



La tutela dei dati personali nella giurisprudenza della Corte di giustizia

di Francesco Rossi Dal Pozzo¹

SOMMARIO: 1. La protezione dei dati personali nel settore digitale tra nuove sfide e antichi dilemmi. – 2. Il nuovo quadro giuridico dell’Unione europea per la (progressiva) costruzione di un mercato unico digitale. – 3. L’evoluzione della giurisprudenza della Corte di giustizia in tema di protezione dei dati personali. - 3.1. Il tenue legame tra la protezione dei dati personali e le libertà fondamentali sancite dai Trattati. – 4. La protezione dei dati personali come nuova competenza dell’Unione europea. – 4.1. ... e come un autonomo diritto fondamentale. – 5. La nozione di dati personali nella giurisprudenza della Corte di giustizia. – 6. Il rapporto fra il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata e familiare nella giurisprudenza della Corte di giustizia. – 7. Il bilanciamento fra diritto alla protezione dei dati personali e altri diritti fondamentali garantiti dalla Carta nella giurisprudenza della Corte di giustizia. – 8. Alcune (brevi) riflessioni conclusive.

1. La protezione dei dati personali nel settore digitale tra nuove sfide e antichi dilemmi.

Nel settore digitale tutto scorre a un ritmo accelerato: un ritmo che si impone non solo a chi opera in questo campo, ma anche a chi è chiamato a stabilire le regole e a chi è tenuto ad assicurare che tali regole non soltanto siano rispettate, ma non finiscano per confliggere con principi giuridici che vengono enunciati e riconosciuti molto più lentamente e che, anche per questo motivo, sono ad esse gerarchicamente sovraordinati.

Una realtà complessa e sfaccettata con cui anche la Corte di giustizia si è dovuta misurare, e lo ha fatto con non poca fatica per la complessità e la delicatezza dei profili che entrano in gioco, spesso rappresentativi di interessi diversi, talora persino contrapposti, ma ugualmente meritevoli di tutela.

I dati personali rappresentano, invero, una componente essenziale dell’identità di ciascun individuo che va preservata con ogni mezzo, ma, occorre aggiungere, entro

¹ Associato di diritto dell’Unione europea nell’Università degli Studi di Milano. Relazione tenuta al I convegno annuale dell’Associazione italiana studiosi di diritto dell’Unione europea (AISDUE), Roma, 26-27 ottobre 2018.

alcuni precisi confini, così che l'interesse privato e l'interesse pubblico possano pacificamente convivere. Se, infatti, la protezione dei dati personali è una dimensione del diritto alla vita privata, parimenti non si può non tenere conto che le normative in tema di dati personali perseguono alcune finalità divergenti, a volte persino opposte, alla tutela di questo diritto che sarà qualificato nel tempo come fondamentale anche nell'ordinamento dell'Unione europea.

Di qui, la difficoltà nella delimitazione degli ambiti concettuali, ma anche applicativi, della disciplina di riferimento proprio in ragione della eterogeneità dei fini perseguiti che si traduce in una progressiva tensione fra l'esigenza di tutelare il privato cui si riferiscono i dati trattati e quella di garantire la circolazione delle informazioni per finalità sociali, commerciali e di pubblica sicurezza². Una tensione fra esigenze contrapposte sovente risolta dalla Corte, nel suo ruolo di "guardiana costituzionale" dell'ordinamento dell'Unione, a favore della centralità del diritto alla protezione dei dati personali, sia pure in presenza di istanze securitarie³⁴, a seguito di un attento bilanciamento tra diritti fondamentali differenti in relazione al loro contenuto essenziale

2 Sul tema, cfr., fra gli altri, C. MAGNUSSON SJÖBERG, *Threats to personal data security: how does the EU protect its citizens?*, *The European Union*, Cheltenham, 2018, p. 163; F. M.-P. GRANGER, K. IRION, *The right to protection of personal data: the new posterchild of European Union citizenship?*, *Civil rights and EU citizenship*, 2018, p. 279; L. POTVIN-SOLIS, *Objectif de sécurité et protection des données personnelles: projection dans l'ordre international d'un système constitutionnel propre à l'Union européenne*, (a cura di) E. NEFRAMI, M. GATTI, *Constitutional issues of EU external relations law*, Buch, Wissenschaft, 2018, p. 343; M. PUGLIA, *La protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'UE*, in (a cura di) AA.VV., *Liber amicorum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Torino, 2018, p. 788; F. BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, *Il diritto dell'Unione europea*, 1 (2015), p. 25; M. DE SALVIA, *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida*, in (a cura di) M. FUMAGALLI MERAVIGLIA, *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, Napoli, 2015, p. 11; O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Il diritto dell'informazione e dell'informatica*, 2015, p. 741; O. POLLICINO, *Diritto all'oblio e conservazione di dati: la Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giurisprudenza costituzionale*, 2014, p. 2949; O. POLLICINO, M. BASSINI, *Reconciling right to be forgotten and freedom of information in the digital age: past and future of personal data protection in the EU*, in *Diritto pubblico comparato ed europeo*, 2014, p. 640; G. GONZÁLEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU Law*, Cham, 2014, p. 274; H.R. KRANENBORG, *Article 8, Protection of personal data*, *The EU Charter of Fundamental Rights: a commentary*, in (eds.) S. PEERS, T. HERVEY, J. KENNER, A. WARD, *The EU Charter of Fundamental Rights: A Commentary*, 2014, p. 223; O. POLLICINO, M. BASSINI, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in *Il diritto dell'Unione europea*, 2014, p. 601; V. ZENO-ZENCOVICH, *La "comunione" di dati personali: un contributo al sistema dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, 2009, p. 5; F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in (a cura di) P. BILANCIA, M. D'AMICO, *La nuova Europa dopo il Trattato di Lisbona*, Milano, 2009, p. 83.

3 M. CARTABIA, *Convergenze e divergenze nell'interpretazione delle clausole finali della carta dei diritti fondamentali dell'Unione europea*, in *Rivista Associazione Italiana Costituzionalisti*, 2018, p. 2.

e alla necessità e proporzionalità delle misure adottate dall'Unione europea e dagli Stati membri.

Un compito di estrema complessità quello che la Corte è chiamata a svolgere, anche perché l'evoluzione tecnologica ha in pochi anni modificato punti di vista e prospettive. Ogni discorso di carattere sociologico su questo tema sarebbe qui del tutto inappropriato. Di certo, la Corte si è dovuta, nell'arco di pochi anni, confrontare con problemi che sono propri di un nuovo mondo, il mondo digitale, dove non esiste come nel mondo reale il passato⁵, perché ogni elemento è sempre presente, potendone conservare traccia, oppure semplicemente non esiste perché è stato eliminato.

2. Il nuovo quadro giuridico dell'Unione europea per la (progressiva) costruzione di un mercato unico digitale.

Oggi la Corte si trova a interpretare un quadro giuridico in materia profondamente innovato negli ultimi anni, anche se ancora incompleto e, invero, molto frammentato per la presenza di una pluralità di norme di cui appare, talora, difficile individuarne il campo di applicazione e, di conseguenza, garantirne un efficace coordinamento, anche per la quantità, qualità e diversità delle attività di trattamento dei dati personali.

Per questo motivo, la creazione di un mercato unico digitale, completo e coerente, rappresenta per l'Unione europea una delle principali sfide su cui concentrare i propri sforzi anche negli anni a venire, tenuto conto che ci troviamo in presenza di un settore non trascurabile neppure sul piano economico.

Fra gli atti adottati, volgendo lo sguardo alla sola categoria dei "dati personali", sulla cui definizione si tornerà più avanti, spicca per complessità e rilevanza il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che trae origine da una proposta della Commissione del 25 gennaio 2012 ed è divenuto direttamente e integralmente applicabile a partire dal 25 maggio 2018, dunque circa due anni dopo la sua entrata in vigore.

Il Regolamento (UE) n. 2016/679 (anche definito "Regolamento generale") si inserisce in un pacchetto di riforme che hanno profondamente mutato il quadro normativo europeo in tema di tutela dei dati personali⁶.

4 Cfr. F. FABBRINI, *Privacy and National Security in the Digital Age*, in *Tilburg Law Review, Journal of International and European Law*, 2015, p. 8 e D. J. SOLOVE, *Nothing to Hide – the False Tradeoff between Privacy and Security*, New Haven, 2011, spec. p. 24 e ss.

5 Cfr. V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Medialaws*, 2/2018, p. 32

6 Infatti, si ricorda che, insieme al Regolamento generale, sono entrate in vigore due direttive: la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la decisione quadro 2008/977/GAI del Consiglio e la direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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, il cui termine di recepimento negli ordinamenti nazionali era, rispettivamente, il 6 e il 25 maggio di quest'anno. La Commissione ha previsto anche l'adozione di un Regolamento in materia di *e-privacy* che andrà a sostituire l'attuale direttiva 2002/58/CE (in

Questo nuovo quadro giuridico di cui si sta dotando l'Unione europea trae ispirazione dal “Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini”⁷, in cui il Consiglio europeo ha invitato la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione in materia di protezione dei dati e a presentare, se quest'ultima lo avesse ritenuto necessario, iniziative a carattere legislativo o anche prive di tale natura. Nella sua risoluzione sul programma di Stoccolma, il Parlamento europeo ha accolto con favore la proposta relativa ad un quadro giuridico completo in materia di protezione dei dati nell'UE, mentre la Commissione, nel piano d'azione per l'attuazione di tale programma, ha sottolineato la necessità di assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee.

In una successiva comunicazione del 2010, dal titolo “Un approccio globale alla protezione dei dati personali nell'Unione europea”, la Commissione ha sostenuto che l'Unione europea avesse bisogno di una politica più completa e coerente in tema di protezione dei dati personali⁸.

La *ratio* di una tale riforma organica è da rinvenirsi nella necessità di introdurre specifiche regole in grado di rispondere alle nuove sfide che la tecnologia e il suo evolvere pongono rispetto al diritto alla tutela dei dati personali. Si avvertiva già allora, dunque, l'esigenza di adeguare l'impianto normativo al nuovo contesto tecnologico, al fine di instaurare un clima di fiducia negli ambienti *on line* e permettere al tempo stesso un continuo sviluppo economico⁹, fondato su applicazioni tecniche innovative.

GUUE L 201 del 31 luglio 2002, p. 37) con l'obiettivo di estendere, in quanto *lex specialis*, l'ambito di applicazione della disciplina sulla tutela dei dati personali anche ai trattamenti legati allo scambio di e-mail e di messaggi, comunicazioni via *social network* e a tutto quanto rientri nella definizione di comunicazione elettronica. La proposta di regolamento è attualmente in discussione al Consiglio. Infine, non va dimenticato che il diritto alla protezione dei dati personali si applica anche al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione. La disciplina è oggi contenuta nel Regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il Regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (in *GUUE* L 295 del 21 novembre 2018, p. 39). Il Regolamento (UE) n. 2018/1725 abroga e sostituisce il Regolamento (CE) n. 45/2001 – pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali – che è stato adottato nel 2001 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali in tutta l'Unione. Il nuovo regolamento ha lo scopo di adeguare le disposizioni contenute nel Regolamento (CE) n. 45/2001 ai principi e alle norme stabiliti nel Regolamento (UE) n. 2016/679, così da fornire un quadro di protezione dei dati solido e coerente nell'Unione e consentire di applicare contemporaneamente entrambi gli strumenti giuridici. L'allineamento, per quanto possibile, delle norme sulla protezione dei dati per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione a quelle adottate per il settore pubblico degli Stati membri è, insomma, necessario al fine di garantire un approccio coerente in materia di protezione dei dati personali in tutta l'Unione.

⁷ In *GUUE* L 115 del 4 maggio 2010, p. 1.

⁸ COM(2010) 609 def.

⁹ Cfr. la proposta della Commissione (COM(2012) 11 def.), a partire dalla quale è stato adottato il Regolamento (UE) n. 679/2016, dove, al punto 1, l'istituzione UE nell'illustrare il contesto della Proposta afferma che gli «incalzanti sviluppi tecnologici hanno allontanato le

3. L'evoluzione della giurisprudenza della Corte di giustizia in tema di protezione dei dati personali.

Il nuovo impianto normativo, così adottato, codifica alcune pronunce della Corte di giustizia in merito all'applicazione, anche in un contesto digitale, delle regole sulla *privacy*.

L'*acquis communautaire* in materia di protezione dei dati personali ha, infatti, visto quale fondamentale attore la Corte di giustizia la quale, ancora prima dell'entrata in vigore della direttiva 95/46/CE¹⁰ che il Regolamento (UE) n. 2016/679 sostituisce, ha permesso di edificare in via pretoria un diritto alla protezione dei dati personali tale da garantire una tutela elevata e il più possibile adeguata all'evoluzione tecnologica, anche quando la stessa direttiva 95/46/CE si è rivelata inadatta o incompleta.

Grazie a questa giurisprudenza evolutiva in materia di protezione dei dati personali, anche a livello di Unione europea, la tutela della *privacy* ha assunto nel tempo connotazioni diverse, passando dall'essere considerata quale mera eccezione alle libertà economiche sancite dai Trattati, per giungere oggi, ben prima dell'applicazione del Regolamento generale, a una configurazione orientata sui diritti fondamentali.

Ed è proprio su questo processo evolutivo, tendente a una progressiva costituzionalizzazione¹¹ del diritto alla protezione dei dati personali, ora opportuno soffermarsi anche per evidenziarne alcune criticità.

3.1. Il tenue legame tra la protezione dei dati personali e le libertà fondamentali sancite dai Trattati.

Volendo ripercorrere, seppure in modo non certamente esaustivo, la giurisprudenza comunitaria prima e dell'Unione poi sul trattamento dei dati personali, un ideale punto di partenza può essere rappresentato dalla sentenza *Stauder*¹² del 1969 che, come è noto, rappresenta una delle prime pronunce nelle quali la Corte si è fatta carico del compito di tutelare, in un contesto di primordiale integrazione politica degli ordinamenti nazionali, i diritti fondamentali della persona, in quanto parte dei principi generali del diritto, sia pure nei limiti della loro compatibilità con la struttura e le finalità della allora Comunità economica europea¹³. Già in questa risalente pronuncia, che anticipa l'ampia e

frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso: la tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano».

¹⁰ In *GUCE* L 281 del 23 novembre 1995, p. 31.

¹¹ In questi termini si esprime Oreste Pollicino in diversi suoi scritti di cui si dà parzialmente conto in questo contributo. Cfr., inoltre, G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, p. 9 e P. DE HERT, S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action*, in (eds.) S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT, *Reinventing Data Protection?*, Cham, 2009, p. 3.

¹² Sentenza del 12 novembre 1969, *Stauder*, 29/69, EU:C:1969:57.

¹³ Cfr. F. BALDUCCI ROMANO, *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia*, in *Rivista italiana di diritto pubblico comunitario*, 2015,

complessa giurisprudenza della Corte sul bilanciamento fra diritti fondamentali differenti, di cui si dirà in seguito, emerge l'obbligo per gli Stati membri di individuare, tra le possibili misure in grado di conseguire l'obiettivo prefissato, quelle meno pregiudizievoli dei diritti della persona, incluso il diritto alla riservatezza. I diritti fondamentali assurgono, dunque, a parametro di legittimità dei comportamenti degli Stati membri in attuazione del diritto comunitario e in questo quadro prende forma il diritto alla protezione dei dati personali quando il loro utilizzo si riverbera e interferisce sulla vita privata dell'individuo.

Nondimeno, la tutela dei dati personali appare, attraverso una possibile lettura di questa pronuncia, indissolubilmente connessa alle misure adottate per la realizzazione del mercato interno.

Di qui sono sorti dubbi sull'ambito di applicazione della prima normativa comunitaria in materia di protezione dei dati personali, la direttiva 95/46/CE, nella misura in cui il suo articolo 3, ma pressoché identica formulazione la ritroviamo anche nel Regolamento (UE) n. 679/2017 all'articolo 2, par. 2, lett. a), afferma che le sue disposizioni non coprono i trattamenti di dati personali effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, oggi dell'Unione europea.

Secondo una prima interpretazione, più restrittiva e, per un verso, più rigorosa nel leggere la norma, l'ambito di applicazione della direttiva andava limitato a quelle situazioni che avessero presentato un nesso sufficiente con l'esercizio delle libertà fondamentali stabilite dall'allora Trattato CE. Un'interpretazione ortodossa finalizzata ad affermare un legame indissolubile e simbiotico fra l'obiettivo di favorire la libera circolazione dei dati (anche) personali e, quello, al contempo, di salvaguardare i diritti fondamentali coinvolti nel loro utilizzo con la conseguenza di escludere l'applicazione del diritto alla protezione dei dati personali ai trattamenti effettuati per l'esercizio di attività di rilevanza puramente interna.

In linea con questa interpretazione, l'avvocato generale Tizzano, nelle conclusioni rese nella causa *ÖRF*¹⁴, aveva escluso l'applicazione della direttiva 95/46/CE poiché, in quel caso, i trattamenti dei dati personali erano inerenti l'esercizio di un'attività pubblica di controllo contabile non rientrante nel campo di intervento del diritto comunitario. Riprendendo quanto già affermato nelle sue conclusioni rese nella causa *Lindqvist*¹⁵, a parere dell'avvocato generale Tizzano il legislatore, nel perseguire un livello di tutela "equivalente in tutti gli Stati membri", ha sì tenuto conto dell'esigenza di salvaguardare "i diritti fondamentali della persona", ma solo al fine di realizzare l'obiettivo principale della direttiva, che si ricorda essere stata adottata sulla base dell'art. 100 A del Trattato CEE (poi divenuto art. 95 del TCE e oggi art. 114 del TFUE), ossia "favorire la libera circolazione dei dati personali, in quanto ritenuta «fondamentale per il mercato interno»"¹⁶. Perché, aggiunge l'avvocato generale Tizzano, «[l]a salvaguardia dei diritti fondamentali rappresenta [...] un importante valore ed

p. 1619 e P. OLIVER, *The protection of privacy in the economic sphere before the European Court of Justice*, in *Common Market Law Review*, 2009, p. 113.

14 Conclusioni dell'Avvocato generale Tizzano del 14 novembre 2002 nella causa *ÖRF*, C-465/00, EU:C:2002:662

15 Conclusioni dell'Avvocato generale Tizzano del 19 settembre 2002 nella causa *Lindqvist*, C-101/01, EU:C:2002:513.

16 Cfr. le conclusioni dell'Avvocato generale Tizzano del 14 novembre 2002, cit., punto 53.

un'esigenza di cui il legislatore comunitario ha tenuto conto nel delineare la disciplina armonizzata necessaria per l'instaurazione ed il funzionamento del mercato interno, ma non un autonomo obiettivo della direttiva. Diversamente, si dovrebbe ritenere che la direttiva intenda tutelare gli individui rispetto al trattamento dei dati personali anche a prescindere dall'obiettivo di favorire la libera circolazione di tali dati, con l'incongrua conseguenza di far rientrare nel suo campo di applicazione anche trattamenti effettuati per l'esercizio di attività che non presentino alcun rapporto con l'instaurazione ed il funzionamento del mercato interno».

Di diverso e contrario avviso la Corte¹⁷ che, discostandosi dalle conclusioni dell'avvocato generale Tizzano, ha escluso che l'applicazione della direttiva 95/46 potesse dipendere dall'esistenza di un nesso fra le situazioni concrete prese in considerazione e l'esercizio delle libertà fondamentali garantite dal Trattato (CEE). Infatti, a giudizio della Corte, «un'interpretazione in senso contrario rischierebbe di rendere particolarmente incerti ed aleatori i limiti del campo di applicazione della detta direttiva, il che sarebbe contrario al suo obiettivo essenziale, che è quello di ravvicinare le disposizioni legislative, regolamentari, ed amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali».

Per la verità, a questa soluzione si potrebbe giungere limitandosi a prendere in esame il titolo della direttiva 95/46/CE (e, in seguito, del Regolamento (UE) n. 679/2017), il quale, nel perseguire l'obiettivo di tutelare l'individuo, tiene distinto il momento in cui i dati personali vengono trattati da quello in cui gli stessi circolano, quasi a dire che quest'ultimo rappresenta un evento ulteriore ed eventuale e non una condizione indefettibile per l'applicazione della disciplina. Oppure, rileggendo, sotto una diversa angolazione, l'art. 3, par. 2 della direttiva che va a specificare, almeno a titolo esemplificativo, i casi in cui le disposizioni della direttiva non si applicano, venendo in rilievo trattamenti di dati personali effettuati per l'esercizio di attività non coperte dal diritto comunitario. Rimane, certo, un'ambiguità di fondo della norma, peraltro non fugata, ma anzi, per un verso, acuita dalle analoghe disposizioni del Regolamento (UE) n. 2016/679 dal quale sarebbe stato lecito attendersi una maggiore precisione linguistica. Il suo art. 2, invece, se possibile, genera ancora più confusione andando a elencare, in modo tassativo, i casi in cui il Regolamento non si applica, ossia in relazione a trattamenti di dati personali *a*) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; *b*) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; *c*) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; *d*) 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.

Non sorprende certamente che sia escluso dal campo di applicazione del nuovo regolamento (così come lo era anche in relazione alla direttiva 95/46/CE) il trattamento effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale e domestico (lett. *c*), che rappresenta di per sé una garanzia per l'individuo o il trattamento dei dati nel quadro della PESC (lett. *b*) o della cooperazione di polizia o giudiziaria in materia penale (lett. *d*), essendo quest'ultimo disciplinato dalla direttiva 2016/680/UE.

17 Sentenza del 20 marzo 2003, *ÖRF*, C-465/00, EU:C:2003:294, punto 42.

Qualche problema interpretativo si pone, invece, rispetto a quanto previsto dalla lett. a), ovvero la non applicazione del Regolamento per i trattamenti di dati personali effettuati per attività che non rientrino nell'ambito di applicazione del diritto dell'Unione, laddove il legislatore sembra avere individuato con tale lettera una categoria residuale, essendo stata superata, con il Trattato di Lisbona, la dicotomia fra diritto comunitario e diritto UE.

Di questa disposizione si possono, dunque, dare due letture diverse. La prima richiama la distinzione fra fattispecie puramente interne e fattispecie in cui trova attuazione il diritto dell'Unione¹⁸.

Una tale interpretazione costringerebbe l'operatore e l'interprete a complesse analisi e valutazioni in considerazione del contesto in cui operano, privando così del suo effetto utile la disciplina introdotta dal legislatore.

La seconda lettura, l'unica che pare corretta, porta, invece, a ritenere la disciplina contenuta nel regolamento oggi e nella direttiva ieri comunque applicabile in tutti i casi in cui vengono in rilievo dati personali, a prescindere dalla cittadinanza dell'interessato, essendo l'espressione "ambito di applicazione del diritto dell'Unione" da intendersi come comprensiva di tutte quelle misure nazionali che presentino un collegamento anche solo funzionale con una disposizione del diritto UE, salvo si sia in presenza di attività che effettivamente esulino da tale contesto, quali, come ci ricorda il *considerando* sedicesimo del Regolamento (UE) n. 2016/679/UE, quelle che riguardano la sicurezza nazionale. Anche se, per la verità, a questo proposito, non va dimenticato che i concetti di "sicurezza nazionale", "sicurezza interna dell'UE" e "sicurezza internazionale" tendono spesso a sovrapporsi, essendo obiettivi che devono essere tutti necessariamente perseguiti nel rispetto dei valori e dei principi sanciti dall'art. 2 TUE e dalla stessa Carta dei diritti fondamentali.

L'applicazione della disciplina dell'Unione sul trattamento dei dati personali è, d'altra parte, incredibilmente pervasiva, conoscendo pochi limiti, quelli anzidetti, che, peraltro, finiscono per essere interpretati dalla Corte di giustizia in modo molto restrittivo. Ad esempio, il giudice dell'Unione ha recentemente chiarito che non rientra tra le attività esclusivamente personali o domestiche, non coperte dal nuovo regolamento 2016/679/UE, quella di predicazione porta a porta dei testimoni di Geova¹⁹. Per la Corte, il fatto che l'attività di predicazione porta a porta sia tutelata dal diritto fondamentale alla libertà di coscienza e di religione, sancito all'articolo 10, paragrafo 1, della Carta dei diritti fondamentali dell'UE, non ha l'effetto di conferirle un carattere esclusivamente personale e domestico, riferendosi i termini «personale o domestico», utilizzati dalla normativa, all'attività della persona che effettua il trattamento dei dati personali e non alla persona i cui dati sono trattati²⁰.

4. La protezione dei dati personali come nuova competenza dell'Unione europea.

A ulteriore conferma di quanto si è detto sopra con riguardo all'ambito di applicazione del Regolamento (UE) 2016/679/UE, va ricordato che esso poggia su una

¹⁸ Per la definizione di "situazioni puramente interne" si veda la sentenza del 6 dicembre 2012, *O. e S.*, C-356/11 e C-357/11, EU:C:2012:776, punto 43. Cfr. R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione europea*, Milano, 2017, p. 386.

¹⁹ Sentenza del 10 luglio 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551.

²⁰ Cfr. anche la sentenza dell'11 dicembre 2014, *Ryneš*, C-212/13, EU:C:2014:2428, spec. punti 31 e 33.

base giuridica diversa da quella della direttiva 95/46/CE: non più l'art. 100 A del TCE (oggi art. 114 del TFUE), ma l'art. 16 del TFUE²¹, norma che, introdotta con il Trattato di Lisbona, sostituisce l'art. 286 del TCE.

Fra le due disposizioni, appunto l'art. 286 del TCE e l'art. 16 del TFUE, le differenze sono profonde al di là del loro tenore letterale.

L'art. 16 del TFUE ha, invero, una portata assai più ampia di quello della precedente norma, che si limitava a prevedere l'applicabilità degli atti comunitari relativi al diritto alla protezione dei dati personali anche ai trattamenti di dati effettuati da istituzioni e organismi della Comunità²². La nuova disposizione stabilisce direttamente, e non tramite un rimando agli atti legislativi e non eventualmente adottati, che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, con l'effetto di introdurre una nuova autonoma competenza dell'Unione che consente di superare in modo definitivo i dubbi sull'ambito di applicazione della disciplina derivata.

4.1. ... e come un autonomo diritto fondamentale.

Al di là delle considerazioni che precedono, è innegabile che con il tempo la protezione dei dati personali abbia progressivamente allentato ogni legame, inteso come vincolo o elemento di costrizione, con le libertà sancite dai Trattati, finendo per ancorarsi al diritto dell'Unione europea sotto forma di diritto fondamentale divenuto, in seguito, autonomo, almeno sul piano formale.

A questa trasformazione concettuale, frutto di un approccio sostanzialistico, ha, indubbiamente, contribuito una giurisprudenza della Corte di giustizia fortemente influenzata dalle pronunce della Corte di Strasburgo sull'art. 8 della CEDU²³²⁴ e sulla Convenzione n. 108 del 1981²⁵, anch'essa oggetto di un processo di revisione concluso il 18 maggio 2018 con l'adozione da parte del Comitato dei Ministri di un Protocollo di

21 La base giuridica per le norme sul trattamento dei dati personali nel diverso settore della PESC è l'art. 39 del TUE che, derogando in deroga al paragrafo 2 dell'art. 16 del TFUE, affida al solo Consiglio il compito di adottare mediante decisione le norme ad esso relative.

22 L'art. 16 TFUE (ex art. 286 TCE) attribuisce al legislatore europeo la facoltà di adottare, mediante procedura legislativa ordinaria, una normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla loro libera circolazione 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, affidando il rispetto di tali norme ad autorità indipendenti. Cfr. F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, cit. e il commento di B. CORTESE, *Art. 16*, in (a cura di) A. TIZZANO, *Trattati dell'Unione europea*, Milano, 2014, p. 444.

23 Cfr., in particolare, la sentenza del 4 dicembre 2008, *S. e Marper c. Regno Unito*, ricorsi 30562/04 e 30566/04 § 103). In argomento, cfr. M. DE SALVIA, *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida*, in (a cura di) M. FUMAGALLI MERAVIGLIA, *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, cit.

24 Cfr. O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdUE*, (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, 2017, p. 132; G. MARTINICO, *Commento all'art. 7 CdUE*, *ibidem*, p. 114 e J. HERVEG, J.-M. VAN GYSEGHEM, *La protection des données à caractère personnel en droit européen*, in *Journal européen des droits de l'homme*, 2018, p. 33.

ammodernamento²⁶ al fine di garantire il coordinamento e la compatibilità con gli *standard* della disciplina dell'UE.

Per mezzo di tale convenzione, si è proceduto a codificare la giurisprudenza della Corte EDU con la quale il diritto alla protezione dei dati personali era stato incluso nel “diritto al rispetto della vita privata”²⁷. La Convenzione n. 108 del 1981, dunque, in epoca antecedente alla prima proclamazione della Carta, ponendosi a complemento dell'art. 8 della CEDU, ha consentito di fare elevare la tutela dei dati personali a diritto fondamentale.

Lo stesso risultato è stato conseguito a livello di Unione europea attraverso, appunto, la Carta dei diritti fondamentali la quale riconosce, all'art. 8, la protezione dei dati personali come diritto autonomo.

In questo senso, l'articolo 8 della Carta, come osservato con particolare acume²⁸, rappresenta il punto di arrivo di un processo di codificazione e costituzionalizzazione del diritto europeo alla *privacy* e al tempo stesso oggi costituisce la pietra angolare del nuovo impianto normativo di cui l'Unione si è dotata²⁹.

Con l'art. 8 della Carta tale diritto, da una dimensione di carattere essenzialmente negativo (codificata, oltre che dalla CEDU all'art. 8, dall'art. 7 della stessa Carta, nonché espressione del c.d. “*right to be alone*” poiché, come affermato ancora nel 1952 da un giudice della Corte Suprema degli Stati Uniti, «il diritto di essere lasciati in pace è

25 Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108, firmata a Strasburgo il 28 gennaio 1981 ed entrata in vigore il 1° ottobre 1985. Cfr., sul tema, M. FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016, p. 12 e M.E. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e Diritto internazionale*, 2011, p. 449. Al fine di fornire un ulteriore strumento di supporto per gli Stati parte nell'applicazione della Convenzione 108, il *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data* ha adottato il 23 gennaio 2017 le *Linee guida sulla protezione degli individui relative al trattamento di dati personali in un mondo di Big Data*, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>.

26 Il testo del Protocollo è consultabile *online* all'indirizzo <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac918>.

27 La protezione dei dati personali è considerato dalla Corte EDU di fondamentale importanza per il godimento del diritto al rispetto della vita privata e familiare, garantito dall'articolo 8 della Convenzione (cfr., *inter alia*, la sentenza del 27 giugno 2017, *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, ricorso 931/13 § 133 e del 4 maggio 2000, *Rotaru c. Romania* [GC], ricorso 28341/95, § 46).

28 V. O. POLLICINO, M. BASSINI, *Commento all' art. 8 CdfUE*, in (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, cit., p. 135.

29 Le Spiegazioni della Carta fanno espressamente menzione ai riferimenti normativi che hanno contribuito al processo di codificazione del diritto alla *privacy* nell'ordinamento dell'Unione europea: (i) l'art. 16 TFUE; (ii) la direttiva 95/46/CE (oggi il Regolamento (UE) n. 679/2017); (iii) la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981; (iv) il Regolamento (CE) n. 45/2001 (oggi il Regolamento (UE) 2018/1725); (v) l'art. 8 della CEDU.

di fatto l'inizio di ogni libertà»³⁰), approda a una dimensione di carattere positivo, che si traduce nella tutela dei dati personali mediante la creazione di un insieme di regole e principi³¹. Questa norma, dunque, consente di costruire un sistema di controlli e contrappesi che va oltre il concetto di consenso e che permette il trattamento lecito dei dati, talvolta anche prescindendo da un'autorizzazione esplicita dell'interessato. I paragrafi 2 e 3 dell'articolo 8 della Carta precisano che 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, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e, infine, che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente³². Tali prescrizioni, mutate dagli articoli 6, 7, 12, 14 e 28 della direttiva 95/46/CE, sono parimenti codificate nel nuovo Regolamento (UE) n. 679/2016.

L'art. 8, a partire dall'entrata in vigore del Trattato di Lisbona, ma, in verità, già dalla prima proclamazione della Carta, diviene per la Corte di giustizia il vero parametro di legittimità degli atti adottati dall'Unione e dagli Stati membri, essendo oggi, come si è detto, da respingere, anche per la presenza dell'art. 16 del TFUE come base giuridica degli atti di diritto derivato adottati in materia e, dunque, espressione di una nuova competenza dell'Unione europea, l'idea che la protezione dei dati personali da parte del diritto UE sussista solo in presenza di un legame con le libertà fondamentali sancite dai Trattati. Anzi, l'art. 16 del TFUE, avendo introdotto nell'ordinamento giuridico dell'Unione europea una nuova e generale competenza, consente, nel rispetto dell'articolo 51 della Carta, l'applicazione dell'art. 8 della Carta ogni qual volta vengano in rilievo i dati personali, con la sola eccezione dei casi in cui si esuli dal campo di applicazione del diritto UE ovvero si versi in situazioni che ricadono sotto la competenza esclusiva degli Stati membri.

Il Trattato di Lisbona, insomma, ha il pregio di avere creato una perfetta contiguità³³ fra la Carta e i Trattati, determinando una chiara ripartizione funzionale delle due norme evocate cosicché l'art. 16 del TFUE viene richiamato dal legislatore come base giuridica degli atti di rango secondario adottati in materia, mentre l'art. 8 della Carta, nella lettura che di tale norma dà la Corte, sovviene laddove quei medesimi atti o disposizioni di diritto interno comprimano le tutele di questo nuovo diritto fondamentale, con l'ulteriore conseguenza di rendere di fatto pacifica l'efficacia orizzontale dell'art. 8 per osmosi e, dunque, la sua applicazione nelle controversie fra privati³⁴.

30 Cfr. il caso *Public Utilities Commission c. Pollak*, 343 U.S. 451, 467 (1952) e l'opinione del giudice William O. Douglas, dissenziente. Cfr. S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1980, p. 193. Gli autori affermano un diritto alla *privacy*, secondo un'accezione negativa, da intendersi quale *right to be alone* ossia il diritto al rispetto della vita privata e familiare, codificato nell'ordinamento europeo dall'art. 7 della Carta.

31 V. O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdfUE*, in (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, p. 136.

32 Sentenza del 9 marzo 2017, *Manni*, C-398/15, EU:C:2017:197.

33 Un doppio binario di tutela secondo F. BALDUCCI ROMANO, *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia*, cit., p. 1658.

34 Cfr. O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *Rivista diritto dei media*, 2018, p. 1. Sul tema, più in generale, dell'efficacia

Non è un caso che la Corte nelle proprie pronunce faccia sempre riferimento solo all'art. 8 della Carta. D'altra parte, tale norma ha, rispetto all'art. 16 del TFUE, un contenuto assai più ampio e preciso, stabilendo, al paragrafo 2, le condizioni essenziali perché i dati personali possano essere oggetto di trattamento, mentre con il paragrafo successivo, nell'affidare il rispetto delle regole al controllo di autorità indipendenti, il cui ruolo, essenziale per garantire lo stato di diritto, inteso come valore posto a fondamento dell'Unione, sarà progressivamente valorizzato dalla stessa Corte, funge da ideale cerniera tra altre disposizioni di rango primario: l'art. 47 della Carta e gli articoli 4, par. 3 e 19 del TUE.

5. La nozione di dati personali nella giurisprudenza della Corte di giustizia

Dal punto di vista sostanziale, come si è detto, l'art. 8 della Carta sancisce l'esistenza di un diritto nuovo, autonomo, ma, invero, questa autonomia tuttora fatica ad emergere nella giurisprudenza della Corte anche in quella più recente.

Ciò si deve alla difficoltà nel trovare una definizione univoca di dati personali e nel tagliare il cordone ombelicale che separa il diritto posto a loro protezione da quello parimenti tutelato dalla Carta e dalla CEDU, che ha lo scopo di assicurare il rispetto della vita privata e familiare.

Partendo dai profili definitivi, va detto che il confine che separa la categoria dei dati personali da quella dei dati non personali è labile e disegnato dal legislatore UE con un tratto ben poco marcato.

Secondo la Commissione³⁵, i dati non personali possono essere classificati in due modi diversi a seconda della loro origine: dati che fin dall'inizio non riguardano una persona fisica identificata o identificabile (l'esempio più comune sono i dati meteorologici) e dati inizialmente personali e solo successivamente resi privi di tale natura, a seguito di un processo di anonimizzazione, mediante la tecnica della "randomizzazione o della "generalizzazione"³⁶.

orizzontale dei diritti fondamentali, si rinvia anche a F. FERRARO, *Vecchi e nuovi problemi in tema di efficacia diretta orizzontale della Carta*, in *Federalismi.it*, 2019.; E. FRANTZIOU, *The Horizontal Effect of Fundamental Rights in the European Union*, Oxford, 2019; S. WALKILA, *Horizontal Effect of Fundamental Rights in EU Law*, Amsterdam, 2016; R. TINIÈRE, *L'invocabilité des principes de la Charte des droits fondamentaux dans les litiges horizontaux*, in *Revue des droits et libertés fondamentaux*, 2014, chronique n° 14; N. LAZZERINI, *(Some of) the fundamental rights granted by the Charter may be a source of obligations for private parties: AMS*, in *Common Market Law Review*, 2014, p. 907. D. LECZYKIEWICZ, *Horizontal Application of the Charter of Fundamental Rights*, in *European Law Review*, 2013, p. 479; K. LENAERTS, *Exploring the Limits of the EU Charter of Fundamental Rights*, in *European Constitutional Law Review*, 2012, p. 375; E. SPAVENTA, *The Horizontal Application of Fundamental Rights as General Principles of Union Law*, in (eds.) A. ARNULL, C. BARNARD, M. DOUGAN, E. SPAVENTA, *A Constitutional Order of States? Essays in Honour of Alan Dashwood*, Oxford, 2011, p. 199 e A. TIZZANO, *L'application de la Charte de droits fondamentaux dans les Etats membres à la lumière de son article 51, paragraphe 1*, in *Diritto dell'Unione europea*, 2014, p. 429.

³⁵ Comunicazione della Commissione al Parlamento europeo e al Consiglio del 25 settembre 2019, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250 def., paragrafo 2.1.

³⁶ La «randomizzazione» viene definita dal Gruppo di lavoro articolo 29 (WP29) come «una famiglia di tecniche che modifica la veridicità dei dati al fine di eliminare la forte

Insomma, la categoria, residuale, dei dati non personali viene definita con un'accezione negativa. In questo senso sono da leggersi gli articoli 2 e 3 del regolamento (UE) n. 2018/1807³⁷, che si limitano a definire dati non personali quelli che non rientrano nella definizione di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 2016/679 per il quale è, invece, da considerarsi come dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Anche questa nozione di dato personale, contenuta nel Regolamento (UE) n. 2016/679 e non dissimile da quella contenuta nella direttiva 95/46/CE, è stata prima edificata in via pretoria attraverso il contributo dato dal Gruppo di lavoro articolo 29 (*Working Party article 29* o WP29, in quanto previsto dall'art. 29 della direttiva europea 95/46/CE) che, con l'entrata in vigore del Regolamento (UE) n. 2016/679, è stato sostituito dall'European Data Protection Board, o Comitato europeo per la protezione dei dati. Ci si riferisce, in particolare, al Parere 4/2007 del 20 giugno 2007 - WP 136 sul concetto di dati personali. Ti sembra gatto

correlazione che esiste» tra questi e la persona. Essa rappresenta una tutela dai rischi di deduzione e può essere affiancata da altre tecniche per garantire l'anonimato con maggior precisione. Nella randomizzazione rientra ad esempio l'aggiunta del c.d. «rumore statistico». La «generalizzazione» rappresenta la seconda famiglia di tecniche di anonimizzazione e consiste nel «diluire gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza» (anziché riportare un dato relativo a un giorno specifico, lo generalizzo in un *range* di tempo maggiore, come un anno). Il Gruppo di Lavoro 29 colloca in questa famiglia l'«aggregazione» e il «k-anonimato». Esse mirano a non permettere l'identificazione attraverso il raggruppamento di dati concernenti una persona, con dati riguardanti un numero k di soggetti. Ciò avviene ad esempio mescolando casualmente le date di nascita di più individui in uno stesso elenco. Il problema dell'aggregazione e k-anonimato consiste però nella deduzione. In effetti, se i k individui appartengono a un gruppo e il gruppo è noto all'interprete, rimane semplice identificare la persona fisica. Gli errori comuni evidenziati nel WP216 sono: utilizzare pochi soggetti tra i quali mischiare i dati, perché si aumentano le possibilità di correlare fra loro i dati; raggruppare insieme persone in modo disomogeneo, senza per esempio mettere insieme informazioni tutte riguardanti la data di nascita ma alcune riguardanti il colore dei capelli, o l'indirizzo di casa, consentendo una maggior facilità di individuazione; trascurare alcuni quasi-identificatori che possano fungere da mezzi per la deduzione, cioè modi per individuare una persona in un gruppo. Il WP29, infatti, sottolinea in chiusura del documento WP216 «l'impossibilità di rinvenire tecniche che soddisfino con certezza i criteri per un'effettiva anonimizzazione» e la necessità di decidere caso per caso quale tecnica utilizzare, in base alle circostanze concrete.

³⁷ Regolamento (UE) n. 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*, cit., p. 59.

Dunque, sono quattro gli elementi chiave che caratterizzano la definizione di dati personali: a) una “qualsiasi informazione”; b) “riguardante”; c) una “persona fisica”³⁸; d) “identificata o identificabile”.

Poiché la nozione di dati non personali, contenuta nel regolamento (UE) 2018/1807, è una mera negazione di quella utilizzata per i dati personali, ne consegue che i dati non personali devono essere intesi come un’informazione non relativa a una persona fisica identificata o identificabile.

Un’informazione può “riguardare” una persona fisica identificata o identificabile se quest’ultima ne è l’oggetto oppure se è suscettibile di incidere sui suoi diritti. L’“identificabilità” del soggetto cui l’informazione si riferisce può essere “diretta” o “indiretta” tramite un metodo deduttivo; informazioni apparentemente frammentarie e prive di riferimenti diretti all’identità di una persona (il nome) costituiscono un dato personale se il titolare intende utilizzarle per identificare una determinata persona e possiede presumibilmente i mezzi per ricostruire tale identità.

Secondo la giurisprudenza della Corte, anche l’immagine di una persona registrata da una telecamera costituisce un dato personale se e in quanto essa consente di identificare la persona interessata³⁹.

Insomma, si tratta di una definizione molto ampia e dinamica che richiede una valutazione attenta caso per caso.

D’altra parte, la Corte nella sentenza *Nowak*⁴⁰ afferma che «l’uso dell’espressione «qualsiasi informazione» nell’ambito della definizione della nozione di «dati personali», di cui all’articolo 2, lettera a), della direttiva 95/46 riflette l’obiettivo del legislatore dell’Unione di attribuire un’accezione estesa a tale nozione, che non è limitata alle informazioni sensibili o di ordine privato, ma comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano «concernenti» la persona interessata»⁴¹. Inoltre, per la Corte «affinché un dato possa essere qualificato come «dato personale», non si richiede che tutte le informazioni che consentono di identificare la persona interessata siano in possesso di una sola persona»⁴².

In effetti, come sottolineato dalla Corte di giustizia nel caso *Breyer*, una persona può anche essere identificata mediante riferimenti incrociati di informazioni provenienti da responsabili del trattamento differenti. Se i dati non personali possono essere associati in qualche modo a una persona, devono essere considerati personali.

³⁸ La direttiva si riferisce a informazioni concernenti una persona fisica, ma, almeno in determinate circostanze, può essere rilevante anche il trattamento di dati relativi ai defunti. Della stessa tutela possono godere anche le persone giuridiche come ha chiarito la Corte europea di giustizia nella sentenza *Lindqvist* (del 6 novembre 2003, C-101/01, EU:C:2003:596), in base alla quale «nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/Ce a settori non compresi nell’ambito di applicazione di quest’ultima, purché non vi osti alcun altra disposizione del diritto comunitario» (punto 98).

³⁹ Sentenza dell’11 dicembre 2014, *Ryneš*, C-212/13, EU:C:2014:2428, punto 22.

⁴⁰ Sentenza del 20 dicembre 2017, *Nowak*, C-434/16, EU:C:2017:994.

⁴¹ *Ibidem*, punto 34

⁴² *Ibidem*, punto 31 in cui si richiama la sentenza del 19 ottobre 2016, *Breyer*, C-582/14, EU:C:2016:779, punto 43.

In questo contesto risiede l'importanza dell'anonimizzazione dei dati, che in astratto, e con i limiti sopra menzionati, consente di tramutare i dati personali in dati non personali.

6. Il rapporto fra il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata e familiare nella giurisprudenza della Corte di giustizia.

Se è talora difficile differenziare i dati personali dai dati non personali, lo è ancora di più ipotizzare un trattamento dei primi che non incida sulla sfera privata del singolo, intesa come il nocciolo duro della sua sfera personale. È, insomma, possibile ipotizzare una lesione del diritto alla protezione dei dati personali in mancanza di un pregiudizio per il singolo? La risposta a questo interrogativo è necessaria per capire il grado di autonomia di questo diritto da quello che sancisce il rispetto della vita privata e familiare.

Se le adiacenze tra i due diritti sono innegabili ed emergono con chiarezza anche nelle Spiegazioni contenute nella Carta⁴³, meno chiaro è il grado di separazione fra di essi⁴⁴.

Sul punto, la giurisprudenza della Corte di giustizia non è di particolare aiuto, venendo utilizzato nelle sue pronunce un approccio non uniforme e un linguaggio poco rigoroso.

Nella sentenza *Promusicae*⁴⁵, la Corte, ad esempio, afferma l'esistenza di un nuovo diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali "e, quindi, della vita privata"⁴⁶.

Tuttavia, osserva il Tribunale nella sentenza *Bavarian Lager*⁴⁷, "non tutti i dati personali sono per loro natura in grado di pregiudicare la vita privata della persona interessata". Dunque, il diritto fondamentale alla protezione dei dati personali avrebbe, stando a questa pronuncia della Corte, un perimetro di applicazione più ampio.

Questa asserzione della Corte non è del tutto convincente se si passa dall'astrazione del diritto a prevederne la protezione nel concreto.

Non a caso, la Corte è solita affermare nelle proprie pronunce che gli articoli 7 e 8 della Carta sono strettamente legati al punto da poter essere considerati come integranti un «diritto alla vita privata con riguardo al trattamento dei dati personali»⁴⁸.

A ben vedere, al di là delle categorie concettuali, è impervio individuare un diritto alla protezione dei dati personali completamente avulso dalla vita privata della persona cui appartengono. D'altra parte, come si è detto, il collegamento fra dato e vita privata costituisce l'elemento imprescindibile per ritenere che esso sia da considerarsi "personale".

⁴³ Come si è già detto, nella Spiegazione relativa all'articolo 8 della Carta, si precisa esso si fonda in particolare sull'articolo 8 della CEDU che sancisce il diritto alla vita privata.

⁴⁴ Cfr. J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, p. 222.

⁴⁵ Sentenza del 29 gennaio 2008, *Promusicae*, C-275/06, EU:C:2008:54.

⁴⁶ *Ibidem*, punto 63.

⁴⁷ Sentenza dell'8 novembre 2007, *Bavarian Lager*, T-194/04, EU:T:2007:334.

⁴⁸ Sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09, EU:C:2010:662, punto 52.

Parimenti, in caso di violazione dei principi posti alla base del diritto alla protezione dei dati personali, è difficile individuare rimedi (accesso ai dati, rettifica, cancellazione, anonimizzazione dei dati) che non siano volti a difendere la sfera privata e familiare.

Correttamente, la Corte ci ricorda che la tutela del diritto fondamentale al rispetto della vita privata implica, in particolare, che qualsiasi persona fisica possa assicurarsi che i dati personali che la riguardano siano esatti e che siano trattati in maniera lecita. È al fine di effettuare le necessarie verifiche che la persona interessata gode, ad esempio, di un diritto di accesso ai dati che la riguardano e che sono oggetto di trattamento. Tale diritto di accesso è necessario proprio per consentire alla persona interessata di ottenere, se del caso, da parte del responsabile del trattamento la rettifica, la cancellazione o il congelamento di tali dati⁴⁹.

Si finisce così per preferire la giurisprudenza della Corte di Strasburgo che, richiamando la Convenzione 108 del 1981, tende a utilizzare i principi generali sul trattamento dei dati, per dare contenuto al diritto alla vita privata. Il trattamento dei dati personali non sempre interferisce con la vita privata della persona, ma la protezione di quegli stessi dati avviene in funzione di una siffatta interferenza.

Non del tutto convincente è anche la tesi dell'Avvocato generale Villalón il quale, nel tentativo di affermare l'autonomia concettuale dei due diritti, sostiene, nelle proprie conclusioni presentate nella causa *Digital Rights Ireland*, che il legame che li unisce dipende essenzialmente dalla natura dei dati considerati⁵⁰.

Secondo il suo, sottile e raffinato, ragionamento, esistono dati che sono, in un certo qual modo, più che personali. Per questi dati, le problematiche iniziano, per così dire, già «a monte», per il solo fatto che circostanze che attengono alla sfera più intima di una persona abbiano potuto cristallizzarsi in forma di dati, ossia in una forma che può essere assoggettata a un trattamento e dunque per essi sarebbe giustificato un richiamo anche all'art. 7 della Carta.

Si tratterebbe, dunque, di un diverso posizionamento dei due diritti fondamentali. Dunque, gli articoli 7 e 8 andrebbero entrambi richiamati per valutare, sotto il profilo della legittimità, il momento in cui l'informazione personale si trasforma in dato, laddove tale procedimento sia contestato dal soggetto cui l'informazione prima e il dato poi si riferiscono. Risulterebbe sufficiente il rinvio all'art. 8 della Carta in caso il titolare del dato personale ne contesti le modalità con cui esso viene conservato, trattato o trasferito oppure lamenti una violazione o una compressione del diritto, in virtù di tale norma, ad avvalersi di una serie di rimedi per porre fine ad un comportamento non conforme da parte del titolare del trattamento.

Come si è detto, questa elaborazione non pare sempre idonea a individuare i casi in cui sarebbe sufficiente il richiamo al solo articolo 8 della Carta, consentendo di addivenire a una separazione funzionale dei due diritti.

Piuttosto, per questa via, si potrebbe giungere a un bilanciamento più equilibrato con altri diritti parimenti previsti dalla Carta con i quali si viene sovente a creare una naturale tensione⁵¹.

49 Sentenza del 17 luglio 2014, YS e a., C 141/12 e C 372/12, in EU:C:2014:2081, punto 44 e giurisprudenza ivi citata.

50 Cfr. le conclusioni dell'Avvocato generale Villalón presentate il 12 dicembre 2013 nella causa *Digital Rights Ireland*, C-293/12, EU:C:2013:845, punto 65.

51 Sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, cit., punto 52.

7. *Il bilanciamento fra diritto alla protezione dei dati personali e altri diritti fondamentali garantiti dalla Carta nella giurisprudenza della Corte di giustizia.*

Anche il diritto alla protezione dei dati personali, come ricorda la Corte in diverse pronunce, non costituisce una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale.

Il riferimento è all'art. 52, par. 1 della Carta secondo cui «[e]ventuali limitazioni all'esercizio dei diritti e delle libertà [...] devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui»⁵².

Nel dare applicazione a questa norma, la Corte accerta, in primo luogo, se la limitazione del diritto alla protezione dei dati personali sia prevista dalla legge che, secondo la dottrina della c.d. "qualità della legge" elaborata dalla Corte EDU, deve essere sufficientemente chiara⁵³ e prevedibile⁵⁴ per quanto riguarda il significato e la natura delle misure applicabili, dovendo consentire al cittadino di immaginare le conseguenze del proprio comportamento⁵⁵. In secondo luogo, occorre valutare se la norma limitativa del diritto persegua una finalità legittima che, tuttavia, non va presa in considerazione in astratto (ad esempio, la tutela dell'ordine pubblico, la lotta alla criminalità, la prevenzione dei reati), determinando, diversamente, il rischio di una compressione o limitazione del diritto che viene in rilievo⁵⁶.

In terzo luogo, si deve verificare se la limitazione apportata al diritto non ne pregiudichi il contenuto essenziale⁵⁷, sia idonea a realizzare l'obiettivo perseguito e non

52 Cfr. F. FERRARO, N. LAZZERINI, *Commento all'art. 52 CdfUE*, (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, cit., p. 1061.

53 Sentenza del 3 luglio 2007, *Tan c. Turchia*, ricorso 9460/03.

54 Sentenza del 24 aprile 1990, *Kruslin c. Francia*, ric. 11801/85, e del 25 settembre 2006, *Coban c. Spagna*, ric. 17060/02.

55 Cfr. le conclusioni dell'Avvocato generale Villalón presentate il 14 aprile 2011 nella causa *Scarlet*, C-70/10, EU:C:2011:255, punto 100. Cfr. L. MILANO, *Contrôle de constitutionnalité et qualité de la loi*, in *Revue du Droit public*, 2006, p. 637; P. RRAPI, *La mauvaise qualité de la loi: Vagueness Doctrine at the French Constitutional Council*, in *Hastings Constitutional Law Quarterly*, 2010, p. 243 e H. MOYSAN, *L'accessibilité et l'intelligibilité de la loi. Des objectifs à l'épreuve de la pratique normative*, in *AJDA*, 2001, p. 428.

56 Sentenza del 16 dicembre 2008, *Huber*, C-524/06, EU:C:2008:724, punto 69 e ss.

57 Sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, EU:C:2014:238, punto 39. Per un commento, cfr. L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giurisprudenza italiana*, 2014, p. 1850; O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, 3/2014; M. P. GRANGER, K. IRON, *The Court of Justice and the Data retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching lesson in privacy and data protection*, in *European Law Review*, 2014, p. 835 e O. LYNSKEY, *The Data retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2016, p. 1789.

vada oltre quanto necessario per conseguirlo e, dunque, non violi i principi di proporzionalità⁵⁸ e necessità⁵⁹.

Numerose sono, a tale riguardo, le pronunce in cui la Corte si è soffermata sul rapporto fra la protezione dei dati personali, la libertà di espressione e i diritti economici degli operatori. Si possono, ad esempio, menzionare le sentenze *Satamedia*⁶⁰, *Scarlet*⁶¹, *SABAM*⁶² e *Lindqvist*⁶³.

Nella sentenza *Lindqvist*, la Corte ricorda che «le disposizioni [oggi del Regolamento (UE) n. 679/2016] non pongono, di per sé, una restrizione incompatibile con il principio generale di libertà di espressione o con altri diritti e libertà, all'interno dell'Unione europea e che trovano corrispondenza, tra l'altro, nell'art. 10 della CEDU. Spetta alle autorità e ai giudici nazionali incaricati di applicare la normativa nazionale [...] garantire il giusto equilibrio tra i diritti e gli interessi in gioco, ivi compresi i diritti fondamentali tutelati dall'ordinamento giuridico comunitario»⁶⁴.

L'approccio pragmatico ed equilibrato da sempre utilizzato dalla Corte nel ponderare gli interessi in gioco deve però oggi misurarsi con il continuo progredire della tecnologia⁶⁵. Il mondo digitale pone nuovi problemi anche perché si sviluppa molto più velocemente del diritto che lo deve disciplinare, con la conseguenza di indurre il potere giudiziario ad appropriarsi di sfere di competenza proprie del potere legislativo nel tentativo di colmarne le lacune.

Emblematica, dibattuta e controversa è la pronuncia *Google Spain*⁶⁶ in cui la Corte, in parte, discostandosi dal pensiero dell'Avvocato generale Jääskinen, acconsente a che ragioni del “diritto ad essere dimenticati”⁶⁷ possano prevalere su un generale interesse a

58 Si vedano anche le conclusioni dell'Avvocato generale Trstenjak del 27 giugno 2012 nella causa *K*, C-245/11, EU:C:2012:389, punto 75 e ss.

59 Sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, cit., punto 52. Per la Corte, le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondono a quelle tollerate nell'ambito dell'art. 8 della CEDU (*ibidem* punto 54).

60 Sentenza del 16 dicembre 2008, *Satamedia*, C-73/07, EU:C:2008:727.

61 Sentenza del 24 novembre 2011, *Scarlet*, C-70/10, cit.

62 Sentenza del 16 febbraio 2012, *SABAM*, C-360/10, EU:C:2012:85.

63 Sentenza del 6 novembre 2003, *Lindqvist*, C-101/01, cit.

64 *Ibidem*, punto 90.

65 Per vari spunti critici sull'approccio della Corte di giustizia alla protezione dei dati personali nel mondo digitale, cfr. O. POLLICINO, *Il “senso” della Corte di giustizia per la tutela dei dati personali*, in (a cura di) AA.VV., *Liber amicorum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, cit., p. 751.

66 Sentenza del 13 maggio 2014, *Google Spain*, C-131/12, EU:C:2014:317. Cfr. O. POLLICINO, M. BASSINI, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo?: il ruolo degli Artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Il diritto dell'informazione e dell'informatica*, 2014, p. 569.

67 Cfr. Conclusioni dell'Avvocato generale Jääskinen presentate il 25 giugno 2013 nella causa *Google Spain*, C-131/12, EU:C:2013:424, spec. punti 108-110, ove l'Avvocato generale ha affermato di non ritenere sussistente, ai sensi della direttiva 95/46/CE, «un diritto generale all'oblio nel senso che una persona interessata abbia il diritto di limitare o di porre fine alla diffusione di dati personali che consideri nocivi o contrari ai propri interessi. Sono lo scopo del trattamento e gli interessi da esso tutelati, confrontati con quelli della persona interessata, e non le preferenze di quest'ultima, i criteri da applicare allorché i dati vengono trattati senza il consenso della stessa. Di per sé, una preferenza soggettiva non costituisce un motivo preminente

un più rapido e agevole accesso alle informazioni e sui diritti economici dei fornitori di servizi di comunicazione.

Più precisamente, La Corte, interpretando alcune delle disposizioni contenute nella direttiva 95/46/CE alla luce degli articoli 7 e 8 della Carta, ha riconosciuto il diritto del singolo interessato a chiedere, in presenza di determinate condizioni, al gestore del motore di ricerca prima, e alle autorità competenti poi, l'eliminazione dei *links* verso pagine *web* pubblicate da terzi dall'elenco dei risultati che appare a seguito di una ricerca effettuata a partire dal nome di tale soggetto, sulla base della considerazione che «[l']attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di internet secondo un determinato ordine di preferenza, deve essere qualificato come trattamento di dati personali, e che il gestore di detto motore di ricerca deve essere considerato come il responsabile del trattamento»⁶⁸.

In questa pronuncia la Corte ha operato, dunque, un bilanciamento fra interessi contrapposti, ritenendo prevalente il diritto alla protezione della vita privata e dei dati personali rispetto alla libertà economica dei fornitori di servizi elettronici. Beninteso, non certo rispetto alla libertà di espressione e di informazione, che, peraltro, costituisce nel nuovo Regolamento (UE) n. 679/2016 una delle eccezioni al cd. "diritto all'oblio".

Non a caso, la Corte nella sentenza *Manni*⁶⁹ accorda prevalenza, in ossequio al principio di proporzionalità, alle finalità di pubblicità legale rispetto alle esigenze del singolo, all'interno di un corretto rapporto regola/eccezione, in linea con la giurisprudenza della Corte di Strasburgo⁷⁰.

Di certo, la Corte di giustizia ha affermato l'inapplicabilità di una normativa nazionale che stabilisca a priori ed in modo definitivo il risultato del bilanciamento dei diritti e degli interessi contrapposti, senza consentire un diverso risultato in ragione delle specifiche circostanze del caso concreto⁷¹. Si tratta perciò di un'operazione indispensabile qualora il conflitto riguardi diritti fondamentali della persona; né gli Stati possono escludere o limitare il potere del giudice di riequilibrare le controversie, perché ciò è vietato dall'art. 52 della Carta.

Il capitolo più delicato è, però, quello che vede in apparente contrapposizione il diritto alla tutela dei dati personali e l'interesse generale alla sicurezza e alla prevenzione dei reati⁷².

Anche in questo caso la giurisprudenza della Corte non è stata esente da critiche da parte di coloro che ritengono sia oggi data troppa attenzione al tema della protezione dei dati personali a scapito di diritti o interessi della collettività.

e legittimo ai sensi dell'articolo 14, lettera a), della direttiva».

⁶⁸ *Ibidem*, punto 41.

⁶⁹ Sentenza del 9 marzo 2017, *Manni*, C-398/15, EU:C:2017:197. Per un commento, si veda M. FORTI, *Diritto all'oblio e conservazione dei dati iscritti nei pubblici registri: qualche considerazione a margine della sentenza della Corte di giustizia nel caso Manni*, in *Contratto e impresa. Europa*, 2018, p. 565.

⁷⁰ *Inter alia*, la sentenza della Corte EDU del 16 luglio 2013, *Wegrzynowski and Smolczewski v. Poland*, ric. 33846/07.

⁷¹ Sentenza del 24 novembre 2011, *ASNEF*, C-468 e 469/10, EU:C:2011:777, punto 47.

⁷² Sul rapporto fra diritto alla protezione dei dati personali e sicurezza, si veda, fra gli altri, M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Medialaws*, 2/2018, p. 82.

In tema, la sentenza probabilmente più nota è *Digital Rights Ireland*⁷³ con la quale la Corte ha dichiarato invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, c.d. direttiva “*data retention*”, sulla conservazione di dati generati o trattati nell’ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Quest’ultima non prevedeva, infatti, a giudizio della Corte, garanzie sufficienti ad assicurare una protezione efficace dei dati personali contro i rischi di abusi e contro qualsiasi accesso e utilizzo illeciti degli stessi, dal momento che «la conservazione ed il successivo utilizzo dei dati avvengano senza che l’abbonato o l’utente registrato ne siano informati può ingenerare negli interessati la sensazione che la loro vita privata sia oggetto di costante sorveglianza»⁷⁴. Se, dunque, la conservazione dei dati ai fini della loro eventuale trasmissione alle autorità nazionali competenti può rispondere effettivamente a un obiettivo di interesse generale, la pubblica sicurezza, al tempo stesso tale pratica non deve eccedere i limiti imposti dal rispetto del principio di proporzionalità⁷⁵.

In questa pronuncia la Corte ha osservato che, in considerazione, da un lato, dell’importante ruolo svolto dalla protezione dei dati personali nei confronti del diritto fondamentale al rispetto della vita privata e, dall’altro lato, della portata e della gravità dell’ingerenza in tale diritto che la direttiva comporta, fosse necessario il controllo di un giudice o di un ente amministrativo indipendente sull’utilizzo da parte delle autorità nazionali competenti dei dati personali per finalità di prevenzione o contrasto di reati⁷⁶.

Secondo la Corte la normativa dell’Unione avrebbe dovuto prevedere regole chiare e precise con cui stabilire strumenti idonei a proteggere efficacemente i dati personali dal rischio di abusi, nonché da eventuali accessi e usi illeciti nelle attività di trattamento⁷⁷.

73 Sentenza del 8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, cit. Si noti peraltro che in tale pronuncia la Corte ha deciso per la prima volta nella storia del processo di integrazione europea di dichiarare nullo un atto di diritto derivato dell’Unione perché in contrasto con la Carta dei diritti fondamentali (articoli 7, 8 e 52, paragrafo 1), avendo il legislatore UE ecceduto i limiti imposti dal rispetto del principio di proporzionalità.

74 *Ibidem* punto 37.

75 *Ibidem*, punti 45 ss. e giurisprudenza ivi citata.

76 Sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09, cit., spec. punto 47. Per un commento, cfr. E. DEGRAVE, *Arrêt “Volker und Markus Schecke et Eifert” : le droit fondamental à la protection des données à caractère personnel et la transparence administrative*, in *Journal de droit européen*, 2011, p. 97; D. DERO-BUGNY, *Protection des personnes physiques à l’égard du traitement des données à caractère personnel*, in *Journal du droit international*, 2011, p. 492 e I. ANDOULSI, *L’arrêt de la Cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d’Hessen (C-92/09 et C-93/09) : une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles?*, in *Cahiers de droit européen*, 2011, p. 471. Si aggiunga che l’accesso delle autorità nazionali competenti ai dati di natura personale costituisce di per sé un’ingerenza supplementare in tali diritti fondamentali. In questo senso, con riferimento all’applicazione dell’art. 8 della Convenzione europea, cfr. le sentenze della Corte di Strasburgo del 26 marzo 1987, *Leander c. Svezia*, ricorso 9248/81, § 48, e del 4 maggio 2000, *Rotaru c. Romania* [GC], cit., § 46.

77 Sentenza del 8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, cit., punto 54.

Il ragionamento svolto dalla Corte vale anche se ad essere scrutinate sono le normative degli Stati membri come nel caso *Tele 2 Sverige*⁷⁸, in cui la Corte afferma che le garanzie minime fissate dalla sentenza *Digital Rights Ireland* sono requisiti di carattere imperativo del diritto dell'UE applicabili, dunque, anche ai regimi nazionali.

Ma vi è di più, il carattere imperativo degli standard fissati dalla Corte la induce a svolgere indirettamente un sindacato di compatibilità dei regimi giuridici di Stati terzi con il sistema di tutele delle libertà e dei diritti fondamentali previsto dall'ordinamento dell'Unione.

Si tratta, ovviamente, di un controllo che viene svolto in via mediata su una decisione di adeguatezza della Commissione, che, poi, di fatto, sottintende un giudizio di sostanziale equivalenza (come nel caso *Schrems*⁷⁹ o, per usare un termine più evocativo, "Facebook"), o su una decisione con cui sia stato concluso un accordo internazionale. Qui il riferimento è al parere 1/15 della Corte in merito all'accordo sul trasferimento dei codici di prenotazione (PNR) concluso dall'Unione europea con il Canada⁸⁰.

La sentenza *Schrems* è di grande interesse proprio nella misura in cui, affermando che le autorità nazionali di vigilanza nazionali, pur in presenza di una decisione di adeguatezza della Commissione, conservano un potere di intervento laddove venga da loro ritenuto pregiudicato il rispetto degli articoli 7, 8 e 47 della Carta, finisce per consacrare l'estensione della applicazione territoriale della normativa di diritto derivato ai trattamenti effettuati in Paesi terzi, anticipando così l'intervento chiarificatore del legislatore dell'Unione con l'articolo 4 del Regolamento (UE) n. 679/2017⁸¹.

In base a questa pronuncia, anche qualora la Commissione abbia adottato una decisione di adeguatezza ai sensi dell'art. 45 del Regolamento (UE) n. 679/2016, le autorità nazionali di controllo conservano il potere di valutare in piena indipendenza se il trasferimento di tali dati verso Paesi terzi rispetti i requisiti fissati dalla normativa e, dunque, se tale trattamento rispecchi le tutele garantite dagli articoli 7 e 8 della Carta⁸².

78 Sentenza del 21 dicembre 2016, *Tele2 Sverige*, C-203/15, EU:C:2016:970. Cfr. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2/2018, p. 64.

79 Sentenza del 6 ottobre 2015, *Schrems*, C-362/14, EU:C:2015:650. Per un primo commento, cfr. F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, 2016, p. 690.

80 Parere 1/15 della Corte del 26 luglio 2017, EU:C:2017:592.

81 Per la verità, anche prima del nuovo regolamento generale era indubbio che i poteri conferiti alle autorità di controllo dall'art. 28, paragrafi 1 e 6, della direttiva 95/46/CE riguardassero anche i trattamenti di dati personali effettuati nel territorio del rispettivo Stato membro. La Corte, in proposito, ricorda che il trasferimento dei dati personali da uno Stato membro verso un Paese terzo costituisce, di per sé, un trattamento degli stessi ai sensi dell'art. 2, lett. b), della direttiva 95/46/CE, effettuato nel territorio di uno Stato membro. Cfr. la sentenza del 30 maggio 2006, *Parlamento c. Consiglio*, C-317/04 e C-318/04, ECLI:EU:C:2006:346. La norma richiamata, invero, definisce il trattamento di dati personali alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

82 Cfr., per evidenti analogie, la sentenza *Digital Rights Ireland*, cit., punto 68.

La Corte, insomma, giunge a riconoscere un'applicazione extraterritoriale degli standard europei di tutela dei dati personali.

Ampliando la prospettiva, la Corte ha affermato, in diverse occasioni, ad esempio con la sentenza *N.S.*⁸³, che gli Stati membri sono tenuti, non solo a interpretare il rispettivo diritto nazionale conformemente al diritto dell'Unione, ma anche a fare in modo di non basarsi su un'interpretazione di norme di diritto derivato che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico dell'Unione o con gli altri principi generali del diritto UE. Dunque, se si applica per estensione tale ragionamento al caso in esame, ne consegue che la presunzione sottesa all'art. 25, par. 6, della direttiva 95/46/CE, secondo cui il trasferimento di dati verso un Paese terzo rispetta i diritti fondamentali, deve essere considerata relativa e non assoluta. Laddove vengano riscontrate carenze sistematiche nel trattamento di tali dati, pur in presenza di una decisione di adeguatezza adottata dalla Commissione, le autorità degli Stati membri, in osservanza del loro ruolo di garanti, devono ugualmente poter adottare le misure necessarie per salvaguardare quei diritti fondamentali della persona, la cui tutela si impone per effetto dell'applicazione degli articoli 7, 8 e 47 della Carta dei diritti fondamentali.

Solo in questo modo le autorità nazionali per la protezione dei dati personali possono esercitare i poteri che derivano loro in virtù della stessa normativa UE, considerato che, come si evince dalla *ratio* e dallo spirito della direttiva 95/46/CE, un sistema di controllo esterno, sotto forma di un'autorità che agisca in modo indipendente in ciascuno Stato membro, è un requisito essenziale per assicurare una tutela effettiva al singolo. Poteri conferiti alle autorità nazionali di controllo dei dati, non solo nei casi di trasferimento dei dati nell'ambito dell'Unione Europea, ma anche nei casi di trasferimento degli stessi verso gli Stati terzi, dovendosi riconoscere uguale tutela alla riservatezza delle persone coinvolte, sia che i loro dati vengano trattati all'interno del territorio dell'UE, sia che vengano trasferiti al di fuori di esso.

Tuttavia, come si è detto, siffatti poteri conoscono dei limiti ben precisi: di certo, essi non possono alterare, né tantomeno sovvertire, una giurisprudenza consolidata della Corte⁸⁴ secondo cui, in virtù del primato del diritto dell'Unione europea sui diritti nazionali, solo il giudice dell'UE, e non anche le autorità nazionali, quale sia la loro natura, è competente ad accertare in via definitiva la legittimità di una decisione della Commissione, così come di qualsiasi atto dell'Unione⁸⁵, e ciò allo scopo di garantire

83 Sentenza del 21 dicembre 2011, *N.S. e altri*, C-411/10 e C-493/10, EU:C:2011:865, punto 77. Per un commento a tale pronuncia si veda J. BUCKLEY, *NS v Secretary of State for the Home Department (C-411/10)*, in *European Human Rights Law Review*, 2012, p. 208; G. MORGESE, *Regolamento Dublino II e applicazione del principio di mutua fiducia tra Stati membri: la pronuncia della Corte di giustizia nel caso N.S. e altri*, in *Studi sull'integrazione europea*, 2012, p. 147; G. MELLON, *The Charter of Fundamental Rights and the Dublin Convention: An Analysis of N.S. v. Secretary of State for the Home Department (C-411/10)*, in *European Public Law*, 2012, p. 655.

84 Sentenza del 21 febbraio 1991, *Zuckerfabrik*, C-143/88 e C-92/89, EU:C:1991:65, punto 17, e sentenza del 21 marzo 2000, *Greenpeace France e a.*, C-6/99, EU:C:2000:148, punto 54.

85 Ad ulteriore dimostrazione del fatto che anche le decisioni adottate dalla Commissione in forza dell'art. 25, par. 6, della direttiva 95/46/CE non possono sfuggire al controllo di validità effettuato dalla Corte in via esclusiva, quest'ultima richiama la propria giurisprudenza costante secondo cui l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggette al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto, nonché ai diritti fondamentali (cfr., in particolare, le sentenze del 18 luglio 2013, *Kadi*,

l'uniforme applicazione del diritto UE all'interno degli ordinamenti nazionali. Verrebbe, altrimenti, compromessa la stessa unità dell'ordinamento giuridico UE in quanto risulterebbe leso il principio fondamentale della certezza del diritto⁸⁶. Gli atti dell'Unione (ne è la logica conseguenza) si presumono, infatti, legittimi e producono effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità⁸⁷.

8. Alcune (brevi) riflessioni conclusive.

Dalla giurisprudenza sopra richiamata emerge chiara l'incompatibilità con gli articoli 7 e 8 della Carta di qualsiasi accesso generalizzato e incondizionato da parte di autorità pubbliche ai dati personali, anche se la finalità è la lotta contro la criminalità grave e poco importa che le informazioni relative alla vita privata del singolo abbiano un carattere sensibile o che l'interessato abbia realmente patito conseguenze negative a seguito di una tale ingerenza.

L'accesso ai dati personali da parte di autorità pubbliche è, dunque, consentito solo se "mirato" e l'obiettivo perseguito dalle norme che disciplinano tale accesso deve essere adeguato alla gravità dell'ingerenza nei diritti fondamentali. In questi termini si è espressa la Corte nella recente sentenza *Ministerio fiscal*⁸⁸.

Il delicato equilibrio fra limitazioni dei diritti fondamentali ed esigenze securitarie passa, pertanto, sotto il vaglio di un test di (stretta) proporzionalità che consente alla Corte di valorizzare la centralità del diritto alla protezione dei dati e del diritto al rispetto della vita privata e che, integrando il test di necessità, si pone come meccanismo di salvaguardia a difesa dei valori di una società democratica.

Certo, viene da chiedersi sino a che punto la protezione dei dati personali con la sua nuova fisionomia di diritto fondamentale possa talora prevalere non solo su interessi di carattere economico e sociale, ma anche su esigenze di sicurezza.

La risposta a tale domanda è problematica perché la strada per trovare un equilibrio tra queste istanze è molto scivolosa.

La protezione dei dati personali non è solo un diritto individuale, ma rappresenta anche un interesse pubblico, una garanzia per la vita democratica e, dunque, per i valori su cui si fonda l'Unione e al tempo stesso la sicurezza non è solo un bene pubblico, ma è anche un diritto individuale. Un bisogno primario dell'uomo che egli è naturalmente portato ad appagare unendosi a una comunità alla ricerca di protezione. Quella comunità è oggi l'Unione europea su cui grava un'obbligazione anche di carattere positivo.

D'altra parte, l'art. 6 della Carta ci dice che ogni persona ha diritto alla libertà e alla sicurezza, sebbene il significato di quest'ultima espressione, cui si fatica a riconoscere la dignità di diritto autonomo, sia nella giurisprudenza della Corte ancora indefinito⁸⁹.

C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66 e del 19 dicembre 2013, *Telefónica c. Commissione*, C-274/12 P, EU:C:2013:852, punto 56).

⁸⁶ Sentenza del 22 ottobre 1987, *Foto Frost*, 314/85, EU:C:1987:452, punto 15; sentenza del 15 aprile 1997, *Bakers of Nailsea*, C-27/95, EU:C:1997:188, punto 20, e sentenza del 6 dicembre 2005, *Gaston Schul Douane-expediteur*, C-461/03, EU:C:2005:742, punto 21.

⁸⁷ Sentenza del 5 ottobre 2004, *Commissione c. Grecia*, C-475/01, EU:C:2004:585, punto 18 e la giurisprudenza ivi citata.

⁸⁸ Sentenza del 2 ottobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788.

Insomma, il rapporto fra protezione dei dati personali e sicurezza non va visto necessariamente in una dimensione antinomica.

Al di là delle categorie concettuali, resta fermo il convincimento che la Corte, affinando ulteriormente la propria giurisprudenza, così da renderla più lineare, saprà ricondurre il diritto fondamentale alla protezione dei dati personali nella sua giusta dimensione, senza cedere alla tentazione di darvi una valenza acronica assolutizzante, ma parimenti consapevole che esso oramai si configura come un presidio costituzionale irrinunciabile e anche uno dei punti più alti del processo di integrazione europea.

89 Cfr. F. ROSSI DAL POZZO, M. GIALUZ, *Commento all'art. 6 CdfUE*, (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, cit., p. 94.