L'applicazione del Bill of Rights europeo tra bilanciamento asimmetrico e paradosso federale: il caso della privacy digitale

di Luca Pietro Vanoni

Abstract: The European Bill of Rights between asymmetry and federal paradox. The case of digital privacy – Since it entered into force in 2009, the European Charter of Fundamental Rights played an important role in shaping the European Union framework. In particular, it impacted the unique European federal structure imposing a centralizing effect and providing the grounds to confirm and steadily expand the scope of application of EU fundamental rights to the Member States. The European Court of Justice increasingly referred to the Charter in order to interpret the EU law, directly enforcing the Charter's provisions in its judgements. In doing so, the European judges empowered their role as human rights adjudicators, but they didn't fully consider the federal paradox of their rulings. This paper will examine the impact of the Charter's federalizing force within the field of digital privacy. First it will analyze the clash between the rights to privacy and data protection guaranteed in art. 7 and 8 of the Charter and the need to ensure national security expressively reserved by art. 4 TUE to the Member States. The paper will then analyze the Data Protection Saga, claiming that in seeking to establish itself as the ultimate protector of fundamental rights in Europe, the Court of Justice has arguably neglected the importance of respect for other fundamental constitutional principles relating to the proper division of competences. Finally, the article will argue that especially if the Court of Justice want to address itself as the Constitutional court of Europe it has to take its role of federal jurisdiction seriously, balancing the protection of human rights with the federal division of powers between UE and the Member States.

Keywords: Privacy; European Charter of Fundamental Rights; Federalism; Data Protection.

1. Prologo. La portata federale della Carta dei diritti fondamentali: alle origini del paradosso europeo

Quasi venti anni fa, a seguito della approvazione della Carta dei diritti fondamentali voluta dal Consiglio Europeo di Nizza, Joseph Weiler si interrogava su come tale documento avrebbe potuto incidere sul futuro del costituzionalismo europeo: «la Carta europea è stata proclamata e dobbiamo trarne il massimo vantaggio. Ma vale ancora la pena chiedersi se l'Europa ne aveva davvero bisogno: migliorerà davvero la protezione dei diritti umani fondamentali nell'Unione?»[1]. Tale riflessione si inserisce, più compiutamente, all'interno dell'illustre dibattito

[1] J.H.H. Weiler, *Diritti umani, costituzionalismo ed integrazione: iconografia e feticismo*, in *Quad. Cost.*, 2002, 526.

sulla Costituzione europea e sulla necessità di approvare un catalogo dei diritti europei all'interno di tale documento[2]. Accantonato, come noto, il sogno di redigere una Costituzione in senso tecnico-formale, la Carta dei diritti è confluita nel 2009 nel Trattato di Lisbona diventando a tutti gli effetti diritto primario dell'Unione europea.

La dottrina si è a lungo interrogata sulla portata di tale novità nel contesto del costituzionalismo europeo. Già all'inizio degli anni duemila, in piena fase "costituente", Von Bogdandy rifletteva sulla opportunità che l'Unione europea fosse, o dovesse in futuro diventare, una organizzazione finalizzata alla difesa dei diritti umani[3]. Il dibattito dottrinale che è seguito ha affrontato il tema soprattutto partendo da tale fondamentale questione, indagando cioè le problematiche relative alla predisposizione di un *Bill of Rights* europeo nel quadro degli equilibri del diritto comunitario e, ancor di più, come pilastro del processo di costituzionalizzazione dell'Unione. Questa prospettiva trovava la sua giustificazione nelle conclusioni dei Consigli europei di Colonia e di Tampere del 1999, dove i governi europei avevano indicato tra i principali obiettivi della Unione «l'esigenza di *avvicinare ai cittadini* al sistema giuridico europeo, *rendendo più visibili i diritti* in esso garantiti e codificandoli in una apposita Carta»[4].

Si coglie, in queste parole, tutta la portata "costituzionale" di un documento volto a trasformare quella che per molti decenni è stata percepita una Comunità economica in una nuova Unione finalmente orientata alla tutela dei diritti. Tale obiettivo è stato salutato in termini sostanzialmente positivi dalla dottrina, che ha prevalentemente focalizzato i suoi studi sulle potenzialità della Carta di accelerare la nascita di un *ethos* costituzionale europeo finalizzato al riconoscimento di valori universali (e forse identitari[5]) comuni che favorissero lo sviluppo di una Unione sempre più stretta tra popoli. Non che gli studiosi non si siano interrogati in profondità anche sull'effetto di tale documento rispetto agli ordinamenti nazionali; come ricordato da Grimm, «nella misura in cui la Carta va considerata come vigente, non è possibile che non subentrino ripercussioni sulle costituzioni nazionali» perché «se le diverse sfere fossero accuratamente separate si avrebbe la situazione per cui, ad esempio in Germania, sarebbero in vigore quattro diversi cataloghi dei diritti per ogni cittadino: i diritti fondamentali garantiti dalla Costituzione del *Land*, quelli sanciti dal *Grungesetz*, quelli dell'Unione europea e

[2] Si veda, in particolare, il dibattito tra Habermas, Grimm e Weiler raccolto in G. Zagrebelsky, *Diritti e costituzione nell'Unione europea*, Roma-Bari, 2003.

[3] A. Von Bogdandy, *The European Union as a human rights organization? Human rights and the core of the European Union*, 37 CML Rev., 2000, 1307-1338.

[4] M. Olivetti, *Verso la Costituzione europea*, in *Proposta Educativa*,n. 1/2004, 23.

[5] Come ricordato da J.H.H. Weiler, *Diritti umani, costituzionalismo ed integrazione: iconografia e feticismo*, cit., 527 «agli occhi dei promotori della Carta, era molto importante la questione della percezione e dell'identità. Fin da Maastricht, la legittimazione politica della costruzione europea ha rappresentato una questione vitale (…) Una Carta, dicono i suoi sostenitori, renderà visibile ed immediatamente identificabile ciò che fino ad ora era conosciuto solo da polverosi avvocati. Inoltre, la Carta, in quanto simbolo importante, potrà controbilanciare l'Euro e diventare parte dell'iconografia dell'integrazione europea e contribuire sia all'identità che all'identificazione con l'Europa».

quelli della Convenzione europea dei diritti dell'uomo»[6]. Tuttavia, tale riflessione si è articolata per lo più attorno alla interazione tra le diverse giurisdizioni chiamate a tutelare i diritti e, dunque, sulle conseguenze prodotte dalla codificazione dei diritti sul sistema comunitario multilivello[7]. Lo stesso Grimm, del resto, aveva notato a riguardo come «non sussista in effetti una ripercussione immediata della Carta sulle costituzioni nazionali» in quanto essa «non prevede modifiche in merito al raggio di azione della giustizia costituzionale» e che pertanto – sebbene sia ragionevole pensare che la Carta favorisca in qualche misura «processi di adattamento» nell'interpretazione dei diritti – essa non pareva destinata a diventare parte costitutiva di una «una super-costituzione europea»[8].

Prendendo le mosse da questo angolo prospettico, la dottrina ha concentrato la sua attenzione sulla applicazione dei diritti ai cittadini europei, ma ha lasciato sullo sfondo la questione federale, ovverosia l'impatto per così dire strutturale che l'introduzione di una Carta dei diritti sempre genera sulla ripartizione verticale dei poteri, e dunque – nello specifico – su quello che è stato definito «lo speciale federalismo europeo»[9]. Sebbene l'Unione europea non possa essere infatti tecnicamente descritta con i tratti di un sistema federale compiuto, non vi è dubbio che il processo di integrazione europea possieda le caratteristiche di un processo federativo in cui, costantemente, le cessioni di sovranità degli Stati membri ne definiscono i concreti contorni.

Tale impatto "strutturale" emerge in modo significativo soprattutto se si volge lo sguardo, in ottica comparata, al ruolo storicamente occupato dal *Bill of Rights* nel sistema federale americano; come messo in luce da Akhil Amar, l'introduzione dei primi dieci emendamenti della Costituzione americana in un momento successivo a quello della sua approvazione aveva lo scopo di limitare l'ingerenza del Governo federale, preservando – nel campo dei diritti fondamentali – quella naturale propensione delle ex colonie a regolare autonomamente ambiti anche molto ampi[10]. Il dibattito sull'introduzione del *Bill of Rights* nella Costituzione americana, del resto, è stato profondamente condizionato dalla

[6] D. Grimm, *Il significato della stesura di un catalogo europeo dei diritti fondamentali nell'ottica della critica dell'ipotesi di Costituzione europea*, in G. Zagrebelsky , *Diritti e costituzione nell'Unione europea*, Laterza, Roma-Bari, 2003, 12.

[7] Così, ad esempio. T. Groppi, *The Bill of Rights in the European Constitution and the New World Constitutionalism*, relazione a *VII World Congress Of IACL*, 11 giugno 2007, 2 in citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.492.9519&rep=rep1&type=pdf, : «what reason can there be for drawing up a charter of rights if it is not justified, as often occurs at both national and international level, by the necessity to reverse a situation characterised by the widespread violation of fundamental rights, and if doing so will not change anything in relation to the previous situation (in contrast to the case of the ECHR and many national constitutions)? Secondly, what are the consequences for the Community system of setting norms on fundamental rights in writing?».

[8] D. Grimm, *Il significato della stesura di un catalogo europeo dei diritti fondamentali nell'ottica della critica dell'ipotesi di Costituzione europea*, in G. Zagrebelsky, *Diritti e costituzione nell'Unione europea*, Roma-Bari, 2003, 13.

[9] G. Bognetti, *Lo speciale federalismo europeo*, in *Modelli giuridici ed economici per la Costituzione europea*, a cura di A.M. Petroni, Bologna, 2001, 245.

[10] A.R. Amar, *The Bill of Rights. Creation and Reconstruction*, Yale University Press, 1998, passim.

preoccupazione dei cittadini delle colonie di non perdere quelle libertà appena sottratte al sovrano inglese a vantaggio del Governo federale, al punto da mettere in dubbio la stessa utilità di un catalogo di libertà individuali. Per queste ragioni, il *Bill of Rights* americano fu «solidamente fondato sulla teoria del federalismo»[11] e la sua approvazione non fu orientata al solo fine di «limitare i poteri statali, ma a limitare il potere legislativo della federazione che, nella sua attività normativa, sarebbe stata costretta, da quel momento in poi, a rispettare il catalogo dei diritti appena approvato»[12].

Questo scopo originale è poi mutato nel corso della storia costituzionale americana per effetto della approvazione del XIV Emendamento e della relativa dottrina della incorporation, che ha esteso l'applicazione del *Bill of Rights* anche all'interno degli Stati, e della conseguente investitura della Corte suprema quale «guardiano dei diritti individuali»[13]. Ma, allo stesso tempo, la riflessione teorica dei Framers sui limiti federali dei diritti è rimasta radicata nello spirito del costituzionalismo americano, e la separazione verticale dei poteri costituisce ancora oggi, in qualche misura, un freno al livello di governo federale.

La storia costituzionale europea non mostra, sotto il profilo teorico, la stessa attenzione inizialmente riservata dai *Framers* americani alla portata "federale" del *Bill of rights*. Molte sono le ragioni che giustificano questa sostanziale differenza. In primo luogo, l'Unione europea non è una federazione, ma opera piuttosto come «ordinamento di nuovo genere nella storia del diritto internazionale»[14] a favore del quale gli Stati membri hanno rinunciato (e continuano a rinunciare) a porzioni più o meno ampie della propria sovranità in aree o settori determinati. Non è un mistero che le stesse parole "federalismo" o "federazione" furono a lungo evitate nei lavori intergovernativi europei a causa del timore da esse suscitato ad esempio nel governo britannico, che, nel suo storico euroscetticismo, vedeva in tali termini il rischio di un rafforzamento troppo significativo delle competenze comunitarie sulla scorta del sistema federale tedesco. È anche per questa ragione che, probabilmente, nell'art. 1 del Trattato costituzionale discusso dalla Convenzione europea nel 2002 le parole «*federal* way» della bozza iniziale furono sostituite da quelle meno impegnative di «*Community* way»[15].

[11] K.T. Lash, *Commentary on Akhir Reed Amar's the Bill of Rights: Creation and Reconstruction of two Movements of Constitutional Symphony*, in U. Rich. L. Rev., 1999, 488.
[12] C. Bologna, *Stato federale e "national interest". Le istanze unitarie nell'esperienza statunitense*, Bologna, 2010, 61.
[13] W.J. Brennan, *The Bill of Rights and the States: The Revival of State Constitutions as Guardians of Individual Rights*, 61 N.Y.U. L. Rev. 536, 543 (1986). Come noto, la trasformazione degli obiettivi del federalismo americano, e del contestuale ruolo della Corte suprema, ha avuto luogo, in particolare, con la stagione dei Diritti Civili e il conseguente attivismo giudiziale della Corte Warren (1954-1969) che, attraverso un utilizzo creativo delle clausole costituzionali contenute nel XIV Emendamento, ha stravolto il tradizionale impianto federale duale al punto che, come osservato da Ricker nel 1964 e riportato da R.A. Shapiro, *Polyphonic Federalism. Toward the Protection of Fundamental Rights*, Chicago-London, 2009, 46 «se negli Stati Uniti una persona oggi disapprova il razzismo, allora dovrebbe disapprovare anche il federalismo».
[14] Così la sentenza della Corte di Giustizia *Van Gen den Loos*, caso C- 26/62, 1963.
[15] In particolare: «The Union [...] shall exercise in the federal way [sur le mode fédéra] the competences they confer on it». This wording was later changed into «The Union [...] shall

In secondo luogo, il progetto ideale che ha spinto i costituenti europei ad immaginare un'Unione sempre più stretta tra i popoli europei appare profondamente diverso da quello che aveva mosso i *Framers* americani; mentre questi ultimi guardavano con un certo sospetto la nascita di una nuova sovranità federale, la cessione di competenze statali a favore di un organismo sovranazionale ha rappresentato il principale mezzo con cui i funzionalisti europei hanno perseguito l'ideale della pace nel loro continente. Prendendo a prestito le categorie di Smith, insomma, se la Costituzione americana nasce dallo scontro con un nemico *esterno* (la monarchia inglese) e si pone come scopo quello di limitare il potere del futuro "sovrano" federale, la Comunità europea si sviluppa invece in opposizione ad un nemico *interno*, ponendosi come argine ai nazionalismi degli Stati membri o, quanto meno, alla loro manifestazione belligerante. Anche per questa ragione, non è possibile sovrapporre acriticamente l'esperienza dei due processi "federativi", che nascono e si sviluppano seguendo ideali e tecniche giuridiche anche profondamente diverse e lontane tra loro.

Allo stesso tempo, però, come avvenuto negli Stati Uniti, anche il sistema europeo non ha previsto fin dall'origine un catalogo di diritti quale fondamento del proprio ordinamento costituzionale. Per molti anni, i diritti garantiti ai cittadini europei sono stati di volta in volta introdotti dalla legislazione europea, o ricostruiti giudiziariamente attraverso il confronto tra la Corte di Giustizia e i giudici nazionali[16]. In un lento ma costante processo di aggiornamento, le istituzioni europee e quelle nazionali hanno lavorato insieme per integrare le diverse discipline riservate ai diritti all'interno del continente europeo, prevedendone specifiche modalità di armonizzazione. Tuttavia, l'ambito di applicazione dei diritti europei è rimasto, a lungo – almeno formalmente – confinato dal principio di attribuzione delle competenze, secondo il quale l'Unione agisce solo negli ambiti che le sono espressamente riservati dal Trattato.

L'introduzione della Carta nel testo dei Trattati ha riaperto il dibattito sulla applicazione e sull'adattamento multidimensionale dei diritti in Europa. Spostando la tutela dei diritti dal piano del diritto secondario a quello primario, tale documento ha assunto una portata para-costituzionale che inevitabilmente incide sull'equilibrio federale tra centro e periferia. Gli articoli 51 e 53 hanno provato a definire i limiti "federali" della Carta, stabilendo rispettivamente che le disposizioni ivi contenute si applicano agli Stati membri «esclusivamente nell'attuazione del diritto dell'Unione»[17], e non possono essere interpretate in modo limitativo o lesivo «dei

exercise in the Community way [sur le mode communautaire] the competences they confer on it». Cfr. J. Ziller, *Separation of Powers in the European Union's Intertwined System of Government A Treaty Based Analysis for the Use of Political Scientists and Constitutional Lawyers*, in *Il Politico*, 2008, 135 ss.

[16] Come noto, un ruolo fondamentale in questo processo è stato riservato dai giudici comunitari, che hanno svolto la funzione di veri e propri motori dell'integrazione, ampliando in modo determinante la portata del diritto europeo anche attraverso l'introduzione di principi para-federali quali quello dell'effetto diretto e della supremazia del diritto comunitario che costituiscono, ancora oggi, i pilastri giuridici su cui si regge l'ordinamento costituzionale europeo.

[17] Così art. 51: "Le disposizioni della presente Carta si applicano alle istituzioni e agli organi dell'Unione nel rispetto del principio di sussidiarietà come pure agli Stati membri

diritti dell'uomo e delle libertà fondamentali riconosciuti (…) dalle costituzioni nazionali»[18]. Tali previsioni appaiono però troppo vaghe per chiarire i confini della Carta e per contenerne gli effetti centripeti[19], soprattutto se si considera che la loro interpretazione è interamente demandata alla Corte di Giustizia, ovverosia ad un giudice che, tradizionalmente, ha mostrato una certa inclinazione nel definire in modo estensivo l'ambito e l'applicazione del diritto europeo[20].

In definitiva, dunque, l'introduzione di un *Bill of Rights* all'interno di un processo federale ha sempre l'effetto di "centralizzare" la tutela dei diritti anche in ragione della portata "universale" di tale documento[21]. Ma mentre l'introduzione dei primi dieci emendamenti nella Costituzione americana è stata controbilanciata da una solida teoria federale volta in qualche misura a contenerne gli effetti centripeti, l'introduzione della Carta di Nizza nei Trattati europei non è stata accompagnata da una struttura costituzionale di separazione dei poteri, e pare piuttosto orientata a «dare visibilità» ai diritti ivi contenuti per «rafforzarne la tutela alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi

esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti rispettano i diritti, osservano i principi e ne promuovono l'applicazione secondo le rispettive competenze".

[18] Art. 53: «Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti, nel rispettivo ambito di applicazione, dal diritto dell'Unione, dal diritto internazionale, dalle convenzioni internazionali delle quali l'Unione, la Comunità o tutti gli Stati membri sono parti contraenti, in particolare la convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, e dalle costituzioni degli Stati membri».

[19] Così A. Torrez Perez, *The federalizing force of the EU Charter of Fundamental Rights*, I•CON Vol. 15 No. 4, 2017, 1082 rispetto alla formulazione dell'art. 51 «The vagueness of what it means to "implement" EU law coupled with the porous division in the allocation of powers between the EU and the Member States makes the boundaries of the Charter uncertain. Moreover, the approach to the scope of application of the Charter from the federal perspective is coming under stress by the claims for protection from EU citizens differently situated with regard to EU law». Cfr. anche D. Sarmiento, *Who's Afraid of the Charter? The Court of Justice, National Courts and the New Framework of Fundamental Rights Protection in Europe*, 50 Common Mkt. L. Rev., 2013, 1270.

[20] In riferimento alla tradizionale propensione della Corte di Giustizia ad estendere le competenze comunitarie tramite l'interpretazione del diritto europeo cfr. (per tutti) J.H.H. Weiler, M. Cartabia, *L'Italia in Europa*, il Mulino, 2000, che descrive questo fenomeno attraverso i principi dell'assorbimento, della estensione, della incorporazione e della espansione delle competenze comunitarie. L'esito di tale processo è che, già negli anni '80, «il principio dei poteri enumerati quale limite della competenza materiale della Comunità (in assenza di ogni revisione del trattato) viene eroso dal punto di vista sostanziale fino a sparire virtualmente nella pratica. (…) Come sostiene il giudice Lenaerts, eminente autorità in materia, valutando la situazione in cui versa oggi la Comunità, "semplicemente non vi è più alcun nucleo di sovranità che gli Stati membri possano invocare, come tale, contro l'azione della Comunità"».

[21] Come ricordato da T. Groppi, *The Bill of Rights in the European Constitution and the New World Constitutionalism*, cit., 13 «the experience of federal states shows how the enactment of a charter of rights usually works in a centripetal manner, augmenting the competences of the federation. This has occurred in the USA, where the application of the first ten amendments has been extended to all states (albeit as the consequence of an event as serious as the Civil War), and in Canada, where the fears voiced by the Provinces when the Canadian Charter of Rights was included in the Constitution appear to have been fully confirmed by the jurisprudence of the Supreme Court: as the Charter's main supporter Prime Minister Pierre Trudeau had hoped, the Charter has effectively acted as an instrument for the creation of a "Canadian identity"».

scientifici e tecnologici»[22].

È in questa prospettiva che occorre allora riformulare la domanda con cui Weiler aveva commentato la redazione della Carta; trascorsi dieci anni dalla sua introduzione nei Trattati europei, occorre cioè domandarsi non più solo se essa abbia concorso ad implementare la protezione dei diritti fondamentali, ma anche se e in che modo la sua applicazione abbia inciso sull'equilibrio federale raggiunto dal *Sonderweg* europeo. In definitiva, occorre chiedersi quali sono gli effetti della *federalizing force* della Carta sulla divisione verticale dei poteri in Europa.

2. Un particolare esempio dell'effetto centralizzante della Carta: il diritto alla privacy digitale nell'Unione europea.

Negli ultimi anni, la dottrina si è interrogata sugli effetti "federali" della Carta dei diritti fondamentali a partire da quelle decisioni dalla Corte di giustizia che mostrano un effetto "centralizzante" nella protezione di tali diritti. Come acutamente rilevato da Torres Perez, infatti, la tradizionale propensione della Corte ad estendere le competenze europee unitamente con l'entrata in vigore della Carta «has empowered the CJEU vis-à-vis state courts and state constitutional rights»[23].

Un esempio di tale tendenza è rappresentato dal caso C-617/10 *Akerberg Fransson*, in cui la Corte ha dichiarato, in forza dell'art. 50 della Carta dei diritti fondamentali, la propria competenza a decidere sul ricorso pregiudiziale presentato da un cittadino svedese contro una sanzione amministrativa riguardante un caso di evasione fiscale, intervenendo dunque in una materia – quella tributaria – generalmente riservata alla competenza degli Stati membri. In tale decisione, la Corte di giustizia «ha stabilito che l'applicazione del diritto europeo è messa in gioco ogni qual volta uno stato membro agisca in una materia che è in qualche modo, anche remoto, regolata a livello sovranazionale»; attraverso tale interpretazione i giudici di Lussemburgo hanno esteso l'ambito di applicazione del diritto europeo al punto da «rendere gli stati membri responsabili per le possibili violazioni dei diritti fondamentali dell'UE in praticamente quasi ogni settore»[24].

L'interpretazione estensiva dell'ambito di applicazione dei principi contenuti nella Carta produce però effetti particolari soprattutto quando il diritto che si intende garantire necessita di essere ponderato alla luce di altri diritti, anch'essi di rilievo costituzionale. In questi casi, infatti, la Corte di giustizia è chiamata ad operare alla stregua di un giudice costituzionale, bilanciando i diversi interessi in gioco alla ricerca del giusto equilibrio tra la tutela massima dei diritti individuali della Carta, da una parte, e, dall'altra, la garanzia necessaria degli interessi

[22] Come espressamente previsto dal Preambolo stesso della Carta dei diritti Fondamentali: «A tal fine è necessario rafforzare la tutela dei diritti fondamentali, alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici, rendendo tali diritti più visibili in una Carta».

[23] A. Torrez Perez, *The federalizing force of the EU Charter of Fundamental Rights*, cit., 1081.

[24] F. Fabbrini, *Introduzione al diritto dell'Unione europea*, Il Mulino, 2018, 214.

ISSN: 2037-6677

collettivi dei singoli Stati membri.

Sotto questo profilo, un interessante campo di osservazione degli effetti centripeti prodotti dalla Carta nel sistema federale europeo riguarda il diritto alla privacy digitale e la protezione dei dati personali sanciti dagli artt. 7 e 8. Due, in particolare, sono le ragioni che giustificano la scelta di tale campo di indagine.

In primo luogo, il bilanciamento tra privacy digitale e sicurezza nazionale costituisce una delle sfide più complicate del costituzionalismo contemporaneo. La ragione di ciò è duplice: innanzitutto, lo sviluppo tecnologico ha profondamente inciso sulla vita dei cittadini, cambiando in maniera radicale le loro abitudini relative all'informazione, alla comunicazione e al commercio. La rapidità con cui procede la digitalizzazione delle nostre vite rende particolarmente difficile per il legislatore inquadrare in modo preciso e definitivo il tema della *data protection*, costringendolo ad un continuo aggiornamento normativo che deve stare al passo e per lo più inseguire i cambiamenti tecnologici. Inoltre, la lotta al terrorismo internazionale ha ampliato la portata e i limiti della protezione della privacy, perché l'avvento dell'era digitale ha fornito a tutti (e quindi anche ai terroristi) nuove modalità di comunicazione che, qualora siano utilizzate per fini criminogeni o sovversivi, necessitano di essere preventivamente controllate.

Nel contesto di paura inauguratosi nel nuovo millennio, i governi nazionali hanno così rafforzato i propri meccanismi di sorveglianza digitale al fine di raccogliere in modo generalizzato il maggior numero di informazioni possibili e utilizzarle per prevenire future minacce. Pur perseguendo uno scopo legittimo, il ricorso a tali strumenti di conservazione (*data retention*) e accesso ai dati o metadati ha sollevato fondati dubbi di legittimità quando è stato condotto a partire da sospetti vaghi e generici o, persino, in mancanza di elementi circostanziati[25]. L'avvento dell'era digitale, per questi motivi, ha accresciuto tanto la domanda di privacy quanto, al contempo, quella di sicurezza, alimentando un conflitto tra interessi legittimi che, anche in Europa, è destinato a crescere in modo esponenziale.

La seconda ragione è connessa all'interesse quasi pionieristico mostrato dal continente europeo per la problematica della privacy digitale, che gode di una doppia protezione particolarmente ampia e risalente nel tempo, delineata sia

[25] In particolare, le critiche sollevate rispetto all'utilizzo governativo dei sistemi di sorveglianza di massa riguarda la natura preventiva di tali strumenti. Al fine di combattere il terrorismo internazionale, infatti, i governi utilizzano spesso gli strumenti tipici della lotta alla criminalità, quali le intercettazioni, le ispezioni e le perquisizioni. Ma l'utilizzo delle tecniche digitali di sorveglianza di massa persegue in realtà uno scopo diverso da quello del diritto penale, perché mentre i pubblici ufficiali che indagano sui delitti usano tali strumenti per ricostruire la verità processuale e punire i colpevoli di un fatto già commesso, le indagini terroristiche cercano invece di acquisire in anticipo gli elementi utili a prevenire una minaccia non ancora concretizzatasi e seguono dunque uno schema investigativo che può risultare potenzialmente molto diffuso e invasivo per la privacy dei cittadini. Per questa ragione, i meccanismi di controllo e tutela delle agenzie di sicurezza nazionale sono spesso esercitati a partire da sospetti vaghi e generici, che sollevano più di un dubbio circa la loro legittimità; mentre generalmente nessuno metterebbe mai in dubbio che di fronte a fondati sospetti di attività illegali la polizia possa predisporre un sistema di sorveglianza dell'indagato, le indagini antiterroristiche sono condotte in un terreno dai confini più confusi in cui è più complicato identificare preventivamente standard probatori chiari e definiti.

all'interno della Convenzione europea dei diritti dell'uomo sia dall'ordinamento dell'Unione. Il Consiglio d'Europa, in particolare, ha mostrato una particolare sensibilità per il tema fin dalla predisposizione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108 del 1981) che, nel regolamentare il traffico e la raccolta dei dati digitali, sancisce il diritto dell'individuo di essere informato della conservazione di informazioni che lo riguardano e di chiederne la rettifica. L'Unione, dal canto suo, ha provveduto alla regolamentazione della materia a partire dagli anni '90 con la direttiva 95/46/CE[26]. Adottata il 24 ottobre 1995, tale direttiva fu prevista al fine di armonizzare le numerose leggi approvate dagli Stati membri in materia, favorendo la libertà di circolazione di merci, persone e capitali che, all'epoca, appariva frenata da una disciplina diversificata del trattamento dei dati personali. Fin da subito, pertanto, l'obiettivo dell'Unione europea è stato quello di uniformare a livello sovranazionale le modalità di trattamento dei dati personali, assicurando un alto livello di tutela della privacy digitale. Come ricordato dalla stessa Corte di Giustizia nei casi C-468/10 e C-469/10, «la direttiva 95/46 mira (…) a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. (…) Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità. (…) L'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, sia completa»[27].

L'attenzione mostrata dall'Unione europea per la tutela dei dati personali emerge in modo sintomatico se si confronta la politica europea di protezione della privacy digitale con quella degli Stati Uniti: mentre l'Unione «has long enacted omnibus information privacy laws, the United States has promulgated only sectoral laws (…) regulat[ing] only a specific context of information use»[28]. La parcellizzazione legislativa americana sulla protezione dei dati personali dipende da una pluralità di ragioni ampiamente approfondite – anche in prospettiva comparata – dalla dottrina[29]. Per quel che qui rileva, tale approccio mette in luce

[26] Direttiva 95/46/CE del Parlamento e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[27] CGUE, C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) Federación de Comercio Electrónico y Marketing Directo (FECEMD)*, 24 novembre 2011, p.ti 28 e 29.

[28] Shwarz, *The Value of Privacy Federalism*, in B. Roessler e D. Mokrosinska (eds.), *Social Dimension of Privacy*, Cambridge, 2015, 325-326.

[29] Per una recente analisi comparata tra la tutela dei dati personali in EU e in US cfr. (tra gli altri) P.M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev., 2013, 1966 ss.; P.M. Schwartz e D.J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Calif. L. Rev., 2014, 877 ss.; I. Tourkochoriti, *The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation: In Search For Legal Protection Against Surveillance*, 36 University of Pennsylvania Journal of International Law, 2014, 459 ss.; F. Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the

la sostanziale differenza federale tra il sistema costituzionale americano e quello europeo: mentre nel primo il sistema di protezione della privacy si inserisce all'interno di un sistema duale in cui «legislative power is shared between the federal government and the fifty states [who] played a historically important leadership role in privacy law»[30], lo speciale federalismo europeo si è sviluppato in modo fluido; in un costante processo di integrazione tra i vari livelli, si è così legittimato, soprattutto in questa materia, un intervento "dall'alto" che ha favorito «a high level of harmonization»[31].

Quanto fin qui detto dà ragione del perché il diritto alla privacy digitale costituisca un ambito particolarmente interessante per verificare l'applicazione giurisdizionale della Carta dei diritti e il suo effetto centripeto all'interno dello speciale federalismo europeo. Sotto il profilo generale, questo diritto chiede ai giudici costituzionali di sciogliere un nodo particolarmente intricato bilanciando le ragioni della privacy con quelle della sicurezza nazionale. Sotto il profilo più specificamente europeo, invece, tale materia è da tempo oggetto di interventi legislativi di armonizzazione che hanno di fatto consegnato alle istituzioni europee un ruolo fondamentale nel definire i contorni del diritto costituzionale alla privacy europea.

3. La protezione dei dati digitali come diritto costituzionale europeo

Come già anticipato, la protezione della privacy e dei dati personali all'interno dell'Unione europea gode di una regolamentazione particolarmente articolata e risalente nel tempo. A seguito della approvazione della già ricordata direttiva 95/46/CE, l'Unione ha infatti continuato a disciplinare la materia con interventi specifici che, a partire soprattutto dal nuovo millennio, specificano in modo più puntuale i limiti dell'intervento pubblico nel trattamento dei dati personali dei cittadini europei. Così, ad esempio, l'Unione ha approvato il regolamento n.

LIBE Committee, 2015, in papers.ssrn.com/sol3/papers.cfm?abstract_id=2705618; F. Fabbrini, *The European Court of Justice ruling in the Data retention case and its lessons for privacy and surveillance in the US*, in Harvard Human Rights Journal, 28/2015, 65 ss.; L.P. Vanoni, *Balancing privacy and national security in the global digital era: a comparative perspective of the Eu and US constitutional systems*¸ in L. Violini, A. Baraggia (cur.), *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and non-Judicial Actors*, Elgar Publish, 2018.

[30] P.M. Shwarz, *The Value of Privacy Federalism*, cit., 326-327: «Certain aspects of the structure of US information privacy law can best be understood through reference to American federalism. One classic distinction is between express preemption, where Congress has in explicit terms declared its intention to preclude state regulation in a given area and implied preemption, where Congress, through the structure or objectives of federal law, has impliedly precluded state regulation in the area. Preemption can also take the form of either field preemption or conflict preemption. Field preemption occurs when Congress intended to occupy an entire field of regulation. Conflict preemption takes place where Congress did not necessarily intend complete exclusion of state regulation in a given area, but to block it where a particular state law conflicts directly with federal law, or interferes with the accomplishment of federal objective».

[31] Così B. Petkova, *The Safeguards of Privacy Federalism*, 20 Lewis & Clark L. Rev., 2016, 598: «while EU is not a fully-fledged federation, in the area of data privacy it has opted for a high level of harmonization».

45/2001/CE[32] che estende tale protezione anche al trattamento dei dati personali operato dalle istituzioni e degli organismi dell'UE, o la direttiva 2002/58/CE[33] riguardante la conservazione di dati elettronici. Più di recente, la regolamentazione della privacy europea è affidata al regolamento UE 2016/679[34] che (sostituendo interamente la direttiva 95/46/CE) introduce nel diritto dell'Unione una regolazione generale ed omogenea della materia finalizzata ad assicurare un livello di tutela dei dati coerente ed elevato. Tale provvedimento (unitamente alla direttiva UE 2016/680[35] che regola la protezione dei dati nei settori della cooperazione giudiziaria e di polizia in materia penale) fornisce una nuova pervasiva protezione centralizzata della privacy europea, recependo anche le indicazioni fornite, negli anni, dalla Corte di giustizia e dal Gruppo di lavoro Art. 29.

La centralizzazione del diritto europeo alla privacy è legata a molteplici fattori tra loro interconnessi In parte essa dipende certamente dalla insoddisfazione causata dalla eccessiva frammentazione di una disciplina che, se affidata interamente alla attuazione delle direttive europee da parte degli stati membri, può correre il rischio di costringere le compagnie internazionali a confrontarsi con «twenty-eight different regulatory regimes when seeking to comply with EU privacy law»[36]. Accanto a tali ragioni di natura pratica non deve essere però sottovalutato anche l'impulso centripeto impresso al federalismo europeo dalla adozione del Trattato di Lisbona nonché dalla Carta europea dei diritti fondamentali.

In primo luogo, l'art. 16 del Trattato sul Funzionamento dell'Unione europea regola il diritto fondamentale al trattamento dei dati personali stabilendo le procedure necessarie alla relativa tutela legislativa. Tale disposizione, in particolare, fonda le competenze dell'Unione in materia di protezione dei dati personali statuendo che Parlamento e Consiglio approvano, con procedura ordinaria, misure legislative atte a proteggere i cittadini dall'indebito utilizzo dei loro dati personali operato sia dalle istituzioni europee che dai governi nazionali in quelle materie che rientrano nell'ambito di applicazione del diritto europeo. In

[32] Regolamento CE 45/2001 del Parlamento e del Consiglio Europeo del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.
[33] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).
[34] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
[35] Direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/ GAI del Consiglio.
[36] P.M. Shwarz, *The Value of Privacy Federalism*, cit., 335. Come ricordato dalla stessa Commissione europea a giustificazione della adozione del regolamento, del resto «Heavy criticism has been expressed regarding the current fragmentation of personal data protection in the Union, in particular by economic stakeholders who asked for increased legal certainty and harmonization of the rules on the protection of personal data» (European Commission 2012: 4).

questo senso, l'art. 16 va oltre il mero riconoscimento del diritto alla privacy perché fornisce la base giuridica per l'esercizio delle funzioni europee. Esso opera, infatti, in combinato disposto con tutte le competenze europee e, in particolar modo, in relazione alle disposizioni sul mercato interno, la cui creazione ha generato – unitamente all'avvento dell'era digitale – la trasmissione costante di dati e informazioni digitali. Fondando la base giuridica del trattamento europeo dei dati sul riconoscimento di una libertà fondamentale, inoltre, l'art. 16 chiarisce che «laddove il conflitto tra tutela della riservatezza e circolazione dei dati personali non consenta di trovare un punto di equilibrio (…) dovrà prevalere la prima»[37].

La novità più rilevante in materia di privacy digitale si registra però con l'entrata in vigore della Carta dei diritti fondamentali, con particolare riferimento agli artt. 7 e 8. Per tal via si offre una tutela para-costituzionale a tale libertà all'interno dello spazio giuridico dell'Unione affermando, in termini generali, il diritto di «ogni individuo» al rispetto «della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni» (art. 7), e riconoscendo in modo specifico la protezione dei dati personali che devono essere trattati «secondo il principio di lealtà e per finalità determinate» solo previo «consenso della persona interessata», la quale ha «il diritto di accedere ai dati che lo riguardano al fine di ottenerne la rettifica» (art. 8).

Come emerge dallo stesso tenore letterale delle disposizioni, l'art. 8 sancisce un diritto autonomo rispetto a quello garantito dall'art. 7 del quale costituisce però una specificazione, regolando la protezione della riservatezza individuale anche rispetto alle sfide dell'era digitale. Sotto questo profilo, l'art. 8 può essere letto come una applicazione del principio generale previsto dal Preambolo della Carta, secondo cui la tutela dei diritti fondamentali deve essere garantita «alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici»[38].

Si aggiunga poi che le norme contenute negli artt. 7 e 8 della Carta possono essere lette congiuntamente alla protezione della vita privata garantita dall'art. 8 della Convenzione europea dei diritti dell'uomo; pur appartenendo a due sistemi distinti di protezione della libertà dei cittadini, tali misure interagiscono tra loro mediante le disposizioni contenute nell'art. 53 della Carta. La stessa Corte di Giustizia ha più volte ricordato come «da un lato il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta, sia riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile» (come già riconosciuto dalla Corte europea dei diritti dell'uomo[39]) «e dall'altro che le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle

[37] B. Cortese, *Protezione dei dati di carattere personale nel diritto dell'Unione europea*, in *Diritto dell'Unione Europea*, 2013, n. 2, 316.
[38] Così il preambolo della Carta dei diritti fondamentali 2012/C 326/02.
[39] V., ad esempio, Corte EDU, A*mann c. Svizzera* del 16 febbraio 2000, e *Rotaru c. Romania* del 4 maggio 2000.

tollerate nell'ambito dell'art. 8 della CEDU»[40].

In definitiva, dunque, la Carta ha introdotto importanti garanzie all'interno del sistema europeo che sono poste a fondamento del più ampio ed articolato sistema di *data protection* già regolato dalla legislazione secondaria. In questa prospettiva, la Carta dei diritti fondamentali disegna «una struttura omnicomprensiva inclusiva di tutte le politiche europee (…)»; le sue norme, inoltre, «elevano le garanzie ivi contenute al livello della legislazione primaria» rafforzandone la protezione e «creando un effetto diretto nei confronti dei cittadini»[41], in ottemperanza a quanto stabilito dall'art. 6 TUE[42].

Le potenzialità insite nell'inserimento del diritto alla privacy digitale all'interno di un vero e proprio *Bill of Rights* sono significative. Già in sede di approvazione della Carta la dottrina più attenta aveva osservato come la codificazione delle libertà in tale documento para-costituzionale avrebbe consentito di orientare l'interpretazione dei giudici nella applicazione del diritto comunitario: «l'obbligo di interpretazione conforme costituisce uno degli effetti "strutturali" della norma comunitaria che consente assieme allo strumento più "invasivo" dell'efficacia diretta, l'adeguamento del diritto interno ai contenuti e agli obbiettivi dell'ordinamento comunitario», per cui se tale obbligo si impone per ogni norma di diritto comunitario a prescindere dalla diretta applicabilità, questa è la strada maestra per consentire ai giudici una applicazione «più vincolante della Carta di Nizza»[43]. Con l'entrata in vigore della Carta, tale lettura si è chiaramente fortificata; l'introduzione della privacy all'interno del *Bill of Rights* europeo ha consentito ai giudici europei di mutare il proprio *legal reasoning*, che risulta oggi rafforzato da parametri interpretativi capaci di favorire una rivisitazione «costituzionalmente orientata» dell'intera disciplina[44].

4. Privacy europea vs. sicurezza nazionale: il nodo delle competenze nello speciale federalismo europeo

Pur evidenziando numerose disposizioni che garantiscono, regolano e tutelano la privacy dei cittadini europei, il sistema della *data protection* nell'Unione non è tuttavia illimitato, e «contiene un certo numero di debolezze e deroghe che finiscono con il diluire la capacità del diritto europeo di proteggere concretamente

[40] Corte di Giustizia, 9 novembre 2010, C-92/09 e C-93/09, *Volker und Markus Schecke and Eifert*, par. 52.
[41] F. Boehm, *A comparison between US and EU data protection legislation for law enforcement purposes*, Study for Libe Comettee www.europarl.europa.eu/, 2015, 16.
[42] Tale articolo, come noto, «riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000 (…) che ha lo stesso valore giuridico dei trattati».
[43] Così A. Celotto, *Giudici nazionali e carta di Nizza: Disapplicazione o interpretazione conforme?*, in R. Bifulco, M. Cartabia, A. Celotto (cur.), *L'Europa dei diritti. Commento alla Carta dei diritti dell'Unione europea*, Bologna, 2001, 43.
[44] Cfr. O. Pollicino e M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta, V. Zeno-Zencovich (cur.), *La protezione transnazionale dei dati personali*, Roma, 2016, 75 ss.

tale diritto»[45].

Necessariamente, il diritto alla privacy subisce le compressioni relative al bilanciamento con altri diritti. Così, ad esempio, la tutela dei dati personali trova un primo naturale limite nella disposizione contenuta nell'art. 11 della Carta europea in cui si sancisce «la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche». Il bilanciamento tra questi due diritti è espressamente regolato dalla normativa europea; l'art. 85 del regolamento UE 2016/679 sancisce, ad esempio, la possibilità per gli Stati membri di prevedere «deroghe ed eccezioni» alle regole comunitarie ove queste siano necessarie «per conciliare il diritto alla protezione dei dati personali e la libertà di espressione e di informazione». In modo analogo, la *data protection* europea si scontra altresì con le esigenze legate al libero scambio delle merci e dei servizi che, soprattutto a seguito della digitalizzazione del c.d. e-commerce, implica la trasmissione di moltissimi dati digitali dei consumatori a beneficio di aziende ed operatori digitali; a questo fine, il già menzionato regolamento dedica numerose disposizioni al trattamento dei dati da parte delle imprese, disciplinando le «nuove sfide» riguardanti il diritto alla privacy in connessione al consistente «aumento dei flussi di dati personali da paesi al di fuori dell'Unione e organizzazioni internazionali» necessario alla «espansione del commercio internazionale»[46].

Tra i molti limiti legati al bilanciamento tra *data protection* ed altri diritti/interessi, un posto di rilievo è riservato alla tutela sicurezza nazionale; quest'ultima entra inevitabilmente in collisione con il diritto alla privacy ogni volta che la sicurezza è tutelata attraverso sofisticati programmi di sorveglianza di massa effettuata tramite la raccolta e l'immagazzinamento dei dati digitali, i quali costituiscono peraltro il principale e più diffuso strumento di prevenzione e lotta al terrorismo internazionale. La particolare rilevanza di tale limite è legata al fatto che, oltre a riguardare un rapporto tra due diritti tra loro direttamente confliggenti, esso si colloca a cavallo di competenze attribuite a due livelli di governo differenti, dando origine ad un bilanciamento che si potrebbe qualificare come asimmetrico.

Per apprezzare pienamente questa peculiarità europea, si può provare a guardarla in controluce rispetto alla disciplina americana. Negli Stati Uniti, alla disciplina frammentata in materia di privacy si accompagna una attribuzione delle competenze al governo federale in materia di sicurezza nazionale, sancite – nel corso del Novecento e, in particolare, a partire dal secondo conflitto mondiale – da numerose leggi federali quali, per primo, il National Security Act del 1947. Allo stesso tempo, però, nella tradizione costituzionale americana il termine "security" (che è oggi prevalentemente usato come sinonimo di *national* o *homeland security*) comprende anche il diritto dei cittadini di essere protetti (*to be secure*) dagli abusi del potere governativo, garantito dal IV emendamento della Costituzione[47]. Per

[45] D. Cole, F. Fabbrini, *Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders*, in «I-CON» 2016, Vol. 14, n.1, 225.

[46] Così il regolamento UE 2016/679, 101 considerando.

[47] La Costituzione americana ammette limitazioni al diritto alla riservatezza solo nel caso in cui vengano rispettate le disposizioni contenute nel IV emendamento: «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».

questa ragione, il sistema costituzionale americano chiede governo di risolvere il conflitto tra *personal* e *national* security originato, dai programmi di sorveglianza di massa posti in essere dalla National Security Agency operando un bilanciamento che è interamente svolto a livello federale.

La simmetria americana tra personal e national security non trova riscontro nell'ordinamento federale europeo. Sebbene l'Unione abbia tentato di adottare una serie di misure legislative volte ad armonizzare le legislazioni nazionali in materia di politica estera e difesa comune[48], la tutela della sicurezza nazionale è oggi interamente affidata alla disciplina degli Stati, finanche costituendo una competenza rafforzata dalle disposizioni dell'art. 4(2) TUE che, dopo aver elencato le funzioni essenziali degli Stati membri, indica «in particolare» tale materia come una «competenza esclusiva» riservata ad essi[49].

Il riconoscimento esplicito di tale competenza esclusiva porta ovviamente con sé uno spettro di ricadute pratiche sulla legislazione europea della privacy che riconosce limiti espressi nell'applicazione delle sue norme di fronte a problematiche connesse alla sicurezza nazionale degli Stati. Già la direttiva 95/46/CE ammetteva tra le eccezioni ad una piena armonizzazione della tutela del trattamento dei dati nazionali tutte quelle misure legislative necessarie ai fini della pubblica sicurezza o della difesa dello stato[50] e deroghe analoghe sono disciplinate oggi anche dal regolamento UE 2016/679[51].

Ulteriori eccezioni al diritto alla privacy digitale dei cittadini europei sono inoltre previste da disposizioni normative specifiche. Così, ad esempio, il Parlamento europeo ha approvato la direttiva *Data Retention* (2006/24/CE)[52] che consente agli Stati membri di immagazzinare i metadati telefonici e telematici per finalità riguardanti la pubblica sicurezza e la prevenzione della criminalità e del terrorismo internazionale. Sotto questo profilo, la direttiva 2006/24/CE costituisce l'esemplificazione normativa di un «rovesciamento della strategia politica europea» che segna una «significativa inversione di tendenza» dell'azione comunitaria in materia, caratterizzata dal passaggio «dalla *protection* alla *retention* dei metadata» e da un «revirement securitario che dal 2002, e in modo più marcato dal 2006, pare connotare l'azione dell'Unione europea»[53]. D'altro canto, tuttavia, tale direttiva (che come vedremo in seguito è stata invalidata dalla Corte di Giustizia) fu adottata dalle autorità europee in risposta agli attentati di Madrid e Londra del 2005, e testimonia il tentativo dell'Unione di definire un nuovo

[48] Cfr. (tra gli altri) V. Mitsilegas. J. Monar, W. Rees, *The European Union And Internal Security*, New York, 2003.

[49] Così l'art. 4(2) TUE: «L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro».

[50] Cfr. art. 13 della direttiva 95/46/CE «qualora tale restrizione costituisca una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza (…)».

[51] Cfr. infra par. 8.

[52] 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.

[53] A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *DPCE*, 2015, 1224 ss.

bilanciamento tra la protezione della privacy digitale dei cittadini europei, da un lato, e l'esigenza di fornire ai servizi di intelligence delle nazioni europee efficaci strumenti di lotta al terrorismo internazionale, dall'altro. A prescindere dalla lettura che si voglia dare a tale atto normativo, esso – e la successiva pronuncia della Corte di Giustizia che l'ha resa invalida – rappresentano bene lo scontro tra privacy e security che coinvolge ormai tutte le nostre democrazie.

La ricaduta pratica più significativa connessa al riconoscimento della competenza esclusiva in materia di sicurezza nazionale si registra però sul piano del diritto interno. Soprattutto a seguito degli attentati terroristici di inizio millennio, infatti, i paesi europei si sono dotati di atti normativi specifici volti a rafforzare le disposizioni di sicurezza all'interno del loro territorio, anche a costo di comprimere i diritti garantiti dalle loro Costituzioni. Oltre ad aprire problematiche generali connesse al diritto costituzionale alla sicurezza[54], tali normative incidono in modo significativo proprio sul trattamento dei dati personali, disponendo sofisticati meccanismi di raccolta capillare dei metadati elettronici o digitali dei loro cittadini e obbligando gli operatori a conservarli per un periodo più o meno esteso di tempo e a trasmetterli, su richiesta, ai servizi di intelligence[55].

L'asimmetria tra la competenza in materia di privacy e quella sulla sicurezza nazionale produce così il seguente paradosso federale: i diritti europei alla privacy e alla protezione dei dati personali – pur sanciti in modo "quanto più uniforme" a livello comunitario già a partire dal 1995 – entrano in conflitto con le misure di *data retention* previste dalle *laws of fear* nazionali[56]. Ciò vale non solo per la disciplina stabilita dal diritto europeo secondario, ma anche per l'applicazione delle disposizioni contenute nella Carta dei diritti fondamentali: rientrando nelle competenze degli Stati membri, le *laws of fear* non sono direttamente sottoposte all'applicazione degli art. 7 e 8 che, come precisato dall'art. 51 della Carta, «si applicano alle istituzioni europee e ai [suoi] organi», mentre gli Stati membri sono tenuti a rispettarli «esclusivamente nell'attuazione del diritto dell'Unione».

Per effetto del principio di attribuzione di competenze, pertanto, la protezione effettiva dei cittadini europei dalle investigazioni elettroniche risulta affidata più alla legislazione domestica che a quella europea. Il risultato,

[54] Cfr. T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in *Forum Quad. Cost.*, 2006 www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/440.pdf

[55] Molte sono le disposizioni degli Stati europei in materia. la Francia ha adottato il *Décret n. 2015-125 du 5 février 2015* e la *Loi sur le renseignement* (19/3/2015) che consente una raccolta capillare dei metadati e del contenuto delle conversazioni telefoniche, obbligando gli operatori a conservarli per un periodo indeterminato di tempo e a trasmetterli, su richiesta, ai servizi di intelligence. Anche il Regno Unito è da tempo attivo in questo campo, come testimonia la severa politica avviata dal *Regulation of Investigatory Power Act* (2000) e dell'*Anti-terrorism, Crime and Security Act* (2001), e recentemente rafforzata dalle disposizioni contenute nel *Counter-Terrorism and Security Act* (2015), che ha introdotto nuove disposizioni sulla sicurezza, tra cui restrizioni di viaggio per le persone sospettate di coinvolgimento in attività connesse al terrorismo. In Italia, infine, la legge 17 aprile 2015 di conversione del decreto legge 7/2015 recante misure urgenti per il contrasto al terrorismo ha suscitato il biasimo dell'autorità garante per la privacy, che ha espresso la sua preoccupazione in particolare per l'art. 7 della legge che porta a 2 anni il termine di conservazione dei dati di traffico telematico ai fini di indagini. In riferimento a tale legislazione in prospettiva comparata, v. (tra gli altri) D. Cole – F. Fabbrini – A. Vedaschi (eds), *Secrecy, national security and the vindication of constitutional law*, Edward Elgar Publishing, 2014; G. De Minico, *Le libertà fondamentali in tempo di ordinario terrorismo*, in «Federalismi.it», 2015, n. 10, 2-28.

[56] In riferimento a tale definizione, v. per primo C.R. Sunstein, *Laws of Fear*, Cambridge University Press, 2005.

paradossale, è che, pur oggetto di una disciplina specifica sempre più centralizzata e costituzionalizzata all'interno della Carta, i diritti europei alla privacy e alla protezione dei dati digitali rischiano oggi di essere sempre più soggetti a specifiche ma sostanziali deroghe nazionali. Tale paradosso è, come vedremo, proprio all'origine dei numerosi conflitti sollevati di fronte ai giudici nazionali per la corretta interpretazione del diritto europeo alla privacy, e dei conseguenti ricorsi pregiudiziali alla Corte di Giustizia. In sostanza, quindi, l'asimmetria federale tra le competenze in materia di privacy e di sicurezza nazionale ha accresciuto il contenzioso all'interno degli Stati membri e, con esso, il compito della Corte di Giustizia di «final and most important decision-makers in interpreting the new EU law of privacy»[57].

5. Il diritto alla privacy digitale di fronte alla Corte di giustizia: la *data protection saga*

Le considerazioni che precedono spiegano le difficoltà strutturali a cui i giudici europei sono oggi chiamati nel definire gli ambiti e i limiti del diritto europeo alla privacy digitale. Da un lato, la centralizzazione della disciplina derivante (anche) dalla entrata in vigore della Carta ha rafforzato i giudici nell'assunto ruolo di interpreti dei Trattati. Dall'altro, il combinato disposto tra art. 4 TUE e art. 51 della Carta delimita l'ambito di decisione dei giudici quando la tutela degli artt. 7 e 8 si scontra con i programmi di raccolta dei dati per finalità connesse alla sicurezza nazionale. In altri termini, nel bilanciamento tra diritti/interessi si ripropone, a livello giudiziale, il paradosso federale già ricordato in precedenza.

Nell'affrontare queste difficoltà, la Corte di Giustizia ha assunto dapprima un atteggiamento prudente, evitando cioè di pronunciarsi direttamente sulle ipotetiche compressioni di libertà dei cittadini circa il trattamento dei propri dati elettronici e preferendo piuttosto decidere le controversie evidenziando l'erroneo fondamento giuridico degli atti contestati[58]. Tale atteggiamento descrive per lo più «l'approccio esitante della Corte ad affrontare le questioni sostanziali relative alla protezione dei diritti fondamentali prima della entrata in vigore del Trattato

[57] P.M. Shwarz, *The Value of Privacy Federalism*, cit. 339.

[58] Si veda, a riguardo, Corte di Giustizia, C-317/04 e C-318/04, *Parliament v. Council*, in cui la Corte di giustizia si è pronunciata sui ricorsi riguardanti l'applicazione dei c.d. Passenger Name Records (PNR), ovvero di specifici accordi bilaterali – e conseguenti decisioni di adeguatezza della Commissione – che consentivano (e in alcuni casi consentono) il trasferimento dei dati personali dei passeggeri aerei in transito verso o dagli Stati Uniti o dal Canada. Lungamente contestate dalla dottrina (E.A. Rossi, *Recenti sviluppi in tema di diritto alla privacy e alla protezione dei dati personali nello spazio giuridico europeo*, in *Federalismi.it*, 2/2015) ma anche dal Gruppo ex art. 29, tali disposizioni sono state oggetto di pronuncia della Corte di Giustizia anche in riferimento alla ipotetica incompatibilità di tali misure con il livello di protezione dei dati sancito dalla normativa comunitaria. Pur espressamente sollecitati dai ricorrenti a pronunciarsi su tale presunta incompatibilità, i giudici hanno invece preferito risolvere la controversia concentrandosi sulla errata base legale della decisione in oggetto, mantenendo così una certa distanza critica circa la lesione sostanziale del diritto alla privacy europeo (cfr. U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, 2008, 181 ss.). Non dissimile, sotto il profilo della struttura argomentativa, sono le conclusioni del caso C-301/06, *Ireland v. Parliament and Council* con cui la Corte ha respinto un ricorso irlandese presentato per contestare la legittimità della (già menzionata) direttiva 2006/24/CE sulla conservazione dei dati elettronici; anche in questo caso il ragionamento dei giudici si è concentrato sulla scelta del fondamento normativo dell'atto contestato, evitando di pronunciarsi sulla ipotetica compressione delle libertà dei cittadini circa il trattamento dei propri dati elettronici predisposte dalla direttiva.

di Lisbona»[59]; prima del 2009, infatti, la natura non vincolante della Carta, unitamente alle limitate competenze conferite ai giudici europei nelle materie del terzo pilastro dell'Unione, hanno di fatto causato un sostanziale *self restraint* della Corte nei casi in cui essa è stata chiamata a bilanciare la tutela della privacy con gli interessi legati alla sicurezza nazionale.

L'approvazione del Trattato di Lisbona, tuttavia, ha infuso un nuovo coraggio nei giudici europei, agevolando le condizioni per un radicale cambiamento di approccio di questi ultimi nella decisione dei casi loro sottoposti. Tale cambiamento, in particolare, è avvenuto a partire dai casi C-131/12 *Google Spain* (2014)[60] e C-293/12 e C-594/12 *Digital Rights Ireland* (2014)[61] decisi dalla Corte di giustizia a distanza di pochi mesi l'uno dall'altro. Entrambe le decisioni testimoniano in modo esemplare il peso giocato dalla Carta nel bilanciamento operato dai giudici europei tra gli artt. 7 e 8 e altri interessi-diritti con essi confliggenti; se però *Google Spain* risolve il contrasto tra privacy e diritto all'informazione[62], la sentenza *Digital Rights Ireland* affronta, direttamente, il tema qui esaminato del conflitto tra privacy e sicurezza nazionale, e costituisce dunque un punto di partenza irrinunciabile per comprendere la attuazione del diritto alla *data protection* in Europa.

Il caso è noto e ampiamente studiato dalla dottrina[63]: chiamati a pronunciarsi sulla legittimità della direttiva sulla data retention che stabiliva regole di conservazione dei dati digitali e prescriveva di renderle disponibili alle autorità nazionali per contrastare e prevenire gravi crimini, i giudici europei hanno contestato l'illegittimità di tale atto ravvisando «una ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta di vasta portata e di particolare gravità» che non pare supportata «da norme chiare e precise che permettano di garantire che [la sua applicazione] sia effettivamente limitata a quanto strettamente necessario» (p.to 65).

Nel giungere a tale decisione, la Corte fa leva sui diritti sanciti dalla Carta letti alla luce del principio di proporzionalità, rilevando un «bilanciamento

---

[59] F. Boehm, *A comparison between US and EU data protection legislation for law enforcement purposes*, cit., 18.

[60] Corte di Giustizia, 13 maggio 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos e Mario Costeja Gonzalez.*

[61] Corte di Giustizia, Grande Sezione, 8 aprile 2014, cause riunite C-293/14 e C-594/12, *Digital Rights Ireland Ltd, Seitlinger e a.*

[62] La sentenza, in particolare, riconosce nel territorio europeo il diritto all'oblio inteso come pretesa a ottenere la cancellazione dei contenuti delle pagine web ritenuti offrire una rappresentazione non più attuale della propria persona. In riferimento alle implicazioni pratiche e giuridiche legate a tale sentenza, v. (per tutti) le considerazioni espresse nel volume G. Resta e V. Zeno-Zencovich (cur.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015.

[63] A commento della sentenza v. (tra i molti) A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Dir Pubb Comp ed Eur*, 3/2014; L. Trucco, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. It.*, 2014, 8-9, 1850 ss; R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. data retention contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. Cont.*, 2/2014, 178 ss.; M. Granger, K. Iron, *The Court of Justice and the Data retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching lesson in privacy and data protection*, in 39 European Law Review 6, 2014, 835 ss.; O. Lynskey, *The Data retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in 51 Com. Mar. L. Rev. 6, 2016, 1789 ss.

ineguale» tra sicurezza pubblica collettiva e i diritti individuali[64]. In altri termini, invalidando per la prima volta un intero atto comunitario per contrasto con i diritti fondamentali sanciti dalla Carta di Nizza, la Corte di giustizia dimostra di aver compreso le potenzialità insite nella "costituzionalizzazione" dei diritti europei oltre che quelle insite nel suo ruolo di «human rights adjudicator»[65].

Proprio sviluppando tali potenzialità, la Corte ha poi utilizzato il *legal reasoning* di *Digital Rights Ireland* per risolvere altre controversie, estendendo l'ambito e la portata della *digital rule of law* europea. La forza centripeta del *Bill of Rights* europeo ha così consentito ai giudici di dispiegare gli effetti delle loro pronunce a) al di fuori del continente europeo e b) all'interno delle competenze riservate agli Stati membri.

Estendendo il suo raggio di azione oltre i confini europei, la Corte ha fatto aggio sul combinato disposto tra protezione dei dati personali e principio di proporzionalità per invalidare accordi – e relative decisioni di adeguatezza della Commissione – sulla trasmissione transfrontaliera dei dati digitali siglati dalle istituzioni europee con gli Stati Uniti (caso C-362/14 *Maximillian Schrems*[66]) e il Canada (parere della Corte di Giustizia 1/15 del 26 luglio 2017[67]). In entrambi i

[64] Nel decidere la controversia, la Corte ha innanzitutto osservato che, sebbene la raccolta massiva di tali dati non riguardi il contenuto delle conversazioni, essa tuttavia è in grado di fornire una serie di informazioni quali il luogo, la durata, il tempo, l'identità delle comunicazioni dei cittadini europei. Permettendo alle autorità degli Stati la raccolta e l'accesso a tali informazioni, la direttiva interferisce in modo «particolarmente grave» con i diritti sanciti dagli artt. 7 e 8 della Carta perché «può ingenerare nelle persone interessate la sensazione che la loro vita privata sia oggetto di costante sorveglianza» (p.to 37).
A partire da queste considerazioni, i giudici hanno quindi verificato se tale interferenza fosse o meno giustificata alla luce delle norme del Trattato, e in particolare dell'art. 52 della Carta che consente limitazioni alle libertà europee nel caso in cui rispettino il loro contenuto essenziale, siano motivate da finalità di interesse generale e siano proporzionate allo scopo prefisso. Quanto al primo profilo, i giudici hanno ritenuto che, sebbene la conservazione dei dati imposta costituisca un'ingerenza particolarmente seria dei diritti alla privacy dei cittadini, essa non comprometta in sé il contenuto essenziale di tale diritto, in quanto si limita all'utilizzo dei dati e non concerne il contenuto delle comunicazioni. La raccolta dei dati, inoltre, è finalizzata alla prevenzione e alla lotta alla criminalità, e dunque è giustificata, secondo la Corte, da ragioni di pubblica sicurezza. Essa però difetta sotto il profilo della proporzionalità per tre ordini di ragioni: in primo luogo, secondo i giudici, le disposizioni normative della direttiva appaiono lacunose e generiche in riferimento alle persone interessate dalla raccolta dei dati, che è rivolta «alla totalità della popolazione europea» (p.to 56) e coinvolge «qualsiasi persona e qualsiasi mezzo di comunicazione elettronica (…) senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi» (p.to 57). In secondo luogo, la direttiva non prevede «criteri oggettivi utili a garantire» che l'accesso ai dati da parte delle autorità nazionali sia realmente limitato ai casi di prevenzione e accertamento di gravi reati (p.to 60), né stabilisce «i presupposti formali e procedurali» che consentono agli organi competenti «di avere accesso ai dati e di farne successivo uso» non prevedendo, ad esempio, che tale accesso «sia subordinato al previo controllo di un giudice o di un ente amministrativo indipendente» (p.to 62). Infine, la direttiva difetta nel delineare regole chiare utili a distinguere la durata di conservazione dei diversi dati raccolti, limitandosi a statuire che tale conservazione «si colloca tra un minimo di sei mesi e un massimo di ventiquattro mesi» senza precisare «i criteri obiettivi utili al fine di garantire che [essa] sia limitata allo stretto necessario» (p.to 64).

[65] Sul ruolo della Carta nel processo decisionale della Corte di Giustizia v. per tutti G. De Burca, *After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, NYU School of Law, Public Law Research Paper No. 13-51, 2013, in SSRN: ssrn.com/abstract=2319175.

[66] Corte di Giustizia, 6 ottobre 2015, C-362/14, *Maximillian Schrems v. Data protection commissioner*.

[67] Corte di Giustizia, Parere 1/15 (Accordo PNR EU-Canada) del 26 luglio 2017

casi, il ragionamento dei giudici si sviluppa a partire dalla tutela della privacy digitale desunta dagli artt. 7 e 8 della Carta. In *Schrems* la Corte ha annullato il c.d. accordo di *Safe Harbour* tra la Commisione europea e gli Stati Uniti giudicando non sufficientemente adeguata la protezione offerta dal sistema americano ai cittadini europei circa le informazioni personali raccolte dalle sedi europee delle grandi società informatiche (nel caso di specie Facebook) e poi trasferite, su richiesta, alla National Security Agency americana (NSA)[68]. Nell'invalidare tale accordo, la Corte accoglie le pretese del ricorrente, giudicando illegittima una normativa «che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche» e che quindi pregiudica «il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta» (p.to 94), specialmente laddove (come nel caso di specie) «non si prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenerne la rettifica o la soppressione» (p.to 95)[69].

In modo non dissimile, la Corte si è poi recentemente pronunciata – in sede consultiva – riscontrando l'incompatibilità con il diritto comunitario della bozza di accordo sulla condivisione dei dati e dei codici di prenotazione aerea (PNR) tra Canada e Unione[70]. Ripercorrendo lo schema argomentativo già collaudato in *Digital Rights Ireland* e in *Schrems*, la Corte conduce uno scrutinio di

[68] Il caso è stato è stato sollevato dall'avvocato austriaco Maximillian Schrems, che aveva adito le autorità amministrative e giurisdizionali irlandesi prima, e la Corte di giustizia poi, al fine di dichiarare illegittimo, perché in violazione degli artt. 7 e 8 della Carta, il trasferimento dei propri dati personali acquisiti da Facebook dalla filiale irlandese di tale azienda a quella californiana. Il traffico transfrontaliero dei dati digitali costituisce da tempo un importante e necessario elemento delle relazioni transatlantiche, in particolar modo in un epoca come la nostra sempre più caratterizzata da scambi economici e transazioni commerciali effettuate attraverso la rete; per questa ragione, in attuazione a quanto previsto adottata a norma della direttiva 95/46/CE la Commissione aveva adottato la decisione 2000/520/CE, autorizzando il trasferimento di dati dall'UE alle società statunitensi che avevano ratificato il cd. «approdo sicuro», ossia i principi a protezione del diritto alla vita privata come garantito dalle norme europee.

[69] La Corte, in particolare, ha invalidato l'accordo *Safe Harbour*, sostenendo che esso «non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda (…) relativa alla protezione dei loro diritti e delle loro libertà» (p.to 53). In questo modo, la Corte ha rafforzato i poteri delle autorità nazionali di controllo dei dati, che devono poter esaminare in piena indipendenza se il trasferimento dei dati di una persona verso un paese terzo rispetti i requisiti stabiliti dalla direttiva, pur non potendo, da sole, determinane l'invalidità. In secondo luogo, l'analisi dei giudici si è concentra sul contenuto della decisione della Commissione, verificando se essa sia o meno conforme allo standard di protezione dei dati definito dalle norme europee primarie e secondarie. Sotto questo profilo, i giudici hanno rilevato che lo schema di «*Safe Harbour*» vincola solo le aziende americane che lo sottoscrivono, ma soccombe di fronte alle richieste del governo statunitense quando esse sono giustificate da esigenze legate alla sicurezza nazionale; in sostanza, quindi, il regime americano dell'approdo sicuro non tutela realmente la privacy dei cittadini europei, perché non mette al riparo i loro dati dalle possibili (e legittime) ingerenze da parte delle autorità pubbliche americane previste dal sistema normativo in vigore negli Stati Uniti.

[70] Tale accordo, sottoscritto dalla Commissione e dal governo canadese il 25 giugno 2014 per consentire il sistematico trasferimento da e verso le autorità areoportuali dei dati dei passeggeri e regolarne il trattamento, la conservazione, e l'utilizzo da parte delle autorità di law enforcement canadesi per finalità legate alla lotta al terrorismo e di altri gravi reati di carattere transforntaliero era stato sottoposto dal Parlamento europeo alla Corte di Giustizia, chiamata a pronunciarsi preventivamente tramite parere sulla conformità di tale atto con il diritto dell'Unione.

proporzionalità particolarmente stringente sulle norme relative al trasferimento, eccependo così una serie di censure dell'accordo contestato[71].

Entrambe le decisioni in esame segnano un passo decisivo nel riconoscimento pieno del diritto alla privacy digitale in Europa. Estendendo il proprio controllo anche ad atti con cui la Commissione ha ratificato accordi internazionali con gli Stati Uniti e il Canada, o ha certificato l'adeguatezza del livello di protezione garantito dagli Stati terzi, la Corte di Giustizia ha fornito «una interpretazione forte del diritto alla privacy» che produce effetti «transnazionali o addirittura globali», capaci di travalicare i confini dell'Unione europea estendendo la portata delle decisioni del giudice comunitario «sostanzialmente al di fuori dell'Unione europea»[72]. In sostanza, la Corte non solo ribadisce la prevalenza del diritto alla privacy nel bilanciamento con altri interessi, ma afferma altresì la sostanziale applicabilità di tale diritto e del livello di protezione garantito in UE a soggetti non europei i cui dati vengono elaborati fuori dal continente.

Come ricordato, la forza attrattiva derivante dalla "costituzionalizzazione" del diritto alla privacy europeo non ha avuto solo conseguenze transfrontaliere; essa ha infatti in qualche misura alterato anche l'equilibrio raggiunto dallo speciale federalismo europeo, incidendo cioè sulle competenze riservate agli Stati membri e sui limiti stabiliti dagli artt. 51 e 53 della Carta. La questione si è posta, in particolare, a seguito del caso *Digital Rights Ireland*: sebbene quella pronuncia si riferisca esclusivamente ad un atto dell'Unione europea (dovendosi quindi

[71] La Corte, in particolare, si accerta in primo luogo che i dati oggetto del trasferimento «considerati complessivamente» siano in grado di incidere in modo significativo sui i diritti sanciti dagli artt. 7 e 8 della Carta perché potenzialmente capaci di rivelare significative informazioni sensibili dei passeggeri quali «le loro abitudini di viaggio, la loro situazione finanziaria, le loro abitudini alimentari, il loro stato di salute» (par. 128). Accertato quindi che l'accordo in esame incide sui diritti fondamentali, i giudici ricordano quindi che, di fronte a tale ingerenza, la normativa può ambire a superare il test di proporzionalità sancito dall'art. 52 co. 1 della Carta solo qualora preveda «norme chiare e precise» che delimitino «l'applicazione e la portata della misura considerata» garantendo agli interessati «che l'ingerenza sia limitata allo stretto necessario» (par. 141). A partire da tali considerazioni, i giudici hanno poi condotto uno scrutinio di proporzionalità stretto, rilevando diversi profili di incompatibilità dell'accordo: così, ad esempio, la Corte ha contestato la formulazione delle rubriche 5, 7 e 12 nella parte in cui esse non definiscono con sufficiente chiarezza i dati PNR che dovrebbero essere trasferiti, mentre, sotto il profilo del trattamento dei dati sensibili, i giudici hanno rilevato come l'accordo non l'accordo non contenga sufficienti garanzie rispetto al fatto che essi siano utilizzati senza violare il principio di non discriminazione, e per finalità unicamente legate alla lotta al terrorismo internazionale. Inoltre, riprendendo le argomentazioni già sviluppate in *Digital Rights Ireland*, la Corte censura le norme relative alla conservazione dei dati (cinque anni dalla data della acquisizione) e la previsione per cui esse non distinguono circa l'utilizzo dei dati acquisiti «*prima* dell'arrivo dei passeggeri aerei, *durante* il loro soggiorno in Canada e *al momento* della loro uscita dal Paese» (Cfr. M. Leffi, *L'Accordo PNR tra Canada e UE non prende il volo. Nota sul parere della Corte di giustizia europea a proposito del trasferimento dei dati del codice di prenotazione*, in *MediaLaws Law and Policy of the Media in a Comparative Perspective*, 1/2017, www.medialaws.eu.). Infine, sono considerate contrarie al diritto comunitario le disposizioni riguardanti il trasferimento alle autorità nazionali dei dati dei passeggeri, che non si limitano allo stretto necessario, e soprattutto non consentono ai cittadini interessati di «esercitare i loro diritti richiedendo l'accesso ai dati» e di proporre, eventualmente, «un ricorso effettivo dinanzi a un giudice» (par. 219). A commento della decisione v. A. Vedaschi, *Pnr Agreements Between Fundamental Rights and National Security: Opinion 1/15*, in europeanlawblog.eu/, 23 gennaio 2018.

[72] 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 *Federalism.it*, 2017, 9.

circoscrivere i suoi effetti all'interno dei limiti sanciti dall'art. 51 della Carta), lo scrutinio della Corte assume una coloritura tipicamente costituzionale dal momento che i parametri entro i quali un programma di raccolta dei metadati può dirsi legittimo vengono definiti alla luce del principio di proporzionalità. La decisione della Corte produce così l'effetto, indiretto, di mettere in discussione anche i *Bulk metadata programs* delineati dalle *law of fears* di ciascuno Stato, sollevando il seguente interrogativo presso i giudici e i legislatori nazionali: con la decisione *Digital Rights Ireland* i giudici europei si sono limitati a dichiarare l'illegittimità della direttiva o volevano invece delineare una serie di principi di carattere generale applicabili, indifferentemente, anche alle disposizioni nazionali?[73]. A rispondere a tale domanda non ha contribuito nemmeno il comportamento tenuto dalle istituzioni europee: il giorno della pubblicazione della sentenza, infatti, la Commissione ha assunto una posizione piuttosto ambigua, affermando che le discipline nazionali devono essere modificate «solo nella parte in cui sono divenute contrarie al diritto dell'Unione a seguito della sentenza» e che, in ogni caso, «la declaratoria di invalidità non elimina il potere degli Stati di richiedere la conservazione dei dati sulla base della direttiva 2002/58/CE»[74].

L'occasione per fugare ogni dubbio viene offerta alla Corte pochi anni più tardi dal caso *Tele2 Sverige e Watson*[75]. Il caso scaturiva da due rinvii pregiudiziali sollevati dalla Corte d'appello amministrativa di Stoccolma (caso C-203/15) e dalla Corte d'appello civile di Inghilterra e Galles (C-698/15) con cui si chiedeva ai giudici europei di definire – ovviamente in maniera indiretta – la legittimità di due disposizioni normative nazionali (specificamente: LEK e DRIPA) volte alla conservazione e alla acquisizione di dati elettronici da parte delle autorità nazionali per finalità legate alla lotta al terrorismo[76]. Pur fondati su motivi parzialmente

[73] A questo proposito, v. le considerazioni di A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quad. Cost.*, 2014, 723: «occorre domandarsi se le discipline sulla conservazione dei dati che alcuni Stati membri hanno introdotto per recepire la direttiva 2006/24 sono tutt'ora soggette al rispetto della Carta dei diritti fondamentali, come richiesto dall'art. 51, par. 1, della Carta per le misure nazionali adottate nell'attuazione del diritto dell'Unione». La decisione apre anche la possibilità per i cittadini europei La decisione apre la possibilità ai cittadini europei di impugnare le norme nazionali sulla *data retention* innanzi alle proprie Corti Costituzionali per violazione del diritto fondamentale alla protezione dei dati personali; non è un caso che, anche a seguito della decisione della Corte di giustizia, molte giurisdizioni nazionali abbiano effettivamente dichiarato l'incostituzionalità di tali norme, confermando l'accresciuta attenzione di tutto il continente verso tale diritto (cfr. a riguardo N. Vainio – S. Miettinen, *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States*, in 23 International Journal of Law and Information Technology, n. 3 2015, 290-309.

[74] Così il comunicato stampa Memo 8 aprile 2014, Frequently Asked Questions: the Data Retention Directive, riportato da A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, cit., 723.

[75] Corte di Giustizia, 21 Dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB contro Post-och telestyrelsen e Secretary of State for the Home Department contro Tom Watson et. Al.*

[76] In particolare, il LEK svedese stabiliva l'obbligo per le compagnie telefoniche svedesi di conservare i tabulati telefonici e telematici dei propri clienti; di fronte al rifiuto della compagnia *Tele2* di provvedere a tale obbligo – scaturito a seguito della già ricordata pronuncia *Digital Ireland* – il governo svedese aveva denunciato tale compagnia, ritenendo compatibile la direttiva nazionale con i pronunciamenti della Corte di Giustizia sulla privacy digitale. Quanto al secondo ricorso, esso riguardava invece la disciplina contenuta nel *Data Retention and Investigatory Powers Act* 2014 (DRIPA), che consentiva al Governo britannico di approvare un "avviso sulla conservazione" dei dati, attraverso cui si disponeva l'obbligo a carico delle compagnie di telecomunicazione britanniche di conservazione dei dati dei loro

diversi, «sullo sfondo di entrambe le questioni sollevate in via pregiudiziale si coglie un diffuso atteggiamento di incertezza sulle effettive implicazioni della decisione *Digital Rights Ireland*»[77] e, dunque, sugli effetti di tale sentenza sulle disposizioni nazionali che prevedono programmi di *mass surveilliance* predisposti per finalità connesse alla sicurezza nazionale.

Nell'affrontare la controversia, i giudici europei hanno preliminarmente stabilito che le misure legislative adottate dagli Stati membri circa «la conservazione» (par. 75) e anche «l'accesso delle autorità nazionali ai dati conservati» (par. 76) rientrano nell'ambito della direttiva sulle Comunicazioni Elettroniche (2002/58/EC), ma forniscono una lettura restrittiva dell'art. 15 par. 1 di tale disposizione che – a giudizio dei ricorrenti – consentiva agli Stati membri di derogare al principio che esige la riservatezza delle comunicazioni e dei dati di traffico[78]. Secondo la Corte, infatti, l'unica interpretazione che consente di salvare il tenore generale della direttiva in esame[79] è quella per cui la conservazione dei dati dei cittadini è ammessa qualora le normative nazionali contengano «norme chiare e precise che disciplinino la portata di tale misura» e forniscano alle persone interessate «garanzie sufficienti» che le proteggano contro «i rischi di abuso» (par. 109).

La Corte sfida quindi la compatibilità dei programmi di sorveglianza di massa con gli articoli 7 e 8 della Carta, ritenendo che, anche nel caso di misure riguardanti la lotta al terrorismo o gravi reati, le eccezioni alla tutela generale dei dati personali debbano limitarsi allo stretto necessario. Nel fare ciò, i giudici sottopongono le normative nazionali in esame ad un controllo di proporzionalità stretto ricavandolo – come avvenuto in passato – dall'art. 52 della Carta. È alla luce di tale test che è desunta, indirettamente, l'incompatibilità (o di "incostituzionalità"?) delle normative contestate con il diritto comunitario[80]. Viene infatti statuito che esse «forniscono gli strumenti per stabilire (…) il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni» (par. 99) e

clienti. Pur se limitata nel tempo (e comunque non superiore ai dodici mesi) tale disposizione era stata contestata dal parlamentare Tom Watson per incompatibilità con gli articoli 7 e 8 della Carta di Nizza.

[77] M. Bassini, O. Pollicino, *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 *Diritto Penale Contemporaneo*, 9 gennaio 2017, 5.

[78] L. Woods, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in ulawanalysis.blogspot.it, 21 dicembre 2016.

[79] Così O. Pollicino e 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 Quad. Cost.*, 16 gennaio 2017, www.forumcostituzionale.it/wordpress/wp-content/uploads/2001/01/pollicino_vigevani.pdf, 3: «Il margine di manovra riguardo alla conservazione dei dati che l'articolo 15 della direttiva del 2002 concede agli stati, trattandosi di una deroga al regime ordinario di tutela della riservatezza e in specie al divieto di memorizzare dati di traffico senza il consenso dell'interessato, deve essere interpretato in modo restrittivo. Altrimenti, le misure che tale disposizione autorizza a titolo di eccezione finirebbero per divenire la regola, rovesciando l'ordine di priorità indicato dal legislatore europeo e non rispettando il principio di proporzionalità che deve orientare ogni restrizione dei diritti fondamentali».

[80] Tale valutazione, in realtà, si articola non attorno alla interpretazione dell'art. 15 della direttiva e-privacy e non, direttamente, sulla compatibilità delle norme nazionali, che non è direttamente valutata dalla Corte di giustizia. Tuttavia, de facto, l'interpretazione del diritto comunitario fatta alla luce del test di proporzionalità finisce con incidere con la compatibilità della legislazione nazionale.

dunque predispongono una ingerenza «particolarmente grave» nei diritti fondamentali dei cittadini. La normativa in esame, inoltre, «non richiede alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica», «travalica i limiti dello stretto necessario» (par. 106) e non può essere quindi «considerata giustificata, in una società democratica così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta» (par. 107)[81].

Due sono le considerazioni utili ad inquadrare il caso *Tele2 Sverige* nella prospettiva dello speciale federalismo europeo. Il percorso argomentativo seguito dai giudici non pare particolarmente innovativo, limitandosi a ricalcare quanto già sviluppato in *Digital Rights Ireland* e *Schrems*; piuttosto, l'importanza della sentenza risiede nel fatto che la Corte ha applicato questo medesimo *reasoning* a delle discipline nazionali, limitando l'autonomia legislativa statale attraverso i principi di necessità e di proporzionalità che invece in *Digital Rights Ireland* vincolavano il solo legislatore europeo. Si aggiunga, inoltre, che i giudici europei hanno mostrato un atteggiamento di assoluta controtendenza rispetto al generale clima securitario delle nostre democrazie[82], calandosi sempre più nelle vesti di una corte dei diritti capace di orientare il dibattito su scala globale. Non a torto la sentenza *Tele2* è stata definita «iconica (…) per la radicalità delle soluzioni» e «per il tono imperativo utilizzato»[83]. Mentre in precedenza i giudici avevano forse «legittimato sul piano teorico i programmi di sorveglianza di massa» limitandosi a definire «sotto il profilo pratico (…) una serie di restrizioni tali da rendere molto difficoltosa la loro applicazione concreta»[84], in *Tele2* la Corte afferma «per la prima volta inequivocabilmente» che la conservazione generalizzata e indifferenziata di metadati è «in contrasto con i diritti fondamentali protetti dalla Carta dei diritti dell'Unione»[85].

6. Uno sguardo d'insieme alle sentenze sulla privacy: la Corte di Giustizia come Corte costituzionale "federale"?

A partire dai casi *Google Spain* e *Digital Ireland* la Corte di giustizia sembra dunque aver assunto un ruolo da protagonista nella definizione del diritto alla privacy digitale in Europa che ha portato ad un significativo rafforzamento di tale libertà sotto il profilo "costituzionale". Tale approccio è particolarmente evidente se si considerano i casi riguardanti il bilanciamento tra privacy e sicurezza nazionale;

[81] Tale considerazione è estesa inoltre anche alle condizioni di accesso ai dati da parte delle autorità nazionali: come ricordato nella sentenza, infatti, il diritto dell'EU «deve essere interpretato» come contrario ad una normativa nazionale che «disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione» (par. 125).

[82] Così anche O. Pollicino G. Vigevani, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza* Tele2 Sverige *della Corte di giustizia UE*, cit.

[83] G. Tiberi, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla data retention*, in *Quad. Cost.*, 2017, 436.

[84] Come osservato a commento della Opinion 1/15 da A. Vedaschi, *Pnr Agreements Between Fundamental Rights and National Security: Opinion 1/15*, cit.

[85] G. Tiberi, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla data retention*, cit., 438.

dopo aver tratteggiato in *Digital Ireland* le regole di ingaggio, i giudici comunitari hanno indirettamente esteso gli effetti del loro *legal reasoning* anche nei confronti dell'ordinamento americano (caso *Schrems*) e degli Stati membri (*Tele2 Sverige*), sancendo così la prevalenza interna ed esterna delle ragioni della privacy digitale su quelle della sicurezza nazionale. Decretando la sostanziale superiorità di tale diritto rispetto ad altri – pur legittimi – diritti-interessi, i giudici comunitari hanno potuto costruire, sentenza dopo sentenza, le fondamenta di quella che è oggi definita the *Europe's Privacy Fortress*[86], ovverosia un sistema che garantisce ai propri cittadini un elevato livello di protezione dei dati digitali.

Molte sono le ragioni sottese a tale approccio. In primo luogo, il diritto alla privacy si presta, per sua natura, ad una regolamentazione unitaria ed integrata a livello europeo (e non solo) in ragione dei cambiamenti radicali causati dall'avvento dell'era digitale che, connettendo gli utenti a reti globali, supera i naturali confini nazionali. La Corte, attraverso le sue decisioni, non fa altro che spingere nella direzione della massima unitarietà del sistema di protezione dei dati già da tempo seguita dall'ordinamento europeo; già nella direttiva del 1995, infatti, si invitavano gli Stati membri ad adottare un livello massimo di armonizzazione delle direttive nazionali, orientato cioè al raggiungimento di un elevato livello tutela[87].

In secondo luogo, le sentenze successive al caso *Digital Rights Ireland* hanno probabilmente risentito delle tensioni politiche e diplomatiche originate dal caso Datagate e delle reazioni innescate da tale scandalo nei leader europei[88]. Tali tensioni hanno fatto emergere le debolezze del sistema americano di protezione della privacy e, allo stesso tempo, hanno ricompattato il fronte politico europeo rispetto alla protezione dei dati digitali, portando le stesse istituzioni a supportare risoluzioni unitarie di condanna all'utilizzo dei programmi di sorveglianza di massa americani[89]. Da questo panorama politicamente complesso, la Corte sembra aver ricavato una sorta di legittimazione ad agire dalle posizioni assunte dai singoli Stati membri e dagli organi europei, traendo da tale comune consenso la spinta necessaria per innalzare il livello di protezione della privacy in Europa. I giudici sembrano però essersi in questo modo auto-investiti di un ruolo quasi politico, riaffermando la «sovranità digitale» dell'Unione europea sul trattamento dei dati e «statuendo la [propria] supremazia giudiziale su temi del più alto livello politico, come» tra l'altro «la politica internazionale»[90].

Nel perseguire tale scopo, la Corte si è fatta carico di tutta la portata innovativa contenuta negli art. 7 e 8 della Carta, che vengono oggi utilizzati a tutti gli effetti come parametri costituzionali per giudicare la compatibilità degli atti

[86] *Europe's Privacy Fortress*, WSJ, 17 dicembre 2015, www.wsj.com/articles/europes-privacy-fortress-1450398921

[87] Sottolinea questo aspetto anche A. Ruggeri, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in *Consulta online*, n. 3/2016.

[88] Si vedano, ad esempio, le dure reazioni del cancelliere tedesco Angela Merkel a seguito delle rivelazioni di Snowden: *Nsa e spie doppiogiochiste, la Germania accusa gli Usa: "Tradita la fiducia"*, in La Repubblica- on line, 7 luglio 2014

[89] Cfr., a riguardo e tra gli altri, *Risoluzione del Parlamento europeo del 29 ottobre 2015 sul seguito dato alla risoluzione del Parlamento europeo del 12 marzo 2014 sulla sorveglianza elettronica di massa dei cittadini dell'Unione*, P8 TA (2015)0388, in www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//IT&language=IT

[90] V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems:la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta – V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali*, Roma, 2016, 9.

comunitari (e, come visto, non solo) rispetto al livello di privacy digitale da essi garantito. Facendo leva sulla Carta di Nizza, la Corte sgancia «la protezione dei dati personali dalla dimensione economica del libero scambio che pure in parte ancora caratterizzava l'adozione della prima direttiva in materia di protezione dati a metà anni novanta»[91]. Emerge, in questo senso, tutta la «centralizing force» della Carta dei diritti fondamentali che produce un effetto aggregante all'interno del sistema costituzionale europeo «[providing] the grounds to confirm and steadily expand the scope of application of EU fundamental rights to the Member States and thereby the jurisdiction of the CJEU for the interpretation of those rights»[92].

Lette sotto questa luce, le sentenze sulla privacy indicano un nuovo ruolo della Corte che sfrutta pienamente le potenzialità del nuovo *Bill of Rights* europeo. Tale atteggiamento è stato salutato con entusiasmo per l'importanza della materia trattata, in quanto i giudici europei «hanno sperimentato la loro capacità di essere rigorosi nella tutela dei diritti su uno dei terreni più spinosi, dato che la gravità della situazione internazionale tende ad attutire la sensibilità verso i diritti dei sospetti terroristi e genera una maggiore propensione verso le esigenze della sicurezza piuttosto che verso quelle della giustizia e della libertà»[93]. Allo stesso tempo, però, se guardato attraverso il prisma dello speciale federalismo europeo, il *legal reasoning* dei giudici nelle sentenze sulla *data retention* pone più di un problema agli interpreti, svelando in modo paradigmatico tutti gli effetti del paradosso federale europeo.

Lo stile argomentativo della Corte sembra svelare un approccio nuovo dei giudici comunitari; fondando le sue decisioni sul controllo di proporzionalità stretto condotto alla luce dei parametri contenuti negli artt. 7 e 8 della Carta, la Corte usa uno stile argomentativo più simile a quello di «"giudice costituzionale" dell'Unione» che non a quello, più tradizionale, di «"giudice dell'integrazione"»[94]. Poggiare le proprie decisioni sul principio di proporzionalità, non evita ai giudici europei di sfuggire al paradosso federale che attribuisce gli interessi in gioco a diversi livelli di governo. Il frutto di un simile atteggiamento è quindi un bilanciamento del tutto asimmetrico, in cui i giudici rischiano di incidere sulle ragioni della sicurezza nazionale che la Corte richiama saltuariamente nelle sue sentenze, ma che poi fatica a tenere in debita considerazione.

Tale approccio argomentativo è riscontrabile sin dalla pronuncia *Google Spain*, in cui la Corte – nel definire i tratti essenziali del diritto all'oblio – sembra dimenticare le ragioni legate al diritto all'informazione; come acutamente osservato, infatti, essa si assume interamente il compito di farsi protettrice dei diritti costituzionali sanciti dagli artt. 7 e 8, ma non assolve l'onere – generalmente incombente sui giudizi di costituzionalità classicamente intesi – di operare un corretta valutazione tra tutte le libertà in gioco, preferendo invece partire da una sorta di «presunzione di prevalenza» della privacy digitale, che rende

[91] 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*, cit., 12.

[92] A. Torrez Perez, *The federalizing force of the EU Charter of Fundamental Rights*, cit., 1081.

[93] M. Cartabia, *L'ora dei diritti fondamentali nell'Unione Europea*, in M. Cartabia (a cura di), *I diritti in azione*, Il Mulino, 2007, 13, citato anche da G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in *Osservatorio AIC*, 3/2018, 475.

[94] M. Cartabia, *La tutela multilivello dei diritti fondamentali - il cammino della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in www.cortecostituzionale.it/documenti/convegni_seminari/RI_Cartabia_santiago2014.pdf, 2014, 3

«asimmetrico» e «del tutto sbilanciato già in partenza» il bilanciamento tra diritti contrastanti[95]. Se in *Google Spain* questa presunzione di prevalenza opera a danno di un'altra libertà sancita dalla Carta, nelle sentenze sulla *data retention* essa finisce per comprimere le ragioni della sicurezza nazionale, che – come visto – costituiscono un limite espresso non solo alla regolamentazione della privacy, ma anche una competenza esclusiva rafforzata degli Stati membri. Il bilanciamento sui diritti, in ragione della sua strutturale asimmetria, finisce così per incidere direttamente sulla ripartizione delle competenze comunitarie, tramutandosi – di fatto – in un conflitto tra diversi livelli di governo. La Corte, che mostra coraggio nell'indossare gli abiti di "giudice costituzionale" nella tutela dei diritti, si fa timida nel momento di assumere il ruolo di corte federale nella divisione verticale delle competenze.

Questa timidezza che può essere vista come un sintomo della fragilità federale del *Bill of Rights* europeo. Mentre negli Stati Uniti l'inserimento di un catalogo dei diritti è stato solidamente fondato sulla teoria del federalismo inteso come limite al potere centrale, in Europa tale riflessione è rimasta sullo sfondo. Non solo: nata come uno dei pilasti portanti della futura Costituzione europea, la Carta dei diritti è stata poi introdotta nei Trattati solo a seguito del fallimento del progetto costituzionale, e dunque non è stata accompagnata da una adeguata riflessione *costituente* sui limiti e i confini della federazione rispetto agli Stati membri. Del resto, la dottrina aveva già sottolineato durante il processo costituente europeo che «la scrittura della Costituzione europea non varrà a contenere i margini di discrezionalità dei giudici, come si sarebbe invece portati a pensare secondo la tradizione dello stato di diritto»; l'introduzione della Carta di Nizza nei Trattati pare aver rafforzato tale ipotesi spingendo i giudici comunitari ad utilizzare «la tutela dei diritti fondamentali» come «solida base di legittimazione per oltrepassare i limiti dei poteri consentiti dal sillogismo giudiziale»[96].

L'insieme di questi fattori si traduce in un livello di protezione della privacy più elevato di quello previsto nel resto del mondo e, in particolare, dal sistema americano. Negli Stati Uniti, dove la protezione della privacy digitale è diminuita anche a seguito del rafforzamento degli strumenti tecnologici di lotta al terrorismo internazionale, gli strumenti costituzionali di tutela di tale diritto sembrano oggi mostrare tutta la loro inadeguatezza rispetto alle sfide dell'era digitale[97]. Allo stesso tempo, però, il corretto bilanciamento operato oltreoceano tra privacy e sicurezza nazionale rappresenta una sfida reale interamente ricadente sul livello federale: come ricordato dal 2013 Report of Intelligence commissionato dal Presidente Obama, infatti, «the problem here is that the United States Government must protect, at once, two different forms of security: *national*

[95] Così O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain*, in *Il diritto all'oblio su internet dopo il caso Google v. Spain*, cit., 2015, 15.

[96] Così, acutamente, M. Cartabia, *La scrittura di una Costituzione europea e i poteri dei giudici*, intervento al Convegno di Napoli, del 6 aprile 2004 "*Stato di diritto e principio di legalita' nell'evoluzione della forma di stato europea*", versione pubblicata su *Astrid-online* – Archivio 2004-2005.

[97] In riferimento alle complesse vicende legate alla legittimità dei sistemi di sorveglianza nazionale operati dalla National Security Agency e, più in generale, sul bilanciamento tra privacy e sicurezza nazionale negli Stati Uniti d'America si permetta di rinviare alle mie considerazioni svolte in L.P. Vanoni, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e datagate: Security v. Privacy*, in *Federalismi.it*, n.1 2015.

security and *personal* security (which is "the right of the people *to be secure* in their persons, houses, papers" established by the IV Amendment)»[98].

L'Europa, al contrario, non deve confrontarsi con lo stesso problema: come cittadini europei, noi chiediamo all'Unione di garantire un alto livello di protezione dei nostri dati personali ma, contemporaneamente, pretendiamo che i nostri governi tutelino la nostra sicurezza adottando misure di prevenzione degli attacchi terroristici. Questa asimmetria rende molto più semplice per la Corte di giustizia definire standard elevati per il rispetto della privacy digitale, ma non risolve ultimamente il problema del corretto equilibrio tra quest'ultima e la sicurezza dei cittadini, che ricade invece interamente sulle spalle degli Stati membri e, come vedremo, sui giudici nazionali.

7. Tra incudine e martello: il diritto alla privacy digitale dopo Tele2 Sveridge

La mancanza di una riflessione europea sul nesso tra il federalismo e la tutela dei diritti che ha accompagnato la redazione e l'entrata in vigore della Carta dei diritti non ha però prodotto conseguenze solo sul piano della "forma di stato" europea. Al contrario, il disallineamento europeo tra privacy e security ha manifestato i suoi effetti anche sul piano pratico del dialogo federale tra Corti, complicando il lavoro dei giudici nazionali chiamati a rispettare quanto statuito dai giudici comunitari. Il tema non è nuovo: da sempre, infatti, lo speciale federalismo europeo interroga i giuristi sulla necessaria interazione tra diversi livelli di giurisdizione. Anche su questo aspetto la *data retention saga* può aiutare ad illuminare un profilo particolare di questo rapporto riguardante gli effetti "costituzionali" delle pronunce della Corte.

In primo luogo, poggiando quasi interamente le argomentazioni sul principio di proporzionalità come bilanciamento tra diritti, i giudici europei escono dal terreno della pura interpretazione del diritto comunitario sconfinando nel campo di considerazioni politico-valoriali: come ricordato, «proportionality between means and ends is more conducive to a principled practice of judicial review, while proportionality as balancing is an invitation to more or less arbitrary judicial decision making»[99]. La questione è sicuramente molto ampia e già profondamente indagata dalla dottrina; per quel che qui interessa, è sufficiente ricordare che «per loro intrinseca natura, i diritti fondamentali non possono essere saturati dalla definizione legale», perché rifuggono «la pura riduzione alla legalità e vivono piuttosto – nella dimensione sovranazionale quasi interamente – nella

[98] Così *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* pubblicato il 12 dicembre 2013 con il titolo *Liberty and Security In a Changing World*, in www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, 14-15: «In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people *to be secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated (…)" (emphasis added). Both forms of security *must* be protected».

[99] Così G. Huscroft, B.W. Miller, G. Webber, *Introduction*, in *Proportionality and the Rule of Law. Rights, Justification, Reasoning*, Cambridge, 2014, 4.

forma loro conferita dalla giurisprudenza»[100]. Il tema, generalmente, è affrontato all'interno della strutturale interconnessione tra dimensione *politica* e/o *giuridica* della tutela dei diritti, e dunque nel rapporto tra legislatore e giudice costituzionale: come acutamente ricordato da Mark Dawson «where Courts choose to discuss balancing through concepts and values of their own making, to what extent do they leave room for political actors to engage in a proactive dialogue?»[101]. Ma, a ben guardare, la difficoltà a definire i confini del test di proporzionalità usato come bilanciamento tra diritti rischia forse di riverberare i suoi effetti non solo sul dialogo tra le Corti e gli attori politici, ma anche su quello tra i giudici integrati all'interno del complesso sistema giurisdizionale europeo.

In secondo luogo, sotto il profilo procedurale, l'approvazione della Carta dei diritti ha favorito un intensificarsi dell'utilizzo dello strumento del rinvio pregiudiziale ex art. 267 TFUE da parte dai giudici comuni ma soprattutto da parte delle Corti costituzionali stesse, «tradizionalmente molto restie» a rivolgersi alla Corte di giustizia[102]. I casi sulla privacy confermano tale tendenza, come ben testimoniato dal caso *Digital Rights Ireland* sollevato dalle Corti supreme austriaca ed irlandese, ma anche dai numerosi ricorsi sollevati dai giudici comuni di diversi paesi a seguito di tale pronuncia. L'incrementarsi dell'utilizzo del rinvio pregiudiziale sembrerebbe, da un lato, confermare una rinnovata propensione al dialogo tra giudici europei. Allo stesso tempo, però, tale approccio descrive l'accentuarsi di un dialogo «non solo irenico ma anche polemico» tra i diversi livelli giurisdizionali, perché le sentenze europee «pur formalmente rinviando ai giudici nazionali» il compito di accertare il rispetto dei principi sulla privacy digitale da parte delle rispettive normative nazionali, di fatto svolgono esse stesse tale scrutino «argomentando minuziosamente sui punti di contrasto e sulle omissioni di tali normative», superando le decisioni di alcune Corti costituzionali in materia e ponendosi «in competizione sul piano interpretativo» con esse[103].

[100] Così, esemplarmente, G. Scaccia, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle corti europee*, in *Rivista AIC*, n. 2/2017, 27.

[101] M. Dawson, *The political face of judicial activism: EuropÈs law-politics imbalance*, in M. Dawson, B. De Witte, E. Muir (eds.), *Judicial activism at the European Court of Justice: causes, responses and solutions*, Edward Elgar, 2013, 11 ss.

[102] Tale tendenza sarebbe da ascriversi alla approvazione del Trattato di Lisbona. Come ricordato da M. Cartabia, *Convergenze e divergenze nell'interpretazione delle clausole finali della carta dei diritti fondamentali dell'unione europea*, in *Rivista AIC*, n. 2/2018, 1-2 «l'entrata in vigore del trattato di Lisbona ha coinciso con l'intensificarsi dell'uso del rinvio pregiudiziale ex art. 267 TFUE da parte delle corti supreme e costituzionali. Tradizionalmente restie ad utilizzare uno strumento processuale volto a coinvolgere la Corte di giustizia europea nella definizione di un problema giuridico rilevante in un procedimento nazionale, negli anni più recenti, numerose corti supreme e costituzionali nazionali hanno rotto gli indugi e si sono aperte a un dialogo franco e costruttivo, talvolta apertamente dialettico, con la Corte europea. Se fino ad anni assai recenti il rinvio pregiudiziale è stato utilizzato solo eccezionalmente e quasi esclusivamente da alcune di esse – in particolare dalle Corti costituzionali austriaca e belga – in seguito all'entrata in vigore del Trattato di Lisbona molte giurisdizioni costituzionali nazionali hanno seguito la strada segnata dalle avanguardie del dialogo costituzionale europeo».

[103] Come rilevato da G. Tiberi, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla data retention*, cit., 437-438, infatti, nella sentenza *Tele2* «la Corte di Giustizia va oltre quanto sinora affermato dalle Corti costituzionali nazionali e, per la prima volta inequivocabilmente, afferma che la conservazione generalizzata e indifferenziata di metadati da parte delle normative nazionali è in contrasto con i diritti fondamentali protetti dalla Carta dei diritti dell'Unione, mente le Corti costituzionali nazionali (esemplare in tal senso il Tribunale costituzionale federale tedesco nella sua decisione del 2 marzo 2010)

I giudici nazionali rischiano quindi di trovarsi tra l'incudine delle disposizioni sulla sicurezza predisposte dai loro governi e il martello degli alti standards di protezione della privacy digitale imposti dalle sentenze europee. Emblematica è, in tal senso, la ricaduta sugli ordinamenti nazionali dei parametri definiti dalla Corte di giustizia nella sentenza *Tele2 Sveridge*. Tale sentenza avrebbe dovuto definire l'applicazione dei principi sanciti da *Digital Rights Ireland*. Configurando «un definitivo "scacco matto" alla prevalenza delle ragioni di sicurezza pubblica su quelle di protezione della privacy digitale»[104], *Tele2 Sveridge* avrebbe dovuto rendere uniforme la tutela della privacy digitale in tutto il continente, liberando il campo da qualsiasi dubbio[105]. Eppure, tale pronuncia non ha esaurito tutta la complessità insita nel difficile bilanciamento tra privacy e security in Europa, provocando al contrario un misto di incertezza e scetticismo che è ben documentato dal proseguimento della *data protection saga* in campo nazionale ed europeo.

7.1. To be continued… da Ministerio Fiscal a Privacy International

Il primo esempio di tale complessità riguarda un ulteriore sentenza della Corte di giustizia sollevata da un giudice spagnolo[106]. La questione riguardava, nello specifico, l'attività di indagine svolta dalla polizia spagnola a seguito di una rapina in cui erano stati sottratti un portafoglio e un telefono cellulare. Al fine di perseguire l'autore del reato, gli investigatori avevano chiesto al giudice competente l'autorizzazione ad accedere ai dati identificativi dei titolari dei numeri attivati dal telefono rubato per un periodo di 12 giorni dalla data di consumazione del reato. Il tribunale di Terragona, investito della questione, aveva negato tale autorizzazione sostenendo che l'accesso ai dati digitali è ammissibile solo per perseguire "gravi reati", tra i quali non rientrava l'ipotesi del furto nel caso di specie secondo quanto disposto dal codice penale spagnolo. Di fronte a tale diniego, il Pubblico ministero spagnolo aveva così presentato appello, sollevando la questione di fronte alla Corte di giustizia.

Nel caso C-207/16 *Ministerio Fiscal* la Corte di giustizia è stata dunque sollecitata a verificare la legittimità dell'accesso ai dati personali conservati da fornitori di servizi telefonici da parte delle autorità nazionali competenti nel caso di accertamento di reati "non gravi". Il caso si allaccia ad uno dei parametri espressamente definiti dalla sentenza *Tele2 Sveridge*, anche se – in realtà – il ricorso è stato presentato prima della pubblicazione di tale pronuncia e, pertanto, alla luce dei soli parametri di *Digital Rights Ireland*. Al di là delle problematiche processuali, la domanda dei giudici spagnoli riguarda più in generale la compatibilità della propria legislazione con i parametri di rispetto della privacy digitale definiti dalla

avevano ragionato della violazione del principio di proporzionalità di una pur generalizzata attività di data retention».

[104] M. Bassini, O. Pollicino, *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*, cit., 10.

[105] Come si domanda, provocatoriamente, G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in *Osservatorio AIC*, 3/2018, 459: «la Corte, con la sua giurisprudenza, ha fornito criteri dettagliati che arricchiscono di limiti e di condizioni specifiche il dettato piuttosto generico e riassuntivo dell'art. 15, direttiva e-privacy: ogni dubbio quindi è risolto?»

[106] Corte di Giustizia, Grande Camera, sentenza 2 ottobre 2018, C-207/16 *Ministerio Fiscal*.

Corte di giustizia[107].

Nel risolvere la controversia, il giudice comunitario affronta due ordini di problemi. Il primo è legato alla presunta incompetenza della Corte di giustizia, eccepita dal governo spagnolo e supportata dal Regno Unito, in quanto la legislazione europea escluderebbe le attività legate alla sicurezza nazionale dal suo ambito di applicazione e, di conseguenza, anche dall'ambito di applicazione della Carta dei diritti[108]. Per rispondere al possibile vizio di incompetenza, la Corte di giustizia analizza il dettato della direttiva 2002/58/CE alla luce di quanto già statuito in *Tele2 Sverige*, ritenendo che «national legislation implementing an exception to a European directive still falls within the scope of EU law»[109].

Risolta «forse troppo sbrigativamente»[110] tale questione, la Corte entra nel merito della controversia, affrontando il secondo motivo sollevato dal giudice spagnolo relativo alla espressione "gravi reati". Preliminarmente, la Corte ricorda che l'accesso da parte delle autorità pubbliche ai dati conservati dai fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione della direttiva 2002/58/CE e che, pertanto, «l'accesso ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti nella Carta» (par. 48). Tuttavia, nel caso di specie, essa ritiene che l'ingerenza predisposta dalla polizia spagnola non presenti una gravità tale da dover limitare il suddetto accesso, perché riguardante un ristretto numero di dati e una specifica tipologia di dati confinata a quelli identificativi del soggetto titolare di tale carta, ulteriormente ristretta da un contenuto periodo di tempo di dodici giorni[111]. Sulla base di queste

[107] Come rilevato da G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit., 460 il ricorso riguardava «l'adozione (…) della legge organica 13/201516. Tale normativa andava ad incidere sulle modalità di determinazione del concetto di "gravità" del reato, stabilendo due criteri alternativi: un criterio materiale (rilevanza criminosa della condotta e grave lesione dei beni giuridici) e uno normativo formale, meramente basato sulla durata della pena che, per determinare la gravità del reato, doveva essere non inferiore a tre anni. Ebbene, quest'ultimo criterio, che avrebbe potuto potenzialmente portare al di sopra della soglia di gravità la maggior parte dei reati, faceva sorgere in capo al giudice dell'appello un dubbio di conformità della normativa rispetto alla tutela dei diritti fondamentali sanciti dalla Carta di Nizza e dai principi enucleati della Corte di Giustizia nella pronuncia *Digital Rights Ireland* . Di fronte a tali dubbi il giudice spagnolo sottoponeva dunque alla Corte di Giustizia due questioni pregiudiziali, chiedendo (i) quale dei criteri individuati dalla più recente normativa spagnola fosse corretto, se quello formale o materiale, e (ii) chiedendo in subordine che fosse specificata la compatibilità "rispetto ai principi costituzionali dell'Unione" di una soglia di tre anni di reclusione come criterio formale di gravità del crimine».

[108] Cfr. par. 29: «il governo spagnolo ha espresso il parere, condiviso dal governo del Regno Unito durante l'udienza, secondo il quale la Corte non sarebbe competente a rispondere alla domanda di pronuncia pregiudiziale poiché il procedimento principale è, ai sensi dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46 e dell'articolo 1, paragrafo 3, della direttiva 2002/58, escluso dall'ambito di applicazione di queste due direttive. Tale causa non rientrerebbe dunque nell'ambito di applicazione del diritto dell'Unione, e quindi la Carta, ai sensi del suo articolo 51, paragrafo 1, non sarebbe applicabile».

[109] E. Celeste, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *EU Const.*, 2019, in corso di pubblicazione.

[110] G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit., 462.

[111] Così par. 59: « la domanda di cui al procedimento principale attraverso la quale la polizia giudiziaria chiede, ai fini di un'indagine penale, l'autorizzazione giudiziaria per l'accesso a dati personali conservati da alcuni fornitori di servizi di comunicazioni elettroniche, ha il solo scopo

considerazioni, la Corte sposta l'oggetto della sua analisi dalla gravità dei reati alla gravità della ingerenza compiuta dalla autorità pubblica e, allontanandosi dalle conclusioni di *Tele2 Sverige*[112], ritiene che nella circostanza di specie «l'accesso ai soli dati oggetto della domanda di cui trattasi nel procedimento principale non può essere qualificato come un'ingerenza "grave" nei diritti fondamentali delle persone i cui dati sono oggetto di attenzione» (par. 61)[113].

Senza soffermarsi sul merito della decisione, è in questa sede interessante notare che la sentenza in esame evita di pronunciarsi sulle condizioni della *conservazione* dei dati personali previste dalla normativa spagnola perché estranee al procedimento principale, che riguarda solo le condizioni di *accesso*[114]. Così facendo, la Corte si concentra sui profili specifici del caso, consentendo l'accesso "targhettizzato" ai dati conservati, senza sciogliere il nodo della legittimità dei *Bulk metadata programs* nazionali. Il modo con cui la Corte è in grado di risolvere la fattispecie in esame è separando l'attività di conservazione da quella di accesso: ciò non toglie che, dal lato pratico, tale distinzione appare poco utile a chiarire il quadro generale, perché i programmi di raccolta e l'acquisizione dei dati sono, logicamente, un requisito necessario per poi procedere al loro accesso[115]. Nella

di identificare i titolari delle carte SIM attivate, per un periodo di dodici giorni, con il codice IMEI del telefono cellulare rubato. Come rilevato al precedente punto 40, tale domanda riguarda l'accesso ai soli numeri di telefono corrispondenti a tali carte SIM e ai dati relativi all'identità civile dei titolari di dette carte, quali il loro cognome e, se del caso, indirizzo. Al contrario, tali dati non riguardano, come confermato sia dal governo spagnolo sia dal pubblico ministero in udienza, le comunicazioni effettuate con il telefono cellulare rubato o l'ubicazione di quest'ultimo»

[112] Come acutamente rilevato da G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit., 463 «Nel caso *Tele2 Sverige* la Corte aveva ritenuto sussistente una ingerenza grave rispetto ai diritti fondamentali poiché l'accesso aveva ad oggetto una mole indiscriminata di dati personali che "considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione" (par. 99, *Tele2 Sverige*). Nel caso in esame invece, come sottolineano i giudici, l'accesso ha ad oggetto non solo un ristretto numero di dati ovvero solo i numeri di telefono legati alla carta SIM attivata usando il codice IMEI del telefono rubato, ma anche una ristretta tipologia di dati ovvero solo quelli identificativi del soggetto titolare di tale carta, ristretti inoltre ad uno specifico e limitato periodo di tempo di dodici giorni (par. 59)».

[113] Anche in questo caso, la pronuncia fa leva sul principio di proporzionalità: come rilevato da G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit., 463, «sulla base del principio di proporzionalità, solo la lotta alla criminalità connotata dal carattere di gravità legittima una ingerenza grave nei diritti alla riservatezza e alla protezione dei dati. Ne deriva, ragionando a contrario, che qualora l'ingerenza non sia grave, non verrà richiesta, ai fini della legittimità dell'accesso e dell'obiettivo perseguito mediante esso, la presenza di un reato grave. Ecco dunque che, per comprendere se sia richiesta la natura grave del reato, si rende necessaria una previa valutazione circa la natura grave o meno dell'ingerenza»

[114] Così par. 49: «emerge dalla decisione di rinvio che, come rilevato in sostanza dall'avvocato generale al paragrafo 38 delle sue conclusioni, la domanda di pronuncia pregiudiziale non mira a stabilire se i dati personali di cui trattasi nel procedimento principale siano stati conservati dai fornitori di servizi di comunicazione elettronica in conformità con le condizioni di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta. Tale domanda verte, come emerge dal punto 46 della presente sentenza, esclusivamente sulla questione se e in quale misura l'obiettivo perseguito dalla normativa di cui trattasi nel procedimento principale sia idoneo a giustificare l'accesso delle pubbliche autorità, come la polizia giudiziaria, a tali dati, senza che le altre condizioni di accesso risultanti da tale articolo 15, paragrafo 1, siano oggetto della suddetta domanda».

[115] Analogamente G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit., 471: «Una conservazione del dato è infatti

sentenza in esame emergono tutti i limiti del sistema giurisdizionale europeo che, non permettendo ai giudici di andare oltre a quanto loro chiesto, «increases the state of uncertainty at national level, amplifies national divergence, and ultimately appears to be in stark contrast with the proactive approach that the Court adopted so far in the data retention saga»[116].

Un secondo esempio delle incertezze generate dalla *data retention saga* riguarda l'applicazione dei principi della sentenza *Tele2 Sverige* operata dai giudici della Corte d'Appello di Inghilterra e Galles del caso *Watson*. Chiamato a definire la controversia dopo i chiarimenti ottenuti dalla Corte attraverso rinvio pregiudiziale, il giudice Lord Lloyd-Jones scrive: «I regret to say that the task now facing this court is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity».[117] In forza di tali considerazioni, il giudice britannico ha applicato al caso di specie solo alcuni dei parametri identificati dal giudice comunitario (e segnatamente: a) la previsione per cui l'accesso e l'utilizzo dei dati conservati è limitato ai casi riguardanti la lotta a crimini gravi e b) quella che consente tale utilizzo solo a seguito di una pronuncia di una autorità giudiziaria o amministrativa indipendente), escludendone però altri. Tale esclusione è giustificata dalla Corte di appello per due ordini di motivi; in primo luogo, il giudice osserva che, nelle more del giudizio, le disposizioni contestate sono state modificate dal Parlamento di Westminster con l'approvazione dell'Investigatory Powers Act 2016 e che, su tale normativa, pende un nuovo ricorso pregiudiziale presso la Corte di giustizia. In secondo luogo, egli osserva che parte delle considerazioni dei giudici comunitari riguardano domande sollevate dal giudice svedese nel caso C-203/15 (*Tele2 Sveridge*) che poco si adattano al ricorso inglese (C-698/15 *Watson*). Attraverso queste due motivazioni, la Corte britannica evita, con un discutibile «display of legal gymnastics», di applicare alcune delle previsioni di *Tele2 Sveridge* al sistema inglese, ed elude forse «the compatibility of general data retention with fundamental rights», ovverosia «the most central issue in the data retention debate»[118].

Entrambi gli esempi qui riportati mostrano le difficoltà legate alla applicazione degli standards definiti dalla sentenza *Tele2 Sverige*. Come visto, tale pronuncia riguardava l'utilizzo dei dati raccolti dalle compagnie telefoniche per la lotta alla criminalità, ma i criteri elaborati dal giudice comunitario potrebbero, in astratto, essere applicati anche ai programmi di raccolta preventiva di metadati elettronici effettuata dalle agenzie di intelligence. La questione non è di poco conto se si considera che, letta congiuntamente a *Ministerio Fiscal*, la sentenza *Tele2 Sverige* parrebbe legittimare un sistema di *data retention* successiva e supportata da sospetti giustificati mentre, per loro natura, i programmi predisposti dalle agenzie di intelligence sono per loro natura preventivi perché finalizzati ad impedire

prerequisito fondamentale per poter procedere successivamente ad un accesso. Pur non trattando la questione relativa alla conservazione, non di meno viene da chiedersi quali potrebbero essere le conseguenze o l'impatto del ragionamento della Corte, riferito all'accesso, rispetto alla disciplina della data retention. In altre parole, il quesito che emerge è se sia possibile parlare di accesso mirato o meno, se prima alla base non vi è una conservazione generalizzata o se e in quale misura, avendo come base una conservazione mirata, sia possibile parlare nella stessa misura di requisiti necessari per un legittimo accesso».

[116] E. Celeste, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *EU Const.*, 2019, in corso di pubblicazione.

[117] *Secretary of State for the Home Department* v *Watson & Ors* [2018] EWCA Civ 70, para. 7.

[118] M. White, *Data Retention is still here to stay, for now…*, in *Eu Law Analysis*, 5 febbraio 2018, eulawanalysis.blogspot.com/2018/02/data-retention-is-still-here-to-stay.html?m=1

(attraverso l'elaborazione dei dati raccolti) il compimento di atti terroristici. Questa problematica, in particolare, è oggetto del ricorso pregiudiziale del caso *International Privacy*, sollevato dall'*Investigatory Powers Tribunal* di Londra, e sul quale la Corte di giustizia deve ancora pronunciarsi[119].

Due sono le questioni sollevate dal giudice britannico: innanzitutto, occorre capire se le c.d. prescrizioni della sentenza *Tele2Sverige e Watson* si applichino anche ai *Bulk metadata programs* predisposti dalla Security Intelligence Agency (SIA) per combattere il terrorismo, lo spionaggio e la proliferazione delle armi nucleari. La domanda del giudice rimettente, sollecitata dalla Ong Privacy International, va al cuore del problema relativo al bilanciamento tra privacy e sicurezza nazionale, mettendo in luce come una applicazione stringente dei parametri di *Tele2 Sverige* rischierebbe di «vanificare le misure adottate dalla SIA per proteggere la sicurezza nazionale». La funzione principale di tali programmi, infatti, è quella «di rilevare minacce alla sicurezza nazionale precedentemente ignote, attraverso tecniche di raccolta non mirate che si basano sull'aggregazione di BCD in un unico luogo, la cui principale utilità consiste nell'individuazione e nell'elaborazione tempestiva di obiettivi, oltre a fornire una base d'azione a fronte di una minaccia imminente»; ne deriva la natura necessariamente *preventiva* di tali programmi che è ben sintetizzata dalle parole dell'ex Home Secretary inglese Theresa May: «If you are searching for the needle in the haystack, you have to have a haystack in the first place»[120].

In secondo luogo, il giudice britannico richiama alla attenzione della Corte il tema delle competenze espressamente invocando l'art. 4 TUE, troppo spesso dimenticato dalle pronunce sulla *data retention*, e chiedendo se – in virtù di tale disposizione unitamente all'art. 1 par. 2 della direttiva 2002/58/CE – «la prescrizione contenuta in un ordine rivolto da un ministro (*Secretary of State*) a un gestore di reti di comunicazione elettronica di fornire dati di comunicazione in massa alle agenzie di sicurezza e di intelligence (SIA) di uno Stato membro rientri nell'ambito di applicazione del diritto dell'Unione e della direttiva relativa alla vita privata e alle comunicazioni elettroniche»[121].

Così articolato, il ricorso pregiudiziale del caso *Privacy International*, unitamente ad altri sollevati da altri ordinamenti[122], costringerà i giudici comunitari ad approfondire, declinare e forse rettificare le proprie considerazioni circa i parametri e i limiti relativi al bilanciamento tra privacy e security in Europa.

[119] Si tratta della domanda di pronuncia pregiudiziale proposta dall'*Investigatory Powers Tribunal*, Londra (Regno Unito) del 31 ottobre 2017 – *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e a.*, C-623/17.

[120] Cfr. *Theresa May: We need to collect communications data 'haystack'*, in *BBC News*, 16 ottobre 2014, www.bbc.com/news/uk-politics-29642607

[121] Il tema delle competenze costituisce così la prima domanda rivolta alla Corte di giustizia, e integrata dal seguente quesito: «in caso di risposta affermativa alla prima questione, se al menzionato ordine ministeriale si applichi alcuna delle prescrizioni della sentenza Watson o qualsiasi altra prescrizione oltre a quelle imposte dalla CEDU. In caso affermativo, in qual misura ed entro quali limiti si applichino tali prescrizioni, tenuto conto dell'esigenza fondamentale delle SIA di utilizzare tecniche di acquisizione in massa e di trattamento automatizzato per proteggere la sicurezza nazionale, e altresì in qual misura le capacità di cui trattasi, qualora altrimenti conformi alla CEDU, possano essere seriamente ostacolate dall'imposizione di dette prescrizioni».

[122] Vedi, ad esempio, la Domanda di pronuncia pregiudiziale proposta dalla Cour constitutionnelle (Belgio) il 2 agosto 2018, Causa C520/18 su cui si sofferma, diffusamente, G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, cit.

Indipendentemente delle puntuali soluzioni che la Corte vorrà adottare[123], sembra di poter concludere che l'approccio dato-centrico e costituzionalmente orientato abbracciato dalle sentenze sulla *data retention* non pare aver garantito una tutela più uniforme dei diritti sanciti dalla Carta, generando piuttosto incertezza e scetticismo nei giudici chiamati a darne attuazione. Profetiche sembrano essere, sotto questo profilo, le preoccupazioni sollevate dalla dottrina più di venti anni fa durante la fase di scrittura della Costituzione europea e, in particolare, della Carta dei diritti: con l'approvazione di tale documento, «i giudici potranno attingere ad una ricchissima risorsa giuridica – qual è il trattato costituzionale europeo – per applicarlo direttamente, anche contro le leggi nazionali. A beneficiarne, sembrerebbero essere i diritti dei cittadini. A farne le spese, la certezza del diritto e il ruolo delle istituzioni politiche»[124].

8. Prospettive future: la data protection europea dopo l'approvazione del regolamento GDPR

Come ricordato, le decisioni della Corte di Giustizia non sembrano aver interamente risolto il paradosso federale europeo legato al bilanciamento tra privacy e security nel territorio dell'Unione. Cionondimeno, la privacy rimane uno dei temi più caldi della agenda europea, come documenta da ultimo la approvazione del già citato regolamento UE 2016/679 (GDPR) che dispone una regolazione particolarmente ampia della materia.

Tale disposizione è troppo articolata per essere analizzata compiutamente in questa sede[125]. In termini generali, essa ha come obiettivo quello di fornire all'Unione «un tessuto normativo aggiornato» e «più adeguato alle esigenze attuali», definendo una normativa robusta e puntuale che è certamente destinata ad incidere in modo significativo in tutto lo spazio giuridico europeo. Il regolamento rappresenta, infatti, «un enorme salto in avanti nel sistema di protezione dei dati, se non altro perché si passa dal sistema di armonizzazione a legislazioni nazionali differenziate basato sul mutuo riconoscimento, ad un sistema fondato su un regolamento che, per sua natura, è direttamente vincolante per tutti i cittadini dell'Unione»[126]. Proprio quest'ultima considerazione descrive bene l'innalzamento qualitativo voluto dalle istituzioni europee nel definire, sempre più, i contorni di un diritto europeo alla privacy: mentre la direttiva 95/46/CE «[was] a "patchwork" that corrects and modifies elements of then existing national data

[123] In dottrina E. Celeste, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, cit. ha provato a riflettere sulle possibili soluzioni che la Corte potrà in futuro adottare per chiarire i punti inrisolti della data protection in Europa. Tre in particolare sono le ipotesi prospettate dall'autore: «The end of bulk data retention; Modulating the ban on bulk data retention; Re-legitimising bulk data retention».

[124] M. Cartabia, *La scrittura di una Costituzione europea e i poteri dei giudici*, cit., 14.

[125] Senza alcuna pretesa di esaustività, è necessario ricordare tra le novità più significative introdotte dalla nuova normativa è opportuno ricordare il diritto all'oblio, il diritto alla portabilità dei dati, il diritto ad essere informato in modo trasparente e leale sui trattamenti dei propri dati e sulle eventuali violazioni (c.d. *data breach*). Da ultimo, un'attenzione particolare merita l'introduzione della figura del responsabile della protezione dei dati (Data Protection Officer – DPO) a cui spetteranno le principali mansioni nel controllo della sicurezza dei dati e del loro trattamento. Per una analisi delle disposizioni del regolamento UE 2016/679 si veda (per tutti) F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo regolamento europeo*, Giappichelli, Torino, 2016.

[126] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo regolamento europeo*, cit., 177.

protection law»[127], la scelta di adottare un regolamento conduce «to a greater degree of harmonization, since it immediately becomes part of a national legal system» e quindi ad un «substantial shifting of power regarding data protection policymaking from the EU member states and the [data protection authorities] to the Commission»[128]. In questo modo, la disciplina europea della privacy finisce con il discostarsi ancor di più dalla regolamentazione degli Stati Uniti, caratterizzata – come ricordato in precedenza – da un alto grado di frammentazione per materia, rafforzando il ruolo delle istituzioni europee all'interno della European Fortress of Privacy.

L'importanza di tale cambiamento non è peraltro sfuggita neppure agli stati membri, che già durante la redazione della prima bozza di regolamento, avevano avanzato più di una critica attivando la procedura di Early Warning System per violazione del principio di sussidiarietà contenuto nell'art. 5 TUE. Pur non raggiungendo il numero minimo necessario alla revisione della bozza da parte della Commissione, molte delle osservazioni presentate dai parlamenti nazionali avevano sottolineato il significativo rafforzamento dei poteri della Commissione e una eccessiva centralizzazione della disciplina, soffermandosi in particolare sulla necessità di pervenire alla riorganizzazione della materia attraverso una nuova direttiva piuttosto che con un regolamento. Al di là dell'esito della procedura, che ha ad esempio portato il Parlamento europeo a rivedere alcune disposizioni, la discussione sulla necessità di adottare il pacchetto europeo di protezione dei dati digitali mette così in luce la volontà delle istituzioni europee di rafforzare, in modo unitario, la tutela della privacy digitale anche a scapito delle diverse soluzioni nazionali e ripropone così il problematico e delicat1o conflitto tra diversi sistemi tipico dello speciale federalismo europeo[129].

Per quanto riguarda il conflitto tra privacy e security, il regolamento in esame non prevede particolari disposizioni, limitandosi a ricordare nel sedicesimo considerando che «il presente regolamento non si applica (…) ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale»[130] mentre, riprendendo sostanzialmente

[127] Cfr. S. Simitis, *Einleitung in die EG-Datenschutzrichtlinie*, in U. Dammann, e S. Simitis, (eds.) *BG Datenschutzrichtlinie – Kommentar* Baden-Baden: Nomos, 1997, 61 citato da P.M. Shwarz, *The Value of Privacy Federalism*, cit., 335.

[128] C. Kuner, *The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European data protection law*, in Privacy & Security Law Report 11, 2012, rispettivamente 217 e 227.

[129] In riferimento alla vicenda v., in particolare, B. Petkova, *The Safeguards of Privacy Federalism*, cit., 635 ss. che mette in luce come le osservazioni dei Parlamenti nazionali, seppure abbiano in qualche misura evidenziato non solo le presunte violazioni del principio di sussidiarietà, hanno sottolineato comunque le ragioni di una disciplina uniforme e maggiormente armonizzata della privacy europea: «a common thread among the opinions and statements was the Commission's choice of a legal instrument: most of the national parliaments stated a preference for a new or amended directive over a regulation. (…) However the parliaments that submitted reasoned opinions objected to the means and not the necessity of an EU action on data protection, in other words, debating the "how" and not the "if" of the update to the EU data-protection framework. Notably, many of the national parliaments stated that they agreed with the Commission on the need to take action on the European level» (p. 635-636).

[130] Cfr. sedicesimo considerando regolamento UE 2016/679: «il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non

quanto già disposto dalla direttiva direttiva 95/46/CE, l'art. 23 legittima la compressione dei diritti garantiti dal regolamento purché tali limitazioni rispettino «l'essenza delle libertà fondamentali» e costituiscano «una misura necessaria e proporzionata in una società democratica» per salvaguardare la sicurezza pubblica e nazionale e la prevenzione di gravi reati[131].

In sostanza, ancora una volta, il regolamento rivia al legislatore le discipline di dettaglio e alla Corte di giustizia l'accertamento concreto delle violazioni e il bilanciamento tra privacy e security. Inoltre, per quanto concerne la disciplina specifica della *data retention*, le norme del regolamento devono essere lette in combinato disposto con l'art. 15 della direttiva 2002/58/EC che, a seguito dell'annullamento della direttiva 2006/24/CE, rimane – come già ricordato – l'unica disposizione normativa che regola direttamente tale materia. In particolare, come recentemente chiarito dall'European Data Protection Board, il regolamento assume il rango di *lex generalis* della regolamentazione europea della privacy e del trattamento dei dati sensibili, demandando alla direttiva e-Privacy il ruolo di *lex specialis* circa il problema della *data retention*[132].

In conclusione, dunque, il regolamento UE 2016/679 non fornisce particolari indicazioni per il futuro sul conflitto federale tra privacy e sicurezza nazionale in Europa. Ulteriori chiarimenti potranno forse essere ricavati dalla approvazione del regolamento e-Privacy che è destinato in futuro a sostituire la direttiva 2002/58/EC e dunque anche le disposizioni contenute nell'art. 15 su cui si sono concentrate le decisioni della Corte di giustizia nei casi *Tele2 Sveridge* e *Ministerio Fiscal*. Allo stesso tempo, però, la strategia messa in atto dalle istituzioni europee sembra quella di perseguire un pervasivo e costante aggiornamento delle disposizioni relative alla privacy europea capace di rispondere al costante sviluppo tecnologico delle nostre società digitali. Tale strategia, tuttavia, non sembra capace di risolvere del tutto le tensioni federali originate dal conflitto tra privacy e security, né sembra indicare alla Corte nuove modalità di bilanciamento tra diritti/interessi contrapposti. Sotto questo profilo, pertanto, rimangono valide le considerazioni ricordate in precedenza, e ben sintetizzate da Finnely: «the regulation of data retention as there is at the EU level is found in the vague and permissive provision of Article 15(1) of the e-Privacy Directive and the high-level

si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione»

131 Cfr. art. 23: « Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica».

132 Cfr. *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, approvata dall'European Data Protection Board il 12 marzo 2019: «A number of provisions of the ePrivacy Directive "particularise" the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector. In accordance with the principle lex specialis derogate legi generali, special provisions prevail over general rules in situations which they specifically seek to regulate. In situations where the ePrivacy Directive "particularises" (i.e. renders more specific) the rules of the GDPR, the (specific) provisions of the ePrivacy Directive shall, as "lex specialis", take precedence over the (more general) provisions of the GDPR» cfr. edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

principles set down in the judgments of the Court of Justice. For such a complex and important area, this state of affairs is far from satisfactory»[133].

9. Epilogo. Grandi poteri, grandi responsabilità: federalismo, diritti e giudici europei.

Giunti alla fine del nostro percorso, occorre provare a riavvolgere i fili della complessa vicenda della privacy digitale per verificare in che modo essa abbia interagito con lo speciale federalismo europeo e provare così a rispondere al quesito iniziale: quali sono gli effetti della *federalizing force* della Carta sulla divisione verticale dei poteri in Europa?

Le complesse vicende della privacy europea hanno messo in luce i limiti federali connessi alla redazione del *Bill of Rights* europeo. Nelle intenzioni originarie, tale documento avrebbe dovuto costituire, insieme al progetto di Costituzione, uno dei due pilastri portanti del futuro ordinamento "federale" dell'Unione. Complice il fallimento di tale progetto, l'adozione della Carta non è però stata accompagnata da una riflessione adeguata sulla architettura costituzionale europea e, quindi, sui suoi limiti. La Carta stessa esplicitamente autolimita la sua estensione, stabilendo all'articolo 51 che la sua adozione «non modifica le competenze stabilite dai trattati»; ciononostante, tale disposizione si è rivelata troppo debole per contenere, almeno in alcuni settori, la tradizionale forza centripeta del diritto comunitario. Sembra così pertanto avverarsi quanto acutamente ipotizzato da Weiler, secondo cui «redigendo un elenco [di diritti] e, un giorno, forse, incorporandolo nell'ordinamento giuridico, noi avremo sacrificato (…) la capacità di usare il sistema legale di ciascuno Stato membro come un laboratorio organico e vivente nella protezione dei diritti umani»[134]. Tale previsione, peraltro, non costituisce solo «una delle caratteristiche veramente originali dell'architettura costituzionale pre-Carta nel campo dei diritti umani»[135] ma si connette anche, più in generale, con uno degli obiettivi valoriali del principio federale in conformità del quale gli Stati membri di una federazione costituiscono «laboratories for policy innovations» in grado di «provide information about a range of alternative government policies and enable the nation to choose the most desirable one»[136].

Quest'ultima considerazione, peraltro, rafforza il convincimento di chi, in ottica comparata, ha cercato di mostrare, anche sul piano legislativo, i pregi e i difetti del c.d. *Privacy Federalism* in America come in Europa. Il sistema americano deve affrontare il rischio di una eccessiva frammentazione della protezione della privacy in cui «there will be many regulatory "inputs" from the states with too little consolidation at the federal level»[137]. Allo stesso tempo, l'autonomia concessa agli Stati «gives states and localities the ability to defy the policy status quo by developing specific innovative solutions to balance fundamental rights (or

[133] D. Finnelly *Data retention: the life, death and afterlife of a directive*, ERA Forum (2019) 19:673–692, Springer, 25 giugno 2018, 691 link.springer.com/content/pdf/10.1007%2Fs12027-018-0516-5.pdf.
[134] J.H.H., Weiler, *Diritti umani, costituzionalismo e integrazione*, cit., 528.
[135] Ibidem.
[136] M. Feeley e E. Rubin, *Federalism: Political Identity and Tragic Compromise*, University of Michigan Press, 2008, 22.
[137] Shwarz, *The Value of Privacy Federalism*, cit., 343

consumer rights) with other rights and interests»[138]. Al contrario, l'Europa ha tradizionalmente perseguito lo scopo di definire una disciplina quanto più uniforme della privacy digitale, ma «faces a risk of too few future "inputs" from the member states and too much power consolidated at the Commission»[139].

L'adozione della Carta ha così modificato la struttura stessa della integrazione europea, aprendo la stagione della tutela dei diritti. Proprio l''assenza di una architettura politica in grado di controbilanciare gli effetti di tale adozione ha privato il sistema europeo di un argine adatto a contenere gli effetti centripeti che l'introduzione di un *Bill of Rights* sempre provoca sugli ordinamenti federali o para-federali. Il risultato è che i giudici dell'Unione si sono trovati ad utilizzare uno strumento molto ampio e capace, per sua natura, di incidere sul bilanciamento tra le varie opzioni politico-valoriali: «in assenza di rigide gerarchie costituzionali pre-date, l'opera di "pesatura" del valore e di ascrizione ad esso di un contenuto normativo nel confronto con valori antagonisti presenta infatti margini elevati di arbitrarietà»[140].

Sotto questo profilo, le sentenze sulla *data protection* mostrano i limiti di un approccio slegato dal contesto federale di riferimento. Ma anche al di fuori delle specifiche problematiche legate alla privacy, tali riflessioni costringono forse i costituzionalisti a domandarsi se una eccessiva centralizzazione (o addirittura «Charterization») della tutela dei diritti costituisca davvero la risposta più adeguata alle problematiche europee o se, invece, soprattutto nei settori in cui manca una piena armonizzazione, «EU fundamental rights protection must leave a wide margin of discretion to the national authorities, and act primarily as a safety net»[141].

In secondo luogo, la *data retention saga* svela le peculiarità e i limiti del sistema giurisdizionale europeo. Come più volte ricordato, la Corte di giustizia si è fatta carico del suo nuovo ruolo di *human rights adjudicator*, sfruttando le potenzialità insite nella "costituzionalizzazione" dei diritti europei. Al contempo, i giudici europei non hanno risolto l'asimmetria strutturale esistente in Europa tra la tutela della privacy e quella della sicurezza nazionale: «in seeking to establish itself as the ultimate protector of constitutional rights in Europe, the Court of Justice has arguably neglected the importance of respect for other fundamental constitutional principles relating to the proper division of competences and the respective roles of the courts and the political organs in the Union's constitutional order»[142]. La Corte ha il coraggio di ergersi a giudice costituzionale dell'Unione, ma non quello di assumersi interamente la responsabilità di giudice federale che,

---

[138] B. Petkova, *The Safeguards of Privacy Federalism*, cit., 645. L'autrice, in particolare, indica come modello interessante da seguire per una più effettiva ed efficace tutela della privacy l'insieme di leggi statali della California.

[139] Shwarz, *The Value of Privacy Federalism*, cit., 343-344. La considerazione è svolta dall'autore soprattutto in merito alla redazione del regolamento UE 2016/679 di cui si è accennato in precedenza: «In the EU, the goal should be creation of data protection law that is attentive to checks and balances in the Community (…). The resulting balance of power should distribute privacy policymaking power among different EU and international institutions. The current Proposed Regulation falls short in this regard».

[140] G. Scaccia, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle corti europee*, cit., 6.

[141] C. Spaventa, *Should We "Harmonize" Fundamental Rights In The Eu? Some Reflections About Minimum Standards and Fundamental Rights Protection in the Eu Composite Constitutional System*, 55 Comm. Mark. L. Rev., 2018, 1022.

[142] D. Fennelly, *Data retention: the life, death and afterlife of a directive*, in *ERA Forum*, cit. 601.

in un sistema come quello europeo, dovrebbe essere strutturalmente connesso ai sui compiti giurisdizionali soprattutto quando essa è chiamata a decidere utilizzando i diritti sanciti dalla Carta come parametri costituzionali.

Emerge pertanto, in queste battute finali, il nesso tra diritti e federalismo con cui si sono aperte queste pagine e che ci ha accompagnato fino a qui: l'introduzione di un catalogo dei diritti all'interno di un sistema federale o para-federale comporta sempre una centralizzazione delle decisioni, ma allo stesso tempo il principio federale dovrebbe servire, almeno sul piano teorico, a contenerne gli inevitabili effetti centripeti. I giudici costituzionali dei sistemi federali maturi, infatti, hanno il compito di definire il bilanciamento tra diritti/interessi tenendo conto dell'idea del federalismo che, al pari del costituzionalismo, «is a creative commitment that enables governance as much as it limits governments»[143]. In questa prospettiva, il compito di una Corte suprema federale è quello di «control fair play and cohesion among the levels and units of government (…), preserve the organizational integrity of the various levels and units of governments (…) and impose burdens of justification on the central government to help ensure the salience and transparency of what is ultimately a political determination»[144].

Soprattutto quando intende utilizzare i poteri tipici di una Corte costituzionale, la Corte di giustizia dovrebbe quindi farsi carico della responsabilità di ragionare come giudice federale. Ciò significa, innanzitutto, dare spazio a quelle disposizioni della Carta che definiscono gli ambiti della sua applicazione quali, ad esempio, il ruolo occupato dalle tradizioni costituzionali degli Stati membri e dal principio di sussidiarietà. Solo prestando maggiore attenzione alle disposizioni costituzionali nazionali, infatti, sarà possibile riconciliare la protezione uniforme dei diritti fondamentali con la composita struttura dello speciale federalismo europeo. Tale operazione si rende peraltro ancora più necessaria nel campo della tutela dei diritti, che è sempre in qualche modo connessa ad elementi politico-valoriali e quindi alle diverse tradizioni costituzionali; come ricordato, «the balancing exercise between competing rights reflects local concerns and traditions: accommodating some fundamental rights plurality is a sign of constitutional maturity, not of constitutional weakness»[145].

A seguito del caso *Digital Rights Ireland*, la dottrina ha a lungo celebrato le positività del sistema di tutela della privacy in Europa, suggerendo anche in ottica comparata come l'approccio europeo alla *data protection* «offers lessons the US Supreme Court, Congress, and the President may wish to consider»[146]. Al di là di queste giuste considerazioni, può però non essere inopportuno chiedersi se, parallelamente, anche la storia costituzionale americana non possa insegnare qualcosa allo speciale federalismo europeo. La teoria del federalismo come divisione dei poteri che ha accompagnato la redazione del *Bill of Rights* non ha infatti compromesso la naturale spinta centripeta di tale strumento, che è servito – in particolare grazie all'utilizzo del XIV emendamento operato dalla Corte a

[143] D. Halberstam, *Comparative Federalism and the Role of the Judiciary*, in K. Whittington, D. Kelemen, and G. Caldeira (eds), *The Oxford Handbook of Law and Politics*, Oxford, 2008, 338.
[144] Id., 401.
[145] C. Spaventa, *Should We "Harmonize" Fundamental Rights In The Eu? Some Reflections About Minimum Standards And Fundamental Rights Protection In The Eu Composite Constitutional System*, cit., 1023.
[146] F. Fabbrini, *The European Court of Justice ruling in the Data retention case and its lessons for privacy and surveillance in the US*, cit., 95.

seguito della rivoluzione social-democratica del New Deal – a rafforzare i poteri del governo centrale nella tutela di nuovi diritti sociali[147]. Ma nonostante la profondità di tale trasformazione costituzionale, l'ideale connessione tra federalismo e diritti è in qualche modo sopravvissuta alla rivoluzione compiuta della Corte Warren per effetto, ad esempio, delle decisioni della Corte Rehnquist, protagonista di una «nuova ventata federalista che richiamava almeno formalmente le categorie del passato caricandole di significati più moderni»[148]. Come ricordato dalla Corte nel caso *Gregory v. Ahcroft*, infatti, «the constitutionally mandated balance of power between the States and the Federal Government was adopted by the Framers to ensure the protection of our fundamental liberties. (…) If this "double security" is to be effective, there must be a proper balance between the States and the Federal Government. These twin powers will act as mutual restraints only if both are credible. In the tension between federal and state power lies the promise of liberty»[149].

Nelle conclusioni nel caso *Tele2 Sverige*, l'avvocato generale Saugmandsgaard Øe ha introdotto le sue considerazioni con una famosissima citazione tratta dal *The Federalist* n. 51: «Se gli uomini fossero angeli, nessun governo sarebbe necessario. (…) Nel prefigurare un governo di uomini nei confronti di altri uomini, questa è la difficoltà più grande: prima bisogna permettere al governo di controllare i governati, poi obbligare il governo a controllare se stesso»[150]. Queste parole di Madison spiegano bene la «grande difficoltà» dalle nostre democrazie nel trovare il giusto bilanciamento tra privacy e security; da un lato, infatti, la conservazione dei dati elettronici e digitali consente «al governo di controllare i governati» per ragioni connesse alla loro sicurezza. Dall'altro, occorre però «obbligare il governo a controllare se stesso», ovverosia a limitare la sua azione a quanto strettamente necessario: questo, ad avviso dell'avvocato generale, è il compito a cui è chiamata la Corte di giustizia.

Le considerazioni di Saugmandsgaard Øe sembrano però sottovalutare l'importanza che Madison riponeva nella creazione di quelle «garanzie ausiliarie indispensabili» che sono descritte nel proseguo del suo scritto: «nella repubblica federale d'America, avviene che il potere cui il popolo rinuncia sia prima diviso tra due diversi sistemi costituzionali, indi, nell'ambito di ciascuno di essi, nuovamente suddiviso in vari settori ed organi. Di qui la doppia garanzia di libertà per il popolo. I vari governi, infatti, si controlleranno l'un l'altro e al medesimo tempo si

[147] In riferimento si veda, per tutti, G. Bognetti, *Lo spirito del costituzionalismo americano*, Torino, 2000.

[148] A. Pin, *La sovranità in America. Il federalismo di fronte alla corte suprema dalle origini alla crisi economica contemporanea*, Padova, 2012, 74. Si tratta, in particolare, del c.d. Il c.d. *New Federalism* avviato a partire dagli anni Novanta ha così rinnovato l'originario legame tra federalismo e libertà tipico del costituzionalismo americano applicandolo anche a controversie riguardanti i diritti sociali.

[149] Cfr. *Gregory v. Ahcroft* 501 U.S. 727 1991. Ciò spiega perché, anche in tempi più recenti, il principio federalista emerga a volte nelle sentenze della Corte suprema riguardanti il riconoscimento dei c.d. nuovi diritti: come ricordato dal giudice Alito nella sua dissenting opinion relativa al famoso caso *Obergfell v. Hodges* sul riconoscimento federale del diritto al c.d. *same sex marriage*, infatti, «[t]he system of federalism established by our Constitution provides a way for people with different beliefs to live together in a single nation (…) If the issue of same-sex marriage had been left to the people of the States, it is likely that some States would recognize same-sex marriage and others would not» (576 U.S. __2015).

[150] Così la citazione di The Federalist n. 51 riportata dalle Conclusioni Avv. Gen. Cause riunite Tele2 Sverige AB contro Post-och telestyrelsen (C-203/15) e Secretary of State for the Home Department contro Tom Watson et. Al. (C-698/15).

ISSN: 2037-6677

autocontrolleranno»[151]. Questo, in sostanza, è il valore del federalismo che, al pari del costituzionalismo, è uno strumento pensato per contenere verticalmente i poteri e alimentare il pluralismo giuridico all'interno delle nostre società complesse: «federalism is a pre-commitment to the principle of divided powers, which is not reexamined in daily politics, but which nonetheless must remain flexible as societies search for the proper jurisdictional scope for government activity»[152].

[151] *The Federalist*, n. 51, edizione italiana. Bologna, 1997, 459-460.

[152] Così D. Halberstam, Comparative Federalism and the Role of the Judiciary, cit., citando K. Nicolaidis, *Conclusion: The Federal Vision Beyond the Federal State.* In R. Howse, K. Nicolaidis (a cura di) *The Federal Vision: Legitimacy and Levels of Governance in the United States and the European Union*, Oxford, 441.