RIVISTA ITALIANA
PER LE
SCIENZE GIURIDICHE

Fondata da Francesco Schupfer e Guido Fusinato

SOTTO GLI AUSPICI DELLA FACOLTÀ DI GIURISPRUDENZA
DELLA SAPIENZA - UNIVERSITÀ DI ROMA

DIRETTORE

Mario Caravale

nuova serie

8

2017

JOVENE EDITORE

RIVISTA ITALIANA
PER LE
SCIENZE GIURIDICHE

Fondata da Francesco Schupfer e Guido Fusinato

SOTTO GLI AUSPICI DELLA FACOLTÀ DI GIURISPRUDENZA
DELLA SAPIENZA - UNIVERSITÀ DI ROMA

DIRETTORE

Mario Caravale

nuova serie

8

2017

JOVENE EDITORE

Direttore: Mario Caravale

Direzione e redazione: Sapienza - Università di Roma - Facoltà di Giurisprudenza - Presidenza - Piazzale Aldo Moro 5 - 00185 Roma RM

Comitato direttivo: Paolo Ridola - Giuseppe Santoro Passarelli - Enrico del Prato Luisa Avitabile - Nicola Boccella - Enzo Cannizzaro - Mario Caravale - Claudio Consolo Andrea Di Porto - Antonio Fiorella - Laura Moscati - Cesare Pinelli - Leopoldo Tullio

Comitato scientifico: Jean-Bernard Auby (Parigi) - Jurgen Basedow (Amburgo) - Luigi Capogrossi Colognesi (Roma) - Erhard Denninger (Francoforte) - Pierre-Marie Dupuy (Parigi) - Gianni Ferrara (Roma) - Yves Gaudemet (Parigi) - David Gerber (Chicago) Peter Häberle (Bayreuth) - Erik Jayme (Heidelberg) - Natalino Irti (Roma) - Anne Lefebvre Teillard (Parigi) - Gilberto Lozzi (Roma) - Alessandro Pace (Roma) - Mattia Persiani (Roma) - Fabrizio Ramacci (Roma) - Jerome H. Reichman (Durhan) - Pietro Rescigno (Roma) - Stefano Rodotà (Roma) - Alberto Romano (Roma) - Gunther Teubner (Francoforte) - Michel Troper (Parigi) - Hanns Ullrich (Monaco, Baviera)

Redazione: Cesare Pinelli (redattore capo), Nicola Cezzi, Fulvio Costantino

Amministrazione: JOVENE EDITORE - Via Mezzocannone 109 - 80134 Napoli NA Italia Tel. (+39) 081 552 10 19 - Fax (+39) 081 552 06 87 - website: www.jovene.it - email: info@jovene.it

Abbonamento: € 35,00

Il pagamento va effettuato direttamente all'Editore: a) con versamento sul c.c. bancario IBAN: IT62G0307502200CC8500241520 o sul c.c.p. 14015804, indicando chiaramente gli estremi dell'abbonamento; **b)** a ricezione fattura; **c)** on line collegandosi al sito dell'Editore: www.jovene.it.
Gli abbonamenti si intendono rinnovati per l'anno successivo se non disdetti con apposita segnalazione entro la scadenza.
Le comunicazioni in merito a mutamenti di indirizzo vanno indirizzate all'Editore.
I contributi pubblicati in questa Rivista potranno essere riprodotti dall'Editore su altre proprie pubblicazioni, in qualunque forma.

Direttore responsabile: Mario Caravale

ISSN 0390-6760

Registrazione presso il Tribunale di Napoli n. 51 del 18 giugno 2010.

Stampato in Italia Printed in Italy

INDICE

PROLUSIONI

3 Bruno Romano
Ragione giuridica e ragione dialogica in Giorgio Del Vecchio

15 Giorgio Del Vecchio
Sui principî del diritto

SAGGI

67 Guido Alpa
Diritti, libertà fondamentali e disciplina del contratto: modelli a confronto

165 Augusto Cerri
Per un europeismo maturo

187 Gianni Ferrara
Per lo storico della Costituzione italiana e della problematica sulla sua effettività a 70 anni dalla redazione. (Appunti di un costituzionalista coevo)

TECNOLOGIE E DIRITTO

205 Guido Alpa
Tecnologie e diritto privato

315 Luisa Avitabile
Il diritto davanti all'algoritmo

329 Pasquale Bronzo
L'impiego del trojan horse *informatico nelle indagini penali*

357 Fulvio Costantino
Intelligenza artificiale e decisioni amministrative

393 Alberta Fabbricotti, Leonardo Raponi
La struttura multilivello della protezione dei dati personali in Europa

443 Laura Moscati
Sfide tecnologiche e diritto d'autore tra riferimenti storici e direttive europee

467 Cesare Pinelli
«Postverità», verità e libertà di manifestazione del pensiero

479 Oreste Pollicino, Matteo Leffi
Il caso ICANN nel dibattito sulla Internet governance*: una proposta di approccio frazionato*

INCONTRI DI STUDIO

503 Guido Alpa
Ricordo di Stefano Rodotà

521 Enrico Gallucci
L'esercizio del potere di grazia dopo la sentenza n. 200/06 della Corte costituzionale

RECENSIONI

569 Massimo Brutti
L'incontro tra Pilato e Gesù (brevi note su un libro recente)

La struttura multilivello della protezione dei dati personali in Europa

Alberta Fabbricotti e Leonardo Raponi[1]

SOMMARIO: 1. Introduzione. – 2. Terminologia. – 3. Evoluzione dell'*informational privacy* in Europa. – 4. Le garanzie offerte nell'ambito del Consiglio d'Europa. – 5. La complessa normativa dell'UE. – 5.1. La base giuridica della protezione dei dati personali. – 5.2. Il nuovo 'pacchetto europeo di protezione dei dati personali'. – 5.2.1. Il Regolamento 2016/679/UE. – 5.2.2. Il rapporto del GDPR con altri atti di diritto derivato dell'UE. – 5.2.2.1. La direttiva 2002/58/CE (c.d. Direttiva ePrivacy). – 5.2.2.2. Il Regolamento 2001/45/CE. – 5.2.3. La direttiva 2016/680/UE. – 6. Le nuove prospettive dell'*informational privacy*: verso una reale uniformità in Europa. – 7. Conclusioni.

1. *Introduzione*

La protezione dei dati personali del singolo (con le dovute precisazioni terminologiche che saranno fornite poco più avanti) costituisce oggi l'oggetto di una regolamentazione europea assai articolata e ormai piuttosto sofisticata. Questa complessa disciplina ha finito per evidenziare una struttura che può definirsi 'multilivello' o 'multistrato' in quanto, da un lato, essa è il risultato della produzione normativa di più organizzazioni internazionali aventi una natura e una funzione diversa e perché, dall'altro lato, la medesima materia è stata affrontata nel quadro di ciascuno di tali sistemi giuridici particolari a successive riprese e/o con modalità e strumenti aventi una portata ed una efficacia differenti.

Le organizzazioni coinvolte sono essenzialmente tre, l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), il Consiglio d'Europa (CdE) e l'Unione europea (UE); si tratta perciò di organizzazioni tutte caratterizzate da una prevalente, se non esclusiva, componente geografica europea in termini di *membership*[2]. Seb-

[1] Nel complesso il presente saggio è il frutto della cooperazione dei due autori. È tuttavia possibile attribuire i paragrafi 1, 2, 3, 4 e 7 a Alberta Fabbricotti ed i paragrafi 5 e 6 a Leonardo Raponi.

[2] L'OCSE (originariamente OECE, Organizzazione per la Cooperazione Economica Europea) è composta da 35 Stati membri, di cui solo 9 non europei (USA, Canada, Messico, Cile, Australia, Nuova Zelanda, Giappone, Corea del Sud, Israele).

bene all'OCSE vada riconosciuto l'importante merito di aver elaborato le *Linee guida sulla protezione della privacy e dei flussi transnazionali dei dati personali*[3], l'indagine che ci si propone di svolgere in questo saggio si concentrerà sugli strumenti giuridici predisposti nel quadro del CdE e nel diritto dell'UE, al fine di identificarne possibili interazioni, sovrapposizioni e complementarità. Come è noto, soltanto questi strumenti possono dirsi giuridicamente vincolanti, mentre le deliberazioni dell'OCSE appartengono al c.d. *soft law*.

I paragrafi che seguono saranno dedicati, dapprima, a precisare la terminologia tecnico-giuridica utilizzata nel presente scritto (par. 2) e ad illustrare l'evoluzione storica della protezione dei dati personali in Europa (par. 3), e, successivamente, ad analizzare struttura e portata sia delle garanzie offerte dagli strumenti giuridici promossi nel quadro del CdE (par. 4) che della complessa e capillare disciplina fornita dal diritto dell'UE (par. 5). Seguirà una finestra sulle future prospettive di riforma ed attualizzazione delle discipline attualmente in vigore (par. 6). Non mancherà, come di consueto, un epilogo con le conclusioni (par. 7).

Le diverse parti non avranno lo stesso spessore. Dato lo sviluppo, sia in termini quantitativi che qualitativi del regime di protezione dei dati personali dell'UE, soprattutto in vista della riforma che diventerà effettiva nel mese di maggio 2018, al par. 5 sarà riservato uno spazio maggiore, come evidenziato anche dalla sua ripartizione in diversi sottoparagrafi.

2. *Terminologia*

Coniato negli Stati Uniti ad opera di Samuel D. Warren e Louis D. Brandeis, autori del celebre articolo *The Right to Privacy* pubbli-

[3] *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, annexed to the OECD Council of 23 November 1980; le *Guidelines* hanno subìto una profonda revisione nel 2013 al fine di tener conto dell'evoluzione delle tecnologie, dei mercati e dei comportamenti degli utenti e dell'importanza crescente delle identità digitali. Per un approfondimento, v. OECD, *The OECD Privacy Framework*, 2013, *http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf*; C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, 2013, 35-36; L.A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford, 2014, 43-51. In generale, per una ricerca sulle attività dell'OCSE a tutela della privacy si invita a visitare la pagina *http://oe.cd/privacy*.

cato sulla *Harvard Law Review* alla fine del 1890[4], il diritto in questione è stato al centro di un fervido dibattito dottrinale in concomitanza con il manifestarsi da parte della relativa regola di un forte dinamismo quanto al significato e alla portata dei suoi contenuti.

Originariamente concepita come un mero '*right to be let alone*' – quasi declinato come un'estensione del classico diritto di proprietà –, la *privacy* ha esteso i propri confini sino al riconoscimento di un più generale ed omnicomprensivo diritto alla riservatezza della persona. Tale posizione giuridica non si è più esplicata semplicemente in una visione negativa della *privacy* come '*jus solitudinis*' ovvero come diritto a non dover sopportare intrusioni – indesiderate – altrui, ma anche in un'accezione 'pro-attiva' di rispetto dell'individuo e di sviluppo libero della propria personalità. A ciò si aggiunga che un ulteriore ampliamento della nozione si è avuto in concomitanza con l'evoluzione delle tecnologie informatiche e della comunicazione che ne hanno stimolato una nuova configurazione quale diritto all'autodeterminazione informativa ovvero alla protezione dei dati personali[5]. Ed è proprio in questo contesto di progresso tecnologico (dalla seconda metà del XX secolo) che si innesta l'importazione nel vecchio continente del concetto già diffuso negli USA. Nel nuovo ambito geografico, il concetto di *privacy* si evolve adattandosi alle esigenze concrete della società europea e, nello specifico, prediligendo un'accezione strettamente correlata ai nuovi strumenti di comunicazione – quali la televisione e *mass media* – ed informatici – quali i *computer*, i telefoni mobili e così via –.

In Europa, dunque, la *privacy* è principalmente intesa come – sinonimo di – tutela dei dati personali. Da un'analisi più accurata si evince tuttavia che la protezione dei dati non coincide *tout court* con

[4] S.D. Warren e L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, vol. 4, n. 5, 193-220.

[5] Sul punto v. S. Rodotà, in *Repertorio di fine secolo*, Roma-Bari, 1993, 189-190, che osserva «una definizione della *privacy* come diritto d'essere lasciato solo, come semplice riservatezza, ha da tempo perduto un significato generale, anche se individua un valore, continua a cogliere un aspetto essenziale del problema e può essere applicata a specifiche situazioni […]. La privacy, quindi, può in primo luogo, e più precisamente, essere definita come il diritto di mantenere il controllo sulle proprie informazioni. È presumibile che questa tendenza proseguirà nei prossimi anni e che, quindi, regole e definizioni si muoveranno in questa definizione […]». In proposito v. anche S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 62 ss.

la *privacy*, ma ne rappresenta uno specifico ambito di esercizio[6]. Mentre la *privacy* costituisce il diritto individuale di ciascuno di mantenere il controllo del/sul proprio corpo, abitazione, proprietà, pensieri, segreti, identità ecc., la protezione dei dati personali disciplina la raccolta e l'utilizzo delle informazioni relative all'identificazione delle persone, quale ne sia la fonte[7]. Sarebbe dunque più corretto usare la terminologia di '*informational privacy*', di '*information privacy*' ovvero di '*data privacy*'. Tuttavia, per evitare distinzioni e classificazioni che potrebbero ingenerare confusione anziché chiarezza, nel presente testo verrà alternativamente utilizzata la terminologia '*privacy*', 'protezione dei dati personali' o '*informational privacy*', restando inteso qual'è l'accezione accolta.

Così declinata, la *privacy* mostra la propria precisa caratterizzazione proprio nell'epoca contemporanea nell'ambito della quale il progresso tecnologico viaggia a velocità elevatissime. Anche se difficilmente concepibili in un recente passato, i concetti di ICT (*Information and Communications Technology*), di IoT (*Internet of Things*), di '*web* 4.0' o di 'rivoluzione 4.0' appartengono in modo chiaro ed incontrovertibile alla società del XXI secolo. Tali rappresentazioni mentali sono sempre più sorrette da risultati tecnologici concreti e tangibili che impongono una revisione e un ripensamento di gran parte delle tradizionali situazioni giuridiche tra le quali risulta essere protagonista indiscussa proprio la *privacy* (o meglio, l'*informational privacy*). Attraverso la sua disciplina il legislatore e la giurisprudenza tentano di tutelare il singolo da un progresso che nasce ontologicamente neutrale, ma che viene utilizzato dall'uomo in modo aggressivo ed invasivo delle vite dei suoi simili. Ad esempio, si assiste oggi al fenomeno dei c.d. *big data*: la raccolta, conservazione e trattamento dei dati personali ha raggiunto livelli talmente macroscopici da poter potenzialmente coinvolgere l'intera umanità. Ne è un segnale evidente lo scandalo *Facebook - Cambridge Analytica* di queste ultime settimane (marzo 2018), riguardante l'uso dei dati personali di 87 milioni di utenti Facebook al fine presunto di influenzare le ultime elezioni negli USA e il referendum sulla Brexit.

[6] J.Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in *Yale Law Journal*, 2004, vol. 113, n. 1, 1151-1221.

[7] C.B. CASAGRAN, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, Londra/NewYork, 2017, 4.

3. *Evoluzione dell'*informational privacy *in Europa*

Il primo riconoscimento del diritto alla *privacy* a livello europeo va ricondotto, non già all'attività di organizzazioni sovrannazionali o internazionali, bensì all'iniziativa di un ridotto numero di Stati che adottò le prime normative in materia nel corso degli anni Settanta, quando la tecnologia fornita dai *computer* cominciava ad essere utilizzata dalle agenzie governative e dalle grandi industrie private per raccogliere, elaborare ed adoperare i dati personali[8]. Nondimeno, una certa attenzione degli Stati si era andata al contempo manifestando anche nel contesto della cooperazione intergovernativa rappresentata dal CdE. Già nel 1968 l'Assemblea Parlamentare aveva emanato la raccomandazione n. 509 titolata *Human Rights and Modern Scientific and Technological Developments*, attraverso la quale aveva espresso le proprie preoccupazioni in merito a potenziali violazioni dei diritti fondamentali del singolo – «and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights»[9] – causate dalla moderna evoluzione tecnologica e scientifica. A tal fine, l'Assemblea Parlamentare aveva invitato il Comitato dei Ministri ad incaricare la Commissione di esperti sui diritti umani di uno specifico studio sull'adeguatezza del livello di protezione dei dati personali in Europa[10]. Il riscontro negativo della Commissione di esperti aveva condotto l'Assemblea Parlamentare e il Comitato dei Ministri europei della giustizia ad adottare diverse risoluzioni dirette ad elevare il grado di tutela della *privacy* in Europa[11]. I lavori (e le seguenti risoluzioni) del CdE si erano fondati

[8] Si ricordino in proposito il *Datenschutzgesetz* adottato dallo Stato federato tedesco di Hessen nel 1970, il *Data Act* svedese del 1973, la *Federal Data Protection Law* tedesca del 1977 o, ancora, in Francia la *Loi relative à l'informatique, aux fichiers et aux libertés* del 1978. Per un approfondimento si vedano, per tutti, R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 32, e F. BIGNAMI, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, in *Michigan Journal of International Law*, 2005, vol. 26, 818.

[9] Assemblea parlamentare del CdE, *Raccomandazione 509*, 31 gennaio 1968, par. 3. Per un commento della raccomandazione, si vedano A.H. ROBERTSON (ed.), *Privacy and Human Rights: Papers by Experts on An Issue of Growing Importance given under the Auspices of the European Convention on Human Rights*, Manchester, 1973, 379-380; F. POCAR, *Commentario breve ai trattati della Comunità e dell'Unione europea*, Padova, 2001, 959.

[10] *Ibidem*, par. 8.

[11] Tra le prime raccomandazioni del Comitato dei Ministri in materia si ricordano: CDE, *Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle ban-*

su due assunti principali: da un lato, la consapevolezza della necessità di un'opera di ravvicinamento delle legislazioni degli Stati membri e, dall'altro, l'evidenza di uno stretto legame fra il diritto alla protezione dei dati personali e la 'vita privata intima delle persone', come parte integrante del più generale diritto fondamentale al rispetto della vita privata e familiare già tutelato dall'art. 8 della *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* (CEDU).

Queste considerazioni hanno guidato il CdE verso un autonomo riconoscimento del diritto in questione mediante un apposito strumento giuridico, quale è rappresentato dalla *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* (denominata anche Convenzione n. 108 o STCE n. 108)[12], firmata a Strasburgo il 28 gennaio 1981. Di questo trattato si parlerà specificamente più avanti. Ciò che importa segnalare ora è il rapporto tra la Convenzione n. 108 e la (ben più) nota tutela dei dati personali offerta dall'art. 8 della CEDU, per effetto della giurisprudenza della Corte europea dei diritti umani (CtEDU).

Contrariamente a quanto si potrebbe ritenere, è stata probabilmente l'intervenuta firma della Convenzione n. 108 a suggerire alla CtEDU l'interpretazione evolutiva e funzionale in virtù della quale l'art. 8 CEDU, originariamente concepito per tutelare la vita privata e familiare, ha finito per estendere la propria protezione anche ai dati personali, e non viceversa. A riprova di ciò basti considerare che le prime sentenze della CtEDU che riflettono tale interpretazione evolutiva vengono pronunciate solo a partire dal 1981, quando la Convenzione n. 108 era stata da poco aperta alla ratifica degli Stati membri del CdE. Comprensibilmente, infatti, nel testo della CEDU risalente al 1950 è assente un qualsivoglia riferimento al trattamento dei dati personali dell'individuo[13]. Come è noto, è proprio grazie al-

che di dati elettroniche nel settore privato, 26 settembre 1973; CdE, *Risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico*, 20 settembre 1974; CdE, *Raccomandazione n. R(87)15 relativa alla disciplina dell'uso dei dati a carattere personale nell'ambito della pubblica sicurezza*, 17 settembre 1987.

[12] CdE, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, STCE n. 108, 1981.

[13] Secondo F. Pizzetti, l'assenza di riferimenti all'interno della maggior parte delle costituzioni nazionali del dopoguerra e della CEDU è la conseguenza di una concezione

l'attività esegetica evolutiva della CtEDU che la CEDU rappresenta ancora oggi uno strumento attuale ed efficiente – 'diritto vivente', per usare le parole della stessa CtEDU[14] –, e la giurisprudenza in tema di protezione dei dati personali sulla base dell'art. 8 è uno degli esempi più calzanti di questo dinamismo della CEDU.

È con un certo ritardo rispetto ai risultati raggiunti nel quadro della CdE che la *informational privacy* trova una sua specifica tutela nel diritto dell'UE. Presumibilmente il richiamo alla CEDU e ai principi costituzionali comuni operato dall'art. 6 del Trattato sull'Unione europea (TUE) consente di configurare la protezione dei dati personali quale principio generale dell'ordinamento fin dall'epoca di Maastricht. Tuttavia, è solo nel 1995 che l'UE si dota di uno strumento *ad hoc*, la direttiva 95/46 in materia di protezione dei dati personali[15]. Come si vedrà meglio più avanti[16], la finalità di questa direttiva non è tanto quella *sic et simpliciter* di tutelare il singolo nel garantirgli la riservatezza dei suoi dati personali, quanto di favorire la circolazione dei dati personali tra Stati membri UE, in quanto funzionale alle esigenze del mercato unico, ed evitare che questa incontri degli ostacoli a causa dell'attuazione di regolamentazioni domestiche difformi. Questo spiega anche perché si esclude fin da principio che la direttiva possa riguardare attività attinenti alla pubblica sicurezza, alla difesa, alle attività dello Stato in materia di diritto penale[17].

A circa cinque anni di distanza dalla direttiva 95/46, si ha una svolta importante nell'inquadramento giuridico dell'*informational*

tipica dell'epoca che considerava la tecnologia quale mero strumento assoggettato all'individuo, non anche come un fattore capace di influire sui diritti del singolo. Era quindi assente «un'adeguata consapevolezza del ruolo e degli effetti della tecnica sull'evoluzione dei diritti». Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 46/95 al nuovo regolamento europeo. Vol. 4/I*, Torino, 2016, 56-58.

[14] CtEDU, *Tyrer* c. *Regno Unito*, sentenza del 25 aprile 1978, n. 5856/72, par. 31: «the Convention is a living instrument which […] must be interpreted in the light of present-day conditions».

[15] Parlamento europeo e Consiglio, *Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *GUCE* n. L 281 del 23/11/1995, 31-50. Il fatto che tutti e 15 gli Stati membri dell'UE fossero già parti contraenti della Convenzione n. 108 esclude che vi possano essere contraddizioni tra la direttiva e questo trattato.

[16] *Infra*, par. 5.1.

[17] Considerando 13, Preambolo direttiva 95/46/CE. Sul punto, v. Pardolesi, *op. cit.*, 38.

privacy grazie alla Carta dei diritti fondamentali dell'UE (CDFUE) proclamata nel 2000 a Nizza. La *privacy* torna qui ad essere un diritto universale dell'uomo, il cui esercizio deve ritenersi svincolato da condizionamenti di carattere economico-mercantilistico. Inoltre, la protezione dei dati personali assurge finalmente a disciplina a sé stante (art. 8, CDFUE), sapientemente tenuta distinta dal contiguo regime di rispetto della vita privata e familiare (art. 7, CDFUE). La disposizione *de qua* recita:

> «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
> 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
> 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Evidentemente, l'art. 8 non sfugge alle limitazioni che colpiscono in generale l'ambito di applicazione della CDFUE. Ai sensi del noto art. 51, par. 1, della stessa Carta, le garanzie offerte dalla CDFUE operano nei confronti delle istituzioni dell'Unione e degli Stati membri solo nell'attuazione del diritto dell'UE[18]. Una precisazione, questa, che si salda con quella del successivo paragrafo dell'art. 51, come già con l'art. 6, par. 1, TUE, secondo cui le disposizioni della Carta non estendono le competenze dell'Unione definite dai trattati.

Come è noto, solo con il Trattato di Lisbona si è proceduto a riconoscere formalmente un valore giuridico alla CDFUE, la quale è assurta a fonte di diritto primario al pari dei Trattati istitutivi stessi[19]. Tale riconoscimento si è tradotto in risultati tangibili espressi in puntuali richiami all'art. 8 CDFUE nelle sentenze della Corte di giustizia dell'UE (CGUE), e, conseguentemente, in una maggiore tu-

[18] La CGUE ha ricostruito la nozione di 'ambito di applicazione del diritto dell'UE' in modo ampio, facendovi conseguentemente rientrare non solo quelle normative e condotte statali che attuano il diritto dell'UE in maniera diretta, ma anche quelle che interferiscano con il diritto dell'Unione indirettamente. Per un approfondimento, v. per tutti, E. Cannizzaro, *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Seconda edizione, Torino, 2017, 159-165.

[19] Cfr. Art. 6, par. 1, TUE.

tela dei diritti fondamentali a prescindere da una loro connessione con l'esercizio delle libertà poste alla base dello Spazio di libertà, sicurezza e giustizia (SLSG)[20].

Inoltre, con l'entrata in vigore del Trattato di Lisbona nel 2009, e la sostituzione dell'art. 286 del Trattato che istituisce la Comunità europea (TCE) con l'art. 16 TFUE si compie l'ultima tappa fondamentale dell'evoluzione della protezione dei dati personali in Europa. In virtù della nuova disposizione viene conferita alle istituzioni dell'UE una competenza legislativa generale in materia di protezione dei dati personali. Ed è su questa esplicita base giuridica che l'UE ha potuto varare la riforma complessiva della disciplina che diventerà effettiva a partire dal maggio 2018, e sulla quale si dirà profusamente *infra* al par. 5.

4. *Le garanzie offerte nell'ambito del Consiglio d'Europa*

La protezione dei dati personali è un tema verso il quale il CdE ha mostrato un forte interesse fin dall'epoca in cui si sono manifestate le prime preoccupazioni a proposito delle indebite ingerenze nella sfera privata dei singoli per effetto delle nuove scoperte tecnologiche. L'attività del CdE in questo settore ha dato vita a due meccanismi di garanzia che, pur operando parallelamente mediante tec-

[20] Si ricordano, in particolare, CGUE, *Google Spain SL, Google Inc.* c. *AEPD, Mario Costeja Gonzáles*, sentenza del 13 maggio 2012, C-131/12; CGUE, *Digital Rights Ireland LTD*, sentenza dell'8 aprile 2014, C-293/12 e C-594/12; CGUE, *Schrems* c. *Data Protection Commissioner*, sentenza del 6 ottobre 2015, C-362/14. Per una rassegna della giurisprudenza della Corte di Giustizia dell'UE in materia di protezione dei dati personali si rinvia a S. Crespi, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comparato*, 2015, fasc. 3-4, 819-842; R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza Costituzionale*, 2016, fasc. 1, 289-306; M. Brkan e E. Psychogiopoulou, *Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham, 2017, 10-31; I. Cameron, *Balancing Data Protection and Law Enforcement Need: Tele2 Servige and Watson*, in *Common Market Law Review*, 2017, vol. 54, 1467-1496; F. Guella, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *Diritto pubblico comparato ed europeo*, 2017, n. 2, 349-357; A. Pisapia, *The Harmonization of the Data Protection Law. Critical Remarks on the New General European Regulation*, in *Osservatorio del diritto civile e commerciale*, 2017, fasc. 1, 243-260; O. Pollicino e M. Bassini, *Art. 8 CDFUE*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 142-156.

niche e modalità differenti, finiscono in qualche misura per integrarsi. Da un lato, è stato predisposto uno strumento *ad hoc*, vale a dire la citata Convenzione n. 108; dall'altro lato, è stata estesa in via giurisprudenziale la portata dell'art. 8 della CEDU relativo alla protezione della vita privata e familiare, così da ricondurvi anche la fattispecie della *informational privacy*.

Per quanto riguarda la Convenzione n. 108, questa era e rimane l'unico trattato internazionale esistente in materia di protezione dei dati personali. La Convenzione fissa un livello minimo di tutela che protegge l'individuo da eventuali abusi derivanti dalla raccolta e dal trattamento informatizzati dei dati personali, effettuati sia nel settore privato che in quello pubblico, e dallo scambio transfrontaliero con Paesi terzi. L'applicazione della Convenzione è limitata in via di principio alla tutela di persone fisiche dalla raccolta e dal trattamento, necessariamente automatizzato, dei loro dati. Tuttavia, alle Parti contraenti è rilasciato un qualche margine di discrezionalità. Ai sensi del suo art. 3, par. 2, ciascuno Stato può in qualsiasi momento, inoltrando una comunicazione al Segretario Generale del CdE, escludere determinate categorie di raccolte automatizzate di dati dall'ambito di applicazione dell'accordo ovvero estendere quest'ultimo a raccolte non automatizzate o a soggetti diversi dalle persone fisiche. Il successivo art. 9, al par. 2, prevede invece due specifiche finalità il cui perseguimento consente agli Stati di derogare alle disposizioni della stessa Convenzione: in primo luogo, la protezione della sicurezza dello Stato, della sicurezza pubblica, degli interessi monetari dello Stato ovvero la repressione dei reati; in secondo luogo, la protezione di ulteriori interessi della persona soggetta al trattamento dei dati ovvero la tutela dei diritti e delle libertà di altre persone.

Dall'analisi di queste due deroghe si rileva una natura flessibile del sistema della Convenzione n. 108 che può ampliarsi o ritrarsi a seconda dell'esercizio di tali facoltà da parte di ciascuno Stato contraente, con la conseguente possibilità della creazione di sub-regimi di protezione, ciascuno avente un proprio e peculiare ambito applicativo. In aggiunta, la Convenzione, attraverso la clausola di salvaguardia prevista dall'art. 11, non preclude alle Parti contraenti di accordare una protezione più avanzata. Questa disposizione ha consentito e stimolato la produzione, sia a livello nazionale che a livello europeo, di *standard* di tutela più elevati, realizzando così una vera e propria 'cultura della *privacy*' in Europa.

Per ciò che riguarda la sua portata territoriale, la Convenzione n. 108 è aperta non solo a tutti gli Stati membri del CdE (ad oggi, pari a 47), ma anche all'UE. Nel 1999, infatti, sono stati apportati degli emendamenti alla Convenzione per consentire all'Unione di accedervi[21].

Inoltre, l'art. 23 conferisce al Comitato dei Ministri il potere di invitare ad aderire alla Convenzione Stati non membri del CdE anche *extra*-europei[22]. Questa facoltà, che viene esercitata solo a partire dal 2013, ha prodotto una notevole estensione dell'ambito di applicazione territoriale della Convenzione che, nel momento in cui si scrive, annovera anche Mauritius, Senegal, Tunisia, Uruguay e che potrebbe in un prossimo futuro ampliarsi ulteriormente, tenuto conto degli inviti già rivolti ad Argentina, Burkina Faso, Capo Verde e Marocco[23]. La portata della Convenzione n. 108 come *standard* minimo universale, il suo carattere aperto e la circostanza che trattasi del (finora) unico trattato internazionale esistente in materia potrebbero costituire un presupposto per promuovere la protezione dei dati a livello mondiale[24].

L'altro versante, tutt'altro che secondario, della protezione dei dati personali nell'ambito del CdE è, come già detto, quello riconducibile alla stessa CEDU, lo strumento per i diritti umani più evoluto nel diritto internazionale, così come interpretata dalla CtEDU. Quest'ultima, attraverso un'interpretazione evolutiva[25], è giunta a ri-

[21] Cfr. CdE, *Emendamenti alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) che consente alle Comunità europee di accedervi*, 15 giugno 1999.

[22] Tale iniziativa è stata presa per la prima volta durante la Conferenza n. 1168 del 10 aprile 2013. In generale, lo Stato non membro può accogliere l'invito ad aderire ad una convenzione del CdE, entro 5 anni dalla data della notifica dello stesso.

[23] Una lista completa relativa allo stato delle firme, ratifiche nonché degli Stati invitati ad aderire si trova alla pagina *web*: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=dj4Z3fYa* (ultima visita: 27 gennaio 2018).

[24] In tal senso, già Agenzia dell'UE per i diritti fondamentali e CdE, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2014, 17.

[25] Per un'analisi dell'interpretazione dell'art. 8 offerta dalla CtEDU in relazione a pretese violazioni dell'*informational privacy*, si vedano, per tutti, G. Resta, *Il diritto alla protezione dei dati personali*, in F. Cardarelli, S. Sica e V. Zeno-Zencovich, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 35, ove si osserva che la giurisprudenza della Corte di Strasburgo «ha fatto propria una lettura estensiva della formula "vita pri-

condurre la protezione dei dati personali nell'alveo del diritto al rispetto della vita privata e familiare sancito dall'art. 8 della CEDU. Tale disposizione recita:

> «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
> 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

La raccolta e l'uso di dati personali da parte di autorità pubbliche sono stati più volte contestati dinanzi alla CtEDU come violazioni del diritto al rispetto della vita privata. Non è evidentemente possibile in questo saggio render conto della corposa giurisprudenza della CtEDU, mediante la quale ha trovato applicazione l'art. 8 CEDU in relazione a tutti questi casi[26]. Volendo riassumere, può dirsi che l'orientamento delle sentenze è dipeso soprattutto dal peso delle contrapposte giustificazioni avanzate dallo Stato. Nel caso *Leander* c. *Svezia* del 1987, la CtEDU ha ritenuto che la raccolta di dati da parte dei servizi segreti, il cui utilizzo aveva causato la perdita del posto di lavoro del ricorrente, non fosse sproporzionata rispetto all'obiettivo della sicurezza nazionale perseguito, stante l'ampio margine di discrezionalità nel bilanciamento tra interessi pubblici e interessi individuali[27]. All'opposto, nel caso *Amann* c. *Svizzera* del 2000, la mera conservazione di una scheda relativa ad una registrazione telefonica da parte dei servizi segreti, ha comportato una condanna dello Stato elvetico sotto in profilo dell'art. 8[28]. Nella sentenza *S. e*

vata" di cui all'art. 8, affermando in diverse pronunzie l'applicabilità delle relative garanzie anche rispetto all'ipotesi della raccolta e della conservazione dei dati personali».

[26] Si rinvia, per un'indagine più sistematica ed esauriente, alle rassegne curate dall'Ufficio Stampa della CtEDU: *Factsheet on Personal Data Protection* e *Factsheet on New Technologies* (si trovano rispettivamente alle pagine *web http://www.echr.coe.int/ Documents/FS_Data_ENG.pdf* e *http://www.echr.coe.int/Documents/FS_New_technologies _ENG.pdf*, visitate il 27 gennaio 2018). V., inoltre, Agenzia dell'UE per i diritti fondamentali e CdE, *Manuale*, cit.

[27] CtEDU, *Leander* c. *Svezia*, decisione del 26 marzo 1987, n. 9248/81.

[28] CtEDU, *Amann* c. *Svizzera*, decisione del 16 febbraio 2000, n. 27798/95.

Marper c. *Regno Unito* del 2008 la Grande Camera della Corte ha concluso che la conservazione a tempo indeterminato del DNA e delle impronte digitali di indagati poi assolti o prosciolti, in quanto era una misura sproporzionata rispetto alle affermate esigenze di prevenzione della criminalità, equivaleva ad una violazione dell'art. 8[29]. In tema di dati personali relativi alla salute, si ricorda il caso *Z.* c. *Finlandia* del 1997, in cui la CtEDU ha ritenuto violato l'art. 8 a motivo della rivelazione in una sentenza di divorzio, successivamente messa a disposizione della stampa, della circostanza della sieropositività della ricorrente[30]. In questo come in altri casi[31], la questione centrale è quella del bilanciamento dell'esigenza della riservatezza con la contrapposta necessità di assicurare la dovuta circolazione di dati all'interno di strutture sanitarie o di procedimenti giudiziari.

5. *La complessa normativa dell'UE*

5.1. *La base giuridica della protezione dei dati personali*

La disciplina dell'UE in materia di protezione dei dati personali si presenta fortemente frammentata. La *privacy* è tutelata attraverso una molteplicità di atti di diritto derivato che delimitano specifici ambiti di applicazione separati, ma tra loro contigui e, a volte, sovrapponibili. Tuttavia, prima di analizzare la relativa disciplina di dettaglio è opportuno individuare ed esaminare la base giuridica delle competenze dell'UE in materia.

Il Trattato di Lisbona ha attribuito all'Unione una competenza specifica a legiferare nel campo della tutela dei dati personali[32]. L'art. 16 TFUE recita:

[29] CtEDU, *S. e Marper* c. *Regno Unito*, sentenza del 4 dicembre 2008, n. 30562/04 e 30566/04.

[30] CtEDU, *Z.* c. *Finlandia*, sentenza del 25 febbraio 1997, n. 22009/93.

[31] Ad es. CtEDU, *M.S.* c. *Svezia*, sentenza del 27 agosto 1997, n. 20837/92; più di recente, CtEDU, *Avilkina et al.* c. *Russia*, sentenza del 6 giugno 2013, n. 1585/09.

[32] B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. eur.*, 2013, n. 2, 313-335; Cortese, *Art. 16 TFUE*, in Tizzano (a cura di), *Trattati dell'Unione europea*, cit., 445-446; F. Balducci Romano, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, 2015, fasc. 5, 1626; O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, 2015,

> «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
>
> 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
>
> Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea».

Il primo paragrafo, che ricalca pedissequamente l'art. 8 CDFUE, proclama un diritto *erga omnes* dell'individuo che, dunque, deve essere rispettato non solo da qualsiasi soggetto privato, ma anche da parte delle istituzioni e degli organismi dell'Unione, nonché da parte degli Stati membri. Il secondo paragrafo attribuisce all'Unione un'autentica competenza generale in materia. Quest'ultima disposizione conferisce una portata davvero innovativa all'art. 16. Mentre a norma del primo paragrafo, quest'ultimo si allinea alla CDFUE e alla CEDU nel qualificare la protezione dei dati personali quale diritto fondamentale dell'individuo, il secondo paragrafo trasferisce alle istituzioni UE il potere di legiferare in merito alla protezione dei dati a carattere personale. Ciò evidentemente amplifica la portata del TFUE rispetto a quella della Convenzione n. 108 la quale stabilisce meri limiti e livelli minimi di tutela in relazione all'esercizio dei poteri da parte delle Parti contraenti[33]. Invero, a partire dal 2009, il Parlamento e il Consiglio, seguendo la procedura legislativa ordinaria, possono adottare atti ai sensi dell'art. 16 TFUE i quali espletano la propria efficacia «nel campo di applicazione del diritto dell'Unione» ad esclusione del settore della PESC nella quale vige, invece, un

18-19; H. Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art. 16 TFEU*, Amsterdam, 2016, 128; P. Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, in M. Cremona, *New Technologies and EU Law*, Oxford, 2017, 141-142.

[33] Cfr. Cortese, *La protezione dei dati di carattere personale*, cit., 315; Cortese, *Art. 16 TFUE*, cit., 446-447; F. Midiri, *La giuridificazione della protezione dei dati personali in Italia*, in *GIUSTAMM.IT*, 2016, n. 5.

differente fondamento ossia l'art. 39 TUE[34]. In entrambi gli ambiti, poi, l'esercizio della *decision-* e/o *law-making* non è evidentemente dispensato dal rispetto delle fonti sovraordinate, quali la CDFUE e gli accordi ai quali l'UE è vincolata come, per l'appunto, la stessa Convenzione n. 108 e, in via mediata, la CEDU.

La matrice per così dire 'rivoluzionaria' del Trattato di Lisbona si comprende maggiormente se si confronta il nuovo assetto normativo con quello antecedente.

Come già accennato[35], le basi giuridiche precedentemente impiegate ai fini della protezione dei dati personali[36] subordinavano l'intervento dell'UE al perseguimento di obiettivi connessi all'attuazione del mercato interno. Più correttamente, tale perseguimento era avviato dall'Unione attraverso l'adozione di provvedimenti in materia di *privacy*. L'instaurazione e il funzionamento del mercato interno esige, infatti, che i dati personali (dei consumatori, degli operatori economici ecc.) possano circolare liberamente. Tuttavia, le differenze legislative nazionali e il conseguente divario dei livelli di tutela costituivano un limite al libero scambio transfrontaliero di dati. L'armonizzazione delle legislazioni nazionali disciplinanti il fenomeno avrebbe avuto l'effetto di agevolare la circolazione dei dati all'interno dei confini europei. Una tale opera di ravvicinamento era fondata sull'art. 100 A TCE[37] (versione consolidata 1992) che consentiva l'a-

[34] Il settore PESC è fondato su un sistema intergovernativo e le decisioni sono adottate all'unanimità. Nello scenario *ante*-Lisbona non era presente alcuna base giuridica per una tutela dei dati personali nell'ambito PESC. Conseguentemente, la disciplina era rilasciata interamente agli Stati membri i quali erano, in ogni caso, vincolati ai limiti sanciti dalla Convenzione n. 108, dalla CEDU e dalla CDFUE. Cfr. S. Di Minco, *Art 39 TUE*, in C. Curti Gialdino (a cura di), *Codice dell'UE operativo*, Napoli, 2012; Cortese, *La protezione dei dati di carattere personale*, cit., 331-332; F. Pocar e M.C. Baruffi, *Commentario breve ai trattati dell'Unione europea*, Assago, 2014, 123; B. Cortese, *Art. 39 TUE*, in Tizzano (a cura di), *Trattati dell'Unione europea*, cit., 290-291; L. Bolognini, E. Pelino e C. Bistolfi, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 25-26; Casagran, *op. cit.*, *199-200*.

[35] *Supra*, par. 3.

[36] Gli artt. 100 A e 189 TCE (versione consolidata 1992) e gli artt. 95 e 286 TCE (versione consolidata 1999).

[37] Al par. 1, l'art. 100 A, TCE (versione consolidata 1992) recitava: «1. In deroga all'articolo 100 e salvo che il presente trattato non disponga diversamente, si applicano le disposizioni seguenti per la realizzazione degli obiettivi dell'articolo 7 A. Il Consiglio,

dozione di misure di armonizzazione purché finalizzate all'instaurazione progressiva del mercato interno. Dunque, la disciplina in materia presentava una natura bifronte: la protezione dei dati personali era funzionale all'attuazione e al rafforzamento delle quattro libertà economiche. L'individuo era sì tutelato, ma al fine di consentirne una più intensa circolazione delle informazioni all'interno dell'Unione europea tramite il superamento delle differenze normative statali[38].

Questo assunto è fondamentale per comprendere gli effetti della stessa direttiva 95/46/CE che, fondandosi sull'art. 100 A TCE, tutela sì il trattamento e la conservazione dei dati personali, ma al fine di consentirne una maggiore circolazione, la quale concorre alla costituzione di un mercato unico europeo sempre più integrato[39].

Ebbene, si palesa chiaramente la differenza tra le basi giuridiche utilizzate nel quadro *ante* e *post*-Lisbona. A differenza del precedente art. 100 A TCE versione consolidata del 1992 (corrispondente all'art. 95 TCE versione consolidata del 1997), l'art. 16 TFUE conferisce all'Unione una competenza concorrente, nei limiti del diritto europeo e nel rispetto del principio di sussidiarietà, in tema di protezione dei dati personali, a prescindere da una qualsivoglia connessione con la realizzazione di un mercato unico ovvero con una delle quattro libertà economiche[40]. L'art. 16 inverte il rapporto tra obiettivi dell'UE e protezione dei dati personali – o meglio, tra circola-

deliberando in conformità della procedura di cui all'articolo 189 B e previa consultazione del Comitato economico e sociale, adotta le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno».

[38] In proposito Cortese ha giustamente osservato che «l'intervento comunitario perseguiva anzitutto e necessariamente l'obiettivo di assicurare la circolazione dei dati, anche se ciò lo faceva tramite l'armonizzazione delle normative nazionali in materia di trattamento dei dati personali», cfr. Cortese, *Art. 16 TFUE* cit., 446. Sul punto, vedasi anche Pardolesi, *op. cit.*, 35-37; Balducci Romano, *op. cit.*, 1626-1628, 1656-1657; Lynskey, *op. cit.*, 8-9, 46-47, 49-54; G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 29-30; Hustinx, *op. cit.*, 166-167.

[39] In senso analogo, v. Conclusioni dell'avvocato generale Antonio Tizzano presentate il 19 settembre 2002 in relazione alla causa *Lindqvist*, C-101/01, parr. 39-43, già citate da Pardolesi, *op. cit.*, 35-37.

[40] Cfr. Di Minco, *op. cit.*; V. Reding, *The European data protection framework for the twenty-first century*, in *International Data Privacy Law*, 2012, vol. 2, n. 1, 120; Cortese, *La protezione dei dati di carattere personale*, cit., 315; Cortese, *Art. 16 TFUE*, cit., 446; Balducci Romano, *op. cit.*, 1629.

zione dei dati personali e loro protezione – verso una prevalenza della seconda sui primi.

5.2. *Il nuovo 'pacchetto europeo di protezione dei dati personali'*

Come già osservato, l'UE disciplina la protezione dei dati personali attraverso una moltitudine di atti di diritto derivato, ciascuno dei quali regola solo parzialmente il fenomeno.

Nel momento in cui si scrive, la normativa in questione si compone, principalmente, di quattro atti giuridici: la direttiva 'madre' 95/46/CE avente carattere generale, il regolamento 2001/45/CE che impone un onere di rispettare i dati personali in capo alle istituzioni e agli organismi dell'UE, la direttiva 2002/58/CE che disciplina il fenomeno nel settore delle comunicazioni elettroniche e la decisione-quadro 2008/977/GAI che tutela i dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale. A questo nucleo centrale – già alquanto frammentato – si affianca un vero e proprio sistema 'satellitare' costituito da una pluralità di atti che regolano la *privacy* in modo autonomo e per lo più settoriale: trattasi, in particolare, delle iniziative che hanno istituito banche dati all'interno dell'UE, dello Spazio Schengen o del settore della cooperazione giudiziaria e di polizia. Detti atti, nel creare singoli *database*, hanno stabilito distinti apparati di tutela della *privacy* che trovano limitato rilievo e applicazione nel quadro complessivo che si vuole illustrare nella presente indagine. È sembrato comunque opportuno menzionarli.

Dal secondo quadrimestre del 2016, il quadro appena descritto è stato parzialmente modificato. Il Parlamento europeo e il Consiglio, nel dar seguito all'art. 16, par. 2, TFUE, hanno riformato la disciplina varando il c.d. «pacchetto europeo per la protezione dei dati» il quale diverrà pienamente applicabile a partire dal maggio del 2018[41]. Si tratta di un intervento normativo composto da due provvedimenti:

– il regolamento 2016/679/UE che abroga e sostituisce la direttiva 95/46/CE;

– la direttiva 2016/680/UE che abroga e sostituisce la decisione-quadro 2008/977/GAI.

[41] Nello specifico, il GDPR diverrà definitivamente applicabile in via diretta a partire dal 25 maggio 2018, la direttiva 2016/680/UE dal precedente 6 maggio.

Infine, contestualmente a tale intervento, è stato adottato un ulteriore provvedimento nel settore della cooperazione giudiziaria e di polizia in materia penale: la direttiva 2016/681/UE che sancisce e regola l'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi[42].

Le finalità perseguite dalle principali istituzioni dell'UE con il 'pacchetto europeo per la protezione dei dati' sono chiare sin dal principio: si intende, da un lato, adattare la disciplina alle esigenze della società contemporanea e, dall'altro, realizzare una maggiore armonizzazione e uniformità della materia rispetto a quella ottenuta dalla precedente normativa[43]. A tal proposito, la scelta di incentrare la tutela europea della *privacy* su uno strumento più pregnante, quale è il regolamento, è da considerarsi appropriata: non solo l'esecuzione di un regolamento non necessita in via di principio di una normativa d'attuazione nazionale, ma lo stesso è fonte diretta ed immediata di situazioni giuridiche soggettive in capo ai singoli individui. Se con la direttiva 'madre' del 1995 l'armonizzazione era stata diretta a creare un minimo comune denominatore tra le legislazioni degli Stati membri senza rimuovere anche sensibili divergenze tra le regolamentazioni nazionali, oggi essa tende ad instaurare una vera e propria uniformità dello *standard* di protezione che si fonda su un indiscusso riconoscimento del diritto all'*informational privacy* quale diritto fondamentale.

5.2.1. *Il regolamento 2016/679/UE*

Come già anticipato, il 25 maggio 2018 il regolamento 2016/679/UE abrogherà e sostituirà la direttiva 95/46/CE, conosciuta anche come 'direttiva madre' stante il ruolo di protagonista da questa finora svolto all'interno dell'intera disciplina della *privacy* nell'UE. Ne consegue che il regolamento 2016/679/UE non potrà che configurarsi a sua volta come il pilastro fondamentale del nuovo assetto normativo. Difatti, esso è denominato '*General Data Protection Regulation*' (GDPR) a rimarcarne la rilevanza e la portata sia materiale che territoriale.

[42] La direttiva 2016/681/UE, pubblicata nella GUUE il 24 maggio 2016, diventerà applicabile dal 25 maggio 2018.

[43] Cfr. considerando 10, Preambolo GDPR.

Sotto il primo aspetto, per la verità, il regolamento non ha apportato particolari novità alla disciplina preesistente. Ai sensi dell'art. 2, par. 1, il GDPR si applica «al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi». Rimangono pertanto implicitamente esclusi quei trattamenti manuali di dati personali che non siano contenuti in un archivio, inteso quest'ultimo come «insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico»[44].

Oltre a ciò, al successivo par. 2, l'art. 2 provvede a circoscrivere l'ambito di applicazione materiale, elencando espressamente quattro categorie di trattamenti che devono ritenersi escluse dalla disciplina del regolamento.

La prima fattispecie consegue dal combinato disposto degli artt. 4 e 5 TUE i quali, sulla base dei principi di attribuzione, di sussidiarietà e di proporzionalità, sanciscono che «qualsiasi competenza non attribuita all'Unione nei Trattati appartiene agli Stati membri»[45]. Non soggiacciono perciò al GDPR tutti quei trattamenti effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'UE. Dunque, sono escluse tutte le aree di competenza esclusiva degli Stati membri, quali il mantenimento dell'ordine pubblico o la tutela della sicurezza nazionale. Quanto appena affermato non si traduce in una totale assenza di protezione, ma nella mera incompetenza a regolare il fenomeno da parte delle fonti di diritto europeo. Ciò non esclude che altri strumenti nazionali ovvero internazionali possano tutelare i dati personali in tali settori. Ad esempio, potranno trovarvi esecuzione sia la Convenzione n. 108 che la CEDU, nonché la connessa giurisprudenza, stante la ratifica di entrambi questi trattati da parte degli Stati dell'UE[46].

Strettamente connesse con quella appena analizzata sono le fattispecie previste alle lettere *b*) e *d*) dell'art. 2, par. 2, GDPR (da considerarsi la seconda e terza categoria di trattamenti esclusi dalla portata del regolamento). La lettera *b*) estromette dall'applicazione del

[44] Art. 4, n. 6), GDPR.
[45] Art. 4, par. 1, TUE e art. 5, par. 2, TUE.
[46] Bolognini, Pelino e Bistolfi, *op. cit.*, 22-24.

regolamento i trattamenti «effettuati dagli Stati membri nell'esercizio di attività che rientrano nel titolo V, capo 2, TUE». Come è noto, il settore PESC, in tal modo contemplato, esula dalle classiche logiche di integrazione europea e soggiace, invece, ad un metodo tipicamente intergovernativo nel quale è rilasciata ampia discrezionalità decisionale ai singoli Stati membri[47]. Tale disposizione ribadisce quanto è già desumibile dalla base giuridica del regolamento: lo stesso art. 16 TFUE esclude dalla propria portata precettiva l'ambito PESC in relazione al quale trova invece specifica applicazione l'art. 39 TUE[48]. La lettera *d*), invece, estromette dall'ambito del GDPR i trattamenti «effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse»[49]. Come già rilevato nel precedente paragrafo, tale materia è infatti disciplinata da specifici e distinti strumenti normativi: attualmente trova al riguardo ancora applicazione la decisione-quadro 2008/977/GAI che, tuttavia, verrà abrogata e sostituita il 6 maggio 2018 dalla direttiva 2016/680/UE[50].

L'adozione di provvedimenti distinti dalla direttiva 'madre' per tutelare la *privacy* nel settore della cooperazione giudiziaria in materia penale e di polizia (*ex* GAI) è stato il risultato della complessa struttura a pilastri su cui era stata edificata la CE. Solo il primo pilastro ricadeva *ratione materiae* sotto la legislazione comunitaria per così dire 'centralizzata', di cui la direttiva 'madre' era evidentemente un prodotto, con la conseguenza che, per intervenire nel settore GAI si era resa necessaria l'adozione di un atto *ad hoc* costituito per l'appunto dalla decisione-quadro 2008/977/GAI. Oggi, lo sdoppiamento degli strumenti di diritto derivato, ed in particolare l'adozione di un'ulteriore direttiva, trova fondamento in un differente presupposto. La struttura a pilastri, su cui si basava la precedente *ratio*, è stata abolita dal Trattato di Lisbona, il quale ha ricondotto le materie dell'*ex* GAI nel diritto dell'UE e, precisamente, nel c.d. Spazio di libertà, sicurezza e giustizia (SLSG). Questa evoluzione consentirebbe attualmente al legislatore europeo di disciplinare con un unico

[47] Considerando 16, Preambolo GDPR.
[48] Si rinvia *supra*, par 5.1.
[49] Art. 2, par. 2, GDPR. Si veda anche considerando 19, Preambolo GDPR.
[50] Per approfondimenti si rinvia *infra*, par. 5.2.3.

atto normativo le materie rientranti negli *ex* primo e terzo pilastro. Malgrado ciò, la specificità del settore della cooperazione giudiziaria in materia penale e di polizia implica l'impiego di logiche e contemperamenti diversi che impongono l'adozione di una pluralità di provvedimenti distinti[51].

Passando alla quarta ed ultima ipotesi di esclusione, questa è prevista alla lettera *c*) del secondo paragrafo dell'art. 2, a norma della quale non rientrano nel campo di azione del GDPR quei trattamenti «effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico» (c.d. *household exclusion provision*). Riguardo a questa disposizione – e analogamente alla direttiva 'madre' – il legislatore europeo ha preliminarmente maturato un giudizio circa l'irrilevanza o quantomeno la superficialità della lesione del diritto alla protezione dei dati in tutte quelle situazioni che siano frutto di un utilizzo dei dati puramente personale o domestico. Tuttavia, la definizione di 'trattamento personale o domestico' crea non pochi problemi esegetici in quanto essa può ampliare o meno la protezione dei dati personali a seconda dell'accezione accolta[52]. Come chiarito dal considerando 18, Preambolo GDPR, per integrare la fattispecie derogatoria è necessario che il trattamento sia effettuato da una persona fisica e non presenti alcuna connessione con attività commerciali o professionali. Il GDPR, inoltre, ha precisato che «le attività a carattere esclusivamente personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'utilizzo dei *social networks* e attività *online* intraprese nel quadro di tali attività»[53]. La deroga sembra dunque travalicare il mero concetto fisico di spazio domestico o personale estendendo la propria portata al di fuori di

[51] Quanto appena affermato trova riscontro nella dichiarazione n. 21 allegata al Trattato di Lisbona relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, la quale ammette che «potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia». Cfr. Lynskey, *op. cit.*, 19-20.

[52] Cfr. considerando 18, Preambolo GDPR. Per una definizione precisa di 'attività a carattere personale o domestico' si rinvia a Bolognini, Pelino e Bistolfi, *op. cit.*, 36-41; S. Sica, V. D'antonio e G.M. Riccio, *La nuova disciplina europea della privacy*, Padova, 2016, 26; Finocchiaro, *op. cit.*, 31-38.

[53] Considerando 18, Preambolo GDPR.

esso. La norma pare attribuire maggiore rilevanza all'utilizzo e alle finalità delle attività della persona fisica/titolare del trattamento piuttosto che al luogo fisico presso il quale queste sono svolte. La sentenza *Rynes*[54] ne è un chiaro esempio. In questa occasione la CGUE ha ritenuto non compatibile con l'art. 3, par. 2, lett. *b*) della direttiva 'madre' (pienamente corrispondente all'art. 2, par. 2, lett. *d*), GDPR in commento) la diffusione di dati che, benché raccolti nella sfera domestica o personale, siano stati diretti nello spazio virtuale o materiale verso una mole indeterminata di destinatari. La sostanza prevale sulla forma: ai fini del GDPR non è determinante il luogo dove vengono raccolti e trattati i dati, ma le effettive finalità o il concreto utilizzo che la persona fisica persegue o opera.

In definitiva, da quanto esposto, l'ambito di applicazione materiale del GDPR si presenta assai ampio, ma allo stesso modo frammentato dall'esistenza di sfere sostanziali in merito alle quali gli viene precluso di legiferare, quali i trattamenti dei dati *ex* art. 2, par. 3, GDPR ovvero quelli operati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati operati da istituzioni organi.

Tuttavia, vi sono ulteriori elementi di frammentarietà della disciplina comunitaria della protezione dei dati.

In primo luogo, l'art. 2, par. 3, GDPR demarca in maniera indiretta il campo di applicazione materia del GDPR: nell'individuare nel regolamento 2001/45/CE la disciplina competente per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, il GDPR si *autoesclude* dal regolare tali rapporti[55].

In secondo luogo, il GDPR contempla una qualche attività normativa da parte degli Stati membri[56]. Più precisamente, il regolamento generale spesso rinvia, nella definizione di alcuni aspetti ovvero di interi istituti della disciplina comunitaria, alle legislazioni nazionali. In alcuni casi il GDPR prevede una facoltà per le Parti di introdurre disposizioni statali che specificano la regolamentazione

[54] CGUE, *Rynes* c. *Úřad pro ochranu osobních údajù*, sentenza del 11 dicembre 2014, C-212/13.

[55] Per approfondimenti sul regolamento 2001/45/CE e sul rapporto con il GDPR si rinvia, *infra*, par. 5.2.2.2.

[56] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il regolamento europeo 2016/679/UE. Vol. 4/II*, Torino, 2016, 17-36.

esistente ovvero ne introducono nuovi elementi o requisiti di attuazione[57]. In altri casi, invece, il regolamento generale non disciplina una fattispecie che è pienamente rimessa alla potestà legislativa degli Stati membri[58]. È evidente come lo strumento del rinvio alla normativa nazionale inserisca nel sistema di protezione dei dati dell'UE degli elementi di flessibilità che possono condurre a divergenze normative anche sensibili tra gli Stati membri.

Per quanto invece riguarda l'applicazione territoriale, il GDPR ha introdotto considerevoli novità. In virtù dell'art. 3, par. 1, il regolamento si applica al trattamento dei dati personali «effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione» ovvero, ai sensi del par. 3 del medesimo articolo, a quello effettuato da un titolare stabilito in un luogo *extra*-UE ma «soggetto al diritto di uno Stato membro in virtù del diritto internazionale».

La prima di queste disposizioni contempla il più ampio spettro applicativo della disciplina europea della *privacy*. Per ricondurre un trattamento entro tale regolamentazione, il GDPR richiede che il titolare o il responsabile siano stabiliti nell'UE e che il trattamento sia conferente all'attività dello stabilimento considerato, risultando del tutto ininfluente che lo stesso sia compiuto nell'Unione o in un Paese terzo[59]. La seconda disposizione ha invece una rilevanza e un'applicazione marginale, riferendosi a quelle ipotesi di ultraterritorialità in cui il titolare è stabilito in luoghi che, sebbene non ricompresi all'interno dei confini UE, sono in ogni caso soggetti al diritto di uno Stato membro sulla base del diritto internazionale pubblico ovvero di accordi internazionali. Trattasi, a titolo esemplificativo, di aeromobili, navi, consolati e ambasciate all'estero[60]. Ragionando *a contra-*

[57] Cfr. a titolo esemplificativo i rinvii alla legislazione nazionale contenuti nell'art. 6, par. 2, nell'art. 8, par. 1 ovvero nell'art. 9, par. 4, GDPR.

[58] Si rimanda, ad esempio, al sistema sanzionatorio previsto dagli artt. 83-84, GDPR, che rinviano ampiamente alle legislazioni nazionali.

[59] Si veda anche considerando 22, Preambolo GDPR. In realtà, la specificazione dell'irrilevanza del luogo nel quale è realizzato il trattamento è superflua nella fattispecie *ex* art. 3, par. 1, GDPR, in quanto per l'applicazione di tale disposizione risulta sufficiente che il titolare o il responsabile del trattamento siano stabiliti nell'UE.

[60] Cfr. WP179, *Opinione 8/2010 sul diritto applicabile*, 16 dicembre 2010, 17-18; Bolognini, Pelino e Bistolfi, *op. cit.*, 3-4; considerando n. 25, Preambolo GDPR.

rio, la disciplina europea della *privacy* non dovrebbe trovare applicazione ai trattamenti interamente svolti in quelle porzioni di territorio sottoposte al diritto di Stati terzi *extra*-UE.

In entrambe le disposizioni lo 'stabilimento' assume una rilevanza primaria ai fini dell'applicabilità del regolamento. Eppure l'elemento innovativo non è costituito da tale concetto il quale non è affatto estraneo alla direttiva 'madre', anzi, si fonda sulla stessa e sulla sua successiva elaborazione giurisprudenziale[61]. Viceversa, l'originalità deriva dal diverso utilizzo immaginato dal legislatore. Nella direttiva, lo 'stabilimento' costituiva un criterio di collegamento, ossia un parametro attraverso il quale scernere caso per caso la legislazione nazionale applicabile[62]. Ciò si rendeva necessario per la natura stessa della direttiva che, in quanto tale, esigeva singoli atti di recepimento da parte di ciascuno Stato i quali, a loro volta, avrebbero potuto ingenerare conflitti di leggi. Diversamente, nel regolamento rileva individuare se la normativa dell'UE nel suo complesso trovi o meno applicazione ad uno specifico trattamento[63]. In definitiva, la funzione di 'stabilimento' in parte muta: da criterio guida per individuare perlopiù la legge nazionale applicabile all'interno dell'UE a criterio che definisce i confini della intera disciplina europea di protezione dei dati personali.

Da ultimo, atto a delimitare l'estensione territoriale del GDPR è l'art. 3, par. 2, che assume interesse nel momento in cui il titolare o il responsabile del trattamento non abbiano uno stabilimento nell'UE rilevante ai sensi dell'art. 3, par. 1, GDPR. In tal caso il regolamento *de quo* troverà applicazione solo ove le attività di trattamento concer-

[61] Cfr. CGUE, *Google Spain SL*, cit.; CGUE, *Weltimmo s.r.o.* c. *Nemzeti Adatvédelmi és Információszabadság Hatóság*, sentenza del 10 ottobre 2015, C-230/14. V. anche Bolognini, Pelino e Bistolfi, *op. cit.*, 9-12; M.G. Stanzione, *Il regolamento europeo sulla 'privacy': origini e ambito di applicazione*, in *Europa e diritto privato*, 2016, n. 4, 1255-1259; Sica, D'Antonio e Riccio, *op. cit.*, 27-30; P.A. De Miguel Asensio, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation*, in *Revista Española de Derecho Internacional*, 2017, vol. 69, fasc. 1, 81-83; Finocchiaro, *op. cit.*, 39-54.

[62] Cfr. Stanzione, *op. cit.*, 1256; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Vol. 4/I*, cit., 160; Finocchiaro, *op. cit.*, 54-56, riconosce che la direttiva serviva più al mutuo riconoscimento piuttosto che al riconoscimento *extra*-UE della disciplina europea.

[63] Cfr. Stanzione, *op. cit.*, 1256; Pizzetti, *op. ult. cit.*, 159-160; Finocchiaro, *op. cit.*, 40.

nano interessati che si trovino nell'UE e riguardino alternativamente «l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato» oppure «il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione»[64]. Lo scopo di tale disposizione è, come dichiarato anche dal considerando 23 del Preambolo, quello di garantire che ad alcuna persona fisica in Europa possa essere negato il riconoscimento del diritto tutelato dal GDPR. A tal fine i confini dell'ambito territoriale vengono estesi sino a ricomprendere responsabili e titolari del trattamento situati in Paesi terzi *extra*-UE. In realtà, un'efficacia extraterritoriale non è preclusa dalla direttiva 'madre': uno Stato membro può applicare la propria disciplina a soggetti non stabili nell'UE purché gli strumenti di trattamento, automatizzati o non automatizzati, siano localizzati nel territorio di detto Stato, salvo che questi non siano utilizzati ai soli fini di transito nel territorio comunitario. Il GDPR, invece, tutela chiunque si *trovi* nell'Unione ossia qualsiasi persona fisica che, a prescindere dalla propria nazionalità o residenza[65], sia presente nel territorio europeo al momento dell'esecuzione del trattamento da parte di un soggetto non stabilito nell'UE. Tuttavia, affinché venga integrata la fattispecie di cui trattasi è necessario che le attività di trattamento concernano uno dei due impieghi previsti dalla norma.

A tal proposito, se la nozione di 'offerta di beni o servizi' è facilmente intellegibile, lo stesso non può dirsi riguardo all'individuazione dei casi in cui un titolare o un responsabile del trattamento non stabiliti nell'UE indirizzino la propria offerta proprio nel territorio dell'Unione. Un qualche sostegno interpretativo è offerto dal già citato considerando 23, il quale precisa che «la semplice accessibilità del sito *web* del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione». Al contrario, «fattori quali l'utilizzo di una lingua o di una moneta abi-

[64] Art. 3, par. 2, GDPR. Sul punto cfr. anche Bolognini, Pelino e Bistolfi, *op. cit.*, 15-17; Sica, D'Antonio e Riccio, *op. cit.*, 30-31; De Miguel Asensio, *op. cit.*, 83-86; Finocchiaro, *op. cit.*, 46-47.

[65] V. considerando 14, Preambolo GDPR.

tualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione» possono indicare l'intento del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione.

Ancor più indeterminato è il significato di «monitoraggio di comportamenti dell'interessato all'interno dell'Unione». Il considerando 24 del Preambolo, se da un lato individua nel tracciamento su *internet* (anche attraverso successive attività di profilazione) una delle molteplici attività di 'monitoraggio' delle persone fisiche[66], dall'altro nulla riferisce in merito ai criteri da utilizzare per localizzare l'azione individuale entro il territorio dell'Unione. Il problema emerge principalmente quando il comportamento è posto in essere in spazi virtuali nei quali è dubbio se impiegare criteri sulla base dei quali prevalga il luogo del *device* utilizzato, del *server* ovvero del luogo verso cui il comportamento è diretto.

In conclusione, si comprende agevolmente che, in assenza di indicazioni normative più puntuali, i margini di interpretazione dei concetti in questione siano alquanto elastici. Si rende pertanto necessario attendere l'applicazione concreta della disposizione in commento affinché l'operatore giuridico possa trarne le necessarie indicazioni pratiche. Malgrado ciò, si registra in modo chiaro la tendenza della nuova disciplina la quale è diretta ad espandere la propria portata sempre più oltre i propri confini esterni. All'opposto, sebbene abbia elevato gli *standard* di tutela dei dati personali, la sfera materiale del GDPR si manifesta frammentaria: da un lato, per essere disciplinati, gli ambiti esclusi dal regolamento necessitano di ulteriori strumenti giuridici rispetto al GDPR, dall'altro, la presenza di rinvii – sia obbligatori che facoltativi – alla legislazione nazionale non impedirà la proliferazione di una pluralità di normative statali divergenti tra loro.

5.2.2. *Il rapporto del GDPR con altri atti di diritto derivato dell'UE*

Ai sensi dell'art. 94, il GDPR abrogherà, sostituendola, la direttiva 'madre'. Nell'illustrare l'attuale disciplina europea della *privacy* è stato tuttavia evidenziato che questa si compone di una moltitudine

[66] V. considerando 24, Preambolo GDPR.

di atti che non si esauriscono nella direttiva 95/46/CE. Pertanto, gli altri strumenti sono e rimarranno pienamente in vigore. Trascurando momentaneamente la direttiva 2016/680/UE (o la vigente decisione-quadro 2008/977/GAI) che disciplina una branca del diritto europeo della *privacy* relativamente al quale il GDPR ha esplicitamente escluso la propria applicazione, nonché la molteplicità di normative che creano specifici *database*, sembra opportuno soffermarsi qui sul regolamento 2001/45/CE 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, e sulla direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (nel prosieguo 'direttiva ePrivacy'). A differenza della direttiva 2016/680/UE, questi due provvedimenti disciplinano ambiti materiali che rientrano pienamente nella sfera del GPDR. Si verifica, perciò, una sovrapposizione dei campi di applicazione dei vari strumenti normativi che potrebbe condurre a conflitti, quantomeno in astratto. Sembra dunque opportuno esaminare se e come, a livello europeo, queste fonti si raccordino e si coordinino.

5.2.2.1. *La direttiva 2002/58/CE (c.d. Direttiva ePrivacy)*

La direttiva 97/66/CE è l'atto che per primo ha fatto seguito alla direttiva 'madre' con il proposito di integrare l'*informational privacy* limitatamente al settore delle telecomunicazioni elettroniche. Lo sviluppo tecnologico verificatosi alla fine dello scorso millennio ha reso necessario aggiornare tale disciplina alle nuove istanze. Ciò è avvenuto con l'emanazione della direttiva 2002/58/CE detta anche 'direttiva ePrivacy' (successivamente modificata dalla direttiva 2009/136/CE) la quale ha abrogato e sostituito la direttiva 97/66/CE[67].

La direttiva ePrivacy è finalizzata ad armonizzare la materia sia al fine di garantire in maniera adeguata la protezione dei dati personali, sia al fine di consentire una maggiore circolazione non solo di tali dati, ma anche di apparecchiature e servizi di comunicazione elettronica all'interno dell'UE[68]. L'ambito di applicazione è limitato al «trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comuni-

[67] Art. 19, par. 1, direttiva ePrivacy.
[68] Art. 1, par. 1, direttiva ePrivacy.

cazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati»[69]. La specificità della materia trattata rispetto a quella della direttiva 'madre' (e, oggi, del GDPR) appare *icto oculi*[70]. Invero, la direttiva 'madre' contempla tutti i tipi di trattamento automatizzato dei dati, indipendentemente dalla tecnologia utilizzata, mentre la direttiva ePrivacy regola soltanto il trattamento connesso a servizi di comunicazione elettronica.

Sebbene concerna un ambito materiale più limitato, la direttiva *de qua* non ambisce a disciplinare il settore esaustivamente, piuttosto, essa semplicemente *precisa* e *integra* la direttiva 'madre', la quale continua a rappresentare la normativa generale anche in materia di telecomunicazioni[71]. Quest'ultima trova infatti esecuzione per tutti «gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali non specificamente disciplinati dalle disposizioni della presente direttiva», oltre che per tutti quei servizi di comunicazione non accessibili al pubblico[72].

Se il rapporto tra le due direttive in commento è piuttosto chiaro, l'adozione di un ulteriore provvedimento generale avrebbe potuto alterare un tale equilibrio. Il legislatore europeo, consapevole di questo rischio, ha preferito adottare un atteggiamento di *status quo*. Di conseguenza, l'art. 95, GDPR decreta l'assenza di ulteriori obblighi in relazione ai trattamenti rientranti nell'ambito della direttiva ePrivacy. Il GDPR ne lascia quindi impregiudicata la portata precettiva.

L'assenza di oneri supplementari non esime il legislatore euro-

[69] Art. 3, par. 1, direttiva ePrivacy.

[70] Anche le aree di incompetenza materiale della direttiva ePrivacy sono coincidenti con quelle della direttiva 'madre': in merito si rinvia al considerando 11 e agli artt. 1, par. 3 e 15, par. 11, Direttiva ePrivacy. L'unica differenza tra i due atti è costituita dall'ambito soggettivo della direttiva ePrivacy la quale non tutela solamente persone fisiche, ma altresì gli «legittimi interessi degli abbonati che sono persone giuridiche». Tuttavia, ciò non comporta un conseguente obbligo per gli Stati membri di estendere anche l'applicazione della direttiva 'madre' anche nei confronti di persone giuridiche. La tutela degli abbonati che sono persone giuridiche rileva solo ai fini dell'applicazione della direttiva ePrivacy. V. art. 1, par. 2 e considerando 7, 8, 12, direttiva ePrivacy.

[71] Art. 1, par. 2, direttiva ePrivacy. Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Vol. 4/I*, cit., 130-132.

[72] Considerando 10, Preambolo direttiva ePrivacy.

peo dal riesame della direttiva ePrivacy in funzione del GDPR[73]. Sebbene allo stato attuale il coordinamento tra i due provvedimenti sembri essere efficiente, è ritenuto preferibile che vengano al più presto posti in essere quegli emendamenti che rendano interamente coerente l'intero sistema europeo[74] ma, in particolar modo, che venga innalzato lo *standard* di tutela anche nel settore delle telecomunicazioni attraverso un'attualizzazione alle moderne tecnologie e metodi di comunicazione.

5.2.2.2. *Il Regolamento 2001/45/CE*

Il regolamento 2001/45/CE concerne la tutela dei dati personali di persone fisiche da parte delle istituzioni e degli organismi comunitari.

Come anticipato, l'ambito di applicazione materiale di questo regolamento e quello della direttiva 'madre' – nonché del GDPR – coincidono a tal punto che le corrispondenti formulazioni risultano assolutamente identiche. L'art. 3, par. 2, regolamento 2001/45/CE recita: «il presente regolamento si applica al trattamento di dati personali, interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi»[75].

Il fattore discriminante tra i due atti è costituito dal campo di applicazione *ratione personae* ovvero delle categorie di soggetti cui si rivolge la rispettiva disciplina. Il regolamento 2001/45/CE, infatti, è specificamente indirizzato alle sole istituzioni e agli organismi comunitari[76].

Tuttavia, non tutti i tipi di trattamento posti in essere da tali enti sono soggetti al regolamento 2001/45/CE, bensì solo quelli che avvengono «nell'esercizio di attività che rientrano in tutto o in parte nel campo di applicazione del diritto comunitario»[77]. La limitazione

[73] Tale eventualità viene espressamente auspicata al considerando 173 del Preambolo GDPR. Sul punto, v. anche BOLOGNINI, PELINO e BISTOLFI, *op. cit.*, 720-721; SICA, D'ANTONIO e RICCIO, *op. cit.*, 333.

[74] Considerando 173, Preambolo GDPR.

[75] Si confronti l'art. 3, par. 2, regolamento 2001/45/CE con l'art. 3, par. 1, della direttiva 'madre' e con l'art. 2, par. 1, GDPR.

[76] Art. 3, par. 1 e considerando 13-14, regolamento 2001/45/CE.

[77] Art. 3, par. 1, regolamento 2001/45/CE. Cfr. anche i considerando 14-16, Preambolo regolamento 2001/45/CE.

costituisce un'esclusione analoga a quella prevista dalla direttiva 'madre' laddove questa estromette dal proprio ambito applicativo i trattamenti «effettuati per attività non rientranti nel diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'Unione europea»[78]. Di più complessa interpretazione è l'espressione 'in parte', che lascia immaginare l'esistenza di spazi applicativi in settori di non esclusiva competenza del diritto dell'UE. Parte della dottrina ha interpretato tale locuzione tenendo conto anche del contestuale considerando 17 e ha sostenuto che la vaghezza della formula sia (stata) funzionale all'estensione della disciplina a materie che, all'epoca dell'adozione del regolamento in esame, ricadevano solo parzialmente all'interno del diritto comunitario, quali lo Spazio Schengen o il sistema doganale[79].

Ora che è stata dimostrata la coincidenza delle sfere di applicazione del regolamento 2001/45/CE, della direttiva 'madre' e, conseguentemente, del GDPR, può procedersi all'analisi delle modalità di interazione tra i due regolamenti appena menzionati.

Per una piena comprensione della dialettica esistente tra questi due atti è necessario chiarire il perché nel regime generale *ante* e *post*-GDPR la disciplina non si estendesse alle istituzioni e agli organismi comunitari. Questi enti erano di fatto esclusi dall'applicazione della direttiva 'madre', e ciò in mancanza – nei trattati istitutivi – di una formale attribuzione, in capo all'*ex* CE, di una competenza quanto alla regolamentazione delle attività di trattamento poste in essere da detti soggetti. Ne consegue che le istituzioni comunitarie non erano vincolate dalla direttiva 'madre'[80]. Tale lacuna è stata colmata con l'introduzione dell'art. 286 TCE da parte del Trattato di Amsterdam[81] che ha costituito, per l'appunto, la base giuridica del rego-

[78] Art. 3, par. 1, direttiva 'madre'.

[79] V. considerando 17, Preambolo regolamento 2001/45/CE; P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002, 234-235.

[80] Sebbene non vincolati dalla direttiva 'madre' e prima dell'adozione del regolamento 2001/45/CE, Commissione e Consiglio, avendo riconosciuto la centralità della protezione dei dati personali, si sono impegnati con una dichiarazione unilaterale a rispettare le disposizioni dell'UE in materia. Cfr. *Comunicato stampa del Consiglio* del 24 luglio 1995 (9012/95(press226)); WP29, *Seconda relazione annuale*, 30 novembre 1998, DG XVD/5047/98 finale.

[81] Cfr. Pocar, *Commentario breve ai trattati della Comunità e dell'Unione europea*, cit., 958-959, il quale afferma: «Con Amsterdam e l'introduzione dell'art. 286 TCE si è

lamento 2001/45/CE. L'evoluzione espressa dall'art. 286 TCE (versione consolidata 1999) è stata successivamente recepita dal Trattato di Lisbona nell'art. 16 TFUE[82]. Pertanto, il legislatore europeo avrebbe ben potuto, con il nuovo regolamento generale, vincolare anche gli organismi e le istituzioni unionali. Una tale opzione, qualora impiegata, sarebbe giudicata virtuosa sotto un duplice punto di vista: da un lato, essa raggiungerebbe un'uniformità dei livelli di protezione dei dati personali sia nei confronti di privati che di istituzioni pubbliche; dall'altro, essa otterrebbe l'effetto di ridurre la sussistenza di una pluralità di atti derivati regolanti la materia. Ciò nonostante, il legislatore europeo ha preferito lasciare in vigore il precedente atto normativo e prospettare una situazione analoga a quella prevista dal GDPR in relazione alla direttiva ePrivacy: lasciare impregiudicata la portata e l'ambito applicativo del regolamento 2001/45/CE[83]. Quest'ultimo rimarrà in vigore e coesisterà con il GDPR. Tuttavia, le tutele offerte da ciascuno dei due atti esprimono differenti livelli di protezione dei dati personali. Ne consegue che la coerenza del sistema europeo della *privacy* necessita comunque di un riesame del regolamento in commento affinché lo stesso possa essere aggiornato e uniformato ai livelli di protezione così come garantiti dal GDPR[84].

Eppure delle interferenze possono aversi anche nei rapporti tra il regolamento 2001/45/CE e la direttiva ePrivacy. Nello svolgimento delle proprie funzioni le istituzioni e gli organismi europei, infatti, facevano e fanno largo uso di servizi di comunicazione elettronica. Al momento dell'emanazione del regolamento in questione, la materia – delle telecomunicazioni da parte delle istituzioni comunitarie – non era disciplinata da alcun atto dell'Unione. Come è stato poc'anzi rilevato, è con il Trattato di Amsterdam che l'Unione si dota di una base giuridica capace di attribuirle la competenza a vincolare anche gli organismi e le istituzioni comunitarie nell'ambito della tutela della

stabilito che a partire dal 1 gennaio 1999 l'*aquis communitaire* sul trattamento dei dati personali e sulla libera circolazione degli stessi si applichi alle istituzioni e agli organismi istituiti dal presente trattato o sulla base dello stesso».

[82] Si rinvia *supra*, par. 5.1., al dispositivo dell'art. 16, TFUE, e, specificamente, al par. 2.

[83] Art. 2, par. 3 e considerando 17, GDPR.

[84] Considerando 17, art. 2, par. 3, e art. 98, GDPR.

privacy. La direttiva 97/66/CE relativa alla protezione dei dati personali nel settore delle telecomunicazioni (anteriormente alla relativa modifica e abrogazione da parte della direttiva 2002/58/CE) non poteva quindi estendere la propria portata sino ad onerare gli enti comunitari. Per le motivazioni sopra elencate, è stato lo stesso regolamento 2001/45/CE a stabilire agli artt. 34-40 una specifica disciplina di protezione dei dati personali connesso con «l'uso di reti o terminali di telecomunicazione che funzionano sotto il controllo di un'istituzione o di un organismo comunitario»[85]. Tale *status quo* perdura anche a seguito dell'adozione della direttiva ePrivacy (che abroga e sostituisce la direttiva 97/66/CE), la quale non contiene alcun riferimento né al regolamento 2001/45/CE né, più in generale, all'utilizzo di servizi e apparecchi di comunicazione elettronica da parte degli organismi e delle istituzioni comunitarie.

Pertanto, si può concludere che non esiste alcun contrasto tra la disciplina prevista ai sensi del regolamento 2001/45/CE e, da un lato, il GDPR, dall'altro, la direttiva ePrivacy. In entrambe le fattispecie, all'identità – anche solo parziale – degli ambiti materiali corrispondono differenti sfere di applicazione *ratione personae*. Tuttavia, date le competenze di cui è attualmente titolare il legislatore europeo, emergono alcune criticità. Più specificamente, il legislatore avrebbe potuto attuare una riforma più completa e pervasiva, prevedendo l'aggiornamento di tutti i principali strumenti unionali di protezione dei dati personali, non anche una riforma articolata in due tempi ovvero diretta, nel primo, a rinnovare i provvedimenti con il più ampio spettro applicativo e, nel secondo, a svolgere un'attiva di riesame degli altri strumenti esistenti in funzione della disciplina generale così come riformata.

[85] Art. 34, regolamento 2001/45/CE. È bene precisare che l'ambito applicativo del regolamento n. 45 del 2001 nelle telecomunicazioni rientra solo parzialmente nella direttiva ePrivacy. Difatti, il regolamento si riferisce a qualunque «uso di reti o terminali di telecomunicazione che funzionano sotto il controllo di un'istituzione o di un organismo comunitario», mentre la direttiva *ex* art. 3, par. 1, è limitata al «trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati». Pertanto, la portata del regolamento copre anche tutti quei servizi di comunicazione elettronica non accessibili al pubblico, quali reti interne che sono frequentemente utilizzate in ambito lavorativo.

5.2.3. *La direttiva 2016/680/UE*

Il GDPR ha espressamente escluso la propria applicazione al trattamento dei dati personali effettuati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[86]. Come si è già osservato[87], il settore in questione soggiace a logiche e contemperamenti di interessi del tutto peculiari, il che gli consente di assumere una propria individualità e specificità rispetto agli altri campi del diritto dell'UE. I dati e la loro circolazione sono considerati degli strumenti indispensabili per ottenere una cooperazione transnazionale delle autorità giudiziarie e di polizia sempre maggiore. Tuttavia, se da un canto la raccolta, il trattamento e la condivisione di dati appaiono mezzi adeguati per contrastare e prevenire un ampio spettro di forme di criminalità, dall'altro emerge la necessità di salvaguardare il diritto del singolo alla protezione dei propri dati personali.

Riguardo a questa fattispecie, l'UE ha tardato ad intervenire con una apposita disciplina. Nel 2008 è stata adottata la decisione GAI n. 977, la quale si è tuttavia presentata lacunosa sotto vari punti di vista. La decisione tutela sì la persona fisica dal trattamento dei dati a carattere personale nell'ambito della cooperazione giudiziaria e di polizia in materia penale, ma solo per trasferimenti di informazioni transfrontalieri. Ne risultano così escluse tutte quelle operazioni *purely domestic* che implicano scambi di dati tra autorità di uno stesso Stato[88]. Al limitato ambito applicativo si aggiunge l'assenza di un allineamento tra la tutela offerta dalla direttiva 'madre' e quella considerevolmente più modesta della decisione. Pertanto, il quadro giuridico attualmente in vigore presenta una frammentazione sia sul piano normativo sia su quello sostanziale.

Conscio di tali lacune, il legislatore europeo ha ritenuto opportuno regolare l'*informational privacy* in maniera più pervasiva anche in questo specifico settore, affinché potesse essere assicurato un livello di protezione uniforme e più elevato in tutti gli Stati membri[89]. A tal fine è stata adottata la direttiva 2016/680/UE che abrogherà e

[86] Art. 2, par. 2 e considerando 19, GDPR. V. anche considerando 15, direttiva 2016/680/UE

[87] V. *supra*, par. 5.2.

[88] Cfr. Sica, D'Antonio e Riccio, *op. cit.*, 333.

[89] Considerando 7 e art. 1, par. 1, direttiva 2016/680/UE.

sostituirà la decisione-quadro 2008/977/GAI[90]. Da una rapida analisi della nuova direttiva emergono immediatamente due elementi caratterizzanti. In primo luogo, gli obiettivi che l'atto intende realizzare rispecchiano pienamente la natura bifronte dell'intera disciplina comunitaria della *privacy*: ai sensi dell'art. 1, par. 2, la direttiva in questione è finalizzata, da un lato, a tutelare i diritti e le libertà fondamentali delle persone fisiche e, dall'altro, ad agevolare lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione[91]. In secondo luogo, il sistema di protezione offerto è più avanzato rispetto al precedente e costituisce uno *standard* minimo oltre il quale ciascuno Stato membro non può scendere. Viceversa, è riconosciuto ad ogni Stato membro la facoltà di concedere una tutela più garantista rispetto quella sancita dalla direttiva[92].

Per quanto concerne l'ambito di applicazione materiale e al pari del GDPR, la direttiva 2016/680/UE si applica al «trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi»[93]. Tuttavia, queste operazioni devono essere condotte da parte delle autorità competenti ai sensi della direttiva e per i fini di cui all'art. 1, par. 1, ossia «di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica»[94]. L'applicazione è comunque limitata dalle esclusioni previste dall'art. 2, par. 3, che estromette dalla portata della direttiva le attività che non rientrano nel campo di applicazione del diritto dell'Unione[95], i trattamenti effettuati da istituzioni, organi, uffici e agenzie europee per le quali trova applicazione il regolamento 2001/45/CE[96] e, infine,

[90] Art. 59, direttiva 2016/680/UE.

[91] V. anche considerando 4, 15, 93, Preambolo direttiva 2016/680/UE.

[92] Art. 1, par. 3, direttiva 2016/680/UE.

[93] Cfr. Art. 2, par. 2, direttiva 2016/680/UE e art. 1, par. 2, decisione-quadro 2008/977/GAI; Sica, D'Antonio e Riccio, *op. cit.*, 334. Si noti la totale identità tra l'articolo in questione e l'art. 2, par. 1, GDPR. Si rinvia pertanto *supra*, par. 5.2.1., per una definizione più puntuale di «trattamento» rilevante ai fini della disciplina europea in materia di protezione dei dati.

[94] V. anche considerando 12, Preambolo direttiva 2016/680/UE.

[95] Sebbene non sia esplicitamente previsto, è possibile ritenere escluso il settore PESC dall'ambito di applicazione della presente direttiva in quanto non rientrante nel diritto dell'Unione. V. considerando 14, Preambolo direttiva 2016/680/UE.

[96] V. anche considerando 19, Preambolo direttiva 2016/680/UE.

quelli operati nel corso di procedimenti penali per i quali è rimessa a ciascuno Stato la definizione della relativa disciplina[97].

Da quanto appena esposto si desume che la direttiva 2016/680/UE presenta una portata materiale talmente ampia da prevedere finanche una disciplina generale del settore. Invero, diversamente dalla decisione 2008/977/GAI, il nuovo atto dell'UE disciplina sia i trattamenti conseguenti a trasferimenti transnazionali sia quelli *purely domestic*, purché operati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. Inoltre, la nozione di 'autorità competente' adottata dal provvedimento è molto più estesa rispetto alla preesistente disciplina, ricomprendendo non solo «qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica» ma anche «qualsiasi altro organismo o entità incaricate dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici» ai fini summenzionati[98]. Infine, la latitudine della direttiva 2016/680/UE è condizionata anche dalla definizione di alcuni concetti la cui vaghezza lascia aperto qualche margine interpretativo. Nello specifico, si comprende agevolmente come, tra le finalità di cui all'art. 1, par. 1, il concetto di 'minaccia alla sicurezza pubblica' sia estremamente indeterminato[99]. Ciò potrebbe portare ad applicare la direttiva ad ambiti disciplinati da altri provvedimenti quali, ad esempio, il GDPR ovvero il regolamento 2001/45/CE. Difatti, i campi applicativi dei vari provvedimenti, seppure distinti, sono in ogni caso contigui. L'indeterminatezza di alcune disposizioni della direttiva potrebbe in concreto influire sull'applicazione di altri atti dell'UE: un'interpretazione estensiva di nozioni astratte potrebbe condurre ad attuare la direttiva anche ad attività che non presentano alcun col-

[97] V. considerando 20, 49, 107 e art. 18, direttiva 2016/680/UE.

[98] Art. 3, n. 7, direttiva 2016/680/UE. V. anche Sica, D'Antonio e Riccio, *op. cit.*, 334.

[99] In merito P. Troisi ritiene che qualche ausilio possa essere desunto dal considerando 12. Dall'analisi dell'elenco esemplificativo ivi contenuto, l'Autore deduce la probabile adozione di una nozione ristretta di pubblica sicurezza «quale funzione specificamente rivolta alla prevenzione di reati in contesti particolarmente sensibili». Sica, D'Antonio e Riccio, *op. cit.*, 333 -334.

legamento con la prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Questa connessione tra trattamento operato dall'autorità competente ai sensi della direttiva 2016/680/UE e i fini perseguiti è fondamentale per la determinazione dell'atto applicabile: il trattamento di dati personali da parte di un'autorità competente ai fini di prevenzione, indagine, accertamento e perseguimento di reati, qualora sia posto in essere per finalità differenti da quelle previste dalla direttiva *de qua*, non potrà che essere sottoposto a discipline sancite da altri provvedimenti unionali.

Altrettanto complessa è la delimitazione dell'estensione territoriale della direttiva 2016/680/UE. Essendo adottato nell'ambito della cooperazione giudiziaria e di polizia in materia penale o, più in generale, dello SLSG, l'atto dell'UE è vincolante per tutti gli Stati che vi partecipano, salvo l'esistenza di regimi derogatori[100]. Sono pertanto soggetti alla nuova disciplina l'Islanda, la Norvegia, la Svizzera e il Liechtenstein, in quanto la direttiva in questione costituisce uno sviluppo delle disposizioni relative all'*acquis* di Schengen così come stabilite dai rispettivi accordi di associazione. All'opposto, nello SLSG sono presenti alcuni Paesi membri nei confronti dei quali l'attuazione della disciplina richiede un loro consenso espresso ovvero tacito. La Danimarca potrebbe invocare la clausola di *opting-out* attraverso la quale evitare di dare attuazione ad una misura in qualsiasi momento, mentre Gran Bretagna ed Irlanda – trascurando la conclusione della procedura di recesso *ex* art. 50, TUE – potrebbero attivare la clausola di *opting-in* che consente loro "di partecipare, caso per caso, alla procedura di adozione di una misura o all'adozione di una misura già adottata"[101]. Tuttavia, è bene precisare che l'eventuale ricorso a tali riserve non precluderebbe alla Convenzione n. 108 e alla CEDU – e ai rispettivi livelli di tutela – di trovare comunque applicazione.

La direttiva 2016/680/UE, sebbene abbia un campo d'azione molto ampio, non costituisce l'unico strumento di regolamentazione della *privacy* nel settore della cooperazione giudiziaria penale e di

[100] V. considerando 99-103, Preambolo direttiva 2016/680/UE.

[101] *Lo spazio di libertà, sicurezza e giustizia*, 22 settembre 2015, *http://eur-lex.europa.eu/legalcontent/IT/TXT/HTML/?uri=URISERV:ai0022&from=IT*. Cfr. anche D. Rinoldi, *Lo spazio di libertà, sicurezza e giustizia nel diritto dell'integrazione europea. I princìpi generale e aspetti penalistici*, Napoli, 2012, 28, 71-73; S. Montaldo, *I limiti della cooperazione in materia penale dell'Unione europea*, Napoli, 2015, 208-233.

polizia. In questo ambito o, più in generale, nello SLSG, emergono una pluralità di atti ciascuno dei quali, nel regolare particolari flussi di informazioni ovvero nell'instaurare banche dati, ha prescritto uno specifico sistema di tutela dei dati personali. In merito, la direttiva 2016/680/UE lascia impregiudicate «le disposizioni specifiche per la protezione dei dati personali contenute in atti giuridici dell'Unione che sono entrati in vigore il o anteriormente al 6 maggio 2016 nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che disciplinano il trattamento tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei Trattati, nell'ambito di applicazione della presente direttiva»[102]. Ciò costituisce un ulteriore, se non il principale, elemento di frammentazione di tutto il sistema normativo dell'UE in materia.

Nel settore della cooperazione giudiziaria e di polizia operano vari *database* quali l'EIS[103] ('*Europol Information System*'), l'EPOC[104] ('*European Pool against Organized Crime*') ovvero l'archivio istituito con il Trattato di Prüm[105]. Oltre a ciò, durante lo svolgimento delle

[102] Art. 60, direttiva 2016/680/UE.

[103] Istituito con la Convenzione Europol del 26 luglio 1995, poi aggiornato dalla decisione 2009/371/GAI del Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol), a sua volta abrogata e sostituita dal Regolamento 2016/794/UE dell'11 maggio 2016 che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto. Cfr. F. Decli e G. Marando, *Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia*, in M. Gialuz e F. Peroni (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, 122-129; F. Pigliacelli, *Profilo di diritto penale e processuale europeo*, Roma, 2010, 295-297; E. Colombo, *Banche dati UE. Un articolato sistema di informazioni tra diritti della persona ed esigenze di prevenzione e repressione dei reati*, in *Cass. pen.*, 2012, fasc. 5, 1946-1947.

[104] Decisione 2002/187/GAI del Consiglio del 28 febbraio 2002 che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità come modificata dalla decisione 2009/426/GAI del Consiglio del 16 dicembre 2008 relativa al rafforzamento dell'Eurojust e che modifica la decisione 2002/187/GAI che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità. Cfr. Decli e Marando, *op. cit.*, 133-138; Pigliacelli, *op. cit.*, 312-314; Colombo, *op. cit.*, 1947-1948; P. Troisi, *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012, 66-73.

[105] Il quadro di Prüm del 27 maggio 2005 nato da una cooperazione intergovernativa di sette Stati (Austria, Belgio, Francia, Germania, Lussemburgo, Paesi Bassi e Spagna) è stato in parte ricondotto nel diritto dell'UE dalla decisione 2008/615/GAI del 23 giugno 2008 sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera. Tuttavia, detto atto non è stato

proprie attività le autorità competenti a fini di prevenzione, repressione e perseguimento dei reati possono entrare in contatto con altre banche dati istituite nel quadro più generale dello SLSG quali SIS[106] (giunto alla seconda generazione SIS II[107]), VIS[108], Eurodac[109] e SID[110].

L'instaurazione delle prime banche dati comunitarie[111] ha creato non pochi problemi sotto il profilo della tutela dell'*informational*

recepito dalla totalità dei Paesi membri. Cfr. L. Marafioti e L. Lupària (a cura di), *Banca dati del DNA e accertamento penale: commento alla legge di ratifica del Trattato di Prüm, istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Milano, 2010, 189; G. Di Paolo, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in T. Rafaraci (a cura di), *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il trattato di Lisbona*, Milano, 2011, 187-211; C. Di Stasio, *La lotta multilivello al terrorismo internazionale. Garanzia di sicurezza versus tutela dei diritti fondamentali*, Brescia, 2013, 460-466.

[106] Istituita dalla Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985. In merito alla struttura, agli obiettivi e al funzionamento del SIS si veda: Decli e Marando, *op. cit.*, 106-109; Pigliacelli, *op. cit.*, 299-300; E. Falletti e V. Piccone, *Il nodo gordiano tra diritto nazionale e diritto europeo*, Bari, 2012, 290-291; Colombo, *op. cit.*, 1949-1950; Troisi, *op. cit.*, 56-63; C. Flaccomio, *L'ingresso ed il soggiorno nel territorio nazionale*, in A. Macrillò (a cura di), *Il diritto degli stranieri*, Lavis, 2014, 206-209.

[107] Istituito dai regolamenti 1987/2006/CE e 1986/2006/CE e dalla decisione 2007/533/GAI. Cfr. Decli e Marando, *op. cit.*, 110-118; Pigliacelli, *op. cit.*, 300-303; Falletti e Piccone, *op. cit.*, 292; Troisi, *op. cit.*, 56-63; Di Stasio, *op. cit.*, 444-456.

[108] Decisione 2004/512/CE del Consiglio, regolamento (CE) n. 767/2008, decisione 2008/633/GAI del Consiglio. Cfr. Pigliacelli, *op. cit.*, 309-311; B. Balbo, *I cittadini non comunitari*, Torino, 2011, 330-332; Colombo, *op. cit.*, 1950; Troisi, *op. cit.*, 78-81; Di Stasio, *op. cit.*, 434-438; Falletti e Piccone, *op. cit.*, 293; Flaccomio, *op. cit.*, 210-211.

[109] Istituito dal regolamento 2000/2725/CE, recentemente abrogato dal nuovo regolamento 2013/603/UE. Cfr. Pigliacelli, *op. cit.*, 314-318; Troisi, *op. cit.*, 73-78. Riguardo l'ambito territoriale del regolamento 603/2013, esso si applica anche al Regno Unito, alla Danimarca e agli Stati 'associati' Schengen (Islanda, Norvegia, Svizzera, Liechtenstein). L'Irlanda, invece, ha invocato la clausola di *opt-in* contro il regolamento di cui si tratta, ma rimane vincolata alla versione precedente.

[110] Istituito dalla Convenzione sull'uso dell'informatica nel settore doganale del 26 luglio 1995 (c.d. 'convenzione SID') la quale è stata però sostituita, a decorrere dal 27 maggio 2011, dalla Decisione 2009/917/GAI del Consiglio del 30 novembre 2009 sull'uso dell'informatica nel settore doganale, poiché la suddetta Convenzione non risultava sufficiente a conseguire gli obiettivi di prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali.

[111] Si faccia riferimento alla prima versione del SIS (1985), dell'EIS (1995) o dell'EPOC (2002).

privacy. Invero, ciascuna di queste ha creato dei sub-sistemi di protezione dei dati tra loro non coincidenti. Si ravvisa un unico elemento comune: il blando richiamo alla Convenzione n. 108 e alla raccomandazione R(87)15 che hanno costituito la base sulla quale ciascun provvedimento ha costruito un regime di protezione più avanzato e sensibile ai rischi derivanti dal trattamento, dalla conservazione e dallo scambio dei dati personali.

Un'inversione di tendenza è stata invece registrata negli atti che hanno aggiornato i primi archivi informatizzati ovvero che ne hanno istituito di nuovi. Al mero richiamo alla Convenzione n. 108 e alle raccomandazioni del CdE si affiancano rinvii espressi alle discipline previste nell'allora primo e terzo pilastro. Ciò non ha però rimosso completamente le divergenze tra i sistemi di protezione previsti per ciascun *database* e quelli previsti dai provvedimenti generali. Permane ancora un sistema satellitare di micro-discipline che gravitano attorno agli atti generali rappresentati dalla direttiva 'madre' e dalla decisione 2008/977/GAI, presto abrogate e sostituite dal pacchetto europeo di protezione dei dati. Tuttavia, il passaggio dalla prima alla seconda generazione di *database* ravvisa un orientamento volto a garantire in modo più pregnante i diritti connessi alla riservatezza e alla tutela della *privacy* anche all'interno dei sistemi automatizzati dell'UE. Sarebbe tuttavia preferibile sostituire i rinvii a normative generali con la predisposizione e l'applicazione diretta di regole comuni, affinché si possa conferire una maggiore omogeneità alla materia: come già osservato, i sistemi di garanzia apprestati dai singoli atti costitutivi o modificativi dei *database*, sebbene presentino una base comune, creano livelli di protezione e di tutela differenziati.

Infine, la disciplina dell'UE per la protezione dei dati personali diverrà ancora più articolata a partire dal 6 maggio 2018, data in cui sarà definitivamente applicabile la direttiva 2016/681/UE sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi[112]. Questo atto si ripropone di contrastare le

[112] Non è possibile in questa sede analizzare più specificamente il tema del PNR, tutti gli accordi intervenuti tra l'UE e altri Stati *extra*-europei e il connesso dibattito dottrinale sulla fondatezza e sulla proporzionalità di tali misure. Tuttavia, per un approfondimento esaustivo sugli accordi PNR siglati dall'UE con USA, Canada e Australia si invita il lettore a consultare i seguenti testi: A. Terrasi, *La protezione dei dati personali tra*

forme più gravi di criminalità attraverso lo scambio di PNR tra le compagnie aeree e le autorità, statali e dell'Unione, competenti in materia penale per il tramite di uffici nazionali detti UIP ('unità d'informazione sui passeggeri') predisposti alla raccolta, trattamento e trasferimento di tali dati. Al pari dei sistemi d'informazione dell'UE, anche la direttiva PNR dichiara di rispettare nello svolgimento delle varie attività «i diritti fondamentali e i princìpi della Carta, in particolare il diritto alla protezione dei dati personali, il diritto al rispetto della vita privata e il diritto alla non discriminazione, tutelati dagli articoli 8, 7 e 21 della stessa, e dovrebbe essere attuata di conseguenza»[113] e asserisce, al considerando n. 23, di non nuocere all'alto livello di tutela garantito dalla Convenzione n. 108. Inoltre, essa è informata ai princìpi sanciti dalla decisione 2008/977/GAI; anzi, la stessa rinvia espressamente a tale disciplina[114] e prevede per alcuni aspetti delle norme più garantiste per la protezione dei dati personali in ragione dei rischi più elevati dovuti all'oggetto del trattamento. Tuttavia, tralasciando qualsiasi considerazione sull'opportunità e sulla legalità di una tale misura, quel che interessa qui rilevare è l'esistenza, nel panorama della cooperazione giudiziaria e di polizia in materia penale, di un ulteriore strumento che tutela la *privacy* dell'individuo in maniera solo parzialmente analoga a quella del provvedimento generale vigente in materia.

Concludendo, anche il campo della cooperazione giudiziaria e di polizia in materia penale e, più in generale, lo SLSG sono caratterizzati da uno scenario altamente frastagliato, composto da una moltitudine di strumenti giuridici che tutelano la *privacy* in limitati e specifici ambiti sia materiali che territoriali. Questo settore più di altri richiede un intervento serio ed impegnativo del decisore europeo che dovrebbe intervenire simultaneamente sui differenti regimi attualmente esistenti nell'UE per ottenere una più ampia organicità strutturale ed omogeneità nei livelli di tutela offerti. Solo una simile

diritto internazionale e diritto dell'Unione europea, Torino, 2008, 211-223; M. Nino, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, 178-246; Di Stasio, *op. cit.*, 466-477; B. Piattoli, *Principio di proporzionalità UE e trattamento dei dati personali nella lotta al terrorismo*, in *Diritto penale e processo*, 2015, fasc. 7, 885-894; Bolognini, Pelino e Bistolfi, *op. cit.*, 30-31.

[113] Considerando 36 Preambolo direttiva PNR.

[114] Art. 13, direttiva PNR.

riforma potrebbe realmente uniformare la disciplina UE della protezione dei dati personali nel vasto ambito dello SLSG.

6. *Le nuove prospettive dell'*informational privacy*: verso una reale uniformità in Europa*

Nel presente lavoro è stata analizzata tutta la struttura normativa dell'*informational privacy* in Europa approfondendo più specificatamente la protezione dei dati personali offerta all'interno del CdE e dell'UE. Nell'ambito di quest'ultimo organismo, è stata evidenziata la frammentarietà del sistema composto da una molteplicità di atti normativi derivati i cui livelli di tutela non sempre sono pienamente coordinati o allineati. Il quadro così definito si presenta tutt'altro che omogeneo e coerente. Risulta pertanto necessario che il legislatore europeo intervenga nuovamente affinché la pluralità di fonti venga ricondotta in unità, aggiornando e revisionando i singoli atti a tutto campo. Parimenti, un'attività di ammodernamento è richiesta anche ad opera del CdE: la Convenzione n. 108, sebbene costituisca una pietra miliare della protezione della *privacy* in Europa, necessita di un innalzamento del suo standard di tutela.

Ebbene, i lavori in corso delle due organizzazioni internazionali lasciano intravedere delle prospettive di sviluppo abbastanza concrete.

Il CdE ha avviato a partire dal 2010 dei lavori di aggiornamento della Convenzione n. 108 che si sono conclusi nel 2016 con un proposta di modifica del testo pattizio. Tale proposta non introduce innovazioni in merito all'ambito di applicazione materiale o territoriale, ma eleva notevolmente le garanzie apprestate da questo strumento sino a raggiungere un vero e proprio allineamento, da un lato, con le *Guidelines* dell'OCSE come modificate nel 2013, e dall'altro, con il nuovo pacchetto europeo di protezione dei dati dell'UE. L'obiettivo di raggiungere un alto livello di coesione non è percepito soltanto all'interno dell'Unione, ma anche al di fuori. L'accoglimento di una tale proposta consentirebbe la realizzazione di un quadro coerente e armonico in Europa, considerata nel suo complesso.

A tal fine è necessario che la stessa UE si impegni a riesaminare le fonti di diritto derivato già esistenti al fine di creare un sistema organico con gli atti del nuovo pacchetto europeo di protezione dei dati. La pluralità di micro-cosmi di protezione dei dati previsti dagli

atti instauranti singoli *database* rappresenta uno dei problemi principali da risolvere. Come è stato già osservato, la previsione di meri rinvii alla disciplina generale non ha impedito il sorgere di livelli o standard di protezione tra loro divergenti.

Recentemente sembra profilarsi ravvisarsi una qualche prospettiva concreta di revisione riguardo sia alla direttiva 2002/58/CE che al regolamento 2001/45/CE. Il 10 gennaio 2017 sono stati approvati i testi di due proposte di regolamento che, qualora fossero adottate, abrogherebbero e sostituirebbero questi due atti. In entrambe le proposte si legge l'intenzione della Commissione europea di adottarli entro il 25 maggio 2018, data che – non casualmente – coincide con quella in cui diverrà definitivo il GDPR. Le proposte in questione costituiscono infatti dei nuovi tasselli nel mosaico di una più generale e completa riforma della disciplina dell'*informational privacy* nell'UE già parzialmente avviata, appunto, dal 'pacchetto' del 2016.

La direttiva 2002/58/CE potrebbe quindi, a breve, essere sostituita da un regolamento[115]. La scelta dello strumento regolamentare in luogo della direttiva sollecita le stesse considerazioni già svolte in precedenza riguardo al passaggio dalla direttiva 'madre' al GDPR[116]. Il regolamento, non necessitando di attività di recepimento da parte degli Stati membri e riconoscendo i diritti direttamente in capo al singolo, è in grado di raggiungere una maggiore armonizzazione e uniformità normativa della materia all'interno dell'Unione. A ciò si aggiunga che la nuova proposta innalza gli *standard* di tutela offerti allineandosi in tal modo con il GDPR e, di conseguenza, creando un quadro giuridico più coerente. Il coordinamento tra le due fonti si rintraccia non solo nel livello di protezione, nella condivisione terminologica[117] o nei frequenti rinvii al GDPR ma, ancor più esplicitamente, nella dichiarazione del carattere integrativo della proposta alla disciplina generale[118]: il regolamento ePrivacy non può in alcun modo ridurre il grado di tutela offerto dal GDPR[119].

[115] Commissione e Parlamento europeo, *Proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)*, 10 gennaio 2017, COM(2017) 10 final.

[116] Si rinvia *supra* par. 5.2.

[117] V. art. 4, par. 1, proposta regolamento ePrivacy.

[118] Considerando 5 e art. 1, par. 3, proposta regolamento ePrivacy.

[119] Considerando 6, Preambolo proposta regolamento ePrivacy.

Quanto al contenuto della nuova proposta, si registra una notevole estensione dell'ambito di applicazione materiale e territoriale. Il primo viene finalmente aggiornato al fine di stare al passo con la moderna società informatizzata e '*always connected*'. Se l'attuale direttiva regola solamente il «trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico», la proposta di regolamento ePrivacy ricomprenderà, invece, i trattamenti connessi non solo alla fornitura, ma anche all'uso di servizi di comunicazione elettronica oltre che quelli relativi alle «informazioni connesse alle apparecchiature terminali degli utenti finali», potendovi così ricomprendere anche gli OTT ('*Over The Top provider*')[120]. Tuttavia, esulano dal campo del regolamento *de quo*, al pari della direttiva che lo stesso si propone di sostituire, le attività che non rientrano nel campo di applicazione del diritto dell'Unione, quelle rientranti nel settore PESC, quelle operate dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, i trattamenti di dati delle comunicazioni elettroniche soggette al regolamento 2001/45/CE e, infine, i servizi di comunicazione elettronica non accessibili al pubblico[121]. Anche l'ambito territoriale ha un'estensione molto ampia, infatti, – al pari del GDPR – fa riferimento a qualsiasi fornitore di servizi di comunicazione elettronica stabilito nell'Unione ovvero stabilito altrove, ma che tratti dati di utenti finali che si trovino nel territorio dell'Unione[122].

All'opposto, la seconda proposta di regolamento, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione[123], non comporta mutamenti nell'ambito di applicazione del regolamento 2001/45/CE. Essa eleva il grado di salvaguardia dei diritti degli interessati in modo coerente con quello offerto

[120] Art. 2, par. 1, proposta regolamento ePrivacy. Di grande rilievo sono anche i considerando 10-15 i quali passano in rassegna tutte le tecnologie e i mezzi di comunicazione più moderni che non erano in passato ricompresi nell'alveo della direttiva ePrivacy.

[121] Art. 2, parr. 2-3, proposta regolamento ePrivacy.

[122] Considerando 9 e art. 3, proposta regolamento ePrivacy.

[123] Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, Bruxelles, 10 gennaio 2017, COM(2017) 8 final.

dal GDPR e dalla direttiva 2016/680/UE. La coerenza del quadro normativo dell'UE può essere raggiunta solo tramite il riconoscimento di tutele omogenee. Ciò è supportato non solo dai vari rinvii al GDPR, ma anche dall'invito ad interpretare in modo analogo gli stessi concetti presenti in entrambi gli strumenti[124].

In definitiva, il pacchetto europeo dei dati personali costituisce solo il primo passo di un più ampio progetto di riforma che può essere raggiunto soltanto attraverso l'adozione di ulteriori provvedimenti diretti, da un lato, al rinnovamento delle misure e, dall'altro, verso l'uniformità dei livelli di protezione. Sebbene non venga eliminata la pluralità di fonti normative e la relativa frammentazione, una riforma condotta nei termini sopra esposti potrà fissare un omogeneo ed uniforme *standard* di tutela applicabile in tutti gli ambiti del diritto dell'Unione.

7. *Conclusioni*

L'indagine condotta in questo saggio ha messo in luce l'esistenza di una pluralità di regimi europei di protezione dei dati personali, evidenziandone le rispettive aree di intervento e sfere di efficacia. Com'è ovvio, data anche la loro origine e natura, gli strumenti presi in esame differiscono notevolmente sotto il profilo della portata sostanziale della protezione, spaziando da modelli volti a garantire uno *standard* minimo di tutela, come nel caso della Convenzione n. 108 del CdE, a modelli più sofisticati e penetranti, come quelli incorporati nel nuovo "pacchetto" di riforme varato dell'UE. Il presente lavoro ha tuttavia evitato di entrare nel merito dei provvedimenti e soluzioni adottati nei vari strumenti giuridici considerati. Allo stesso tempo, è sembrato qui superfluo soffermarsi tra i diversi sistemi che scaturiscono dalla capacità o meno di questi di porre diritti ed obblighi direttamente in capo ai privati. Questo studio si è concentrato, piuttosto, sulla portata o ambito di applicazione di ciascuno di questi strumenti, con il proposito di individuare le possibili complementarità, sovrapposizioni o lacune determinate dalla struttura multilivello della protezione dei dati personali in Europa.

[124] Considerando 5, Preambolo proposta regolamento concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione.

Si osserva una diversità e frammentarietà relativamente alla copertura *ratione materiae* fornita dai diversi strumenti, vale a dire alle fattispecie concrete che ricadono sotto le loro rispettive discipline. Sotto questo profilo, per misurare la 'capienza' di una determinata disciplina rileva principalmente la sua estensione rispetto alle finalità perseguite dalla raccolta e utilizzo dei dati personali oggetto della regolamentazione. In particolare, è importante verificare se tra queste finalità siano o meno da includervi, e in che misura, quelle che attengono a funzioni pubbliche, quali il mantenimento dell'ordine pubblico e della sicurezza pubblica, la lotta contro l'illegalità, il controllo dell'immigrazione, la cooperazione giudiziaria e penale internazionale, la tutela della salute. Quanto alle fattispecie di trattamento dei dati personali connesse a finalità che attengono alla gestione di rapporti tra privati, *in primis* quelli di carattere commerciale o professionale, dato che trattasi di aree di intervento per così dire 'di ordinaria amministrazione', che di norma non sollevano questioni politicamente sensibili per gli Stati, è in certa misura scontato che queste siano sempre ricomprese negli ambiti materiali dei diversi regimi europei di protezione, anche se solo implicitamente.

Dal punto di vista metodologico, sembra utile procedere nella disamina della portata materiale dei numerosi meccanismi di protezione dei dati personali distinguendo, da un lato, gli strumenti giuridici interamente e specificamente dedicati alla regolamentazione del trattamento dei dati personali, quali la Convenzione n. 108 del CdE e il nuovo 'pacchetto' di misure in attuazione dei Trattati istitutivi adottati dalle istituzioni dell'UE, e, dall'altro lato, i meccanismi di garanzia previsti in trattati o cataloghi generali sui diritti umani, quali l'art. 8 CEDU (alla luce dell'interpretazione della CtEDU) e l'art. 8 CDFUE.

In generale, il confronto tra la Convenzione n. 108 e la disciplina riformata dell'UE, così come diverrà esecutiva a partire dal maggio 2018, mette in luce il diverso approccio sottostante l'adozione di questi strumenti, il quale evidentemente rispecchia la contrapposizione tra la natura internazionale/intergovernativa della Convenzione e quella sovranazionale/centralizzata della legislazione dell'UE.

La Convenzione n. 108 ha, in astratto, un raggio di azione estremamente vasto, in quanto nessun ambito materiale risulta preliminarmente sottratto alla sua disciplina; in particolare, questa riguarda

la raccolta e il trattamento dei dati personali sia nel settore privato che in quello pubblico, e può arrivare a proteggere, oltre che gli individui, anche i gruppi, le associazioni, gli enti, abbiano o no questi personalità giuridica. Tuttavia, la Convenzione contempla una formula di adesione che consente agli Stati di modulare piuttosto liberamente i loro obblighi, ad esempio escludendo che determinate categorie di banche dati siano coperti dalla protezione accordata.

Il 'pacchetto' dell'UE fornisce una disciplina completa e dettagliata che, anche quando rimessa allo strumento della direttiva, non lascia molta scelta agli Stati membri quanto alla portata dei loro obblighi. Ciò si comprende agevolmente se si considera che la riforma è stata approntata soprattutto allo scopo di armonizzare le legislazioni domestiche degli Stati membri in materia, oltre a quello di elevare il livello della protezione al fine di fronteggiare adeguatamente le sfide lanciate dalle nuove tecnologie. Al fine di garantire completezza e dettaglio alla complessa e articolata materia, il legislatore europeo ha ritenuto, nonostante la nuova base giuridica dell'art. 16 TFUE, di lasciare pressoché intatto l'impianto strutturale della preesistente disciplina, caratterizzato dalla coesistenza di più atti aventi ciascuno una determinata delimitazione del campo d'azione, anziché ricondurre le diverse tipologie di fattispecie nel quadro di un unico provvedimento. Questo approccio corrisponde evidentemente, almeno in parte, all'esigenza di rispettare gli ambiti di competenza dell'Unione, il che può spiegare ad esempio l'adozione della direttiva 2016/ 680/CE a coprire l'ambito della cooperazione giudiziaria e di polizia in materia penale separatamente dal GDPR. Tuttavia, non si può negare che questo stesso approccio abbia prodotto un'eccessiva frammentazione della disciplina, con conseguenti rischi per l'omogeneità delle soluzioni e la coerenza del sistema, oltreché, in definitiva, per la stessa certezza del diritto.

Ciò detto, il regime regolatorio della privacy nell'UE complessivamente inteso ha un ambito di applicazione molto esteso: la raccolta e l'uso dei dati personali dei singoli vengono protetti sia nel quadro dei rapporti privati che da ingerenze delle autorità pubbliche, e ciò imponendo obblighi sia nei confronti degli Stati che delle istituzioni e organismi dell'UE. La protezione si estende, seppur con i necessari adattamenti, finanche nel contesto del perseguimento di fattispecie di reati gravi, che possono mettere in pericolo la sicurezza

nazionale, quali il terrorismo. Beneficiari della protezione sono solo le persone fisiche, non anche quelle giuridiche. Ma la maggiore restrizione rispetto alla Convenzione n. 108 è evidentemente data dal limite generale, che colpisce anche la CDFUE, per cui sono esclusi dalla protezione quei trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione.

Passando alle garanzie previste dagli strumenti sui diritti umani, ossia agli 'omonimi' articoli 8 della CEDU e della CDFUE, la loro esatta portata materiale non può certo essere desunta solo dal testo delle corrispondenti disposizioni, data la formulazione concisa di queste. Nel caso della CEDU, il testo dell'art. 8 potrebbe addirittura risultare fuorviante giacché esso, nell'enunciare il diritto dell'individuo al rispetto della propria vita privata e familiare, non contiene alcun riferimento alla protezione dei dati personali. Come è noto, è stata la CtEDU, attraverso un'interpretazione evolutiva, ad estrapolare dall'art. 8 CEDU delle specifiche garanzie a tutela dell'*informational privacy*. Ed è proprio sulla base della vasta esperienza giurisprudenziale maturata ad opera della CtEDU relativamente all'interpretazione dell'8 CEDU, che si può osservare come l'ambito materiale della protezione dei dati personali che scaturisce dai trattati ed altri cataloghi sui diritti umani sia potenzialmente sconfinato. Ciò proprio in considerazione del fatto che, a fare da contrappeso alla genericità e concisione delle corrispondenti disposizioni di tali trattati e cataloghi, si erge la giurisdizione delle Corti internazionali/sovranazionali (in Europa CtEDU, CGUE) preposte a decidere dei ricorsi individuali in casi concreti, e che queste tendono ad estendere per quanto possibile, anche in virtù del 'dialogo' a distanza che si stabilisce tra loro, la portata della tutela dei diritti umani. Va tuttavia sempre tenuto presente il già menzionato limite congenito alla CDFUE, che ovviamente non risparmia il suo art. 8, per il quale la protezione non si estende a quei trattamenti di dati personali che non siano effettuati nell'esercizio di attività disciplinate dal diritto dell'UE.

In considerazione della struttura multilivello della protezione dei dati personali in Europa, generata dalla coesistenza di più fonti e atti giuridici vertenti sulla medesima materia, alle Corti europee si demanda oggi, in realtà, un compito ancora più arduo, che si presume non rientrare strettamente nell'ambito della loro giurisdizione, quello di (cercare di) garantire la coerenza e/o contemperamento tra

i vari strumenti e sistemi europei di protezione dei dati personali, aventi una diversa provenienza e natura giuridica. In quest'ottica, il meccanismo di convergenza su cui fare leva, e che non a caso si rinviene in tutti i regimi normativi esaminati, è quello del bilanciamento tra, da un lato, la protezione dei dati personali dell'individuo e, dall'altro lato, sia le esigenze connesse alla sicurezza nazionale degli Stati, alla pubblica sicurezza e all'ordine pubblico, alla tutela della salute o della morale, sia la salvaguardia dei diritti e delle libertà altrui. E tale bilanciamento, che va effettuato applicando il principio di proporzionalità[125], non può che essere rimesso, per una valutazione caso per caso, alle suddette Corti.

Merita di essere ricordato, comunque, che un coordinamento transnazionale a livello amministrativo tra i numerosi sistemi giuridici europei di protezione dei dati personali – tra cui, la Convenzione n. 108 del CdE, le *Guidelines* OCSE, la disciplina sulla *privacy* dell'UE a norma dell'art. 16 TFUE e 8 CDFUE – viene svolta dalle Autorità nazionali di controllo del rispetto delle normative europee in materia.

Abstract

La protezione dei dati personali in Europa ricade nel quadro delle garanzie previste da molteplici sistemi giuridici internazionali regionali, che fanno capo principalmente al Consiglio d'Europa e all'Unione europea. La coesistenza di questi sistemi ha dato luogo ad una complessa e articolata regolamentazione avente una struttura 'multilivello', al cui interno ciascun 'livello' è rappresentato da uno specifico strumento giuridico il quale si distingue nettamente dagli altri per natura, portata, effetti ed efficacia. Il presente saggio si propone di individuare e descrivere tale struttura multilivello attraverso l'analisi dei singoli strumenti giuridici che la compongono, al fine di rilevarne le reciproche interazioni, sovrapposizioni e complementarità. Attraverso il confronto tra i vari provvedimenti, ci si prefigge di delineare i loro rispettivi ambiti di applicazione materiale e territoriale (o soggettiva), lasciando invece fuori dall'indagine una valutazione di merito sulle soluzioni prospettate. Nell'ambito delle inizia-

[125] Sul punto, v. G. Alpa, *I principi generali. Una lettura giusrealistica*, in questa *Rivista*, 2014, numero speciale, 91-96.

tive del Consiglio d'Europa, vengono presi in considerazione, da un lato, la Convenzione n. 108 del 1980, e, dall'altro, l'articolo 8 della CEDU. L'approccio stesso, mediante il quale entrambi questi strumenti perseguono i loro obiettivi, non può essere più diverso: il primo è un trattato di tipo intergovernativo classico, specificamente dedicato alla materia considerata ma privo di un vero e proprio meccanismo internazionale di azionamento da parte dell'individuo-vittima; il secondo, seppur sintetico nella sua formulazione, funge da recipiente che si riempie nel tempo di nuovi contenuti, e ciò grazie all'interpretazione vivente fornita dalla Corte europea per i diritti dell'uomo. Per quanto riguarda l'ordinamento dell'UE, a maggio 2018 diventerà pienamente esecutiva la normativa che ha riformato la materia attraverso il nuovo 'pacchetto europeo di protezione dei dati personali'. Si tratta di una disciplina completa e dettagliata che si compone del regolamento n. 679 (GDPR) e della direttiva 680, entrambi adottati nel 2016, ai quali si aggiunge la direttiva 681, che opera nel settore della cooperazione giudiziaria e di polizia in materia penale. Questi atti derivati, di cui si dà un'ampia analisi nel presente saggio, se da un lato trovano la loro nuova base giuridica nell'art. 16 del TFUE introdotto con il Trattato di Lisbona, dall'altro danno attuazione all'art. 8 della Carta dei diritti fondamentali dell'UE. Evidentemente, data la sua natura 'sovranazionale', la disciplina dell'UE presenta un più elevato grado di penetrazione negli ordinamenti nazionali e assicura maggiori garanzie di giustizia per gli individui-vittime rispetto agli strumenti di diritto internazionale predisposti nel quadro del Consiglio d'Europa. Ciononostante, la stessa evidenzia anche diverse 'ombre', sia riguardo all'interazione tra i diversi atti in cui si articola il nuovo 'pacchetto', con qualche ricaduta negativa sulla coerenza del sistema, che relativamente alla concreta capacità del singolo di agire a tutela dei propri diritti.

In Europe, the protection of personal data falls under the coverage of several legal international systems, which are mainly the outcome of the activities of the Council of Europe and the European Union. The coexistence of such different sets of rules created a complex and comprehensive legal regime having a multilayered structure, while each layer consists in one specific legal instrument showing distinctiveness regarding its nature, scope, effects and effectiveness. The purpose of this essay is to identify and describe such a

multilayered structure through the analysis of the relevant legal instruments, aiming at detecting their mutual interactions, overlaps and complementarities. Our decisive goal is to highlight the scope of the compared measures, either from a substantial point of view or a territorial (subjective) point of view. Instead, the matter and suitability of each measure will not be discussed here properly. Considering the Council of Europe initiatives, this essay focuses either on the Convention n. 108 of 1980 and on art. 8 of the ECHR. These two instruments take an opposite approach in pursuing their ends: Convention n. 108 is an intergovernmental treaty of a traditional type, specifically devoted to the protection of personal data though devoid of a proper international mechanism having jurisdiction over claims presented by individuals/victims; notwithstanding its conciseness, ECHR art. 8 represents a container which is progressively filled with new contents and meanings, and this thanks to the living interpretation of the European Court of Human Rights. Regarding EU law, a new set of rules on the protection of personal data is going to become finally applicable next May 2018. This is a comprehensive and detailed discipline consisting of EU Regulation n. 679 (GDPR) and EU Directive 680 both adopted 2016. Additionally, EU Directive 681 applies to the area of police and judicial cooperation in criminal matters. These acts of secondary law, which are thoroughly investigated in the present essay, find their legal basis in art. 16 TFEU as amended by the Treaty of Lisbon, while implementing art. 8 of EU Charter of Fundamental Rights. Given its 'supranational' nature, EU legislation is far more suitable than Council of Europe treaty measures in penetrating national legal orders and ensuring effective redress to individuals/victims. EU legislation shows nevertheless some shortcomings. There is, on the one side, a risk of fragmentation in the EU legal asset resulting from the multitude of legal acts cross-regulating the matter of the personal data protection. On the other side, the access to EU judicial remedies against data protection infringements are not always open to the individuals/victims.