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974.

rezza[66]. Si è trattato di interventi quasi sempre tesi ad ampliare il margine di operatività della norma, tutelando il cd. *tracing* come strumento di particolare importanza rispetto alla risoluzione dei reati, in specie quelli terroristici. Insomma, l'ampliamento dei tempi di conservazione dei dati, conseguenti a momenti di particolari emergenze terroristiche, ha determinato quello che è stato definito, in maniera assolutamente condivisibile, un "pasticcio normativo"[67].

Ultimo esempio, in ordine di tempo, di tale "disordine" si è avuto il 19 luglio scorso, quando, durante le votazioni sulla cd. legge comunitaria 2017[68], è stato approvato alla Camera un emendamento di particolare rilevanza (A.C. 4505-A). Nello specifico, gli onorevoli Verini, Berretta e Mucci hanno presentato una modifica di legge[69] volta a prolungare fino a 72 mesi il termine di conservazione dei dati telefonici e telematici imposto ai *provider*, con un inasprimento delle regole tale da essere duramente criticata sui media[70] oltre ad aprire un vivace dibattito tra esperti e giuristi.

---

[66] Si intende qui parlare di sicurezza nel suo significato ampio e cioè di interesse della collettività che si estende in molteplici modi all'insieme della tutela dei beni costituzionali e ai diversi settori dell'agire pubblico. In questo senso si consultino: M. DOGLIANI, *Il volto costituzionale della sicurezza*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, Giuffrè, 2012, e P. RIDOLA, *Libertà e diritti nello sviluppo del costituzionalismo*, in P. RIDOLA - R. NANIA (a cura di), *I diritti costituzionali*, Torino, Giappichelli, 2006.

[67] P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1/2016, p.36.

[68] Disegno di Legge *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea 2017*.

[69] Nel dettaglio, i tre parlamentari hanno avanzato la loro proposta emendativa prevista all'art.12-ter, che così recita: «Art. 12-ter. (Termini di conservazione dei dati di traffico telefonico e telematico) 1. In attuazione dell'articolo 20 della Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficaci tenuto conto delle straordinarie esigenze di contrasto al fenomeno del terrorismo, anche internazionale, per le finalità di accertamento e repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del decreto legislativo 30 giugno 2003, n. 196, in settantadue mesi».

[70] L. VENDEMIALE, *Lo Stato ci spia: telefoni e web saranno controllati per 6 anni*, in *il Fatto Quotidiano*, 23 luglio 2017, pp. 2/3; F. SARZANA, *6 anni! È il termine di conservazione dei dati telefonici e telematici di tutti i cittadini appena approvato alla Camera. In una direttiva sugli ascensori*, in *Il Sole 24 ore*, 21 luglio 2017.

Cosa ha generato una simile azione, per lo più in un contesto normativo che pare di dubbia opportunità? È necessario un breve *excursus*, che parte proprio da quel decreto legge n. 7 del 18 febbraio 2015 con cui il Governo aveva adottato un provvedimento in materia di lotta al terrorismo, introducendo deroghe al Codice della privacy ed in ispecie proprio all'art. 132. In particolare, la legge n. 43 di conversione del Decreto legge 7/2015 approvata il 17 aprile 2015, prevedeva al suo art. 4 bis[71] che i dati relativi al traffico telefonico e telematico dovessero essere conservati sino al 31 dicembre 2016 a far data dalla entrata in vigore della legge di conversione (quindi per poco più di un anno e mezzo) e così parimenti per i dati relativi alle chiamate senza risposta. La *ratio* dell'estensione temporale rispetto alla normativa previgente si può desumere dalle schede di lettura che accompagnavano l'atto, vale a dire «mettere a disposizione dell'autorità investigativa strumenti efficaci contro una *minaccia* (corsivo nostro), quella del terrorismo, sempre più grave ed estesa, che i mezzi informatici rendono pervasiva annullando i confini temporali e territoriali»[72].

Nel cosiddetto Decreto milleproroghe del dicembre 2015 veniva ulteriormente ampliato il tempo di applicazione della norma fino al 30 giugno 2017, ancora una volta senza ipotizzare un intervento complessivo sulla materia e continuando ad agire in deroga a quanto previsto dal Codice, attraverso l'utilizzo di una legge *omnibus,* per incidere sui diritti individuali.

---

[71] Art. 4-bis Disposizioni in materia di conservazione dei dati di traffico telefonico e telematico 1. I dati relativi al traffico telefonico o telematico, esclusi comunque i contenuti di comunicazione, detenuti dagli operatori dei servizi di telecomunicazione alla data di entrata in vigore della legge di conversione del presente decreto, nonché quelli relativi al traffico telefonico o telematico effettuato successivamente a tale data, sono conservati, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, fino al 30 giugno 2017, per le finalità di accertamento e di repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale. 2. I dati relativi alle chiamate senza risposta, effettuate a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibile al pubblico oppure di una rete pubblica di comunicazione, sono conservati fino al 30 giugno 2017. 3. Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° luglio 2017.

[72] Questa che doveva essere dunque una limitazione temporanea della tutela della privacy nasceva a seguito della necessità e dell'urgenza di contrastare il terrorismo che nelle settimane precedenti aveva mostrato tutta la sua ferocia a Parigi con il tragico attacco alla redazione del settimanale satirico Charlie Hebdo.

Tornando al cuore della questione, ovvero la recentissima scelta del legislatore di triplicare il periodo di conservazione dei dati telefonici per finalità di contrasto al terrorismo rispetto a quanto stabilito fino ad oggi, in modo totalmente difforme dalla media degli altri Paesi europei, è evidente che tale «giro di vite» non può che derivare da una «lettura» politico-emergenziale della situazione, non ravvisandosi alcun'altra spiegazione giuridicamente sostenibile. È vero che il 30 giugno scorso è scaduto l'obbligo di conservazione dei dati del traffico telefonico e telematico che ritornerebbero per così dire in "modalità ordinaria"[73], ma dei due casi l'una: o l'emergenza terroristica è finita ed allora potremmo a buona ragione accettare di ritornare alla normativa pre decretazione d'urgenza, oppure la realtà che viviamo necessità di norme specifiche e ponderate. Purtroppo, da quel lontano 21 aprile 2015 e fino appunto al 30 giugno 2017, il legislatore nulla ha fatto per approvare una complessiva normativa in tema e si ritrova oggi ad inserire una nuova «toppa» che, come si suol dire, risulta essere "peggiore del buco".

Restando all'analisi del testo, risulta evidente da subito come vengano equiparati i dati telematici a quelli telefonici e come più volte detto, che tutti questi dati sarebbero mantenuti per ben 6 anni. Attualmente i tempi di conservazione previsti nel nostro ordinamento, regolati dal Codice della privacy, sono per il traffico telefonico di 24 mesi dalla data della comunicazione (art. 132 comma 1 del Codice della privacy) e di 30 giorni per le chiamate senza risposta (art. 132 comma 1*bis* del Codice della privacy). Diversamente, per quanto riguarda il traffico telematico, i dati possono essere conservati e quindi messi a disposizione dell'autorità giudiziaria per 12 mesi dalla data della comunicazione (art. 132 comma 1 del Codice della privacy). Se invece anche in Senato dovesse passare il recente emendamento, come opportunamente commentato, da Ugo Mattei, «le aziende saranno in possesso di una massa di dati privati enorme, che ha ovviamente un valore economico alto, visto l'uso commerciale improprio che spesso ne viene fatto e che è molto difficile da controllare. Mentre lo Stato si assicura la possibilità di fare un *profiling* dei cittadini per un periodo di una lunghezza esorbitante. Praticamente ci stanno schedando»[74].

[73] Seguendo dunque l'originale disposto dell'art. 132 del Codice della Privacy.

[74] Così riportato da L. VENDEMIALE, *Lo Stato ci spia: telefoni e web saranno controllati per 6 anni*, in *il Fatto Quotidiano*, cit.

Questa improvvisa estensione temporale, non inserita per di più in una disciplina organica della materia, è inoltre a rischio di incompatibilità con il Diritto comunitario, in quanto – come già ricordato nei paragrafi precedenti – con la sentenza *Digital Rights Ireland*[75] la Corte di giustizia ha dichiarato invalida la Direttiva 2006/24/EC sulla *Data retention* (cd Direttiva Frattini), proprio perché prevedeva un obbligo indiscriminato di mantenimento di dati[76]. E non di meno, la sentenza *Tele2 Sverige/Watson* del 21 dicembre 2016 (Corte Giustizia UE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 e Watson*) ha apportato ulteriori indicazioni, spostando l'attenzione dal piano legislativo europeo a quello nazionale e determinando così una complessiva rilettura in senso garantistico del tema. Stupisce come l'emendamento proposto possa rispondere ai criteri richiesti soprattutto per ciò che attiene la conoscibilità dei dati trattenuti.

Come si vede, anche senza qui voler ancora una volta richiamare la lunghezza esorbitante del trattenimento del dato, a cui auspicabilmente il Senato potrà a breve porre rimedio riducendo tale tempistica, rimangono molte e inquietanti le altre criticità aperte, dalle procedure di accesso e di acquisizione delle informazioni, all'individuazione dei «gravi» reati che sono, secondo la giurisprudenza UE, presupposto oggettivo tale da giustificare l'intero procedimento di *Data retention* e richiamati troppo sbrigativamente nell'emendamento. Pretendere che una novità di tale importanza sia innervata all'interno di un articolo, il 12 che riguarda appunto gli adempimenti comunitari, al cui comma precedente si parla di «Disposizioni per l'integrale attuazione della Direttiva 2014/33/UE relativa agli ascensori e ai componenti di sicurezza degli ascensori nonché per l'esercizio degli ascensori» appare del tutto improprio se non improvvido. Inoltre questa «tecnica» legislativa porta con se anche possibili critiche in chiave di legittimità costituzionale poiché è apparsa «in contrasto con l'articolo 117, primo comma della Costituzione, in quanto la disomogeneità tra Direttiva da recepire (quella sugli ascensori) e contenuto del recepimento (la disciplina della *retention* dei dati

[75] Su cui vedi quanto già scritto a p. 4 e ss.

[76] La Corte di giustizia fin da allora ha esplicitato chiaramente come in Europa la conservazione dei dati per fini legati alla protezione dell'ordine pubblico possa divenire eccessivo se non proporzionato al fine che si vuole raggiungere, fine che nella norma *de qua* appare identificato nell'estremamente ampia ragione «di garantire strumenti di indagine efficaci tenuto conto delle straordinarie esigenze di contrasto al fenomeno del terrorismo».

di traffico) potrebbe porsi in contrasto con il canone di esercizio di potestà legislativa in conformità con i "*vincoli dell'ordinamento dell'Unione Europea*", oggi disciplinati sul piano interno dalla legge 234 del 2012»[77].

6. Il precario equilibrio tra prevalenti ragioni securitarie e difficili scelte legislative

Senza presunzione di esaustività, questi ultimi esempi *de iure condendo* offrono la possibilità di una riflessione conclusiva e di insieme su un tema che rimane e rimarrà certo aperto a lungo. Se da una parte può essere osservato come le nuove tecnologie applicate alle investigazioni rappresentino un utile mezzo per combattere la criminalità in generale ed in specie il terrorismo, tuttavia l'impatto di queste tecniche sulle condizioni dell'individuo richiedono un'attenta valutazione, potendo comportare forti limitazioni ai diritti individuali[78].

Fino ad ora la frattura venutasi a creare fra sicurezza e diritto alla privacy è stata arginata, come abbiamo visto, dal lavoro delle Corti (vuoi nazionali o sopranazionali)[79] che hanno funto da motori propulsivi per la successiva revisione delle normative già approvate. Quanto all'Italia, risulta evidente come sia auspicabile un intervento com-

[77] L. SCUDIERO, *La Camera porta di soppiatto la Data retention a sei anni,* in *Lex Digital,* 21 luglio 2016, consultabile at ***www.lexdigital.it***.

[78] Denninger segnala sul piano generale il rischio nascente da un «vago e illimitato» diritto alla sicurezza poiché «sotto il pretesto (…) di allargare la sua offerta di tutela, lo Stato non può elevare illimitatamente la sua richiesta di obbedienza, cioè in altre parole: diminuire progressivamente la sfera di libertà del singolo». E. DENNINGER, *Stato di prevenzione e diritti dell'uomo*, in C. AMIRANTE (a cura di), *Diritti dell'uomo e legge fondamentale*, Torino, Giappichelli, 1998, p. 91.

[79] Il ruolo assunto dalle Corti nella tutela della riservatezza per ciò che attiene il mantenimento massivo di dati determina forti perplessità qualora il Legislatore non intervenga sulla materia con norme specifiche e puntuali, potendo l'attività del Giudice prefigurare "distopie" di sistema: «Ma chi pensasse che il compimento di un simile processo disegni il futuro desiderabile di una cittadinanza consistente in un tessuto di diritti costruiti e garantiti dalle giurisdizioni, nel superamento del circuito della rappresentanza politica, coltiverebbe una distopia autoritaria. Anche le sorti della riservatezza lo dimostrano: nessun diritto fondamentale può essere lasciato nelle mani di un'aristocrazia giudiziale – oggi necessariamente multilivello – che decida essa stessa sui confini del proprio potere, sostanzialmente libera da vincoli normativi. E da questa posizione esclusiva decida sul bilanciamento tra libertà e sicurezza». S. STAIANO, *Diritto alla riservatezza e potere pubblico*, in *Federalismi.it*, n. 17/2017 .

plessivo del legislatore su questo specifico tema in modo che la disciplina sia in linea con quanto previsto dalla giurisprudenza europea, ma soprattutto garantisca attraverso la legge, l'efficienza della lotta al terrorismo, sempre più «emergenza ordinaria» della nostra quotidianità, che esige scelte ponderate nel bilanciamento possibile fra ragioni securitarie e diritti individuali.

Ancor di più viene a manifestarsi la necessità della previsione in questa legislazione di un agile *iter* che consenta al giudice «un accertamento concreto sulla sussistenza del reato 'presupposto', basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire *ex post*, in un lasso di tempo comunque breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici)**,** purché vi sia una definizione: a) di un elevato livello delle "misure di sicurezza" da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento**;** b) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del 'principio di necessità' nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità)»[80].

Per concludere non può essere dimenticato, al netto delle preoccupanti «originalità» del legislatore italiano, come anche quello europeo potrebbe e dovrebbe intervenire cercando di dare sempre più forma a quella necessaria politica anticrimine dell'Unione[81] che

[80] R. FLOR, *Data retention ed art. 132 cod. privacy: vexata quaestio(?)*, in *Dir. Pen. Contemp.*, 29 marzo 2017.

[81] C'è chi sostiene infatti che, «La stessa individuazione dei fenomeni criminali gravi e di natura transnazionale, nonché la conseguente definizione dei "reati presupposto", potrebbe trovare una base legale nell'art. 83, par. 1, TFUE. Il valore aggiunto riguarda, da un lato, l'efficacia, per la forza vincolante delle fonti per gli Stati membri; dall'altro lato le garanzie, che devono circondare la produzione di norme penali (legittimazione democratica e trasparenza del procedimento legislativo, controllabilità politica, da parte dei Parlamenti nazionali durante la fase «ascendente» dei fondamentali principi di sussidiarietà europea e di proporzionalità, ex art. 5 TUE e Protocollo applicativo n. 2 allegato al TFUE, piena controllabilità giudiziaria di tali presupposti da

continua a trovare resistenze, ma su cui siamo chiamati a riflettere in tempi di cronicizzazione del terrorismo.

Certo, in momenti di particolare *stress* come quelli vissuti in molti Paesi, europei e no, presi di mira dai criminali attacchi terroristici, la sicurezza può rendere giustificabile un intervento legislativo temporaneo in senso limitativo di un diritto o di una libertà[82]. Il problema, come già si è avuto modo di osservare[83], è determinare legislativamente (e non giudizialmente) l'equilibrio concreto fra questi due ambiti, soprattutto in una società che evolve verso una «profilatura» globale delle dinamiche individuali, con un conseguente sbilanciamento di poteri tra controllore e controllato. Ed è proprio qui che i "governi" dovrebbero fare ancor più tesoro delle parole del *Federalist* evocate nell'apertura di questo lavoro, per non tendere ad una "normalizzazione" dell'emergenza[84] che li porterebbe fuori da ogni controllo.

parte della Corte di Giustizia ed, indirettamente, delle giurisdizioni nazionali nella fase applicativa». R. FLOR, *Data retention ed art. 132 cod. privacy: vexata quaestio(?)* in *Dir. Pen. Contemp.*, 29 marzo 2017.

[82] In tal senso vedi: M. RUOTOLO, Costituzione e sicurezza tra diritto e società, A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, Maggioli, 2014, p. 588.

[83] L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in A. TORRE, (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, Maggioli, 2013, p. 438.

[84] Si è parlato, infatti, di «una sorta di "cronicizzazione" e di "normalizzazione" dell'emergenza, idonee a trasformare il ricorso a misure eccezionali – quali, ad esempio, la limitazione o la sospensione dei diritti fondamentali – in una sorta di prevenzione senza fine, giustificata dal pericolo del terrorismo», G. M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, Atti del Convegno tenutosi presso l'Università di Roma La Sapienza il 6.12.2007, Napoli, 2009, p. 76.; più generalmente sul tema di una possibile normalizzazione dell'emergenza si v. G. AGAMBEN, *Stato di eccezione*, Torino, Bollati-Boringhieri, 2003.

Costituzionalismo.it

Fondatore e Direttore dal 2003 al 2014 Gianni **FERRARA**

Email: info@costituzionalismo.it

Registrazione presso il Tribunale di Roma

ISSN: 2036-6744 | Costituzionalismo.it (Roma)