MANUALE

Manuale sul diritto europeo in materia di protezione dei dati

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Il presente manuale è stato completato nell'aprile 2014.
Eventuali futuri aggiornamenti saranno messi a disposizione sul sito Internet della FRA all'indirizzo fra.europa.eu, sul sito del Consiglio d'Europa all'indirizzo coe.int/dataprotection e sul sito Internet della Corte europea dei diritti dell'uomo, alla voce "Case-Law", all'indirizzo echr.coe.int.

Europe Direct è un servizio a vostra disposizione per aiutarvi a trovare le risposte ai vostri interrogativi sull'Unione europea.

Numero verde unico (*):

00 800 6 7 8 9 10 11

(*) Le informazioni sono fornite gratuitamente e le chiamate sono nella maggior parte dei casi gratuite (con alcuni operatori e in alcuni alberghi e cabine telefoniche il servizio potrebbe essere a pagamento).

Numerose altre informazioni sull'Unione europea sono disponibili su Internet consultando il portale Europa (http://europa.eu).

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2014

ISBN 978-92-871-9951-5 (CDE)
ISBN 978-92-9239-335-9 (FRA)
doi:10.2811/54588

Printed in Belgium

Stampato su carta riciclata senza cloro (PCF)

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Manuale sul diritto europeo in materia di protezione dei dati

Premessa

Il presente manuale sul diritto europeo in materia di protezione dei dati nasce da una redazione congiunta dell'Agenzia dell'Unione europea per i diritti fondamentali e del Consiglio d'Europa con la Cancelleria della Corte europea dei diritti dell'uomo. Si tratta del terzo di una serie di manuali giuridici stilati congiuntamente dalla FRA e dal Consiglio d'Europa. Nel marzo 2011 è stato pubblicato un primo manuale di diritto europeo in materia di non discriminazione e nell'aprile 2013 ne è stato pubblicato un secondo sul diritto europeo in materia di asilo, frontiere e immigrazione.

Abbiamo deciso di proseguire la nostra collaborazione concentrandoci su un tema di grande attualità che ogni giorno riguarda tutti noi, ossia la protezione dei dati personali. L'Europa vanta uno dei sistemi più all'avanguardia in questo ambito, basato sulla Convenzione n. 108 del Consiglio d'Europa, sugli strumenti giuridici dell'Unione europea (UE) nonché sulla giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU) e della Corte di giustizia dell'Unione europea (CGUE).

Il manuale mira a sensibilizzare e ad accrescere le conoscenze sulle norme in materia di protezione dei dati negli Stati membri dell'Unione europea e del Consiglio d'Europa, fungendo da punto di riferimento principale per i lettori e rivolgendosi a professionisti del settore legale senza specializzazione, giudici, autorità di controllo nazionali e altri soggetti operanti nell'ambito della protezione dei dati.

Con l'entrata in vigore del trattato di Lisbona, nel dicembre 2009, la Carta dei diritti fondamentali dell'Unione europea è divenuta giuridicamente vincolante e con essa il diritto alla protezione dei dati personali è assurto a diritto fondamentale a sé stante. La tutela di questo diritto fondamentale esige una migliore comprensione della Convenzione n. 108 del Consiglio d'Europa e degli strumenti giuridici dell'Unione europea (UE), che hanno creato i presupposti per la protezione dei dati in Europa, nonché della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.

Vorremmo ringraziare il Ludwig Boltzmann Institute of Human Rights per il suo contributo nella stesura di questo manuale. Vorremmo anche esprimere la nostra gratitudine all'ufficio del Garante europeo della protezione dei dati. Desideriamo rivolgere un particolare ringraziamento all'unità Protezione dei dati della Commissione europea per il sostegno nella preparazione del presente manuale. Infine vorremmo esprimere la nostra riconoscenza al Garante per la protezione dei dati personali che ha controllato la traduzione italiana del manuale.

Philippe Boillat

Direttore generale della DG Diritti umani e stato di diritto del Consiglio d'Europa

Morten Kjaerum

Direttore dell'Agenzia dell'Unione europea per i diritti fondamentali

Indice

Sigle e acronimi

ACC	Autorità comuni di controllo
BCR	Norme vincolanti d'impresa
Carta	Carta dei diritti fondamentali dell'Unione europea
CCTV	Televisione a circuito chiuso
CDE	Consiglio d'Europa
CE	Comunità europea
CEDU	Convenzione europea dei diritti dell'uomo
CGUE	Corte di giustizia dell'Unione europea (denominata Corte di giustizia (CG) fino a dicembre 2009)
Convenzione n°108	Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Consiglio d'Europa)
Corte EDU	Corte europea dei diritti dell'uomo
CRM	Gestione dei rapporti con la clientela
EFTA	Associazione europea di libero scambio
ENISA	Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione
ESMA	Autorità europea degli strumenti finanziari e dei mercati
eTEN	Reti di telecomunicazione transeuropee
eu-LISA	Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia
EuroPriSe	Certificazione europea di tutela della vita privata
FRA	Agenzia dell'Unione europea per i diritti fondamentali
GEPD	Garante europeo della protezione dei dati
GPS	Sistema di posizionamento globale
MAE	Mandato d'arresto europeo

OCSE	Organizzazione per la cooperazione e lo sviluppo economico
ONG	Organizzazione non governativa
ONU	Nazioni Unite
PIN	Codice d'identificazione personale
PNR	Codice di prenotazione
SEE	Spazio economico europeo
SEPA	Area unica dei pagamenti in euro
SID	Sistema informativo doganale
SIS	Sistema d'Informazione Schengen
SIS-C	Sistema centrale d'Informazione Schengen
SIS-N	Sistema nazionale d'Informazione Schengen
STCE	Serie dei trattati del Consiglio d'Europa
SWIFT	Società per le telecomunicazioni finanziarie interbancarie mondiali
TFUE	Trattato sul funzionamento dell'Unione europea
TUE	Trattato sull'Unione europea
UDHR	Dichiarazione universale dei diritti dell'uomo
UE	Unione europea
UNE	Unità nazionale Europol
VIS	Sistema d'informazione visti

Come usare il manuale

Il presente manuale presenta una panoramica della normativa applicabile in materia di protezione dei dati nell'ambito di competenza dell'Unione europea (UE) e del Consiglio d'Europa (CDE).

Il manuale, volto ad assistere i professionisti del settore legale non specializzati nel campo della protezione dei dati, è destinato ad avvocati, giudici o altri professionisti e soggetti che collaborano con altri organismi, comprese le organizzazioni non governative (ONG) che potrebbero dover affrontare problematiche giuridiche connesse alla protezione dei dati.

Il manuale intende fornire un primo punto di riferimento in materia di protezione dei dati per quanto riguarda sia il diritto dell'UE sia la Convenzione europea dei diritti dell'uomo (CEDU), oltre a illustrare come questo settore sia disciplinato dal diritto dell'UE e dalla CEDU nonché dalla Convenzione del Consiglio d'Europa (CDE) sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108) e da altri strumenti giuridici dello stesso CDE. All'inizio di ogni capitolo è presente una tabella contenente le disposizioni legali applicabili con un'importante selezione della giurisprudenza secondo i due distinti sistemi giuridici europei. Fanno seguito due presentazioni, l'una successiva all'altra, del diritto dei due ordinamenti europei, così come applicabile a ciascuna tematica, in modo che il lettore possa cogliere le convergenze e le divergenze dei due sistemi giuridici.

Le tabelle poste all'inizio di ogni capitolo elencano gli argomenti trattati nello stesso, oltre a indicare le disposizioni giuridiche applicabili e altri documenti pertinenti, come la giurisprudenza in merito. È possibile che gli argomenti siano trattati in ordine lievemente diverso rispetto alla struttura del testo di un capitolo, qualora tale modifica sia ritenuta utile ai fini di una presentazione più concisa del contenuto dello stesso capitolo. Le tabelle trattano del diritto sia del CDE sia dell'UE, nell'intento di agevolare gli utenti nella ricerca di informazioni chiave relative al proprio caso specifico, specie qualora siano soggetti esclusivamente al diritto del CDE.

I professionisti del settore legale attivi in Stati non membri dell'UE ma che fanno parte del CDE e hanno aderito alla CEDU e alla Convenzione n. 108 possono accedere alle informazioni riguardanti il proprio paese visitando direttamente le sezioni del CDE. I professionisti degli Stati membri dell'UE devono invece consultare tutte e due le sezioni, giacché questi Stati sono vincolati a entrambi gli ordinamenti giuridici. Chi necessita di maggiori informazioni su un particolare argomento può reperire una bibliografia più specialistica nella sezione del manuale riservata agli "Approfondimenti".

Il diritto del CDE è presentato attraverso brevi riferimenti a una selezione di cause della Corte europea dei diritti dell'uomo (Corte EDU) scelte tra le numerose sentenze e decisioni pronunciate dalla Corte EDU in materia di protezione dei dati.

Il diritto dell'UE è illustrato attraverso il riferimento alle misure legislative adottate, alle disposizioni pertinenti dei trattati e alla Carta dei diritti fondamentali dell'Unione europea, come interpretate nella giurisprudenza della Corte di giustizia dell'Unione europea (CGUE, denominata Corte di giustizia o CG fino al 2009).

La giurisprudenza presentata o citata nel presente manuale offre esempi tratti da un ampio *corpus* di giurisprudenza della Corte EDU e della CGUE. Esempi pertinenti sono forniti nei riquadri circoscritti in blu. Le linee guida riportate in fondo al manuale mirano ad assistere il lettore nella ricerca della giurisprudenza online.

All'interno del testo, inoltre, compaiono alcuni riquadri con il fondo blu contenenti esempi pratici connessi a casi ipotetici. Tali esempi mirano a illustrare ulteriormente l'applicazione pratica delle norme europee in materia di protezione dei dati, specie laddove non sussista una giurisprudenza specifica della Corte EDU o della CGUE in materia. Altri riquadri, con il fondo grigio, presentano esempi presi da altre fonti, diverse dalla giurisprudenza e dalla legislazione.

Il manuale inizia con una breve descrizione del ruolo dei due sistemi giuridici, come stabilito dalla CEDU e dal diritto dell'UE (capitolo 1), e prosegue con l'illustrazione delle seguenti tematiche (capitoli da 2 a 8):

- terminologia della protezione dei dati;
- principi fondamentali del diritto europeo in materia di protezione dei dati;
- norme del diritto europeo sulla protezione dei dati;
- diritti degli interessati e loro attuazione;
- flussi transfrontalieri dei dati;
- protezione dei dati nel contesto della pubblica sicurezza e della giustizia penale;
- altre norme europee specifiche in materia di protezione dei dati.

1

Contesto e quadro del diritto europeo in materia di protezione dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Il diritto alla protezione dei dati		
Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*direttiva sulla protezione dei dati*), GU L 281 del 23.11.1995		CEDU, articolo 8 (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza) Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108)
Conciliazione dei diritti		
CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 2010	Generale	
CGUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*, 2008	Libertà di espressione	Corte EDU, *Axel Springer AG c. Germania*, 2012 Corte EDU, *Mosley c. Regno Unito*, 2011
	Libertà delle arti e delle scienze	Corte EDU, *Vereinigung bildender Künstler c. Austria*, 2007
CGUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 2008.	Protezione della proprietà	
CGUE, C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd*, 2010	Accesso ai documenti	Corte EDU, *Társaság a Szabadságjogokért c. Ungheria*, 2009

1.1. Il diritto alla protezione dei dati

Punti salienti

- Ai sensi dell'articolo 8 della CEDU, il diritto alla protezione dei dati personali relativamente alla raccolta e all'utilizzo degli stessi è parte del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.
- La Convenzione n. 108 del Consiglio d'Europa è il primo strumento internazionale giuridicamente vincolante che tratta in maniera esplicita della protezione dei dati.
- Il diritto dell'UE ha disciplinato per la prima volta la protezione dei dati attraverso la direttiva sulla protezione dei dati.
- Il diritto dell'UE ha riconosciuto la protezione dei dati come un diritto fondamentale.

Il diritto alla protezione della sfera privata di un individuo contro le ingerenze altrui, soprattutto da parte dello Stato, è stato sancito per la prima volta da uno strumento giuridico internazionale nell'articolo 12 della Dichiarazione universale dei diritti dell'uomo (UDHR) delle Nazioni Unite (ONU) del 1948 riguardante il rispetto della vita privata e familiare[1]. L'UDHR ha influito sullo sviluppo di altri strumenti relativi ai diritti dell'uomo in Europa.

1.1.1. La Convenzione europea dei diritti dell'uomo

Il Consiglio d'Europa è stato costituito all'indomani della seconda guerra mondiale con l'obiettivo di riunire gli Stati d'Europa e promuovere lo Stato di diritto, la democrazia, i diritti dell'uomo e lo sviluppo sociale. A tal fine, nel 1950 il CDE ha adottato la Convenzione europea dei diritti dell'uomo (CEDU), entrata poi in vigore nel 1953.

Gli Stati hanno l'obbligo internazionale di attenersi alla CEDU. Tutti gli Stati membri del CDE hanno ormai recepito o dato efficacia alla CEDU nel rispettivo diritto nazionale, che impone loro di agire conformemente alle disposizioni contenute nella stessa.

Per garantire che le parti contraenti adempiano i propri obblighi ai sensi della CEDU, nel 1959 è stata istituita a Strasburgo (Francia) la Corte europea dei diritti dell'uomo (Corte EDU). La Corte EDU garantisce che gli Stati adempiano gli obblighi previsti dalla

1 Nazioni unite (ONU), Dichiarazione universale dei diritti dell'uomo (UDHR), 10 dicembre 1948. V. anche art. 17 del Patto internazionale dei diritti civili e politici del 1966.

Convenzione valutando le denunce presentate da singoli individui, gruppi di individui, ONG o persone giuridiche che lamentino l'esistenza di violazioni della Convenzione. Nel 2013 il Consiglio d'Europa era formato da 47 Stati membri, 28 dei quali sono anche Stati membri dell'UE. Per adire la Corte EDU non è necessario essere cittadino di uno degli Stati membri. La Corte EDU può altresì esaminare le cause interstatali intentate da uno o più Stati membri del CDE contro un altro Stato membro.

Il diritto alla protezione dei dati personali rientra nei diritti tutelati dall'articolo 8 della CEDU, che garantisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, e stabilisce le condizioni alle quali il diritto alla protezione dei dati personali può essere soggetto a restrizioni[2].

Con propria giurisprudenza, la Corte EDU ha affrontato il tema della protezione dei dati in più casi, non ultimi quelli riguardanti l'intercettazione delle comunicazioni[3], le varie forme di sorveglianza[4] nonché le garanzie rispetto alla conservazione dei dati personali da parte delle autorità pubbliche[5]. La Corte ha chiarito che l'articolo 8 della CEDU non solo obbliga gli Stati ad astenersi da qualsiasi azione che possa violare questo diritto previsto dalla Convenzione, ma impone anche loro, in talune circostanze, l'obbligo di garantire attivamente l'effettivo rispetto della vita privata e familiare[6]. Molti di questi casi saranno esaminati in modo dettagliato nei capitoli pertinenti.

1.1.2. La Convenzione n. 108 del Consiglio d'Europa

L'emergere delle tecnologie dell'informazione negli anni '60 ha determinato un crescente bisogno di norme più dettagliate per tutelare le persone proteggendone i dati (personali). A metà degli anni '70, il Comitato dei ministri del Consiglio d'Europa ha adottato varie risoluzioni in materia di protezione dei dati personali, facendo

2 CDE, Convenzione europea dei diritti dell'uomo, STCE n. 005, 1950.

3 Cfr., per esempio, Corte EDU, *Malone c. Regno Unito*, n. 8691/79, 2 agosto 1984; Corte EDU, *Copland c. Regno Unito*, n. 62617/00, 3 aprile 2007.

4 Cfr., per esempio, Corte EDU, *Klass e a. c. Germania*, n.°5029/71, 6 settembre 1978; Corte EDU, *Uzun c. Germania*, n.°35623/05, 2 settembre 2010.

5 Cfr., per esempio, Corte EDU, *Leander c. Svezia*, n. 9248/81, 11 luglio 1985; Corte EDU, *S. e Marper c. Regno Unito*, n.°30562/04, 4 dicembre 2008.

6 Cfr., per esempio, Corte EDU, *I. c. Finlandia*, n. 20511/03, 17 luglio 2008; Corte EDU, *K.U. c. Finlandia*, n.°2872/02, 2 dicembre 2008.

riferimento all'articolo 8 della CEDU[7]. Nel 1981 è stata aperta alla firma una Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108)[8]. La Convenzione n. 108 era, e rimane, l'unico strumento internazionale giuridicamente vincolante in materia di protezione dei dati.

La Convenzione n. 108 si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che nel pubblico e, in tale ambito, anche a quelli effettuati da autorità giudiziarie e di polizia. Protegge l'individuo dagli abusi che possono accompagnare la raccolta e il trattamento dei dati personali e, nel contempo, cerca di regolamentare il flusso transfrontaliero di dati personali. Per quanto concerne la raccolta e il trattamento dei dati personali, i principi stabiliti nella Convenzione riguardano, in particolare, la correttezza e liceità della raccolta e del trattamento automatizzato dei dati, archiviati per specifici scopi legittimi, non destinati a un uso incompatibile con tali scopi né conservati oltre il tempo necessario. Tali principi riguardano anche la qualità dei dati, in particolare in riferimento alla loro adeguatezza, pertinenza e non eccedenza (proporzionalità) nonché esattezza.

Oltre a fornire garanzie sulla raccolta e sul trattamento dei dati personali, la Convenzione, in assenza di adeguate garanzie giuridiche, vieta il trattamento dei dati "sensibili", come la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale o i precedenti giudiziari di un individuo.

La Convenzione sancisce inoltre il diritto dell'individuo di essere informato della conservazione di informazioni che lo riguardano e di chiederne la rettifica, se del caso. Le restrizioni dei diritti stabiliti nella Convenzione sono possibili solo quando sono in gioco interessi prevalenti, quali la sicurezza o la difesa dello Stato.

Benché preveda la libera circolazione dei dati personali tra le parti contraenti, la Convenzione impone anche alcune restrizioni su tali flussi verso paesi in cui la regolamentazione giuridica non conferisce una protezione equivalente.

7 CDE, Comitato dei ministri (1973), risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato, 26 settembre 1973; CDE, Comitato dei ministri (1974), risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico, 20 settembre 1974.

8 CDE, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Consiglio d'Europa, STCE n. 108, 1981.

Al fine di sviluppare ulteriormente i principi generali e le norme previste dalla Convenzione n. 108, il Comitato dei ministri del CDE ha adottato diverse raccomandazioni giuridicamente non vincolanti (cfr. i capitoli 7 e 8).

Tutti gli Stati membri dell'UE hanno ratificato la Convenzione n. 108, che nel 1999 è stata emendata per consentire all'UE di diventarne parte contraente[9]. Nel 2001 è stato adottato un Protocollo addizionale alla Convenzione n. 108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti, i cosiddetti paesi terzi, e l'istituzione obbligatoria delle autorità di controllo nazionali per la protezione dei dati[10].

Prospettiva

A seguito della decisione di modernizzare la Convenzione n. 108, una consultazione pubblica effettuata nel 2011 ha consentito di confermare i due obiettivi principali di tale lavoro: il rafforzamento della protezione della vita privata nel settore digitale e il consolidamento del meccanismo di attuazione della Convenzione.

La Convenzione n. 108 è aperta all'adesione degli Stati non membri del CDE, compresi i paesi extraeuropei. La portata della Convenzione come standard universale e il suo carattere aperto potrebbero costituire un presupposto per promuovere la protezione dei dati a livello mondiale.

Finora, 45 delle 46 parti contraenti della Convenzione n. 108 sono Stati membri del CDE. L'Uruguay, il primo paese extraeuropeo, vi ha aderito nell'agosto 2013 e il Marocco, invitato ad aderirvi dal Comitato dei ministri, sta per formalizzare tale adesione.

9 CDE, emendamenti alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE n.°108) che consente alle Comunità europee di accedervi, adottati dal Comitato dei ministri, a Strasburgo, il 15 giugno 1999; articolo 23, paragrafo 2, della Convenzione n. 108 nella sua versione modificata.

10 CDE, Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, concernente le autorità di controllo e i flussi transfrontalieri di dati, STCE n.°181, 2001.

1.1.3. Il diritto dell'Unione europea in materia di protezione dei dati

Il diritto dell'Unione si compone di trattati e del diritto derivato dell'UE. I trattati, vale a dire il trattato sull'Unione europea (TUE) e il trattato sul funzionamento dell'Unione europea (TFUE), noti anche come "diritto primario dell'UE", sono stati approvati da tutti gli Stati membri dell'Unione. I regolamenti, le direttive e le decisioni dell'UE, adottati dalle istituzioni dell'Unione alle quali è stata conferita tale autorità in virtù dei trattati, sono spesso indicati come "diritto derivato dell'UE".

Il principale strumento giuridico dell'UE in materia di protezione dei dati è costituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*direttiva sulla protezione dei dati*)[11]. La direttiva è stata adottata nel 1995, in un momento in cui diversi Stati membri avevano già adottato leggi nazionali in materia. La libera circolazione delle merci, dei capitali, dei servizi e delle persone nel mercato interno ha richiesto la libera circolazione dei dati, che non poteva essere realizzata se gli Stati membri non avessero potuto contare su un livello elevato e uniforme di protezione dei dati.

Poiché è stata adottata allo scopo di armonizzare[12] le normative nazionali sulla protezione dei dati, la direttiva sulla protezione dei dati è caratterizzata da un grado di specificità paragonabile a quella delle legislazioni nazionali (allora) vigenti in materia. Per la Corte di Giustizia dell'Unione europea (CGUE) "la direttiva 95/46 mira [...] a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. [...] Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità. [...]L'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa"[13]. Di conseguenza, gli Stati membri hanno solo una limitata libertà di manovra per quanto riguarda l'attuazione della direttiva. Se prima dell'entrata in vigore della direttiva uno Stato membro presentava già un livello di protezione più elevato ed ampio, detto standard poteva essere mantenuto.

11 Direttiva sulla protezione dei dati, GU L 281 del 23.11.1995, pag. 31.

12 Cfr. per esempio, la direttiva sulla protezione dei dati, considerando 1, 4, 7 e 8.

13 CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado,* 24 novembre 2011, punti 28 e 29.

La direttiva sulla protezione dei dati mira a concretizzare i principi del diritto alla vita privata già contemplati nella Convenzione n. 108, oltre ad estenderne l'applicazione. Il fatto che tutti e 15 gli Stati membri dell'UE nel 1995 fossero anche parti contraenti della Convenzione n. 108 esclude l'adozione di norme contraddittorie in questi due strumenti giuridici. La direttiva sulla protezione dei dati, tuttavia, si avvale della possibilità, prevista dall'articolo 11 della Convenzione n. 108, di prevedere ulteriori strumenti di tutela. In particolare, l'introduzione di autorità di controllo indipendenti come strumento per migliorare l'osservanza delle norme sulla protezione dei dati ha dimostrato di contribuire in modo significativo all'effettiva applicazione del diritto europeo in materia di protezione dei dati (di conseguenza, questa caratteristica è stata ripresa nel diritto del CDE nel 2001 attraverso il Protocollo addizionale alla Convenzione n. 108)[14].

L'applicazione territoriale della direttiva sulla protezione dei dati si estende oltre i 28 Stati membri dell'Unione, comprendendo anche i paesi extra-UE che rientrano nello Spazio economico europeo (SEE)[15], vale a dire l'Islanda, il Liechtenstein e la Norvegia.

La CGUE, con sede a Lussemburgo, è competente a stabilire se uno Stato membro abbia adempiuto i propri obblighi ai sensi della direttiva sulla protezione dei dati e a pronunciarsi in via pregiudiziale sulla validità e sull'interpretazione della direttiva, al fine di garantirne l'effettiva e uniforme applicazione negli Stati membri. Una deroga importante all'applicabilità della direttiva sulla protezione dei dati è la cosiddetta esenzione per l'esercizio di attività a carattere personale o domestico, vale a dire il trattamento dei dati personali da parte di privati per fini esclusivamente personali o domestici[16], che è generalmente considerato come facente parte delle libertà dell'individuo.

L'ambito di applicazione materiale della direttiva sulla protezione dei dati, che corrisponde a quello del diritto primario dell'UE in vigore al momento dell'adozione della stessa, si limita alle questioni relative al mercato interno. Esulano da detto ambito, segnatamente, le questioni riguardanti la cooperazione a livello di pubblica sicurezza

14 Così come il Gruppo per la tutela delle persone col riguardo al trattamento dei dati personali (Gruppo di lavoro articolo 29), a carattere consultivo e indipendente, cui partecipano le autorità di controllo, contribuisce all'applicazione armonizzata delle sue disposizioni. Cfr. direttiva sulla protezione dei dati, articolo 29. I documenti e le informazioni relative alle attività del Gruppo di lavoro sono disponibili all'indirizzo: http://ec.europa.eu/justice/data-protection/index_en.htm.

15 Accordo sullo Spazio economico europeo, GU L 1 del 3.1.1994, entrato in vigore il 1° gennaio 1994.

16 Direttiva sulla protezione dei dati, articolo 3, paragrafo 2, secondo trattino.

e giustizia penale. La protezione dei dati in questa materia è resa possibile da diversi strumenti giuridici, di cui si offre una descrizione dettagliata al capitolo 7.

Poiché la direttiva sulla protezione dei dati poteva rivolgersi solo agli Stati membri dell'UE, si è avvertita l'esigenza di introdurre un ulteriore strumento giuridico al fine di mettere in atto la protezione dei dati nell'ambito del trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE. Questo compito è svolto dal regolamento (CE) n. 45/2001, 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 (*regolamento sulla protezione dei dati da parte delle istituzioni dell'UE*)[17].

Inoltre, anche negli ambiti interessati dalla direttiva sulla protezione dei dati sono spesso necessarie disposizioni più dettagliate per ottenere la chiarezza necessaria a conciliare altri interessi legittimi. Ne sono due esempi la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*)[18] e la direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (*direttiva sulla conservazione dei dati,* invalidata il 8 aprile 2014)[19]. Altri esempi saranno discussi nel capitolo 8. Tali disposizioni devono essere in linea con la direttiva sulla protezione dei dati.

La Carta dei diritti fondamentali dell'Unione europea

I trattati originari delle Comunità europee non fanno riferimento ai diritti dell'uomo o alla loro protezione. Tuttavia, con il sopraggiungere di ricorsi per presunte violazioni dei diritti dell'uomo in aree rientranti nell'ambito di applicazione del diritto dell'UE, l'allora Corte di giustizia delle comunità europee (CG, ora CGUE) ha adottato

17 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2001, 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 (GU L 8 del 12.1.2001).

18 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*) (GU L 201 del 31.7.2002).

19 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (*direttiva sulla conservazione dei dati*) (GU L 105 del 13.4.2006), invalidata il 8 aprile 2014.

un nuovo approccio. Per garantire protezione agli individui, la Corte ha incluso i diritti fondamentali nei cosiddetti "principi generali" del diritto europeo che, secondo la stessa CGUE, rispecchiano il dettato della protezione dei diritti dell'uomo garantita dalle costituzioni nazionali e dai trattati sui diritti dell'uomo, in particolare la CEDU. La CGUE ha espresso il proprio impegno a garantire la conformità del diritto dell'UE a tali principi.

Consapevole delle eventuali ripercussioni delle proprie politiche in materia di diritti dell'uomo e nel tentativo di far sentire i cittadini "più vicini" all'Unione, nel 2000 l'UE ha proclamato la Carta dei diritti fondamentali dell'Unione europea (la Carta), che abbraccia l'intera serie dei diritti civili, politici, economici e sociali dei cittadini europei, sintetizzando le tradizioni costituzionali e gli obblighi internazionali comuni agli Stati membri. I diritti descritti nella Carta sono suddivisi in sei sezioni: dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia.

Pur trattandosi inizialmente solo di un documento politico, la Carta è divenuta giuridicamente vincolante[20] come diritto primario dell'UE (cfr. l'articolo 6, paragrafo 1, del TUE) con l'entrata in vigore del trattato di Lisbona il 1° dicembre 2009[21].

Il diritto primario dell'UE prevede anche che l'Unione sia generalmente competente a legiferare in materia di protezione dei dati (articolo 16 del TFUE).

La Carta non solo garantisce il rispetto della vita privata e della vita familiare (articolo 7), ma stabilisce anche il diritto alla protezione dei dati (articolo 8), innalzando esplicitamente il livello di tale protezione a quello di un diritto fondamentale nell'ambito del diritto dell'Unione. Le istituzioni dell'UE e gli Stati membri devono rispettare e garantire questo diritto, che vale anche per gli Stati membri nell'attuazione del diritto dell'Unione (articolo 51 della Carta). Formulato diversi anni dopo la direttiva sulla protezione dei dati, l'articolo 8 della Carta deve essere inteso come comprensivo del diritto dell'UE preesistente in materia di protezione dei dati. La Carta, dunque, non solo menziona esplicitamente, all'articolo 8, paragrafo 1, il diritto alla protezione dei dati, ma all'articolo 8, paragrafo 2, fa altresì riferimento ai principi fondamentali della protezione dei dati. Infine, l'articolo 8, paragrafo 3, della Carta garantisce che un'autorità indipendente controlli l'attuazione di questi principi.

20 UE (2012), Carta dei diritti fondamentali dell'Unione europea, GU C 326 del 26.10.2012.

21 Cfr. le versioni consolidate delle Comunità europee (2012), trattato sull'Unione europea, GU C 326 del 26.10.2012, e delle Comunità europee (2012), TFUE, GU C 326 del 26.10.2012.

Prospettiva

Nel gennaio 2012 la Commissione europea ha proposto un pacchetto di riforme sulla protezione dei dati, affermando l'esigenza di modernizzare le attuali norme in materia alla luce dei rapidi sviluppi tecnologici e della globalizzazione. Il pacchetto di riforme consiste in una proposta di regolamento generale sulla protezione dei dati[22], destinata a sostituire la direttiva sulla protezione dei dati, e in una nuova direttiva sulla protezione dei dati[23], che prevede la protezione dei dati nei settori della cooperazione giudiziaria e di polizia in materia penale. Al momento della pubblicazione del presente manuale, la discussione sul pacchetto di riforme era in corso.

1.2. Bilanciamento dei diritti

Punto saliente

- Il diritto alla protezione dei dati non è un diritto assoluto, ma deve essere contemperato con altri diritti.

Il diritto fondamentale alla protezione dei dati a carattere personale, ai sensi dell'articolo 8 della Carta, "non appare tuttavia come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale"[24]. L'articolo 52, paragrafo 1, della Carta riconosce che possano essere apportate limitazioni all'esercizio di diritti come quelli sanciti dagli articoli 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità d'interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[25].

22 Commissione europea (2012), *Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM(2012) 11 final, Bruxelles, 25 gennaio 2012.

23 Commissione europea (2012), *Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (direttiva generale sulla protezione dei dati)*, COM(2012) 10 final, Bruxelles, 25 gennaio 2012.

24 Cfr. per esempio, CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punto 48.

25 *Ibid.*, punto 50.

Nel sistema giuridico della CEDU la protezione dei dati è garantita dall'articolo 8 (il diritto al rispetto della vita privata e familiare) e, come nel sistema giuridico della Carta, questo diritto deve essere esercitato rispettando l'ambito di applicazione di altri diritti concorrenti. Ai sensi dell'articolo 8, paragrafo 2, della CEDU, "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 protezione dei diritti e delle libertà altrui".

Di conseguenza, sia la Corte EDU sia la CGUE hanno ripetutamente affermato che un esercizio di contemperamento con altri diritti è necessario in caso di applicazione e interpretazione dell'articolo 8 della CEDU e dell'articolo 8 della Carta[26]. Diversi esempi significativi illustrano come si perviene a tale contemperamento.

1.2.1. Libertà di espressione

Uno dei diritti che ci si attende possa entrare in conflitto con il diritto alla protezione dei dati è il diritto alla libertà di espressione.

La libertà di espressione è sancita dall'articolo 11 della Carta ("Libertà di espressione e d'informazione"). Tale diritto include la "libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera". L'articolo 11 corrisponde all'articolo 10 della CEDU. Ai sensi dell'articolo 52, paragrafo 3, della Carta, nella misura in cui prevede diritti corrispondenti a quelli garantiti dalla CEDU, "il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione". Le limitazioni che possono legittimamente essere imposte al diritto garantito dall'articolo 11 della Carta non possono pertanto andare oltre quelle previste all'articolo 10, paragrafo 2, della CEDU, vale a dire, devono essere previste dalla legge e devono essere necessarie in una società democratica "[...] alla protezione della reputazione o dei diritti altrui". Questo concetto si estende al diritto alla protezione dei dati.

26 Corte EDU, *Von Hannover c. Germania (n. 2)* [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012; CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, punto 48; CGUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 gennaio 2008, punto 68. Cfr. anche Consiglio d'Europa (2013), giurisprudenza della Corte europea dei diritti dell'uomo riguardante la protezione dei dati personali, giurisprudenza (2013) PD, disponibile all'indirizzo: http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_en.asp.

Il rapporto tra la protezione dei dati personali e la libertà di espressione è disciplinato dall'articolo 9 della direttiva sulla tutela dei dati, intitolato "Trattamento di dati personali e libertà d'espressione"[27], secondo il quale gli Stati membri sono chiamati a prevedere determinate deroghe o limitazioni alle disposizioni in materia di tutela dei dati, e quindi del diritto alla vita privata, previste nei capi II, IV e VI di detta direttiva. È consentito applicare tali deroghe esclusivamente per scopi giornalistici o di espressione artistica o letteraria, rientranti nel diritto fondamentale della libertà d'espressione, soltanto nei limiti in cui esse risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà d'espressione.

Esempio: nella causa *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*[28], la CGUE è stata chiamata a interpretare l'articolo 9 della direttiva sulla tutela dei dati e a definire la relazione tra protezione dei dati e libertà di stampa. La Corte ha dovuto esaminare la divulgazione, da parte di Markkinapörssi e Satamedia, dei dati fiscali di circa 1,2 milioni di persone fisiche legittimamente ottenuti dalle autorità fiscali finlandesi. In particolare, la Corte doveva verificare se il trattamento di dati personali, messi a disposizione dalle autorità fiscali, volto a consentire agli utenti di telefonia mobile di ricevere i dati fiscali relativi ad altre persone fisiche, dovesse essere considerato come un'attività esercitata esclusivamente a scopi giornalistici. Dopo aver concluso che le attività di Satakunnan consistevano in un "trattamento di dati personali" ai sensi dell'articolo 3, paragrafo 1, della direttiva sulla protezione dei dati, la Corte è poi passata all'interpretazione dell'articolo 9 della stessa direttiva, rilevando anzitutto l'importanza riconosciuta alla libertà di espressione in ogni società democratica e ribadendo la necessità di interpretare in senso ampio le nozioni a essa correlate, tra cui quella di giornalismo. La Corte ha poi osservato che, al fine di raggiungere un contemperamento tra i due diritti fondamentali, le deroghe e le limitazioni del diritto alla protezione dei dati devono applicarsi solo nella misura in cui esse siano strettamente necessarie. In tali circostanze, la Corte ha ritenuto che attività come quelle svolte da Markkinapörssi e Satamedia, relative ai dati provenienti da documenti che sono di dominio pubblico ai sensi della legislazione nazionale, possono essere qualificate come "attività giornalistiche" qualora siano dirette a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione utilizzato. La Corte ha anche stabilito che queste attività non sono riservate alle imprese operanti nel settore dei media e

27 Articolo 9 della direttiva sulla protezione dei dati.

28 CGUE, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*, 16 dicembre 2008, punti 56, 61 e 62.

possono essere connesse a uno scopo di lucro. Tuttavia, relativamente al caso di specie, la CGUE ha rimesso la valutazione in questione al giudice nazionale.

Per quanto riguarda la conciliazione del diritto alla protezione dei dati con il diritto alla libertà di espressione, la Corte EDU ha emesso diverse sentenze importanti.

Esempio: nella causa *Axel Springer AG c. Germania*[29], la Corte EDU ha considerato che il divieto imposto da un tribunale nazionale al responsabile di un giornale, che intendeva pubblicare un articolo sull'arresto e sulla condanna di un noto attore, costituisse una violazione dell'articolo 10 della CEDU. La Corte EDU ha ribadito i criteri stabiliti nella propria giurisprudenza in materia di contemperamento del diritto alla libertà di espressione con il diritto al rispetto della vita privata:

- in primo luogo, se il fatto pubblicato dall'articolo in questione rivesta un interesse generale: l'arresto e la condanna di una persona erano un fatto giudiziario pubblico e quindi d'interesse pubblico;
- in secondo luogo, se l'interessato sia un personaggio pubblico: la persona in questione era un attore sufficientemente noto per figurare quale personaggio pubblico;
- in terzo luogo, in che modo l'informazione sia stata ottenuta e se sia affidabile: l'informazione era stata fornita dall'ufficio della procura e l'esattezza delle informazioni contenute in entrambe le pubblicazioni non era oggetto di contenzioso tra le parti.

Pertanto, la Corte EDU ha stabilito che le restrizioni alla pubblicazione imposte al giornale non erano state ragionevolmente proporzionate rispetto allo scopo legittimo di proteggere la vita privata del ricorrente. La Corte ha concluso riscontrando una violazione dell'articolo 10 della CEDU.

Esempio: nella causa *Von Hannover c. Germania (n. 2)*[30], la Corte EDU non ha riscontrato alcuna violazione del diritto al rispetto della vita privata ai sensi dell'articolo 8 della CEDU quando alla principessa Carolina di Monaco è stato

29 Corte EDU, *Axel Springer AG c. Germania* [GC], n. 39954/08, 7 febbraio 2012, punti 90 e 91.

30 Corte EDU, *Von Hannover c. Germania (n. 2)* [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012, punti 118 e 124.

negato un provvedimento inibitorio contro la pubblicazione di una fotografia che ritraeva lei e il marito durante una vacanza sulla neve. La fotografia era corredata di un articolo che riportava, tra l'altro, le cattive condizioni di salute del principe Ranieri. La Corte EDU ha concluso che i tribunali nazionali avevano accuratamente conciliato il diritto delle case editrici alla libertà di espressione con il diritto al rispetto della vita privata dei ricorrenti. La qualificazione, da parte dei tribunali nazionali, della malattia del Principe Ranieri come un evento della società contemporanea non poteva essere ritenuta irragionevole e la Corte EDU ha potuto convenire che la fotografia, considerata alla luce di questo articolo, ha contribuito almeno in qualche misura a un dibattito d'interesse generale. La Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Nella giurisprudenza della Corte EDU, uno dei criteri fondamentali per quanto riguarda il contemperamento di questi diritti è quello di stabilire se la forma di espressione oggetto di valutazione contribuisca o meno a un dibattito d'interesse pubblico generale.

Esempio: nella causa *Mosley c. Regno Unito*[31], un settimanale nazionale ha pubblicato fotografie private del ricorrente. Questi ha addotto una violazione dell'articolo 8 della CEDU poiché non gli era stato possibile chiedere un provvedimento inibitorio prima della pubblicazione delle foto in questione, a causa della mancanza di un obbligo di notifica preliminare per il quotidiano in caso di pubblicazione di materiale che potesse violare il diritto alla vita privata. Sebbene la divulgazione di materiale di tale genere avesse generalmente finalità d'intrattenimento e non d'informazione, la stessa godeva indubbiamente della protezione prevista dall'articolo 10 della CEDU, sul quale possono prevalere gli interessi giuridici tutelati dall'articolo 8 della CEDU nel caso in cui l'informazione sia di natura intima e privata e la divulgazione sia priva di interesse pubblico. Tuttavia, particolare attenzione deve essere rivolta in sede di esame delle restrizioni che possono costituire una forma di censura prima della pubblicazione. Alla luce dell'eventuale effetto dissuasivo che insorgerebbe in caso di obbligo di notifica preliminare, dei dubbi sulla sua efficacia e dell'ampio margine di apprezzamento in questo ambito, la Corte EDU ha concluso che l'esistenza di un obbligo di notifica preliminare vincolante non era richiesta ai sensi dell'articolo 8. Di conseguenza, la Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8.

31 Corte EDU, *Mosley c. Regno Unito*, n. 48009/08, 10 maggio 2011, punti 129 e 130.

Esempio: nella causa *Biriuk c. Lituania*[32], la ricorrente ha chiesto il risarcimento del danno nei confronti di un quotidiano per la pubblicazione di un articolo che ne riportava la sieropositività. Tale informazione era stata presumibilmente confermata dai medici dell'ospedale locale. La Corte EDU ha ritenuto che l'articolo in questione non contribuisse ad alcun dibattito d'interesse generale e ha ribadito che la protezione dei dati personali, e non ultimo dei dati sanitari, è fondamentale affinché una persona possa godere del proprio diritto al rispetto della vita privata e familiare sancito dall'articolo 8 della CEDU. La Corte ha attribuito particolare rilievo al fatto che, secondo l'articolo del giornale, il personale medico di un ospedale avesse fornito informazioni sull'infezione da HIV della ricorrente in manifesta violazione dell'obbligo al segreto medico. Di conseguenza, lo Stato non era riuscito a garantire il diritto della ricorrente al rispetto della vita privata. La Corte ha concluso asserendo una violazione dell'articolo 8 della CEDU.

1.2.2. Accesso ai documenti

La libertà d'informazione ai sensi dell'articolo 11 della Carta e dell'articolo 10 della CEDU tutela non solo il diritto a trasmettere, ma anche a *ricevere* informazioni. Vi è una crescente consapevolezza dell'importanza della trasparenza a livello governativo per il funzionamento di una società democratica. Di conseguenza, negli ultimi due decenni, il diritto di accedere ai documenti in possesso delle autorità pubbliche è stato riconosciuto come un importante diritto di ogni cittadino dell'UE nonché di ogni persona fisica o giuridica che risieda o abbia sede legale in uno Stato membro.

Ai sensi del diritto del CDE è possibile fare riferimento ai principi contemplati nella Raccomandazione sull'accesso ai documenti ufficiali, che hanno ispirato i redattori della Convenzione sull'accesso ai documenti ufficiali (*Convenzione n. 205*)[33]. **Ai sensi del diritto dell'UE**, il diritto di accesso ai documenti è garantito dal regolamento n. 1049/2001 relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (*regolamento sull'accesso ai documenti*)[34]. L'articolo 42 della Carta e l'articolo 15, paragrafo 3, del TFUE hanno esteso tale diritto di accesso "ai documenti delle istituzioni, organi e organismi dell'Unione, a

32 Corte EDU, *Biriuk c Lituania*, n. 23373/03, 25 novembre 2008.

33 Consiglio d'Europa, Comitato dei ministri (2002), raccomandazione Rec(2002)2 agli Stati membri in materia di accesso ai documenti ufficiali, 21 febbraio 2002; Consiglio d'Europa, Convenzione sull'accesso ai documenti ufficiali, STCE n.°205, 18 giugno 2009. La Convenzione non è ancora entrata in vigore.

34 Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione, GU L 145 del 31.5.2001.

prescindere dal loro supporto". Ai sensi dell'articolo 52, paragrafo 2, della Carta, il diritto di accesso ai documenti è esercitato anche alle condizioni e nei limiti del disposto dell'articolo 15, paragrafo 3, del TFUE. Questo diritto può entrare in conflitto con il diritto alla protezione dei dati qualora l'accesso a un documento riveli dati personali altrui. Le istanze di accesso ai documenti o alle informazioni in possesso delle autorità pubbliche possono quindi richiedere uncontemperamento con il diritto alla protezione dei dati delle persone i cui dati sono contenuti nei documenti richiesti.

Esempio: nella causa *Commissione c. Bavarian Lager*[35], la CGUE ha definito la portata della protezione dei dati personali nel contesto dell'accesso ai documenti delle istituzioni dell'UE e secondo il rapporto tra i regolamenti n. 1049/2001 (*regolamento sull'accesso ai documenti*) e n. 45/2001 (*regolamento sulla protezione dei dati*). La società Bavarian Lager, fondata nel 1992, importa birra tedesca in bottiglia nel Regno Unito, principalmente per locali pubblici e bar. Tuttavia, la società riscontrava difficoltà perché la legislazione britannica favoriva di fatto i produttori nazionali. In risposta alla denuncia della Bavarian Lager, la Commissione europea ha deciso di avviare un procedimento contro il Regno Unito per mancato adempimento dei propri obblighi, che ha portato a modificare le disposizioni controverse e ad allinearle con il diritto dell'UE. La Bavarian Lager ha poi chiesto alla Commissione, fra gli altri documenti, una copia del verbale di una riunione cui avevano partecipato i rappresentanti della Commissione, le autorità britanniche e la *Confédération des Brasseurs du Marché Commun* (CBMC). La Commissione ha accettato di divulgare alcuni documenti relativi alla riunione, cancellando tuttavia cinque nomi che figuravano a verbale, ossia due persone che si erano esplicitamente opposte alla divulgazione della loro identità e altre tre che la Commissione non riusciva a contattare. Con decisione del 18 marzo 2004, la Commissione ha respinto una nuova domanda della Bavarian Lager volta a ottenere il verbale integrale della riunione, citando in particolare la protezione della vita privata delle persone, come garantito dal regolamento sulla protezione dei dati. Non soddisfatta di tale decisione, la Bavarian Lager ha proposto un ricorso dinanzi al Tribunale, che ha annullato la decisione della Commissione con sentenza dell'8 novembre 2007 (causa T-194/04, *Bavarian Lager c. Commissione*), considerando in particolare che l'inserimento dei soli nomi delle persone in questione nell'elenco di partecipanti alla riunione per conto dell'organismo che rappresentavano non costituisse pregiudizio alla vita privata né un pericolo per la vita privata di tali persone.

35 CGUE, C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd.*, 29 giugno 2010, punti 60, 63, 76, 78 e 79.

Su ricorso della Commissione, la CGUE ha annullato la sentenza del Tribunale di primo grado, statuendo che il regolamento sull'accesso ai documenti prevede "un regime specifico e rafforzato di tutela di una persona i cui dati personali possano, eventualmente, essere comunicati al pubblico". Secondo la CGUE, nel caso di una domanda fondata sul regolamento sull'accesso ai documenti che sia diretta a ottenere l'accesso a documenti contenenti dati personali, sono integralmente applicabili le disposizioni del regolamento sulla protezione dei dati. La CGUE ha concluso quindi che la Commissione aveva legittimamente respinto la domanda di accesso al verbale completo della riunione dell'ottobre 1996. In assenza del consenso dei cinque partecipanti a tale riunione, la Commissione, diffondendo una versione del documento controverso priva dei nomi in questione, aveva ottemperato sufficientemente al proprio obbligo di trasparenza.

Inoltre, secondo la CGUE, "dal momento che la Bavarian Lager non ha fornito alcuna motivazione espressa e legittima né alcun argomento convincente per dimostrare la necessità del trasferimento di questi dati personali, la Commissione non ha potuto soppesare i differenti interessi delle parti in causa. Essa non era neppure in grado di verificare se sussistevano ragioni per presumere che tale trasferimento avrebbe arrecato pregiudizio agli interessi legittimi delle persone coinvolte", come richiesto dal regolamento sulla protezione dei dati.

Secondo questa sentenza, l'ingerenza nel diritto alla protezione dei dati per quanto riguarda l'accesso ai documenti esige una ragione specifica e motivata. Il diritto di accesso ai documenti non può prevalere automaticamente sul diritto alla protezione dei dati[36].

Un aspetto particolare di una richiesta di accesso è stato affrontato nella sentenza della Corte EDU illustrata di seguito.

Esempio: nella causa *Társaság a Szabadságjogokért c. Ungheria*[37], la ricorrente, un'ONG per i diritti umani, aveva adito la Corte costituzionale richiedendo l'accesso a informazioni su una causa pendente. Senza consultare il membro del

36 Cfr., tuttavia, le deliberazioni dettagliate nel documento del Garante europeo della protezione dei dati (GEPD) (2011), *Public access to documents containing personal data after the Bavarian Lager ruling* (*Accesso pubblico a documenti contenenti dati personali dopo la sentenza Bavarian Lager*), Bruxelles, 24 marzo 2011, disponibile all'indirizzo: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

37 Corte EDU, *Társaság a Szabadságjogokért c. Ungheria*, n. 37374/05, 14 aprile 2009; cfr. punti 27 e 36–38.

parlamento che aveva presentato detta causa, la Corte Costituzionale ha respinto la richiesta di accesso adducendo che i ricorsi proposti innanzi alla Corte stessa potevano essere resi disponibili a terzi solo previa approvazione del ricorrente. I tribunali nazionali hanno accolto il diniego in ragione del fatto che altri interessi legittimi, compresa l'accessibilità alle informazioni pubbliche, non potevano prevalere sulla protezione dei dati personali. La ricorrente aveva agito come un "*watchdog* sociale", le cui attività sono meritevoli di una protezione simile a quelle della stampa. In relazione alla libertà di stampa, la Corte EDU ha coerentemente affermato il diritto del pubblico di ricevere informazioni d'interesse generale. Le informazioni richieste dalla ricorrente erano "pronte e disponibili" e non richiedevano alcuna raccolta di dati. In tali circostanze, lo Stato aveva l'obbligo di non ostacolare il flusso d'informazioni richieste dalla ricorrente. In sintesi, la Corte EDU ha ritenuto che gli ostacoli all'accesso alle informazioni d'interesse pubblico potessero scoraggiare gli operatori nei settori dei mezzi di comunicazione o affini dallo svolgere il loro ruolo cruciale di "*watchdog* pubblico". La Corte ha concluso asserendo una violazione dell'articolo 10 della CEDU.

Il diritto dell'UE stabilisce fermamente l'importanza della trasparenza, principio sancito dagli articoli 1 e 10 del TUE nonché dall'articolo 15, paragrafo 1, del TFUE[38]. Ai sensi del regolamento (CE) n. 1049/2001, considerando 2, la politica di trasparenza consente una migliore partecipazione dei cittadini al processo decisionale e garantisce una maggiore legittimità, efficienza e responsabilità dell'amministrazione nei confronti dei cittadini in un sistema democratico[39].

Seguendo questo ragionamento, il regolamento (CE) n. 1290/2005 del Consiglio relativo al finanziamento della politica agricola comune e il regolamento (CE) n. 259/2008 della Commissione recante modalità di applicazione del regolamento (CE) n. 1290/2005 richiedono la pubblicazione d'informazioni sui beneficiari di taluni fondi dell'UE nel settore agricolo e degli importi percepiti da ogni beneficiario[40]. La

38 UE (2012), Versioni consolidate del trattato sull'Unione europea e del TFUE, GU C 326 del 26.10.2012.

39 CGUE, C-41/00 P, *Interporc Im- und Export GmbH c. Commissione delle Comunità europee*, 6 marzo 2003, punto 39; e CGUE, C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd.*, 29 giugno 2010, punto 54.

40 Regolamento (CE) n. 1290/2005 del Consiglio, del 21 giugno 2005, relativo al finanziamento della politica agricola comune, GU L 209 dell'11.8.2005, e regolamento (CE) n. 259/2008 della Commissione, del 18 marzo 2008, recante modalità di applicazione del regolamento (CE) n. 1290/2005 del Consiglio per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR), GU L 76 del 19.3.2008.

pubblicazione dovrebbe contribuire al controllo pubblico sul corretto utilizzo dei fondi pubblici da parte dell'amministrazione. Tuttavia, la proporzionalità di questa pubblicazione è stata contestata da più beneficiari.

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[41], la CGUE ha dovuto giudicare in merito alla proporzionalità della pubblicazione, prevista dalla normativa dell'UE, del nome dei beneficiari delle sovvenzioni agricole dell'Unione e degli importi percepiti.

La Corte, pur rilevando che il diritto alla protezione dei dati non è assoluto, ha sostenuto che la pubblicazione su un sito Internet dei dati contenenti i nominativi dei beneficiari di due fondi per gli aiuti agricoli dell'UE e gli importi precisi percepiti costituisce un'ingerenza nella loro vita privata, in generale, e nella protezione dei dati personali, in particolare.

La Corte ha ritenuto che tali ingerenze con gli articoli 7 e 8 della Carta erano previste dalla legge e rispondevano a una finalità d'interesse generale riconosciuta dall'UE, comprendente segnatamente un rafforzamento della trasparenza sull'uso dei fondi dell'Unione. Tuttavia, la CGUE ha statuito che la pubblicazione dei nomi delle persone fisiche beneficiarie di aiuti agricoli dell'UE provenienti da questi due fondi e degli importi precisi percepiti costituiva una misura sproporzionata e non era giustificata in considerazione dell'articolo 52, paragrafo 1, della Carta. La Corte ha quindi dichiarato parzialmente nulla la legislazione dell'UE sulla pubblicazione delle informazioni relative ai beneficiari dei fondi agricoli europei.

1.2.3. Libertà delle arti e delle scienze

Un altro diritto da contemperare con il diritto al rispetto della vita privata e alla protezione dei dati è costituito dalla libertà delle arti e delle scienze, espressamente tutelata dall'articolo 13 della Carta. Questo diritto è desunto in primo luogo dal diritto alla libertà di pensiero e di espressione e deve essere esercitato alla luce dell'articolo 1 della Carta (Dignità umana). La Corte EDU ritiene che la libertà delle arti sia tutelata

41 CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punti 47–52, 58, 66–67, 75, 86 e 92.

dall'articolo 10 della CEDU[42], che autorizza l'applicazione di restrizioni alle quali può anche essere soggetto il diritto garantito dall'articolo 13 della Carta[43].

Esempio: nella causa *Vereinigung bildender Künstler c. Austria*[44], i giudici austriaci hanno vietato all'associazione ricorrente di continuare a esporre un dipinto contenente le foto delle teste di alcune personalità pubbliche ritratte in atti sessuali. Un parlamentare austriaco, la cui foto era stata utilizzata nel dipinto, ha intentato un'azione legale contro l'associazione ricorrente per ottenere un'ingiunzione che vietasse l'esposizione del dipinto. Il giudice nazionale ha emesso l'ingiunzione accogliendo la richiesta. La Corte EDU ha ribadito l'applicabilità dell'articolo 10 della CEDU alla comunicazione di idee che offendono, scioccano o preoccupano lo Stato o una fascia della popolazione, rilevando tuttavia che coloro che creano, eseguono, distribuiscono o espongono opere d'arte contribuiscono allo scambio di idee e opinioni e lo Stato ha l'obbligo di non interferire indebitamente sulla loro libertà di espressione. Poiché il dipinto era un collage in cui erano utilizzate foto che ritraevano solo le teste dei soggetti, i cui corpi erano stati dipinti in modo irrealistico ed esagerato senza voler ovviamente riflettere o alludere alla realtà, la Corte EDU ha dichiarato altresì che "difficilmente il dipinto potrebbe essere interpretato come un'opera volta a rappresentare i dettagli della vita privata del soggetto raffigurato; esso, piuttosto, illustrerebbe la sua attività di politico", aggiungendo inoltre che "in tale veste, il soggetto raffigurato doveva mostrare una maggiore tolleranza nei confronti della critica". Ponderando i diversi interessi in gioco, la Corte EDU ha rilevato che il divieto illimitato di un'ulteriore esposizione del dipinto era sproporzionato. La Corte ha concluso asserendo una violazione dell'articolo 10 della CEDU.

Relativamente alla scienza, il diritto europeo sulla protezione dei dati ne riconosce il grande valore per la società, riducendo pertanto la portata delle restrizioni generali all'utilizzo dei dati personali. Sia la direttiva sulla protezione dei dati sia la Convenzione n. 108 consentono la conservazione dei dati a fini di ricerca scientifica una volta che questi non siano più necessari allo scopo per il quale erano stati raccolti inizialmente. Inoltre, il successivo utilizzo dei dati personali per la ricerca scientifica non deve essere considerato un fine incompatibile. Al diritto nazionale è affidato il compito di sviluppare disposizioni più dettagliate, comprese le garanzie necessarie,

42 Corte EDU, *Müller e a. c. Svizzera*, n. 10737/84, 24 maggio 1988.

43 Spiegazioni relative alla Carta dei diritti fondamentali, GU C 303 del 14.12.2007.

44 Corte EDU, *Vereinigung bildender Künstler c. Austria*, n. 68345/01, 25 gennaio 2007; cfr., in particolare, punti 26 e 34.

per conciliare l'interesse per la ricerca scientifica e il diritto alla protezione dei dati (cfr. anche i paragrafi 3.3.3 e 8.4).

1.2.4. Protezione della proprietà

Il diritto alla protezione della proprietà è sancito dall'articolo 1 del primo Protocollo alla CEDU nonché dall'articolo 17, paragrafo 1, della Carta, mentre il paragrafo 2 dello stesso articolo menziona esplicitamente un aspetto importante del diritto alla proprietà, ossia la protezione della proprietà intellettuale. L'ordinamento giuridico dell'UE prevede diverse direttive volte all'effettiva tutela della proprietà intellettuale, in particolare i diritti d'autore. La proprietà intellettuale abbraccia non solo la proprietà letteraria e artistica, ma anche brevetti, marchi e diritti connessi.

Come chiarito dalla giurisprudenza della CGUE, la protezione del diritto fondamentale alla proprietà dev'essere conciliata con la protezione di altri diritti fondamentali, in particolare con il diritto alla protezione dei dati[45]. Si sono verificati casi in cui gli enti preposti alla protezione del diritto d'autore chiedevano ai fornitori di servizi Internet di rivelare l'identità degli utenti di piattaforme di condivisione di file online. Tali piattaforme spesso consentono agli utenti di Internet di scaricare brani musicali gratuitamente, anche se questi sono protetti dal diritto d'autore.

Esempio: la causa *Promusicae c. Telefónica de España*[46] verteva sul rifiuto di un fornitore spagnolo di servizi di accesso a Internet – la società Telefónica di rivelare a Promusicae, un'organizzazione senza fini di lucro di produttori musicali ed editori di registrazioni musicali e audiovisive, i dati personali di talune persone alle quali quest'ultima forniva servizi di accesso a Internet. Promusicae ha chiesto la comunicazione delle informazioni in modo da poter avviare un procedimento civile nei confronti delle persone che, a suo avviso, utilizzavano un programma di scambio di file che forniva accesso ai fonogrammi i cui diritti di sfruttamento erano detenuti dai membri di Promusicae.

Il giudice spagnolo ha rinviato la questione alla CGUE, chiedendo se tali dati personali dovessero essere comunicati, ai sensi del diritto dell'UE, nel contesto di un procedimento civile, al fine di garantire l'effettiva tutela del diritto d'autore. Il giudice ha richiamato le direttive 2000/31, 2001/29 e 2004/48, anche alla luce

45 Corte EDU, *Ashby Donald e a. c. Francia*, n. 36769/08, 10 gennaio 2013.

46 CGUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 gennaio 2008, punti 54 e 60.

degli articoli 17 e 47 della Carta. La Corte ha concluso che queste tre direttive, nonché la direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58), non ostano a che gli Stati membri stabiliscano l'obbligo di comunicare dati personali nel contesto di un procedimento civile, al fine di garantire la tutela effettiva del diritto d'autore.

La CGUE ha rilevato che il caso sollevava quindi la questione del necessario contemperamento degli obblighi connessi alla tutela di diversi diritti fondamentali, ossia del diritto al rispetto della vita privata con i diritti alla tutela della proprietà e a un ricorso effettivo.

La Corte ha concluso che "gli Stati membri sono tenuti, in occasione della trasposizione delle suddette direttive, a fondarsi su un'interpretazione di queste ultime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento di tali direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme alle dette direttive, ma anche provvedere a non fondarsi su un'interpretazione di esse che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità"[47].

47 *Ibid.*, punti 65 e 68; cfr. anche CGUE, C-360/10, *SABAM c. Netlog N.V.*, 16 febbraio 2012.

2

Terminologia della protezione dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Dati personali		
Direttiva sulla protezione dei dati, articolo 2, lettera a) CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010 CGUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 gennaio 2008	**Definizione giuridica**	Convenzione n. 108, articolo 2, lettera a) Corte EDU, *Bernh Larsen Holding AS e altri c. Norvegia*, n. 24117/08, 14 marzo 2013
Direttiva sulla protezione dei dati, articolo 8, paragrafo 1 CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Categorie particolari di dati personali (dati sensibili)**	Convenzione n. 108, articolo 6
Direttiva sulla protezione dei dati, articolo 6, paragrafo 1, lettera e)	**Dati anonimizzati e pseudonimizzati**	Convenzione n. 108, articolo 5, lettera e) Convenzione n. 108, rapporto esplicativo, articolo 42
Trattamento dei dati		
Direttiva sulla protezione dei dati, articolo 2, lettera b) CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Definizioni**	Convenzione n. 108, articolo 2, lettera c)

Utenti dei dati		
Direttiva sulla protezione dei dati, articolo 2, lettera d)	**Titolare del trattamento**	Convenzione n. 108, articolo 2, lettera d) Raccomandazione sulla profilazione, articolo 1, lettera g)*
Direttiva sulla protezione dei dati, articolo 2, lettera e) CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Responsabile del trattamento**	Raccomandazione sulla profilazione, articolo 1, lettera h)
Direttiva sulla protezione dei dati, articolo 2, lettera g)	**Destinatario**	Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 1
Direttiva sulla protezione dei dati, articolo 2, lettera f)	**Terzi**	
Consenso		
Direttiva sulla protezione dei dati, articolo 2, lettera h) CGUE, C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 maggio 2011	**Definizione e requisiti per un consenso valido**	Raccomandazione sui dati sanitari, articolo 6, e varie raccomandazioni successive

Nota: ***Consiglio d'Europa, Comitato dei ministri (2010), raccomandazione Rec(2010)13 agli Stati membri sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto della profilazione* (raccomandazione sulla profilazione)*, 23 novembre 2010.*

2.1. Dato personale

Punti salienti

- I dati personali sono tali se si riferiscono a una persona identificata o almeno identificabile (l'interessato).
- Una persona è identificabile se altre informazioni possono essere ottenute senza sforzi irragionevoli, consentendo l'identificazione dell'interessato.
- Per autenticazione s'intende il processo teso a verificare che una persona possiede una determinata identità e/o è autorizzata a svolgere determinate attività.
- Esistono categorie particolari di dati, i cosiddetti dati sensibili, elencati nella Convenzione n. 108 e nella direttiva sulla protezione dei dati, che richiedono una maggiore protezione e, pertanto, sono soggetti a un regime giuridico specifico.

- I dati sono anonimizzati quando non contengono più alcun mezzo identificativo, mentre sono pseudonimizzati se i mezzi identificativi sono criptati.
- A differenza dei dati anonimizzati, i dati pseudonimizzati sono dati personali.

2.1.1. Aspetti principali del concetto di dato personale

Nel quadro del diritto dell'UE e **del diritto del CDE**, i "dati personali" sono definiti come qualsiasi informazione concernente una persona fisica identificata o identificabile[48], ossia informazioni che riguardano una persona la cui identità è manifestamente chiara o può almeno essere accertata mediante l'ottenimento d'informazioni supplementari.

Con il trattamento di dati relativi a tale persona, quest'ultima viene definita "interessato".

La persona

Il diritto alla protezione dei dati si è sviluppato a partire dal diritto al rispetto della vita privata. Il concetto di vita privata si riferisce agli esseri umani. Le persone fisiche sono, dunque, i principali beneficiari della protezione dei dati. Inoltre, secondo il parere espresso dal Gruppo di lavoro articolo 29 per la protezione dei dati, solo le *persone viventi* sono protette dal diritto europeo in materia di protezione dei dati[49].

La giurisprudenza della Corte EDU relativa all'articolo 8 della CEDU evidenzia la possibile difficoltà di operare una netta separazione tra le questioni della vita privata e quelle della vita professionale[50].

Esempio: nella causa *Amann c. Svizzera*[51], le autorità hanno intercettato una telefonata d'affari destinata al ricorrente, sulla base della quale le autorità hanno avviato indagini e redatto una scheda relativa al ricorrente ai fini del fascicolo destinato a garantire la sicurezza nazionale. Anche se l'intercettazione riguardava una telefonata d'affari, la Corte EDU ha ritenuto che la conservazione

48 Direttiva sulla protezione dei dati, articolo 2, lettera a); Convenzione n. 108, articolo 2, lettera a).

49 Gruppo di lavoro articolo 29 (2007), *Parere 4/2007 sul concetto di dati personali,* WP 136, 20 giugno 2007, pag. 22.

50 Cfr. per esempio, Corte EDU, *Rotaru c. Romania* [GC], n. 28341/95, 4 maggio 2000, punto 43; Corte EDU, *Niemitz c. Germania*, n. 13710/88, 16 dicembre 1992, punto 29.

51 Corte EDU, *Amann c. Svizzera* [GC], n. 27798/95, 16 febbraio 2000, punto 65.

dei dati di tale chiamata fosse attinente alla vita privata del ricorrente e ha sottolineato che l'espressione "vita privata" non deve essere interpretata in senso restrittivo, in particolare dal momento che il rispetto della vita privata include il diritto d'instaurare e sviluppare relazioni con i propri simili. Inoltre, nessun motivo di principio consentiva di escludere le attività di natura professionale o commerciale dalla nozione di "vita privata". Questa interpretazione di ampio respiro rispondeva a quella della Convenzione n. 108. La Corte EDU ha constatato inoltre che l'ingerenza nel caso di specie non era conforme alla legge, in quanto il diritto nazionale non conteneva disposizioni specifiche e dettagliate sulla raccolta, la registrazione e la conservazione delle informazioni. Pertanto, la Corte EDU ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Inoltre, se anche le questioni legate alla vita professionale possono costituire oggetto di protezione dei dati, sembra legittimo chiedersi se la protezione possa essere garantita solo alle persone fisiche. I diritti ai sensi della CEDU sono garantiti non solo alle persone fisiche, bensì a tutti.

La giurisprudenza della Corte EDU contiene alcune sentenze riguardanti ricorsi presentati da persone giuridiche e vertenti sulla violazione del diritto alla protezione contro l'uso dei loro dati ai sensi dell'articolo 8 della CEDU. La Corte EDU, tuttavia, ha esaminato questi casi nell'ambito del diritto al rispetto del domicilio e della corrispondenza, anziché nella sfera della vita privata.

Esempio: la causa *Bernh Larsen Holding AS e altri c. Norvegia*[52] riguardava una denuncia presentata da tre società norvegesi in merito a una decisione dell'autorità fiscale che ordinava loro di fornire agli ispettori fiscali una copia di tutti i dati contenuti nel server del computer condiviso dalle tre società.

La Corte EDU ha rilevato che un tale obbligo per le società ricorrenti costituiva un'ingerenza nel loro diritto al rispetto del "domicilio" e della "corrispondenza" ai fini dell'articolo 8 della CEDU. Tuttavia, ha anche riscontrato che le autorità fiscali disponevano di garanzie efficaci e adeguate contro ogni abuso: le società ricorrenti avevano ricevuto un largo preavviso, erano presenti e in grado di formulare osservazioni durante l'intervento in loco e il materiale doveva essere distrutto una volta che l'ispezione fiscale fosse stata portata a termine. In tali

52 Corte EDU, *Bernh Larsen Holding AS e a. c. Norvegia*, n. 24117/08, 14 marzo 2013. Tuttavia, cfr. anche Corte EDU, *Liberty e a. c. Regno Unito*, n. 58243/00, 1 luglio 2008.

circostanze era stato conciliato, da un lato, il diritto delle società ricorrenti al rispetto del "domicilio" e della "corrispondenza" e il loro interesse a proteggere la vita privata delle persone che lavorano per loro e, dall'altro lato, l'interesse pubblico a garantire un'ispezione efficiente ai fini dell'accertamento fiscale. La Corte EDU ha statuito che non vi era stata quindi alcuna violazione dell'articolo 8 della CEDU.

Secondo la Convenzione n. 108, la protezione dei dati interessa, in primo luogo, la tutela delle persone fisiche; tuttavia, le parti contraenti possono estendere, nel rispettivo diritto nazionale, la protezione dei dati alle persone giuridiche, quali società e associazioni. **Il diritto dell'UE in materia di protezione dei dati** non contempla, in generale, la tutela delle persone giuridiche rispetto al trattamento dei dati che le riguardano. I legislatori nazionali godono di discrezionalità nel disciplinare tale materia[53].

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[54], la CGUE, riferendosi alla pubblicazione di dati personali relativi ai beneficiari di aiuti agricoli, ha considerato che "le persone giuridiche possono invocare la tutela degli artt. 7 e 8 della Carta nei confronti di una simile identificazione solamente qualora la ragione sociale della persona giuridica identifichi una o più persone fisiche. [...I]l rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta, [è] riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile[...]"[55].

Identificabilità di una persona

Secondo il diritto dell'UE nonché **quello del CDE**, le informazioni contengono dati riguardanti una persona se:

- un individuo è identificato sulla base di tali informazioni; o

53 Direttiva sulla tutela dei dati, considerando 24.

54 CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punto 53.

55 *Ibid*., punto 52.

- le informazioni descrivono un individuo, per quanto non identificato, in modo tale da consentire di svelare l'identità dell'interessato conducendo ulteriori ricerche.

Entrambi i tipi d'informazione sono tutelati in modo analogo dal diritto europeo in materia di protezione dei dati. La Corte EDU ha ripetutamente dichiarato che la nozione di "dati personali" ai sensi della CEDU equivale a quella contenuta nella Convenzione n. 108, in particolare per quanto riguarda il loro riferirsi a persone identificate o identificabili[56].

Le definizioni giuridiche di dato personale non chiariscono ulteriormente quando si debba considerare che una persona è identificata[57]. Evidentemente, l'identificazione richiede elementi che descrivano una persona in modo tale da poterla distinguere da qualsiasi altro soggetto e riconoscere come individuo. Il nome di una persona costituisce un ottimo esempio di tali elementi descrittivi. In casi eccezionali, altri mezzi identificativi possono avere una funzione simile a quella del nome. Per esempio, nel caso di una persona di rilievo pubblico, può essere sufficiente indicarne la qualifica, come "Presidente della Commissione europea".

> Esempio: nella causa *Promusicae*[58] la CGUE ha statuito che "[n]on è contestata neppure la circostanza che la comunicazione, richiesta dalla Promusicae, dei nominativi e degli indirizzi di taluni utilizzatori di [una certa piattaforma per lo scambio di file su Internet] implica la messa a disposizione di dati personali, ossia informazioni concernenti persone fisiche identificate o identificabili, in conformità alla definizione di cui all'art. 2, lett. a), della direttiva 95/46 [...]. Tale comunicazione di informazioni che, secondo la Promusicae, vengono archiviate dalla Telefónica – circostanza che quest'ultima non contesta – costituisce un trattamento di dati personali, ai sensi dell'art. 2, primo comma, della direttiva 2002/58, letto in combinato disposto con l'art. 2, lett. b), della direttiva 95/46".

Dal momento che molti nomi non sono univoci, nello stabilire l'identità di una persona possono essere necessari ulteriori mezzi identificativi per garantire che tale persona non venga confusa con altre. La data e il luogo di nascita sono mezzi

56 Cfr. Corte EDU, *Amann c. Svizzera* [GC], n. 27798/95, 16 febbraio 2000, punti 65 *et al.*

57 Cfr. anche Corte EDU, *Odièvre c. Francia* [GC], n. 42326/98, 13 febbraio 2003, e Corte EDU, *Godelli c. Italia*, n. 33783/09, 25 settembre 2012.

58 CGUE, C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 gennaio 2008, punto 45.

utilizzati frequentemente. In aggiunta, per distinguere meglio un cittadino da un altro, alcuni paesi hanno introdotto numeri personalizzati. I dati biometrici, come le impronte digitali, le foto digitali o le scansioni dell'iride, acquisiscono un'importanza sempre maggiore nell'identificazione delle persone nell'era tecnologica.

Ai fini dell'applicabilità del diritto europeo in materia di protezione dei dati, tuttavia, non è necessario raggiungere un elevato livello d'identificazione dell'interessato, ma è sufficiente che la persona sia identificabile. Una persona è considerata identificabile se un'informazione contiene elementi identificativi attraverso i quali la persona può essere identificata, direttamente o indirettamente[59]. In base al considerando 26 della direttiva sulla protezione dei dati, il parametro di riferimento consiste nel determinare la possibilità che mezzi identificativi ragionevoli siano a disposizione e siano gestiti dai potenziali utenti delle informazioni, compresi i destinatari terzi (cfr. il paragrafo 2.3.2).

Esempio: un'autorità locale, avendo deciso di raccogliere dati sulla velocità di percorrenza delle autovetture su strade locali, fotografa dette autovetture, registrando automaticamente l'ora e il luogo, al fine di trasmettere i dati all'autorità competente, cosicché quest'ultima possa elevare una contravvenzione a chi ha violato i limiti di velocità. Un interessato presenta un reclamo, sostenendo che il diritto in materia di protezione dei dati non prevede alcuna base giuridica che autorizzi l'autorità locale a raccogliere questo tipo di dati. L'autorità locale sostiene di non raccogliere dati personali in quanto, a suo avviso, le targhe sono dati relativi a persone anonime. L'autorità locale non avrebbe alcuna autorità giuridica per accedere al registro d'immatricolazione generale e scoprire l'identità del proprietario dell'autovettura o del suo conducente.

Questo ragionamento non è conforme al considerando 26 della direttiva sulla protezione dei dati. Poiché la finalità della raccolta dei dati è chiaramente quella d'identificare e multare i conducenti in eccesso di velocità, è prevedibile che si tenterà di procedere all'identificazione. Anche se non dispongono di un mezzo identificativo diretto, le autorità locali trasmettono i dati all'autorità competente, ossia le forze di polizia, che dispongono di tali mezzi. Il considerando 26 delinea inoltre esplicitamente uno scenario in cui è prevedibile che ulteriori destinatari dei dati, diversi dall'utente che utilizza immediatamente i dati, possano tentare d'identificare la persona. Alla luce del considerando 26, l'azione dell'autorità

59 Direttiva sulla protezione dei dati, articolo 2, lettera a).

locale equivale alla raccolta di dati su persone identificabili e, quindi, richiede una base giuridica ai sensi del diritto in materia di protezione dei dati.

Nell'ambito del diritto del CDE, l'identificabilità è intesa in modo simile. L'articolo 1, paragrafo 2, della Raccomandazione sui dati relativi ai pagamenti[60], per esempio, stabilisce che una persona non è considerata "identificabile" qualora tale identificazione richieda tempi, costi e attività irragionevoli.

Autenticazione

Si tratta di una procedura con cui una persona può dimostrare di possedere una determinata identità e/o è autorizzata a compiere determinate azioni, come accedere a una zona di sicurezza o prelevare denaro da un conto bancario. L'autenticazione può essere ottenuta mediante il confronto di dati biometrici, come per esempio una foto o le impronte digitali nel passaporto, con i dati della persona che si presenta, per esempio, al controllo dell'immigrazione, o mediante la richiesta d'informazioni che dovrebbero essere note solo alla persona che possiede una determinata identità o autorizzazione, per esempio un codice d'identificazione personale (PIN) o una password, o ancora richiedendo l'esibizione di un oggetto specifico, che dovrebbe essere in esclusivo possesso della persona che possiede una determinata identità o autorizzazione, come una tessera con microprocessore o una chiave per l'apertura di una cassetta di sicurezza bancaria. Oltre alla password e alle tessere con microprocessore, talvolta insieme ai PIN, le firme elettroniche sono uno strumento particolarmente idoneo a identificare e autenticare una persona nelle comunicazioni elettroniche.

Natura dei dati

Qualsiasi informazione può essere ritenuta un dato personale, a condizione che si riferisca a una persona.

Esempio: la valutazione di un supervisore in merito alle prestazioni lavorative di un dipendente, archiviata nel fascicolo personale del dipendente, costituisce un insieme di dati personali dello stesso dipendente, benché possa riflettere, in tutto o in parte, solo il parere personale del superiore, come per esempio: "il

60 CDE, Comitato dei ministri (1990), Raccomandazione n. R (90) 19 sulla protezione dei dati personali utilizzati a fini di pagamento e di altre operazioni connesse, 13 settembre 1990.

dipendente non si impegna nel lavoro" e non fatti concreti, quali: "il dipendente è stato assente per cinque settimane negli ultimi sei mesi".

I dati personali riguardano le informazioni sulla vita privata di una persona nonché quelle sulla sua vita professionale o pubblica.

Nella *causa Amann*[61], secondo l'interpretazione della Corte EDU, l'espressione "dati personali" non si limita alle questioni della sfera privata di un individuo (cfr. il paragrafo 2.1.1.). Questo significato attribuito all'espressione "dati personali" è rilevante anche per la direttiva sulla protezione dei dati.

Esempio: nella causa *Volker und Markus Schecke e Hartmut Eifert c. Land Hessen*[62], la CGUE ha statuito che «[...] è irrilevante la circostanza che i dati pubblicati attengano ad attività professionali [...]. La Corte europea dei diritti dell'uomo ha dichiarato, a tale proposito, con riguardo all'interpretazione dell'art. 8 della CEDU, che l'espressione "vita privata" non deve essere interpretata in modo restrittivo e che "nessun motivo di principio consente di escludere le attività professionali [...] dalla nozione di "vita privata"».

I dati riguardano le persone anche quando sono rivelati indirettamente dal contenuto delle informazioni su tale persona. In alcuni casi, in cui vi è uno stretto legame tra un oggetto o un evento – per esempio un telefono cellulare, un'autovettura, un incidente – da un lato e una persona – per esempio, il suo proprietario, un utente, una vittima – dall'altro, le informazioni relative a un oggetto o a un evento dovrebbero essere ugualmente considerate dati personali.

Esempio: nella causa *Uzun c. Germania*[63] il ricorrente e un secondo uomo sono stati posti sotto sorveglianza attraverso un sistema di posizionamento globale (GPS) installato nella vettura di quest'ultimo a causa del loro presunto coinvolgimento in attentati con uso di esplosivi. In questo caso, la Corte EDU ha dichiarato che la sorveglianza del ricorrente via GPS costituiva un'ingerenza nella sua vita privata nella misura in cui questa è tutelata dall'articolo 8 della CEDU. Tuttavia, la sorveglianza via GPS era conforme alla legge e proporzionata al fine legittimo

61 Cfr. Corte EDU, *Amann c. Svizzera*, n. 27798/95, 16 febbraio 2000, punto 65.

62 Cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punto 59.

63 Corte EDU, *Uzun c. Germania*, n. 35623/05, 2 settembre 2010.

di indagare diverse accuse di tentato omicidio e quindi necessaria in una società democratica. La Corte EDU ha statuito che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Formato dei dati

La forma in cui i dati personali sono conservati o utilizzati non è rilevante ai fini dell'applicabilità del diritto in materia di protezione dei dati. Le comunicazioni scritte o orali possono contenere dati personali e lo stesso vale per le immagini[64], compresi i filmati[65] o i suoni[66] rilevati da impianti televisivi a circuito chiuso (CCTV). Le informazioni registrate elettronicamente, come anche le informazioni in formato cartaceo, possono costituire dati personali; anche i campioni cellulari di tessuti umani possono costituire dati personali, dal momento che contengono il DNA di una persona.

2.1.2. Categorie particolari di dati personali

Ai sensi del diritto dell'UE e **del diritto del CDE**, esistono categorie particolari di dati personali che, per loro natura, possono presentare un rischio per gli interessati in fase di trattamento e pertanto devono godere di maggiore protezione. Il trattamento di queste categorie particolari di dati ("dati sensibili") deve essere dunque consentito solo con specifiche garanzie.

Sulla definizione di dati sensibili, sia la Convenzione n. 108 (articolo 6) sia la direttiva sulla protezione dei dati (articolo 8) elencano le seguenti categorie:

- dati personali che rivelano l'origine razziale o etnica;
- dati personali che rivelano le opinioni politiche, le convinzioni religiose o di altro tipo;
- dati personali relativi alla salute o alla vita sessuale.

64 Corte EDU, *Von Hannover c. Germania*, n. 59320/00, 24 giugno 2004; Corte EDU, *Sciacca c. Italia*, n. 50774/99, 11 gennaio 2005.

65 Corte EDU, *Peck c. Regno Unito*, n. 44647/98, 28 gennaio 2003; Corte EDU, *Köpke c. Germania*, n. 420/07, 5 ottobre 2010.

66 Direttiva sulla protezione dei dati, considerando 16 e 17; Corte EDU, *P.G. e J.H. c. Regno Unito*, n. 44787/98, 25 settembre 2001, punti 59 e 60; Corte EDU, *Wisse c. Francia*, n. 71611/01, 20 dicembre 2005.

Esempio: nella causa *Bodil Lindqvist*[67], la CGUE ha statuito che "l'indicazione che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisce un dato personale relativo alla salute ai sensi dell'art. 8, n. 1, della direttiva 95/46".

In aggiunta, fra i dati sensibili, la direttiva sulla protezione dei dati elenca anche l'"appartenenza sindacale", in quanto questa informazione può essere un forte indicatore di convinzioni o di appartenenza politiche.

La Convenzione n. 108 considera dati sensibili anche i dati personali relativi alle condanne penali.

Ai sensi dell'articolo 8, paragrafo 7, della direttiva sulla protezione dei dati, gli Stati membri dell'UE "determinano a quali condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento".

2.1.3. Dati anonimizzati e pseudonimizzati

Secondo il principio della conservazione di dati per un periodo di tempo limitato, contemplato dalla direttiva sulla protezione dei dati nonché dalla Convenzione n. 108 (e discusso in maniera più approfondita nel capitolo 3), i dati devono essere conservati "in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati"[68]. Di conseguenza, i dati dovrebbero essere anonimizzati qualora un titolare del trattamento volesse conservarli dopo che fossero divenuti obsoleti e non più utili al soddisfacimento dello scopo iniziale.

Dati anonimizzati

I dati sono anonimizzati se tutti gli elementi identificativi sono stati eliminati da un insieme di dati personali. Le informazioni non devono mantenere alcun elemento identificativo che, con un ragionevole sforzo, potrebbe servire a identificare

67 CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, punto 51.

68 Direttiva sulla protezione dei dati, articolo 6, paragrafo 1, lettera e); e Convenzione n. 108, articolo 5, lettera e).

nuovamente la persona o le persone interessate[69]. Una volta resi completamente anonimi, i dati non sono più ritenuti personali.

Se i dati personali non sono più utili al soddisfacimento dello scopo iniziale, ma devono essere conservati in forma personalizzata per motivi storici, statistici o scientifici, è possibile conservarli ai sensi della direttiva sulla protezione dei dati e della Convenzione n. 108, a condizione che siano applicate adeguate misure di garanzia contro eventuali abusi[70].

Dati pseudonimizzati

Le informazioni personali contengono elementi identificativi come nome, data di nascita, sesso e indirizzo. Quando le informazioni personali vengono pseudonimizzate, gli elementi identificativi sono sostituiti da uno pseudonimo, che si ottiene, per esempio, crittografando gli elementi identificativi contenuti nei dati personali.

I dati pseudonimizzati non sono esplicitamente menzionati nelle definizioni giuridiche della Convenzione n. 108 o nella direttiva sulla protezione dei dati. Tuttavia, l'articolo 42 del rapporto esplicativo alla Convenzione n. 108 stabilisce che "l'obbligo relativo ai termini per la conservazione dei dati in forma nominativa non significa che i dati debbano essere dopo qualche tempo irrevocabilmente separati dal nome della persona cui si riferiscono, ma soltanto che non dovrebbe essere possibile collegare facilmente i dati e gli elementi identificativi". Si tratta di un effetto che può essere ottenuto mascherando i dati mediante uno pseudonimo. Per chiunque non sia in possesso della chiave di decifratura, i dati pseudonimizzati sono identificabili con difficoltà; il collegamento a un'identità esiste ancora sotto forma di pseudonimo associato alla chiave di decifratura. Chi ha diritto a utilizzare la chiave di decifratura è in grado di risalire all'identità. Occorre prestare particolare attenzione onde evitare l'uso di chiavi crittografiche da parte di persone non autorizzate.

Dal momento che la pseudonimizzazione rappresenta uno degli strumenti più importanti per ottenere la protezione dei dati su larga scala, laddove non si possa evitare completamente l'uso di dati personali, occorre spiegarne la logica e l'effetto in modo più dettagliato.

69 *Ibid.*, considerando 26.

70 *Ibid.*, articolo 6, paragrafo 1, lettera e); e Convenzione n. 108, articolo 5, lettera e).

Esempio: la frase "Charles Spencer, nato il 3 aprile 1967 è padre di quattro figli, due maschi e due femmine" può essere pseudonimizzata come segue:

"C.S. 1967 è padre di quattro figli, due maschi e due femmine", o

"324 è padre di quattro figli, due maschi e due femmine", o

"YESz320l è padre di quattro figli, due maschi e due femmine".

Solitamente, gli utenti che accedono a questi dati pseudonimizzati non hanno alcuna possibilità d'identificare "Charles Spencer, nato il 3 aprile 1967" con "324" o "YESz3201". Pertanto è più probabile che i dati pseudonimizzati non siano esposti a un uso improprio.

Il primo esempio è tuttavia meno sicuro. Se la frase "C.S. 1967 è padre di quattro figli, due maschi e due femmine" è utilizzata nel paesino dove vive Charles Spencer, il signor Spencer può essere facilmente riconoscibile. Il metodo di pseudonimizzazione incide sull'efficacia della protezione dei dati.

Dati personali con elementi identificativi crittografati sono utilizzati in molti contesti per mantenere segreta l'identità delle persone. Ciò si rivela particolarmente utile quando i titolari del trattamento devono accertarsi che si tratti dello stesso interessato, ma non necessitano, o non dovrebbero disporre, delle identità reali degli interessati. È il caso, per esempio, di un ricercatore che studi il decorso di una malattia in pazienti la cui identità è nota solo alla struttura ospedaliera in cui questi sono trattati e dalla quale il ricercatore ottiene le anamnesi in versione pseudonimizzata. La pseudonimizzazione costituisce quindi una solida pratica nel novero delle tecnologie intese a migliorare la tutela della vita privata. Può fungere da elemento importante per realizzare la tutela della vita privata fin dalla progettazione, ossia per integrare la protezione dei dati nei sistemi avanzati di trattamento dei dati.

2.2. Trattamento di dati personali

Punti salienti

- Il termine "trattamento" si riferisce principalmente al trattamento automatizzato.
- Ai sensi del diritto dell'UE, il "trattamento" si riferisce anche al trattamento manuale negli archivi.
- Ai sensi del diritto del CDE, il diritto nazionale può estendere il significato di "trattamento" fino a includere il trattamento manuale.

La protezione dei dati in virtù della Convenzione n. 108 e della direttiva sulla protezione dei dati si concentra principalmente sul trattamento automatizzato di dati.

Ai sensi del **diritto del CDE**, la definizione di trattamento automatizzato riconosce, tuttavia, che tra le varie operazioni automatizzate vi possano essere alcune fasi in cui è richiesto il trattamento manuale dei dati personali. Parimenti, nell'ambito del **diritto dell'UE**, il trattamento automatizzato di dati è definito come il "trattamento di dati personali interamente o parzialmente automatizzato"[71].

Esempio: nella causa *Bodil Lindqvist*[72], la CGUE ha statuito che:

"l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un "trattamento di dati personali interamente o parzialmente automatizzato" ai sensi dell'art. 3, punto 1, della direttiva 95/46".

Anche il trattamento manuale di dati richiede la protezione dei dati.

La protezione dei dati **ai sensi del diritto dell'UE** non è in alcun modo limitata al trattamento automatizzato di dati. Pertanto, conformemente al diritto dell'Unione, la protezione dei dati si applica anche al trattamento di dati personali negli archivi

71 Convenzione n. 108, articolo 2, lettera c) e direttiva sulla protezione dei dati, articolo 2, lettera b), e articolo 3, paragrafo 1.

72 CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, punto 27.

manuali, ossia a fascicoli cartacei appositamente strutturati[73]. Vi sono due motivazioni principali per tale estensione dell'ambito della protezione dei dati:

- i fascicoli cartacei possono essere strutturati in modo tale che la ricerca d'informazioni sia resa semplice e rapida; e

- la conservazione di dati personali in fascicoli cartacei può costituire uno strumento utile a favorire l'elusione delle limitazioni che la legge prevede per il trattamento automatizzato di tali dati[74].

Nel quadro del diritto del CDE, la Convenzione n. 108 disciplina principalmente il trattamento di dati in archivi automatizzati[75]. Tuttavia, essa prevede la possibilità di estendere la protezione ai trattamenti manuali attraverso il diritto nazionale. Molte parti contraenti della Convenzione n. 108 si sono avvalse di questa possibilità e hanno indirizzato dichiarazioni in tal senso al segretario generale del CDE[76]. L'estensione della protezione dei dati nell'ambito di una siffatta dichiarazione deve riguardare tutti i trattamenti manuali dei dati e non può limitarsi al trattamento in archivi manuali[77].

Per quanto concerne la natura delle operazioni di trattamento previste, il concetto di trattamento è inteso in maniera ampia **nell'ambito del diritto sia dell'UE sia del CDE**: "(per) 'trattamento di dati personali' (si intende) [...] qualsiasi operazione [...], come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione"[78], compiuta sui dati personali. Il termine "trattamento" include anche le operazioni in cui i dati passano da un titolare del trattamento a un altro.

Esempio: i datori di lavoro raccolgono e trattano i dati riguardanti i dipendenti, compresi i profili retributivi. Il fondamento giuridico di tali operazioni è il contratto di lavoro.

73 Direttiva sulla tutela dei dati, articolo 3, paragrafo 1.

74 *Ibid*., considerando 27.

75 Convenzione n. 108, articolo 2, lettera b).

76 Cfr. le dichiarazioni formulate ai sensi della Convenzione n. 108, articolo 3, paragrafo 2, lettera c).

77 Cfr. la formulazione della Convenzione n. 108, articolo 3, paragrafo 2.

78 Direttiva sulla tutela dei dati, articolo 2, lettera b). Cfr. anche la Convenzione n. 108, articolo 2, lettera c).

I datori di lavoro devono trasmettere i dati sulle retribuzioni del proprio personale alle autorità fiscali. Questa trasmissione di dati è considerata ugualmente un "trattamento" ai sensi del termine utilizzato nella Convenzione n. 108 e nella direttiva sulla protezione dei dati. Tuttavia, in questo caso, il fondamento giuridico per tale divulgazione non è il contratto di lavoro. È necessario che sussista una base giuridica supplementare per le operazioni di trattamento che comportano il trasferimento dei dati sulle retribuzioni dal datore di lavoro alle autorità fiscali. Tale base giuridica è in genere contenuta nelle disposizioni delle leggi fiscali nazionali. In assenza di tali disposizioni, il trasferimento dei dati sarebbe un trattamento illecito.

2.3. Gli utenti dei dati personali

Punti salienti

- Chiunque decida di trattare dati personali altrui è un "titolare del trattamento" ai sensi del diritto in materia di protezione dei dati; se più persone prendono questa decisione congiuntamente, si parlerà di "cotitolari del trattamento".
- Un "responsabile del trattamento" è un'entità giuridicamente distinta che elabora dati personali per conto del titolare del trattamento.
- Un responsabile del trattamento diventa titolare del trattamento quando utilizza i dati per proprio conto, senza seguire le istruzioni di un titolare del trattamento.
- Chiunque riceva i dati da un titolare del trattamento è un "destinatario".
- Per "terzo" s'intende la persona fisica o giuridica che non opera in base a istruzioni del titolare del trattamento (e non è l'interessato).
- Un "destinatario terzo" è una persona o un'entità giuridicamente distinta dal titolare del trattamento, ma che riceve i dati personali dal titolare del trattamento.

2.3.1. Titolari del trattamento e responsabili del trattamento

La funzione di titolare o di responsabile del trattamento implica quale principale conseguenza la responsabilità giuridica dell'ottemperanza ai rispettivi obblighi previsti dal diritto in materia di protezione dei dati. Solo chi può risponderne ai sensi della legge applicabile può quindi assumere queste funzioni. Nel settore privato questa

responsabilità grava di solito su una persona fisica o giuridica, mentre nel settore pubblico spetta generalmente a un'autorità. Altri soggetti, come gli organismi o gli istituti privi di personalità giuridica, possono essere titolari del trattamento o responsabili del trattamento solo se ciò è previsto da disposizioni specifiche.

Esempio: quando la divisione marketing operante in seno alla società Sunshine prevede di trattare i dati per uno studio di mercato, il titolare del trattamento sarà la società Sunshine e non la divisione in questione. In questo caso, la divisione marketing non può essere il titolare del trattamento, essendo priva di personalità giuridica distinta.

Per quanto concerne i gruppi di società, la società madre e ogni controllata, essendo persone giuridiche distinte, sono considerate come distinti titolari o responsabili del trattamento. A causa di questo status giuridicamente distinto, il trasferimento di dati tra i membri di un gruppo di società dovrà fondarsi su una base giuridica specifica. Non esiste alcuna prerogativa che di per sé consenta lo scambio di dati personali tra le entità giuridiche distinte facenti parte di un gruppo di società.

In tale contesto è opportuno menzionare il ruolo dei privati. **Ai sensi del diritto dell'UE**, i privati, nel trattare i dati relativi ad altri per l'esercizio di attività a carattere esclusivamente personale o domestico, non rientrano nell'ambito di applicazione della direttiva sulla protezione dei dati; pertanto, non sono considerati titolari del trattamento[79].

Tuttavia, la giurisprudenza ha rilevato che il diritto in materia di protezione dei dati trova comunque applicazione quando un soggetto privato, utilizzando Internet, pubblica dati relativi ad altri.

Esempio: nella causa *Bodil Lindqvist*[80] la CGUE ha statuito che:

«l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi [...], costituisce un "trattamento di dati personali interamente o parzialmente automatizzato" ai sensi dell'art. 3, n. 1, della direttiva 95/46»[81].

79 Direttiva sulla tutela dei dati, considerando 12 e articolo 3, paragrafo 2, ultimo trattino.

80 CGUE, C-101/01, *Lindqvist*, 6 novembre 2003.

81 *Ibid.*, punto 27.

Tale trattamento di dati personali non rientra fra le attività a carattere strettamente personale o domestico, che esulano dall'ambito di applicazione della direttiva sulla protezione dei dati, dal momento che tale eccezione "deve [...] interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone"[82].

Titolare del trattamento

Ai sensi del diritto dell'UE, un titolare del trattamento è colui che "da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali"[83]. Il titolare del trattamento decide il motivo e la modalità del trattamento. **Ai sensi del diritto del CDE**, la definizione di titolare del trattamento stabilisce, inoltre, che un titolare del trattamento decide quali categorie di dati personali debbano essere registrate[84].

Nella definizione di titolare del trattamento la Convenzione n. 108 fa riferimento a un ulteriore aspetto della titolarità del trattamento che merita considerazione, ossia alla questione di chi sia legittimato a trattare determinati dati per una determinata finalità. Tuttavia, qualora abbiano luogo operazioni di trattamento asseritamente illecite e debba essere individuato il titolare del trattamento che ne risponde, detto titolare sarà la persona fisica o giuridica, ad esempio una società o un'autorità, che ha deciso di procedere al trattamento dei dati, indipendentemente dal fatto che tale persona fosse legittimamente autorizzata o meno a trattarli[85]. La richiesta di cancellazione deve quindi essere sempre indirizzata al titolare "effettivo" del trattamento.

Cotitolarità

La definizione di titolare del trattamento nella direttiva sulla protezione dei dati prevede anche la possibile esistenza di diverse entità giuridicamente distinte che da sole o insieme ad altre agiscono come titolari del trattamento. Ciò significa che esse

82 *Ibid.*, punto 47.

83 Direttiva sulla protezione dei dati, articolo 2, lettera d).

84 Convenzione n. 108, articolo 2, lettera d).

85 Cfr. anche Gruppo di lavoro "articolo 29" (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 15.

decidono congiuntamente di trattare i dati per una finalità comune[86]. Questo è giuridicamente possibile, tuttavia, solo qualora una base giuridica specifica preveda il trattamento congiunto dei dati per una finalità comune.

Esempio: una banca dati riguardante i clienti insolventi, gestita congiuntamente da diversi istituti di credito, è un esempio tipico di cotitolarità. Quando un soggetto presenta una richiesta relativa all'apertura di una linea di credito presso una banca che condivide la titolarità del trattamento, le banche controllano le informazioni presenti nella banca dati per prendere decisioni informate sulla solvibilità del richiedente.

Le norme non indicano espressamente se la cotitolarità necessiti che la finalità comune sia la stessa per ognuno dei titolari del trattamento o se sia sufficiente la parziale corrispondenza delle rispettive finalità. Tuttavia, a livello europeo non vi è ancora giurisprudenza in materia né sono chiare le conseguenze in termini di responsabilità. Il Gruppo di lavoro articolo 29 sostiene un'interpretazione più ampia del concetto di cotitolarità allo scopo di permettere una certa flessibilità che tenga conto della crescente complessità degli odierni trattamenti dei dati[87]. Un caso relativo alla Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT) illustra la posizione assunta dal suddetto Gruppo di lavoro.

Esempio: nel cosiddetto caso SWIFT, gli istituti bancari europei ricorrevano alla SWIFT, inizialmente quale responsabile del trattamento, per operazioni inerenti al trasferimento di dati nel corso di operazioni bancarie. La SWIFT comunicava tali dati sulle operazioni bancarie, conservati in un centro di assistenza informatica negli Stati Uniti, al dipartimento del Tesoro, senza ricevere istruzioni esplicite in tal senso da parte degli istituti bancari europei che usufruivano dei suoi servizi. Il Gruppo di lavoro articolo 29, nel valutare la legittimità di questa fattispecie, giungeva alla conclusione che gli istituti bancari europei che si avvalevano dei servizi della SWIFT e la stessa SWIFT dovevano essere considerati cotitolari responsabili nei confronti dei clienti europei per la divulgazione dei loro dati alle autorità statunitensi[88]. La SWIFT, decidendo in merito alla divulgazione, aveva

86 Direttiva sulla protezione dei dati, articolo 2, lettera d).

87 Gruppo di lavoro articolo 29 (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 20.

88 Gruppo di lavoro articolo 29 (2006), *Parere 10/2006 sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT)*, WP 128, Bruxelles, 22 novembre 2006.

assunto – illecitamente – il ruolo di titolare del trattamento; gli istituti bancari erano evidentemente in difetto circa il loro obbligo di vigilare sul responsabile del trattamento e, pertanto, non potevano essere completamente assolti dalle proprie responsabilità in quanto titolari del trattamento. La configurazione di fatto genera una situazione di cotitolarità.

Responsabile del trattamento

Ai sensi del diritto dell'UE, si definisce responsabile del trattamento il soggetto che elabora dati personali per conto del titolare del trattamento[89]. Le attività affidate a un responsabile del trattamento possono essere limitate a un compito o a un contesto molto specifico o possono essere molto generali, abbracciando molti aspetti.

Ai sensi del diritto del CDE, il significato attribuito alla funzione di responsabile del trattamento è identico a quello previsto dal diritto dell'UE.

Oltre a elaborare dati per conto di altri soggetti, i responsabili del trattamento saranno anche, di diritto, titolari con riguardo ai trattamenti svolti per proprio conto, ad esempio per la gestione dei propri dipendenti, l'amministrazione delle vendite e la tenuta della contabilità.

Esempio: la società Everready è specializzata nel trattamento di dati per la gestione delle risorse umane per conto di altre aziende. In questa funzione, Everready è responsabile del trattamento.

Tuttavia, quando tratta i dati dei propri dipendenti, Everready è il titolare delle operazioni di trattamento dei dati, che svolge per adempiere i propri obblighi di datore di lavoro.

Il rapporto tra titolare e responsabile del trattamento

Come visto in precedenza, il titolare del trattamento è definito come colui che determina le finalità e gli strumenti del trattamento.

Esempio: il direttore della società Sunshine decide che la società Moonlight, specializzata in analisi di mercato, deve condurre un'analisi di mercato sui dati

89 Direttiva sulla protezione dei dati, articolo 2, lettera e).

dei clienti di Sunshine. Anche se il compito di determinare gli strumenti del trattamento sarà quindi delegato a Moonlight, la società Sunshine resta il titolare del trattamento e Moonlight è solo un responsabile del trattamento in quanto, secondo il contratto, Moonlight può utilizzare i dati dei clienti della società Sunshine solo per le finalità definite da Sunshine.

Se il potere di determinare gli strumenti del trattamento è delegato a un responsabile, il titolare del trattamento deve comunque poter avere voce in capitolo nelle decisioni del responsabile relative a tali strumenti. La responsabilità generale spetta ancora al titolare, che deve sorvegliare i responsabili del trattamento onde garantire che le loro decisioni siano conformi al diritto in materia di protezione dei dati. Un contratto che vieti al titolare del trattamento d'interferire con le decisioni del responsabile sarebbe, dunque, interpretato probabilmente come tale da generare una situazione di cotitolarità, in cui entrambe le parti condividono la responsabilità giuridica che spetta ad ogni titolare di trattamento.

Inoltre, se un responsabile del trattamento non rispetta i limiti di utilizzo dei dati come prescritto dal titolare del trattamento, detto responsabile diventa titolare del trattamento, almeno nella misura in cui non si è attenuto alle istruzioni del titolare. Molto probabilmente tale situazione trasforma il responsabile in un titolare di trattamento che agisce in maniera illecita. A sua volta, il titolare originario dovrà spiegare come sia stato possibile che il responsabile del trattamento sia venuto meno al suo mandato. Infatti, il Gruppo di lavoro articolo 29 tende a presupporre che in questi casi si realizzi una situazione di cotitolarità, poiché quest'ultima tutela in modo ottimale gli interessi degli interessati[90]. Una conseguenza importante della cotitolarità dovrebbe essere l'esistenza dei presupposti per una responsabilità in solido in caso di danni, tale da offrire agli interessati una serie di mezzi di ricorso più ampia.

Un'altra possibile problematica riguarda la ripartizione della responsabilità qualora il titolare del trattamento sia una piccola impresa e il responsabile una grande azienda in grado di dettare le condizioni dei propri servizi. Tuttavia, il Gruppo di lavoro articolo 29 afferma che in casi del genere il livello di responsabilità non dovrebbe ridursi

90 Gruppo di lavoro articolo 29 (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 25; e Gruppo di lavoro articolo 29 (2006), *Parere 10/2006 sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT)*, WP 128, Bruxelles, 22 novembre 2006.

sulla base della sperequazione economica, e che occorre attenersi all'interpretazione del concetto di titolare del trattamento[91].

Per motivi di chiarezza e trasparenza, i dettagli del rapporto tra un titolare del trattamento e un responsabile del trattamento dovrebbero essere disciplinati da un contratto scritto[92]. La mancata stipula di tale contratto costituisce una violazione dell'obbligo del titolare del trattamento di fornire una documentazione scritta delle responsabilità reciproche e potrebbe dar luogo a sanzioni[93].

I responsabili del trattamento potrebbero voler delegare alcuni compiti ad altri responsabili di secondo livello. Ciò è giuridicamente possibile e dipenderà in particolare dalle clausole contrattuali tra il titolare del trattamento e il responsabile del trattamento, anche rispetto all'eventuale necessità dell'autorizzazione del titolare in ogni singolo caso ovvero di una semplice informativa data a quest'ultimo.

Ai sensi del diritto del CDE, è pienamente applicabile l'interpretazione dei concetti di titolare del trattamento e responsabile del trattamento illustrati in precedenza, come dimostrano le raccomandazioni elaborate conformemente alla Convenzione n. 108[94].

2.3.2. Destinatari e terzi

La differenza tra queste due categorie di persone o entità introdotte dalla direttiva sulla protezione dei dati risiede principalmente nel loro rapporto con il titolare del trattamento e, di conseguenza, nel tipo di autorizzazione loro conferita ai fini dell'accesso ai dati personali in possesso di detto titolare del trattamento.

Un "terzo" è un soggetto giuridicamente diverso dal titolare del trattamento. Per la divulgazione dei dati a terzi sarà quindi sempre necessaria una base giuridica specifica. Ai sensi dell'articolo 2, lettera f), della direttiva sulla protezione dei dati, un terzo è "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta". Pertanto, le persone che lavorano in un'altra impresa giuridicamente

91 Gruppo di lavoro articolo 29 (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 26.

92 Direttiva sulla protezione dei dati, articolo 17, paragrafi 3 e 4.

93 Gruppo di lavoro articolo 29 (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 28.

94 Cfr., per esempio, la raccomandazione sulla profilazione, articolo 1.

distinta dal titolare del trattamento, anche se facente parte di uno stesso gruppo o holding, saranno (o faranno parte di) "terzi". Per contro, le succursali di una banca che trattano dati contabili della clientela sotto l'autorità diretta della sede centrale non dovrebbero essere considerate come "terzi"[95].

Il termine "destinatario" è più ampio rispetto a quello di "terzi". Ai sensi dell'articolo 2, lettera g), della direttiva sulla protezione dei dati, un destinatario è "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati, che si tratti o meno di un terzo". Il destinatario può essere una persona esterna al titolare o al responsabile del trattamento – in tal caso sarebbe un terzo – o qualcuno interno al titolare o al responsabile del trattamento, come per esempio un dipendente o un altro reparto all'interno di un'azienda o autorità.

La distinzione tra destinatari e terzi è importante solo in ragione delle condizioni previste per la legittima divulgazione dei dati. I dipendenti di un titolare o di un responsabile del trattamento possono essere, senza ulteriore obbligo giuridico, destinatari dei dati personali se prendono parte alle operazioni di trattamento del titolare o del responsabile. Per contro, un terzo, essendo giuridicamente distinto dal titolare o dal responsabile del trattamento, non è autorizzato a utilizzare i dati personali trattati dal titolare del trattamento, salvespecifiche motivazioni giuridiche nel contesto di un caso particolare. I "destinatari terzi" di dati, quindi, dovranno essere sempre legittimati da una base giuridica per poter ricevere lecitamente i dati personali.

Esempio: il dipendente di un responsabile del trattamento, che utilizza i dati personali nell'ambito dei compiti affidatigli dal datore di lavoro, è un destinatario dei dati, ma non un terzo, dal momento che utilizza i dati in nome e dietro istruzioni di detto responsabile del trattamento.

Se, tuttavia, lo stesso dipendente decide di utilizzare i dati, cui è in grado di accedere come dipendente del responsabile del trattamento, per i propri scopi e li vende a un'altra società, in tal caso il dipendente ha agito come terzo, non eseguendo più gli ordini del responsabile del trattamento (datore di lavoro). In quanto terzo, il dipendente avrebbe bisogno di una base giuridica per l'acquisizione e la vendita dei dati. In questo esempio, il dipendente non dispone certamente di tale base giuridica; pertanto, le sue attività sono illegali.

95 Gruppo di lavoro articolo 29 (2010), *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, WP 169, Bruxelles, 16 febbraio 2010, pag. 31.

2.4. Consenso

Punti salienti

- Il consenso come base giuridica per il trattamento dei dati personali deve essere libero, informato e specifico.
- Il consenso deve essere dato in modo inequivocabile; può essere dato esplicitamente o implicitamente, agendo in modo tale da non lasciare adito a dubbi sul fatto che l'interessato acconsente al trattamento dei propri dati.
- Il trattamento di dati sensibili sulla base del consenso richiede il consenso esplicito.
- Il consenso può essere ritirato in qualsiasi momento.

Per consenso s'intende "qualsiasi manifestazione di volontà libera, specifica e informata con la quale" l'interessato "accetta che i dati personali che la riguardano siano oggetto di un trattamento"[96]. È, in numerosi casi, la base giuridica per il trattamento legittimo di dati (cfr. il paragrafo 4.1).

2.4.1. Gli elementi necessari ai fini della validità del consenso

Il diritto dell'Unione prevede, affinché il consenso sia valido, tre elementi diretti a garantire che gli interessati intendano realmente acconsentire all'uso dei loro dati:

- l'interessato non deve aver ricevuto pressioni al momento di concedere il consenso;
- l'interessato deve essere stato debitamente informato circa l'oggetto e le conseguenze del proprio consenso;
- l'ambito del consenso deve essere ragionevolmente concreto.

Solo se tutti questi requisiti sono soddisfatti il consenso sarà valido ai sensi del diritto in materia di protezione dei dati.

96 Direttiva sulla tutela dei dati, articolo 2, lettera h).

La Convenzione n. 108 non contiene una definizione di consenso, che è lasciata alla competenza del diritto nazionale. Tuttavia, **ai sensi diritto del CDE**, gli elementi necessari perché il consenso sia valido corrispondono a quelli illustrati in precedenza, così come previsto dalle raccomandazioni sviluppate in conformità della Convenzione n. 108[97]. I requisiti per il consenso sono analoghi a quelli di una dichiarazione d'intenti valida ai sensi del diritto civile europeo.

Ulteriori requisiti previsti dal diritto civile per la validità del consenso, come la capacità giuridica, si applicano ovviamente anche nel contesto della protezione dei dati, in quanto tali requisiti sono presupposti giuridici fondamentali. Il consenso non valido, in quanto accordato da persone prive di capacità giuridica, si tradurrà nell'assenza di una base giuridica per il trattamento dei dati di tali persone.

Il consenso può essere dato in modo esplicito[98] o in modo non esplicito. Il primo non lascia dubbi circa le intenzioni dell'interessato e può essere espresso oralmente o per iscritto; il secondo è desunto dalle circostanze. Ogni consenso deve essere manifestato in maniera inequivocabile[99]. Ciò significa che non dovrebbe esserci alcun ragionevole dubbio sul fatto che l'interessato abbia voluto comunicare il proprio consenso al trattamento dei dati che lo riguardano. Per esempio, desumere il consenso dalla semplice inerzia non può costituire una manifestazione di consenso inequivocabile. Qualora i dati da trattare siano sensibili, il consenso esplicito è obbligatorio e deve essere inequivocabile.

Consenso libero

Il consenso può definirsi validamente libero "soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso"[100].

Esempio: in molti aeroporti, i passeggeri devono passare attraverso body scanner per poter accedere all'area d'imbarco[101]. Considerando che i dati dei

97 Cfr., per esempio, la Convenzione n. 108, raccomandazione sui dati statistici, punto 6.

98 Direttiva sulla protezione dei dati, articolo 8, paragrafo 2.

99 *Ibid.*, articolo 7, lettera a) e articolo 26, paragrafo 1.

100 Gruppo di lavoro articolo 29, *Parere 15/2011 sulla definizione di consenso*, WP 187, Bruxelles, 13 luglio 2011, pag. 14.

101 Questo esempio è tratto da *Ibid.*, pag. 18.

passeggeri sono trattati al momento in cui avviene la scansione, il trattamento deve essere conforme a uno dei motivi di liceità di cui all'articolo 7 della direttiva sulla tutela dei dati (cfr. il paragrafo 4.1.1). Talvolta la scansione con il body scanner è presentata ai passeggeri come un'opzione, con la quale si implica che il consenso accordato giustifica il trattamento. Tuttavia, i passeggeri potrebbero temere che un eventuale rifiuto di sottoporsi alla scansione potrebbe creare sospetti o far scattare controlli supplementari, tra i quali una perquisizione personale. Molti passeggeri acconsentono alla scansione per evitare, così facendo, potenziali problemi o ritardi. Si può ipotizzare che il consenso così espresso non rappresenti una manifestazione sufficientemente libera di volontà.

Pertanto, una valida base per la legittimazione può essere rinvenuta solo in un atto del legislatore, conformemente all'articolo 7, lettera e) della direttiva sulla tutela dei dati, risultante nell'obbligo a collaborare posto in capo ai passeggeri a causa dell'interesse pubblico prevalente. Tale legislazione potrebbe comunque prevedere la possibilità di scegliere tra la scansione e il controllo manuale, ma soltanto nell'ambito di misure aggiuntive di controllo di frontiera in circostanze eccezionali, come stabilito dalla Commissione europea nei due regolamenti riguardanti gli scanner di sicurezza nel 2011[102].

La libertà del consenso potrebbe anche essere pregiudicata in situazioni di subordinazione in cui vi è un significativo squilibrio economico o di altro tipo tra il titolare del trattamento che acquisisce il consenso e l'interessato che lo fornisce[103].

Esempio: una grande società prevede di creare un repertorio contenente i nomi di tutti i dipendenti, la loro funzione in seno alla società e i loro indirizzi aziendali, esclusivamente per migliorare le comunicazioni interne. Il responsabile del personale propone di aggiungere una foto di ciascun dipendente al repertorio, per esempio per rendere più facile il riconoscimento dei colleghi durante le riunioni.

102 Regolamento (UE) n. 1141/2011 della Commissione, del 10 novembre 2011, recante modifica del regolamento (CE) n. 272/2009 che integra le norme fondamentali comuni in materia di sicurezza dell'aviazione civile sull'impiego degli scanner di sicurezza (security scanner) negli aeroporti dell'Unione europea, GU L 293 del 2011, e regolamento di esecuzione (UE) n. 1147/2011 della Commissione, dell'11 novembre 2011, recante modifica del regolamento (UE) n. 185/2010 che dà esecuzione alle norme fondamentali comuni in materia di sicurezza dell'aviazione civile sull'impiego degli scanner di sicurezza (security scanner) negli aeroporti dell'Unione europea, GU L 294 del 2011.

103 Cfr. anche Gruppo di lavoro articolo 29 (2001), *Parere 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione*, WP 48, Bruxelles, 13 settembre 2001; e Gruppo di lavoro articolo 29 (2005), Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995, WP 114, Bruxelles, 25 novembre 2005.

I rappresentanti dei dipendenti chiedono che ciò avvenga soltanto con il consenso di ciascun dipendente.

In questo caso, il consenso di un dipendente deve essere riconosciuto come la base giuridica per il trattamento delle foto nel repertorio perché è palese che far pubblicare una foto in tale repertorio non ha conseguenze negative in sé e, inoltre, è credibile che il dipendente non debba andare incontro a ripercussioni negative su iniziativa del datore di lavoro se detto dipendente non desidera che la sua foto sia pubblicata nel repertorio.

Ciò non significa, tuttavia, che il consenso non possa mai essere valido in circostanze in cui il mancato consenso avrebbe conseguenze negative. Se, per esempio, il mancato consenso a ricevere la carta clienti di un supermercato ha come conseguenza solo il fatto di non ottenere riduzioni dei prezzi di determinati prodotti, il consenso è comunque una valida base giuridica per il trattamento dei dati personali di quei clienti che hanno acconsentito ad avere tale carta. Non vi è alcuna situazione di subordinazione tra azienda e cliente e le conseguenze del mancato consenso non sono per l'interessato abbastanza gravi da impedire la libera scelta.

D'altra parte, quando prodotti o servizi sufficientemente importanti possono essere ottenuti solo ed esclusivamente se alcuni dati personali sono comunicati a terzi, il consenso dell'interessato alla divulgazione dei propri dati di solito non può essere considerato frutto di una decisione libera ed è, quindi, non valido ai sensi del diritto in materia di protezione dei dati.

Esempio: l'accordo espresso dai passeggeri di una compagnia aerea alla trasmissione dei cosiddetti codici di prenotazione (PNR), ovvero i dati sulla propria identità, abitudini alimentari o problemi di salute, alle autorità competenti per l'immigrazione di un paese straniero specifico non può essere considerato un consenso valido ai sensi del diritto in materia di protezione dei dati, visto che i passeggeri in viaggio non hanno scelta se vogliono visitare questo paese. Se tali dati devono essere trasferiti legittimamente, è richiesta una base giuridica diversa dal consenso, ossia molto probabilmente una legge specifica.

Consenso informato

L'interessato deve disporre di informazioni sufficienti prima di prendere una decisione. Se le informazioni fornite siano sufficienti è questione che può essere definita

solo caso per caso. Di solito, il consenso informato comprende una descrizione precisa e facilmente comprensibile della materia o della fattispecie rispetto alla quale è richiesto il consenso nonché l'indicazione delle conseguenze del rilascio o del mancato rilascio del consenso. La lingua utilizzata per fornire le informazioni dovrebbe essere adattata ai prevedibili destinatari delle informazioni.

Le informazioni devono essere facilmente accessibili all'interessato. L'accessibilità e la visibilità delle informazioni sono fattori importanti. In un ambiente online, la disponibilità di informative su più livelli può rappresentare una buona soluzione in quanto l'interessato avrà accesso, oltre che a una versione sintetica delle informazioni, anche a una versione più dettagliata.

Consenso specifico

Per essere valido, il consenso deve essere anche specifico. Questa caratteristica va di pari passo con la qualità delle informazioni fornite circa l'oggetto del consenso. In questo contesto, sarà pertinente ciò che costituisce una ragionevole aspettativa per un interessato medio. All'interessato deve essere chiesto nuovamente il consenso in caso di integrazioni o modifiche delle operazioni di trattamento che non avrebbero potuto essere ragionevolmente previste quando è stato dato il consenso iniziale.

Esempio: nella causa *Deutsche Telekom AG*[104], la CGUE ha affrontato la questione se un provider di servizi di telecomunicazione che doveva trasmettere i dati personali degli abbonati ai sensi dell'articolo 12 della *direttiva relativa alla vita privata e alle comunicazioni elettroniche*[105] necessitasse nuovamente del consenso degli interessati, in quanto inizialmente, quando era stato dato il consenso, non erano stati specificati i destinatari.

La CGUE ha ritenuto che non fosse necessario un nuovo consenso ai sensi di tale articolo prima di trasmettere i dati perché gli interessati avevano, ai sensi di detta disposizione, la possibilità di acconsentire solo alla finalità del trattamento, che è la pubblicazione dei loro dati, e non potevano scegliere tra diversi elenchi in cui tali dati potevano essere pubblicati.

104 CJEU, C-543/09, *Deutsche Telekom AG c. Germania*, 5 maggio 2011; cfr., in particolare, i punti 53 e 54.

105 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*) (GU L 201 del 2002).

Come la Corte ha sottolineato, "da un'interpretazione contestuale e sistematica dell'art. 12 della direttiva 'vita privata e comunicazioni elettroniche' risulta che il consenso di cui al n. 2 di tale articolo riguarda lo scopo della pubblicazione dei dati personali in un elenco pubblico e non già l'identità di uno specifico fornitore di elenchi"[106]. Inoltre, "è la pubblicazione in sé di dati personali in un elenco avente uno scopo particolare che può risultare pregiudizievole per un abbonato"[107] e non chi è l'autore di questa pubblicazione.

2.4.2. Il diritto di revoca del consenso in qualsiasi momento

La direttiva sulla protezione dei dati non menziona un diritto generale di revoca del consenso in qualsiasi momento. Generalmente si presume, tuttavia, che tale diritto esista e che debba essere possibile per l'interessato esercitarlo a propria discrezione. Non ci dovrebbe essere alcun obbligo di motivazione per detta revoca e nessun rischio di conseguenze negative al di là della cessazione di eventuali benefici derivanti dall'uso dei dati precedentemente concordato.

Esempio: un cliente accetta di ricevere corrispondenza promozionale a un indirizzo che fornisce a un titolare del trattamento. Se il cliente revoca il consenso, il titolare del trattamento deve interrompere immediatamente l'invio della corrispondenza promozionale. Non dovrebbero essere imposte conseguenze di natura pecuniaria a fini di ritorsione.

Se il cliente riceveva uno sconto del 5 % sul prezzo di una camera d'albergo in cambio del consenso all'utilizzo dei suoi dati ai fini della corrispondenza promozionale, la successiva revoca del consenso a ricevere questo tipo di corrispondenza non dovrebbe comportare l'obbligo di restituzione di tali riduzioni.

106 CGUE, C-543/09, *Deutsche Telekom AG c. Germania*, 5 maggio 2011; cfr., in particolare, il punto 61.

107 *Ibid.*, cfr., in particolare, il punto 62.

3

I principi fondamentali del diritto europeo in materia di protezione dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettere a) e b) CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008 CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010	**Il principio di liceità del trattamento**	Convenzione n. 108, articolo 5, lettere a) e b) Corte EDU, *Rotaru c. Romania* [GC], n. 28341/95, 4 aprile 2000 Corte EDU, *Taylor-Sabori c. Regno Unito*, n. 47114/99, 22 ottobre 2002 Corte EDU, *Peck c. Regno Unito*, n. 44647/98, 28 gennaio 2003 Corte EDU, *Khelili c. Svizzera*, n. 16188/07, 18 ottobre 2011 Corte EDU, *Leander c. Svezia*, n. 9248/81, 11 luglio 1985
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera b)	**Il principio di finalità**	Convenzione n. 108, articolo 5, lettera b)
	Il principio di qualità dei dati:	
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera c)	**pertinenza dei dati**	Convenzione n. 108, articolo 5, lettera c)
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera d)	**esattezza dei dati**	Convenzione n. 108, articolo 5, lettera d)
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera e)	**conservazione dei dati per un periodo di tempo limitato**	Convenzione n. 108, articolo 5, lettera e)

Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera e)	**Deroga per la ricerca scientifica e le statistiche**	Convenzione n. 108, articolo 9, paragrafo 3
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera a)	**Il principio di correttezza del trattamento**	Convenzione n. 108, articolo 5, lettera a) Corte EDU, *Haralambie c. Romania*, n. 21737/03, 27 ottobre 2009 Corte EDU, *K.H. e altri c. Slovacchia*, n. 32881/04, 28 aprile 2009
Direttiva sulla protezione dei dati personali, articolo 6, paragrafo 2	**Il principio di responsabilità**	

I principi di cui all'articolo 5 della Convenzione n. 108 sanciscono l'essenza del diritto europeo in materia di protezione dei dati, figurando anche all'articolo 6 della direttiva sulla protezione dei dati personali quale punto di partenza per disposizioni più dettagliate di cui agli articoli successivi della direttiva stessa. Tutta la normativa seguente sulla tutela dei dati a livello di CDE o di UE deve rispettare questi principi, di cui occorre tener conto all'atto d'interpretare tale normativa. A livello nazionale è possibile prevedere eventuali deroghe e restrizioni a tali principi fondamentali[108] per le quali occorre il soddisfacimento di tutte e tre le seguenti condizioni: essere previste per legge, perseguire uno scopo legittimo ed essere necessarie in una società democratica.

3.1. Il principio di liceità del trattamento

Punti salienti

- Per comprendere il principio di liceità del trattamento è necessario fare riferimento alle condizioni per la legittimità delle limitazioni del diritto alla protezione dei dati alla luce dell'articolo 52, paragrafo 1, della Carta e ai requisiti relativi all'ingerenza giustificata ai sensi dell'articolo 8, paragrafo 2, della CEDU.
- Di conseguenza, il trattamento dei dati personali è lecito soltanto se:
  - è conforme alla legge; e
  - persegue uno scopo legittimo; e
  - è necessario in una società democratica per perseguire uno scopo legittimo.

108 Convenzione n. 108, articolo 9, paragrafo 2; direttiva sulla protezione dei dati, articolo 13, paragrafo 2.

Nel quadro del diritto dell'UE e del CDE in materia di protezione dei dati, il principio di liceità del trattamento è il primo principio menzionato. La sua formulazione è pressoché identica nell'articolo 5 della Convenzione n. 108 e nell'articolo 6 della direttiva sulla protezione dei dati.

Per comprendere quest'espressione giuridica occorre fare riferimento alla conformità del trattamento alla normativa nazionale di riferimento. Tale normativa deve rispettare il principio dell'ingerenza giustificata ai sensi della CEDU, come interpretata dalla giurisprudenza della Corte EDU, nonché le condizioni per la legittimità delle limitazioni ai sensi dell'articolo 52 della Carta.

3.1.1. I requisiti relativi all'ingerenza giustificata ai sensi della CEDU

Il trattamento dei dati personali può costituire un'ingerenza con il diritto al rispetto della vita privata dell'interessato. Il diritto al rispetto della vita privata, tuttavia, non è un diritto assoluto, ma dev'essere bilanciato e conciliato con altri interessi legittimi, siano essi di altre persone (interessi privati) o della società nel suo complesso (interessi pubblici).

L'ingerenza dello Stato è giustificata alle condizioni illustrate di seguito.

Conformità alla legge

Secondo la giurisprudenza della Corte EDU, l'ingerenza avviene conformemente alla legge se si basa su una disposizione di diritto nazionale, che presenta talune caratteristiche. Il diritto dev'essere "accessibile alle persone interessate e prevedibile quanto ai suoi effetti"[109]. Una norma è prevedibile "se formulata in modo molto preciso per consentire all'interessato – avvalendosi, ove necessario, di consulenti esperti

109 Corte EDU, *Amann c. Svizzera* [GC], n. 27798/95, 16 febbraio 2000, punto 50; cfr. anche Corte EDU, *Kopp c. Svizzera*, n. 23224/94, 25 marzo 1998, punto 55, e Corte EDU, *Iordachi e a. c. Moldova,* n. 25198/02, 10 febbraio 2009, punto 50.

– di regolare il proprio comportamento"[110]. "Il grado di precisione della 'legge' richiesto in tale contesto dipenderà dalla materia particolare"[111].

Esempio: nella causa *Rotaru c. Romania*[112], la Corte EDU ha rilevato una violazione dell'articolo 8 della CEDU poiché la legge rumena autorizzava la raccolta, la registrazione e l'archiviazione in fascicoli segreti di informazioni rilevanti per la sicurezza nazionale, senza stabilire limiti all'esercizio di tali poteri rimasti a discrezione delle autorità. Il diritto nazionale non definiva, per esempio, il tipo d'informazioni che avrebbero potuto essere trattate, le categorie di persone nei cui confronti si sarebbero potute adottare misure di sorveglianza, le circostanze in cui tali misure si sarebbero potute prendere o la procedura da seguire. A causa di queste carenze, la Corte EDU ha concluso che il diritto nazionale non rispettava il requisito di prevedibilità ai sensi dell'articolo 8 della CEDU, e che vi era stata una violazione di detto articolo.

Esempio: nella causa *Taylor-Sabori c. Regno Unito*[113], il ricorrente era stato sottoposto alla sorveglianza della polizia. Utilizzando un "clone" del cercapersone del ricorrente, la polizia era in grado di intercettare i messaggi inviatigli. Il ricorrente è stato quindi arrestato e accusato di associazione a delinquere finalizzata al traffico di stupefacenti. Parte dell'impianto accusatorio a suo carico era costituito dai messaggi del cercapersone, che erano stati trascritti dalla polizia. Tuttavia, all'epoca del processo del ricorrente, non vi era alcuna disposizione nella legge britannica che disciplinasse l'intercettazione delle comunicazioni trasmesse attraverso un sistema di telecomunicazioni privato. L'ingerenza con i suoi diritti non era avvenuta, quindi, "conformemente alla legge". La Corte EDU ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

110 Corte EDU, *Amann c. Svizzera* [GC], n. 27798/95, 16 febbraio 2000, punto 56; cfr. anche Corte EDU, *Malone c. Regno Unito*, n. 8691/79, 2 agosto 1984, punto 66, e Corte EDU, *Silver e a. c. Regno Unito,* nn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 marzo 1983, punto 88.

111 Corte EDU, *The Sunday Times c. Regno Unito*, n. 6538/74, 26 aprile 1979, punto 49; cfr. anche Corte EDU, *Silver e a. c. Regno Unito,* nn. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 marzo 1983, punto 88.

112 Corte EDU, *Rotaru c. Romania* [GC], n. 28341/95, 4 aprile 2000, punto 57; cfr. anche Corte EDU, *Association for European Integration and Human Rights e Ekimdzhiev c. Bulgaria*, n. 62540/00, 28 giugno 2007; Corte EDU, *Shimovolos c. Russia,* n. 30194/09, 21 giugno 2011, e Corte EDU, *Vetter c. Francia,* n. 59842/00, 31 maggio 2005.

113 Corte EDU, *Taylor-Sabori c. Regno Unito*, n. 47114/99, 22 ottobre 2002.

Perseguimento di uno scopo legittimo

Lo scopo legittimo può essere costituito da uno degli interessi pubblici menzionati o dai diritti e dalle libertà altrui.

Esempio: nella causa *Peck c. Regno Unito*[114], il ricorrente aveva tentato il suicidio in strada tagliandosi i polsi, ignaro del fatto che una telecamera a circuito chiuso (CCTV) lo avesse filmato durante il tentativo. La polizia, che stava guardando le telecamere CCTV, lo aveva salvato e successivamente aveva trasmesso i filmati a circuito chiuso ai mezzi di comunicazione, che li avevano divulgati senza mascherare il volto del ricorrente. La Corte EDU ha rilevato l'assenza di motivi pertinenti o sufficienti che giustificassero la divulgazione diretta dei filmati da parte delle autorità al pubblico senza aver prima ottenuto il consenso del ricorrente o senza mascherarne l'identità. La Corte ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

Necessità in una società democratica

La Corte EDU ha dichiarato che "la nozione di necessità comporta un'ingerenza basata su un bisogno sociale imperativo e, in particolare, proporzionata al fine legittimo perseguito"[115].

Esempio: nella causa *Khelili c. Svizzera*[116] la polizia, durante un controllo, aveva rilevato che la ricorrente portava con sé biglietti da visita recanti la seguente dicitura: "Donna carina, piacente, sulla trentina avanzata, desidera incontrare un uomo per un drink o uscite saltuarie. Telefonare al numero [...]". La ricorrente ha sostenuto che, a seguito di questa scoperta, la polizia aveva inserito il suo nome nei propri registri classificandola come prostituta, professione che lei aveva costantemente negato di svolgere. La ricorrente aveva richiesto la cancellazione della parola "prostituta" dai registri informatici della polizia. La Corte EDU ha riconosciuto in linea di principio che la conservazione dei dati personali di un individuo, sulla base del fatto che quella persona possa commettere un altro reato, può, in alcune circostanze, essere proporzionata. Tuttavia, nel caso della ricorrente, l'accusa di esercizio illecito della prostituzione appariva troppo vaga

114 Corte EDU, *Peck c. Regno Unito*, n. 44647/98, 28 gennaio 2003, in particolare punto 85.

115 Corte EDU, *Leander c. Svezia*, n. 9248/81, 11 luglio 1985, punto 58.

116 Corte EDU, *Khelili c. Svizzera*, n. 16188/07, 18 ottobre 2011.

e generica, non era suffragata da fatti concreti, poiché la donna non era mai stata condannata per esercizio illecito della prostituzione, e non poteva quindi essere considerata compatibile con un "bisogno sociale imperativo" ai sensi dell'articolo 8 della CEDU. Ritenendo che fossero le autorità a dovere dimostrare l'accuratezza dei dati conservati sulla ricorrente e alla luce della gravità dell'ingerenza con i diritti della stessa, la Corte EDU ha statuito che la conservazione del termine "prostituta" nei fascicoli della polizia per anni non fosse necessaria in una società democratica. La Corte ha concluso che vi era stata violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Leander c. Svezia*[117], la Corte EDU ha stabilito che controllare in segreto le persone che fanno domanda d'impiego in posti di rilievo per la sicurezza nazionale non è, di per sé, in contrasto con il requisito di necessità in una società democratica. Le garanzie specifiche previste dal diritto nazionale a fini di tutela degli interessi dell'interessato – per esempio i controlli esercitati dal Parlamento e dalla Procura – hanno indotto la Corte EDU a concludere che il sistema di controllo svedese sul personale fosse conforme ai requisiti di cui all'articolo 8, paragrafo 2, della CEDU. In considerazione del suo ampio margine di discrezionalità, lo Stato convenuto aveva diritto di ritenere che, nel caso del ricorrente, gli interessi della sicurezza nazionale prevalessero su quelli individuali. La Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

3.1.2. Condizioni per la legittimità delle limitazioni ai sensi della Carta dell'UE

La struttura e la formulazione della Carta differiscono da quelle della CEDU. La Carta non contempla le ingerenze con i diritti garantiti, ma contiene una disposizione sulla o sulle limitazioni dell'esercizio dei diritti e delle libertà da essa riconosciuti.

Ai sensi dell'articolo 52, paragrafo 1, le limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta e, di conseguenza, all'esercizio del diritto alla protezione dei dati personali, come il trattamento di tali dati, sono ammissibili solo se:

- sono previste dalla legge; e
- rispettano il contenuto essenziale del diritto alla protezione dei dati; e

117 Corte EDU, *Leander c. Svezia*, n. 9248/81, 11 luglio 1985, punti 59 e 67.

- sono necessarie, fatto salvo il principio di proporzionalità; e
- rispondono a finalità d'interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

> Esempio: nella causa *Volker und Markus Schecke*[118], la CGUE ha concluso che, imponendo la pubblicazione dei dati personali relativi a ciascuna persona fisica beneficiaria dei sussidi di [taluni fondi agricoli] senza operare distinzioni sulla base di criteri pertinenti, come i periodi durante i quali queste hanno percepito simili aiuti, la frequenza o ancora il tipo e l'entità di questi ultimi, il Consiglio e la Commissione avevano superato i limiti imposti dal rispetto del principio di proporzionalità.
>
> Pertanto, la CGUE ha ritenuto necessario dichiarare nulle alcune disposizioni del regolamento (CE) n. 1290/2005 del Consiglio nonché il regolamento n. 259/2008 nella sua interezza[119].

Nonostante la diversa formulazione, le condizioni per la liceità del trattamento di cui all'articolo 52, paragrafo 1, della Carta rimandano all'articolo 8, paragrafo 2, della CEDU. Infatti, le condizioni elencate all'articolo 52, paragrafo 1, della Carta devono essere ritenute conformi a quelle menzionate all'articolo 8, paragrafo 2, della CEDU, poiché l'articolo 52, paragrafo 3, prima frase, della Carta stabilisce che "laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta Convenzione".

Tuttavia, conformemente all'articolo 52, paragrafo 3, ultima frase, "la presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa". Confrontando l'articolo 8, paragrafo 2, della CEDU con l'articolo 52, paragrafo 3, prima frase, della Carta, emerge senza dubbio che le condizioni soddisfatte

118 CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, punti 89 e 86.

119 Regolamento (CE) n. 1290/2005 del Consiglio, del 21 giugno 2005, relativo al finanziamento della politica agricola comune, GU L 209 dell'11.8.2005; regolamento (CE) n. 259/2008 della Commissione, del 18 marzo 2008, recante modalità di applicazione del regolamento (CE) n. 1290/2005 del Consiglio per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR), GU L 76 del 19.3.2008.

le quali si è in presenza di ingerenze giustificate secondo l'articolo 8, paragrafo 2, della CEDU sono i requisiti minimi perché sussista la legittimità delle limitazioni del diritto alla protezione dei dati secondo la Carta. Di conseguenza, la liceità del trattamento dei dati personali richiede, secondo il diritto dell'Unione, che siano soddisfatte quanto meno le condizioni dell'articolo 8, paragrafo 2, della CEDU; tuttavia, il diritto dell'Unione potrebbe recare requisiti aggiuntivi per casi specifici.

La corrispondenza tra il principio di liceità del trattamento in base al diritto dell'Unione e le disposizioni pertinenti della CEDU è ulteriormente rafforzata dall'articolo 6, paragrafo 3, del TUE, il quale stabilisce che "i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali [...], fanno parte del diritto dell'Unione in quanto principi generali".

3.2. Il principio di finalità

Punti salienti

- La finalità del trattamento dei dati deve essere manifestamente definita prima che il trattamento abbia inizio.
- In base al diritto dell'Unione, la finalità del trattamento dev'essere esplicita; nell'ambito del diritto del CDE, tale questione è lasciata alla competenza del diritto nazionale.
- Il trattamento per finalità indefinite non è conforme al diritto in materia di protezione dei dati.
- L'ulteriore utilizzo dei dati per un'altra finalità necessita di una base giuridica aggiuntiva se la nuova finalità del trattamento non è compatibile con quella originaria.
- Il trasferimento dei dati a terzi è una finalità nuova che necessita di una base giuridica aggiuntiva.

Essenzialmente, il principio di finalità significa che la legittimità del trattamento dei dati personali dipende dalla finalità del trattamento[120]. La finalità dev'essere stata specificata e resa manifesta dal titolare del trattamento prima che il trattamento dei dati abbia inizio[121]. **Ai sensi del diritto dell'UE** tale specificazione deve essere fatta

120 Convenzione n. 108, articolo 5, lettera b); direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera b).

121 Cfr. anche Gruppo di lavoro articolo 29 (2013), *Opinion 03/2013 on purpose limitation* (Parere 3/2013 sulla limitazione della finalità), WP 203, Bruxelles, 2 aprile 2013.

attraverso una dichiarazione, ossia una notifica, all'autorità di controllo competente o, almeno, per mezzo di una documentazione interna che dev'essere messa a disposizione dal titolare del trattamento a fini di ispezione da parte delle autorità di controllo e dev'essere accessibile all'interessato.

Il trattamento dei dati personali per finalità indefinite e/o illimitate è illegittimo.

Ogni nuova finalità di trattamento dei dati deve avere la propria base giuridica specifica e non può fondarsi sul fatto che i dati fossero stati inizialmente acquisiti o trattati per un'altra finalità legittima. A sua volta, il trattamento legittimo è limitato alla finalità iniziale specificata per lo stesso e ogni nuova finalità di trattamento richiede una nuova base giuridica distinta. La divulgazione dei dati a terzi dovrà essere valutata con particolare attenzione, poiché va a costituire di norma una nuova finalità e, pertanto, richiede una base giuridica diversa da quella prevista per la raccolta dei dati.

Esempio: una compagnia aerea raccoglie i dati dei passeggeri per effettuare le prenotazioni e operare i voli correttamente. A tale scopo avrà bisogno di dati relativi a: numeri di posto dei passeggeri; limitazioni fisiche specifiche, come la necessità di una sedia a rotelle; e richieste di pasti speciali, quali il cibo kosher o halal. Se alle compagnie aeree viene chiesto di trasmettere questi dati, contenuti nei codici di prenotazione (PNR), alle autorità preposte al controllo dell'immigrazione all'aeroporto di arrivo, si è in presenza di un utilizzo di tali dati per finalità di controllo dell'immigrazione, che differiscono dalla finalità della raccolta dei dati iniziale. La trasmissione di tali dati a un'autorità di controllo dell'immigrazione richiederebbe una base giuridica nuova e distinta.

Nel considerare l'ambito e i limiti di una particolare finalità, la Convenzione n. 108 e la direttiva sulla protezione dei dati personali ricorrono al concetto di compatibilità: l'utilizzo dei dati per finalità compatibili è consentito in ragione della base giuridica iniziale. Tuttavia, il significato del termine "compatibile" non è definito e resta aperto all'interpretazione a seconda dei casi.

Esempio: la vendita dei dati dei clienti della società Sunshine, acquisiti durante la gestione dei rapporti con la clientela (CRM), a una società di vendita diretta, denominata Moonlight, che intende utilizzare questi dati per sostenere le campagne di promozione commerciale di aziende terze. Tale vendita costituisce una nuova finalità che è incompatibile con la CRM, che è la finalità iniziale della società Sunshine per la raccolta dei dati dei clienti. La vendita dei dati alla società Moonlight necessita pertanto di una propria base giuridica.

Per contro, l'utilizzo dei dati nell'ambito della CRM della società Sunshine per le proprie finalità di promozione commerciale, ossia l'invio di messaggi di promozione commerciale ai propri clienti per i propri prodotti, è generalmente accettata come finalità compatibile.

La direttiva sulla protezione dei dati personali dichiara esplicitamente che "il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate"[122].

Esempi: nell'ambito della CRM, la società Sunshine ha raccolto e conservato i dati relativi ai propri clienti. L'utilizzo successivo di questi dati da parte della società Sunshine per un'analisi statistica delle abitudini di acquisto dei propri clienti è ammissibile, dal momento che le statistiche rappresentano una finalità compatibile. Non occorre alcuna base giuridica aggiuntiva come il consenso degli interessati.

Se gli stessi dati dovessero essere trasmessi a terzi (la società Starlight) per finalità esclusivamente statistiche, la trasmissione sarebbe ammissibile senza base giuridica aggiuntiva, ma solo a condizione che siano state attuate garanzie appropriate, come il mascheramento dell'identità degli interessati, poiché generalmente le identità non sono necessarie per finalità statistiche.

3.3. Principio di qualità dei dati

Punti salienti

- Il principio di qualità dei dati deve essere attuato dal titolare del trattamento in tutte le operazioni di trattamento.
- La conservazione di dati per un periodo di tempo limitato esige la cancellazione dei dati non appena questi non siano più necessari alle finalità per cui sono stati raccolti.
- Le deroghe alla conservazione dei dati per un periodo di tempo limitato devono essere definite per legge e necessitano di specifiche garanzie per la protezione degli interessati.

122 Un esempio di tali disposizioni nazionali è costituito dalla legge austriaca sulla protezione dei dati (*Datenschutzgesetz*), Gazzetta giuridica federale I n. 165/1999, articolo 46, disponibile in inglese all'indirizzo: www.dsk.gv.at/DocView.axd?CobId=41936.

3.3.1. Il principio di pertinenza dei dati

Devono essere trattati solo i dati "adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati"[123]. Le categorie dei dati scelti per il trattamento devono essere necessarie al fine di raggiungere l'obiettivo generale dichiarato delle operazioni di trattamento e il titolare del trattamento dovrebbe limitare strettamente la raccolta dei dati a tali informazioni, poiché direttamente pertinenti alle finalità specifiche perseguite dal trattamento stesso.

Nella società contemporanea il principio di pertinenza dei dati implica una valutazione aggiuntiva: grazie all'utilizzo di speciali tecnologie volte a migliorare la tutela della vita privata, talvolta è possibile evitare del tutto l'utilizzo dei dati personali o utilizzare dati pseudonimizzati offrendo una soluzione rispettosa della vita privata. Questo è particolarmente indicato nei sistemi di trattamento di portata più ampia.

Esempio: un consiglio comunale offre una tessera con microprocessore agli utenti abituali del sistema di trasporto pubblico cittadino dietro pagamento di un certo importo. Il nome dell'utente compare per iscritto sulla superficie della tessera e, in forma elettronica, nel microprocessore. A ogni corsa la tessera dev'essere avvicinata all'apposito lettore installato, per esempio, sugli autobus e sui tram. I dati letti dal dispositivo sono controllati elettronicamente a fronte di quelli di una banca dati contenente i nomi delle persone che hanno acquistato la tessera di trasporto.

Questo sistema non rispetta appieno il principio di pertinenza poiché il controllo della legittimità dell'uso dei mezzi di trasporto da parte di un individuo potrebbe essere effettuato senza confrontare i dati personali presenti sul microprocessore della tessera con quelli di una banca dati. Sarebbe sufficiente, per esempio, disporre di un'immagine elettronica particolare, come un codice a barre, nel microprocessore della tessera che, dopo essere stata avvicinata al lettore, confermerebbe o meno la validità della tessera. Un simile sistema non effettuerebbe alcuna registrazione di chi ha utilizzato un determinato mezzo di trasporto e a che ora. Si creerebbe una situazione in cui non sarebbe raccolto alcun dato personale, soluzione ottimale ai sensi del principio di pertinenza, che comporta l'obbligo di minimizzare la raccolta dei dati.

123 Convenzione n. 108, articolo 5, lettera c); direttiva sulla protezione dei dati personali, articolo 6, paragrafo 1, lettera c).

3.3.2. Il principio di esattezza dei dati

Un titolare del trattamento in possesso di informazioni personali non deve utilizzare tali informazioni senza adottare misure volte a garantire con ragionevole certezza che i dati siano esatti e aggiornati.

L'obbligo di garantire l'esattezza dei dati deve essere visto nel contesto della finalità del trattamento dei dati.

Esempio: una società che vende mobili ha raccolto dati quali l'identità e l'indirizzo di un cliente al fine di emettere fatture a suo carico. Sei mesi dopo, la stessa società desidera avviare una campagna di promozione commerciale e contattare i clienti precedenti. A tal fine, la società intende accedere al registro dell'anagrafe nazionale, che probabilmente contiene gli indirizzi aggiornati, dato che i residenti sono tenuti per legge a informare l'anagrafe circa il loro indirizzo attuale. L'accesso ai dati di questo registro è limitato alle persone e agli enti in grado di fornire una ragione che lo giustifichi.

In questa situazione, la società non può far valere la motivazione secondo cui i dati devono essere mantenuti esatti e aggiornati per sostenere di avere il diritto di raccogliere nuovi dati relativi all'indirizzo di tutti i propri precedenti clienti dal registro dell'anagrafe. I dati sono stati raccolti nel corso della fatturazione; a tal fine, l'indirizzo al momento della vendita è un dato pertinente. Tuttavia, non vi è alcuna base giuridica per la raccolta di nuovi dati sull'indirizzo, poiché la promozione commerciale non è un interesse che prevale sul diritto alla protezione dei dati e, pertanto, non può giustificare l'accesso ai dati del registro.

Possono presentarsi anche casi in cui l'aggiornamento dei dati archiviati è proibito per legge, perché la finalità della conservazione dei dati è principalmente quella di documentare eventi.

Esempio: un protocollo terapeutico non deve essere modificato, in altre parole "aggiornato", anche se, in un secondo momento, risulta che le conclusioni ivi riportate erano errate. In tali circostanze, possono essere effettuate solo aggiunte alle note del protocollo, purché siano chiaramente indicate come elementi apportati in una fase successiva.

D'altra parte, vi sono situazioni in cui il controllo regolare dell'esattezza dei dati, fra cui l'aggiornamento, costituisce una necessità assoluta a causa del potenziale danno per l'interessato qualora i dati dovessero rimanere inesatti.

Esempio: se un soggetto intende stipulare un contratto di finanziamento con un istituto bancario , la banca generalmente controllerà l'affidabilità creditizia del potenziale cliente. A tal fine, sono disponibili banche dati specifiche contenenti i dati sullo storico creditizio dei privati. Se tale banca dati fornisce dati errati o non aggiornati riguardanti un individuo, questa persona può trovarsi di fronte a gravi problemi. Pertanto, i titolari del trattamento di tali banche dati devono adoperarsi in modo specifico per rispettare il principio di esattezza.

Inoltre, i dati che non riguardano fatti ma sospetti, come le indagini penali, possono essere raccolti e conservati purché il titolare del trattamento operi in virtù di una base giuridica per la raccolta di tali informazioni e il sospetto sia sufficientemente fondato.

3.3.3. Conservazione di dati per un periodo di tempo limitato

L'articolo 6, paragrafo 1, lettera e), della direttiva sulla protezione dei dati personali e analogamente l'articolo 5, lettera e), della Convenzione n. 108 impongono agli Stati membri di garantire che i dati personali siano "conservati in modo da consentire l'identificazione" degli interessati "per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati". Pertanto, i dati devono essere cancellati quando tali finalità sono state soddisfatte.

Nella causa *S. e Marper*, la Corte EDU ha concluso che i principi fondamentali degli strumenti pertinenti del Consiglio d'Europa nonché il diritto e la prassi in vigore presso le altre parti contraenti richiedevano che la conservazione dei dati fosse proporzionata allo scopo per il quale essi sono raccolti e limitata nel tempo, in particolare nell'ambito della pubblica sicurezza[124].

124 Corte EDU, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008; cfr. anche, per esempio, Corte EDU, *M.M. c. Regno Unito*, n. 24029/07, 13 novembre 2012.

I limiti di tempo per la conservazione dei dati personali si applicano, tuttavia, solo ai dati conservati in una forma che consenta l'identificazione degli interessati. La conservazione legittima dei dati che non sono più necessari potrebbe essere dunque ottenuta attraverso l'anonimizzazione dei dati.

Il mantenimento dei dati per un futuro utilizzo scientifico, storico o statistico ha luogo in deroga esplicita al principio dalla conservazione di dati per un periodo di tempo limitato di cui alla direttiva sulla protezione dei dati personali[125]. La conservazione e l'utilizzo continui dei dati personali devono essere tuttavia legittimati da garanzie speciali ai sensi del diritto nazionale.

3.4. Il principio di correttezza del trattamento

Punti salienti

- Correttezza del trattamento significa trasparenza del trattamento, soprattutto nei confronti degli interessati.
- I titolari del trattamento devono informare gli interessati prima di trattare i dati, quanto meno in merito alla finalità del trattamento e all'identità e all'indirizzo del titolare del trattamento.
- Salvo se espressamente consentito dalla legge, non deve aver luogo alcun trattamento segreto e occulto dei dati personali.
- Gli interessati hanno il diritto di accedere ai propri dati ovunque essi siano trattati.

Il principio di correttezza del trattamento disciplina in primo luogo il rapporto tra il titolare del trattamento e l'interessato.

3.4.1. Trasparenza

Questo principio stabilisce l'obbligo per il titolare del trattamento di mantenere informati gli interessati sul modo in cui vengono utilizzati i loro dati.

Esempio: nella causa *Haralambie c. Romania*[126], il ricorrente ha richiesto l'accesso al fascicolo che l'organizzazione di servizi segreti aveva conservato su di

125 Direttiva sulla protezione dei dati, articolo 6, paragrafo 1, lettera e).

126 Corte EDU, *Haralambie c. Romania*, n. 21737/03, 27 ottobre 2009.

lui, ma la richiesta è stata accolta solo cinque anni dopo. La Corte EDU ha ribadito che gli individui oggetto dei fascicoli personali tenuti dalle autorità pubbliche avevano un interesse vitale ad accedervi. Le autorità avevano il dovere di mettere a disposizione una procedura efficace per ottenere l'accesso a tali informazioni. La Corte EDU ha ritenuto che né la quantità di fascicoli trasmessi né le lacune del sistema di archivio giustificassero un ritardo di cinque anni nell'accogliere la richiesta di accesso ai fascicoli presentata dal ricorrente. Le autorità non avevano messo a disposizione del ricorrente una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai propri fascicoli personali entro un lasso di tempo ragionevole. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Le operazioni di trattamento devono essere illustrate agli interessati in modo facilmente comprensibile affinché questi possano capire che cosa accadrà ai loro dati. Inoltre, l'interessato ha il diritto di sapere da un titolare del trattamento, su richiesta, se i propri dati sono oggetto di trattamento e, in caso affermativo, quali.

3.4.2. Creazione della fiducia

I titolari del trattamento dovrebbero provare agli interessati e al pubblico in generale che tratteranno i dati in modo lecito e trasparente. Le operazioni di trattamento non devono essere eseguite in segreto e non dovrebbero avere effetti negativi non prevedibili. I titolari del trattamento dovrebbero garantire che i clienti, gli utenti o i cittadini siano informati circa l'uso dei loro dati nonché, per quanto possibile, agire in modo da conformarsi prontamente alla volontà dell'interessato, specialmente quando il suo consenso costituisce la base giuridica del trattamento dei dati.

Esempio: nella causa *K.H. e altri c. Slovacchia*[127], le ricorrenti erano otto donne di origine etnica rom che, durante la gravidanza e il parto, erano state ricoverate in due ospedali della Slovacchia orientale. Successivamente, nessuna di loro aveva potuto concepire nuovamente un figlio, malgrado i ripetuti tentativi. I giudici nazionali hanno ordinato agli ospedali di permettere che le ricorrenti e i loro rappresentanti consultassero le cartelle cliniche annotando a mano degli estratti di informazioni, ma hanno respinto la richiesta di fotocopiare i documenti, presumibilmente al fine di evitare abusi. Tra gli obblighi degli Stati ai sensi dell'articolo 8 della CEDU era previsto necessariamente quello di mettere a disposizione

127 Corte EDU, *K.H. e a. c. Slovacchia*, n. 32881/04, 28 aprile 2009.

degli interessati le copie dei propri fascicoli. Il compito di stabilire le modalità di copia dei fascicoli dei dati personali o, se del caso, di formulare motivi validi di rifiuto spettava allo Stato. Nel caso delle ricorrenti, i giudici nazionali hanno giustificato il divieto di eseguire copie delle cartelle cliniche basandosi principalmente sulla necessità di proteggere le informazioni in questione da eventuali abusi. Tuttavia, la Corte EDU non ha ritenuto che le ricorrenti, alle quali era stato comunque accordato l'accesso a tutti i propri fascicoli medici, avrebbero potuto abusare delle informazioni che le riguardavano. Inoltre, il rischio di tale abuso avrebbe potuto essere evitato con mezzi diversi dal diniego del rilascio di copie dei fascicoli alle ricorrenti, limitando per esempio le categorie di persone aventi diritto di accesso ai fascicoli. Lo Stato non è riuscito a dimostrare l'esistenza di motivi sufficientemente validi per negare alle ricorrenti l'accesso effettivo alle informazioni riguardanti la propria salute. La Corte ha concluso che vi era stata una violazione dell'articolo 8 della CEDU.

In relazione ai servizi Internet, le caratteristiche dei sistemi di trattamento dei dati devono essere tali da consentire agli interessati di comprendere realmente quali operazioni siano effettuate sui propri dati.

La correttezza del trattamento implica anche la disponibilità dei titolari del trattamento ad andare oltre i requisiti minimi giuridici obbligatori per la fornitura di un servizio all'interessato, qualora gli interessi legittimi di quest'ultimo lo richiedano.

3.5. Il principio di responsabilità

Punti salienti

- Il principio di responsabilità richiede l'adozione attiva delle misure da parte dei titolari del trattamento finalizzate alla promozione e salvaguardia della protezione dei dati nelle attività di trattamento.
- I titolari del trattamento sono responsabili della conformità alla normativa in materia di protezione dei dati nell'ambito delle operazioni di trattamento.
- I titolari del trattamento dovrebbero essere in grado di dimostrare in qualsiasi momento agli interessati, al pubblico in generale e alle autorità di controllo che essi operano in conformità delle disposizioni sulla protezione dei dati.

Nel 2013 l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha adottato delle linee-guida sulla vita privata in cui si sottolinea l'importante ruolo dei titolari del trattamento nell'applicazione concreta della protezione dei dati. Le linee-guida sviluppano il principio di responsabilità nel senso che "un titolare del trattamento dovrebbe essere responsabile del rispetto delle misure che danno attuazione ai principi (materiali) sopra enunciati"[128].

Mentre la Convenzione n. 108 non fa alcun riferimento al principio di responsabilità dei titolari del trattamento, lasciando tale questione sostanzialmente al diritto nazionale, l'articolo 6, paragrafo 2, della direttiva sulla protezione dei dati personali stabilisce che il titolare del trattamento è tenuto a garantire il rispetto dei principi relativi alla qualità dei dati di cui al paragrafo 1.

Esempio: un esempio legislativo atto a evidenziare il principio di responsabilità è costituito dalla modifica della direttiva relativa alla vita privata e alle comunicazioni elettroniche 2002/58/CE avvenuta nel 2009[129]. Ai sensi dell'articolo 4 della versione modificata, la direttiva prevede l'obbligo di attuare una politica di sicurezza, vale a dire "garantire l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali". Così, per quanto riguarda le disposizioni sulla sicurezza di tale direttiva, il legislatore ha deciso che era necessario introdurre l'obbligo esplicito di predisporre e attuare una politica di sicurezza.

Secondo il parere 3/2010 del Gruppo di lavoro articolo 29[130], la componente essenziale del principio di responsabilità è data dall'obbligo del titolare del trattamento di:

- mettere in atto misure per garantire – in circostanze normali – che le norme in materia di protezione dei dati siano rispettate nel contesto delle operazioni di trattamento; e

128 OCSE (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data (Linee-guida per la tutela della vita privata e i flussi transfrontalieri di dati personali), articolo 14.

129 Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009, pag. 11.

130 Gruppo di lavoro articolo 29, *Parere 3/2010 sul principio di responsabilità,* WP 173, Bruxelles, 13 luglio 2010.

- disporre di documentazione atta a dimostrare agli interessati e alle autorità di controllo le misure adottate per conseguire il rispetto delle norme in materia di protezione dei dati.

Il principio di responsabilità esige quindi che i titolari del trattamento ne dimostrino attivamente il rispetto, senza limitarsi ad aspettare che gli interessati o le autorità di controllo sottolineino eventuali carenze.

4

Le norme del diritto europeo in materia di protezione dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Norme sulla liceità del trattamento dei dati non sensibili		
Direttiva sulla protezione dei dati personali, articolo 7, lettera a)	**Consenso**	Raccomandazione sulla profilazione, articolo 3.4, lettera b), e articolo 3.6
Direttiva sulla protezione dei dati personali, articolo 7, lettera b)	**Rapporto (pre) contrattuale**	Raccomandazione sulla profilazione, articolo 3.4, lettera b)
Direttiva sulla protezione dei dati personali, articolo 7, lettera c)	**Obblighi legali del titolare del trattamento**	Raccomandazione sulla profilazione, articolo 3.4, lettera a)
Direttiva sulla protezione dei dati personali, articolo 7, lettera d)	**Interessi vitali dell'interessato**	Raccomandazione sulla profilazione, articolo 3.4, lettera b)
Direttiva sulla protezione dei dati personali, articolo 7, lettera e) e articolo 8, paragrafo 4 CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008	**Interesse pubblico ed esercizio di pubblici poteri**	Raccomandazione sulla profilazione, articolo 3.4, lettera b)
Direttiva sulla protezione dei dati personali, articolo 7, lettera f), articolo 8, paragrafo 2, e articolo 8, paragrafo 3 CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011	**Interessi legittimi altrui**	Raccomandazione sulla profilazione, articolo 3.4, lettera b)

Norme sulla liceità del trattamento dei dati sensibili		
Direttiva sulla protezione dei dati personali, articolo 8, paragrafo 1	**Divieto generale del trattamento**	Convenzione n. 108, articolo 6
Direttiva sulla protezione dei dati personali, articolo 8, paragrafi da 2 a 4	**Deroghe al divieto generale**	Convenzione n. 108, articolo 6
Direttiva sulla protezione dei dati personali, articolo 8, paragrafo 5	**Trattamento dei dati riguardanti le condanne (penali)**	Convenzione n. 108, articolo 6
Direttiva sulla protezione dei dati personali, articolo 8, paragrafo 7	**Trattamento dei numeri di identificazione**	
Norme sulla sicurezza del trattamento		
Direttiva sulla protezione dei dati personali, articolo 17	**Obbligo di fornire un trattamento sicuro**	Convenzione n. 108, articolo 7 Corte EDU, *I. c. Finlandia*, n. 20511/03, 17 luglio 2008
Direttiva relativa alla vita privata e alle comunicazioni elettroniche, articolo 4, paragrafo 2	**Notificazioni di violazioni di dati personali**	
Direttiva sulla protezione dei dati personali, articolo 16	**Obbligo di riservatezza**	
Norme sulla trasparenza del trattamento		
	Trasparenza in generale	Convenzione n. 108, articolo 8, lettera a)
Direttiva sulla protezione dei dati personali, articoli 10 e 11	**Informazioni**	Convenzione n. 108, articolo 8, lettera a)
Direttiva sulla protezione dei dati personali, articoli 10 e 11	**Deroghe all'obbligo d'informazione**	Convenzione n. 108, articolo 9
Direttiva sulla protezione dei dati personali, articoli 18 e 19	**Notificazione**	Raccomandazione sulla profilazione, articolo 9.2, lettera a)
Norme relative alla promozione dell'osservanza		
Direttiva sulla protezione dei datipersonali, articolo 20	**Controllo preliminare**	
Direttiva sulla protezione dei dati personali, articolo 18, paragrafo 2	**Responsabili della protezione dei dati personali**	Raccomandazione sulla profilazione, articolo 8.3
Direttiva sulla protezione dei dati personali, articolo 27	**Codici di condotta**	

I principi sono necessariamente di natura generale e la loro applicazione a situazioni concrete lascia un certo margine d'interpretazione e di scelta dei mezzi. Il **diritto del CDE** consente alle parti aderenti alla Convenzione n. 108 di chiarire questo margine

d'interpretazione nel rispettivo diritto nazionale. La situazione nel **diritto dell'UE** è diversa: per instaurare la protezione dei dati nel mercato interno si è ritenuto necessario disporre di norme più dettagliate già a livello di Unione, al fine di armonizzare il grado di protezione dei dati previsto dalle legislazioni nazionali degli Stati membri. La direttiva sulla protezione dei dati personali stabilisce, secondo i principi di cui all'articolo 6, un corpus di norme dettagliate da trasporre fedelmente nella legislazione nazionale. Di conseguenza, le seguenti osservazioni riguardanti le norme dettagliate in materia di protezione dei dati a livello europeo riguardano prevalentemente il diritto dell'UE.

4.1. Norme sulla liceità del trattamento

Punti salienti

- I dati personali possono essere trattati in modo lecito se:
  - il trattamento si basa sul consenso dell'interessato; o
  - gli interessi vitali degli interessati richiedono il trattamento dei loro dati; o
  - gli interessi legittimi altrui costituiscono il motivo del trattamento, ma solo fino a quando non prevalgano gli interessi alla tutela dei diritti fondamentali degli interessati.
- La liceità del trattamento dei dati personali sensibili è data dal rispetto di un regime particolare e più rigoroso.

La direttiva sulla protezione dei dati personali contiene due diversi insiemi di norme sulla liceità del trattamento dei dati: uno per i dati non sensibili di cui all'articolo 7 e uno per i dati sensibili di cui all'articolo 8.

4.1.1. Liceità del trattamento dei dati non sensibili

Il capo II della direttiva 95/46/CE, intitolato "Condizioni generali di liceità dei trattamenti di dati personali", stabilisce che, fatte salve le deroghe consentite ai sensi dell'articolo 13, qualsiasi trattamento dei dati personali dev'essere conforme, da un lato, ai principi relativi alla qualità dei dati, enunciati all'articolo 6 della stessa direttiva sulla protezione dei dati personali e, dall'altro, a uno dei principi relativi alla

legittimità del trattamento dei dati di cui all'articolo 7[131]. Ciò spiega i casi che legittimano il trattamento dei dati personali non sensibili.

Consenso

In base al diritto del CDE, il consenso non è menzionato nell'articolo 8 della CEDU né nella Convenzione n. 108. Tuttavia, è citato nella giurisprudenza della Corte EDU e in diverse raccomandazioni del CDE. **Nell'ambito del diritto dell'UE**, il consenso alla base del trattamento legittimo dei dati è saldamente prescritto dall'articolo 7, lettera a), della direttiva sulla protezione dei dati personali, oltre a essere esplicitamente menzionato nell'articolo 8 della Carta.

Rapporto contrattuale

In base al diritto dell'UE, il fatto che il trattamento sia "necessario all'esecuzione del contratto concluso con" l'interessato, di cui all'articolo 7, lettera b), della direttiva sulla protezione dei dati personali, costituisce un'ulteriore base per la liceità del trattamento dei dati personali. Tale disposizione comprende anche i rapporti precontrattuali. Per esempio: una parte intende stipulare un contratto, ma non vi ha ancora provveduto, probabilmente perché restano da compiere alcuni controlli. Se una parte deve trattare i dati a tal fine, questo trattamento è legittimo fintantoché sia necessario "all'esecuzione di misure precontrattuali prese su richiesta" di tale interessato.

Per quanto concerne il diritto del CDE, "la protezione dei diritti e delle libertà altrui" è menzionata nell'articolo 8, paragrafo 2, della CEDU quale motivo a sostegno della legittimità dell'ingerenza con il diritto alla protezione dei dati.

Obblighi legali del titolare del trattamento

Il diritto dell'UE fa esplicito riferimento a un altro criterio che rende legittimo il trattamento dei dati, ossia se "è necessario per adempiere un obbligo legale al quale è soggetto" il titolare del trattamento (articolo 7, lettera c), della direttiva sulla protezione dei dati personali). Questa disposizione si riferisce ai titolari del trattamento che operano nel settore privato; gli obblighi giuridici dei titolari del trattamento dei

131 CGUE, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e a.,* 20 maggio 2003, punto 65; CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008, punto 48; CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, punto 26.

dati del settore pubblico rientrano nell'ambito di applicazione dell'articolo 7, lettera e), della direttiva. In molti casi i titolari del trattamento del settore privato sono obbligati per legge a trattare dati altrui. I medici e le strutture ospedaliere, ad esempio, per legge hanno il dovere di conservare per diversi anni i dati riguardanti le cure erogate ai pazienti; i datori di lavoro devono trattare i dati dei propri dipendenti per motivi di previdenza sociale e fiscalità, mentre le aziende devono trattare i dati dei propri clienti per motivi di ordine fiscale.

Nell'ambito del trasferimento obbligatorio dei dati dei passeggeri dalle compagnie aeree alle autorità di controllo dell'immigrazione di altri paesi è sorta la questione se gli obblighi giuridici ai sensi del diritto di un paese *straniero* possano costituire o meno una base legittima per il trattamento dei dati ai sensi del diritto dell'UE (la questione è affrontata in modo più dettagliato al paragrafo 6.2.).

Gli obblighi giuridici del titolare del trattamento costituiscono la base per la legittimità del trattamento dei dati anche **in base al diritto del CDE**. Come sottolineato in precedenza, gli obblighi giuridici di un titolare del trattamento del settore privato rappresentano solo un caso specifico di interessi legittimi altrui, come menzionato nell'articolo 8, paragrafo 2, della CEDU. Pertanto, l'esempio illustrato poc'anzi è pertinente anche per il diritto del CDE.

Interessi vitali dell'interessato

Nell'ambito del diritto dell'UE, l'articolo 7, lettera d), della **direttiva sulla protezione dei dati personali** dispone che il trattamento dei dati personali è lecito se "è necessario per la salvaguardia dell'interesse vitale" dell'interessato. Tali interessi, strettamente connessi alla sopravvivenza dell'interessato, potrebbero costituire il fondamento per un utilizzo legittimo dei dati sanitari o dei dati riguardanti le persone scomparse, per esempio.

Nel quadro del diritto del CDE, gli interessi vitali dell'interessato non sono menzionati nell'articolo 8 della CEDU come motivo a sostegno della legittimità dell'ingerenza con il diritto alla protezione dei dati. Tuttavia, in alcune raccomandazioni del CDE che integrano la Convenzione n. 108 in ambiti specifici, gli interessi vitali dell'interessato sono esplicitamente menzionati come fondamento per un trattamento legittimo dei dati[132]. Gli interessi vitali dell'interessato sono evidentemente considerati ricompresi nella serie di ragioni che giustificano il trattamento dei dati: la tutela

132 Raccomandazione sulla profilazione, articolo 3.4, lettera b).

dei diritti fondamentali non dovrebbe mai mettere in pericolo gli interessi vitali della persona protetta.

Interesse pubblico ed esercizio di pubblici poteri

Considerate le molteplici modalità con cui si possono organizzare le attività di carattere pubblico, l'articolo 7, lettera e), della direttiva sulla protezione dei dati personali stabilisce che i dati personali possono essere trattati lecitamente se "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito" il titolare del trattamento "o il terzo a cui vengono comunicati i dati [...]"[133].

Esempio: nella causa *Huber c. Bundesrepublik Deutschland*[134], il sig. Huber, cittadino austriaco residente in Germania, ha chiesto all'Ufficio federale per l'immigrazione e i rifugiati di cancellare i dati che lo riguardano dal registro centrale degli stranieri (denominato "AZR"). Tale registro, contenente i dati personali relativi ai cittadini dell'UE che non hanno la cittadinanza tedesca e che risiedono in Germania da oltre tre mesi, è utilizzato per finalità statistiche nonché dalle forze dell'ordine e dalle autorità giudiziarie nell'ambito d'indagini e operazioni relative ad attività criminali o pregiudizievoli per la pubblica sicurezza. Il giudice del rinvio ha chiesto se il trattamento dei dati personali intrapreso nell'ambito di un registro come il registro centrale degli stranieri, a cui anche altre autorità pubbliche hanno accesso, sia compatibile con il diritto dell'UE, dal momento che non esiste un registro simile per i cittadini tedeschi.

La CGUE ritiene in primo luogo che, ai sensi dell'articolo 7, lettera e), della direttiva, i dati personali possano essere trattati lecitamente solo se è necessario per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri.

Secondo la Corte, "considerato l'obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la nozione di necessità come risultante dall'art. 7, lett. e), della direttiva 95/46 [...] non può avere un contenuto variabile in funzione degli Stati membri. Si tratta quindi di una nozione autonoma del diritto

133 Cfr. anche la direttiva sulla protezione dei dati personali, considerando 32.

134 CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008.

comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva come definita dal suo art. 1, n. 1"[135].

La Corte rileva che il diritto alla libera circolazione di un cittadino dell'Unione nel territorio di uno Stato membro di cui questi non ha la nazionalità non è incondizionato, ma può essere subordinato alle limitazioni e alle condizioni previste dal trattato nonché dalle relative disposizioni di attuazione. Pertanto se, in linea di principio, è legittimo che uno Stato membro disponga di un registro centralizzato come l'AZR quale ausilio per le autorità incaricate di applicare la normativa in materia di soggiorno, un siffatto registro non può contenere informazioni diverse da quelle a tal fine necessarie. La Corte conclude che un siffatto sistema per il trattamento dei dati personali è conforme al diritto dell'Unione se contiene unicamente i dati necessari per l'applicazione di detta normativa e se il suo carattere centralizzato consente un'applicazione più efficace di tale normativa. Il giudice nazionale deve accertare se dette condizioni siano soddisfatte in questo caso particolare. Diversamente, la conservazione e il trattamento dei dati personali in un registro come l'AZR per finalità statistiche non possono, su qualsiasi base, essere considerati necessari ai sensi dell'articolo 7, lettera e), della direttiva 95/46/CE[136].

Infine, per quanto riguarda la questione dell'utilizzo dei dati contenuti nel registro per finalità di lotta alla criminalità, la Corte ritiene che questo obiettivo riguardi "necessariamente la repressione dei reati commessi, a prescindere dalla cittadinanza dei loro autori". Il registro in questione non contiene dati personali relativi ai cittadini dello Stato membro interessato e questa differenza di trattamento costituisce una discriminazione vietata dall'articolo 18 del TFUE. Di conseguenza, tale disposizione, come interpretata dalla Corte, "osta all'istituzione da parte di uno Stato membro, per finalità di lotta alla criminalità, di un sistema di trattamento di dati personali riguardante specificamente i cittadini dell'Unione non aventi la nazionalità di tale Stato membro"[137].

Anche l'utilizzo dei dati personali da parte delle autorità che operano nell'ambito pubblico è subordinato all'articolo 8 della CEDU.

135 *Ibid.*, punto 52.

136 *Ibid.*, punti 54, 58, 59 e 66-68.

137 *Ibid.*, punti 78 e 81.

Interessi legittimi perseguiti dal titolare del trattamento o da terzi

L'interessato non è l'unico soggetto portatore di interessi legittimi. L'articolo 7, lettera f), della direttiva sulla protezione dei dati personali, dispone che i dati personali possono essere trattati lecitamente se il trattamento "è necessario per il perseguimento dell'interesse legittimo" del titolare del trattamento "oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali" dell'interessato, "che richiedono tutela [...]".

Nella sentenza riportata di seguito la CGUE si è pronunciata esplicitamente sull'articolo 7, lettera f), della direttiva.

Esempio: nella causa *ASNEF e FECEMD*[138], la CGUE ha chiarito che la normativa nazionale non è autorizzata ad aggiungere condizioni a quelle previste nell'articolo 7, lettera f), della direttiva per il trattamento lecito dei dati. Questa precisazione fa riferimento ad una disposizione del diritto spagnolo in materia di protezione dei dati secondo la quale altre parti private potrebbero rivendicare un interesse legittimo nel trattamento dei dati personali solo se le informazioni fossero già apparse in fonti accessibili al pubblico.

La Corte ha anzitutto rilevato che la direttiva 95/46 mira a garantire che il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento dei dati personali è equivalente in tutti gli Stati membri. Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nell'UE[139]. Di conseguenza, la CGUE ha dichiarato che "dall'obiettivo consistente nel garantire un livello di protezione equivalente in tutti gli Stati membri deriva che l'art. 7 della direttiva 95/46 prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito". Inoltre, "gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali all'art. 7 della direttiva 95/46, né prevedere requisiti supplementari che vengano a

138 CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011.

139 *Ibid.*, punto 28. Cfr. la direttiva sulla tutela dei dati, considerando 8 e 10.

modificare la portata di uno dei sei principi previsti da detto articolo"[140]. La Corte ha ammesso che "[p]er quanto riguarda la ponderazione necessaria in forza dell'art. 7, lett. f), della direttiva 95/46 è possibile prendere in considerazione il fatto che la gravità della violazione dei diritti fondamentali della persona interessata da tale trattamento possa variare in funzione della circostanza che i dati di cui trattasi figurino già, o no, in fonti accessibili al pubblico".

Tuttavia, "l'art. 7, lett. f), della direttiva, [...] osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico".

Alla luce di tali considerazioni, la Corte ha concluso che "l'art. 7, lett. f), della direttiva 95/46 deve essere interpretato nel senso che osta ad una normativa nazionale che, in assenza del consenso della persona interessata e per autorizzare il trattamento dei suoi dati personali, necessario alla realizzazione del legittimo interesse perseguito dal responsabile di tale trattamento oppure dal o dai terzi ai quali tali dati vengono comunicati, richiede, oltre al rispetto dei diritti e delle libertà fondamentali di detta persona, che i dati in parola figurino in fonti accessibili al pubblico, escludendo quindi in modo categorico e generalizzato qualsiasi trattamento di dati che non figurino in tali fonti"[141].

Formulazioni analoghe possono essere rinvenute nelle raccomandazioni del CDE. La raccomandazione sulla profilazione riconosce la legittimità del trattamento di dati personali per finalità di profilazione se necessario per gli interessi legittimi altrui, tranne qualora prevalgano su tali interessi i diritti e le libertà fondamentali degli interessati[142].

4.1.2. Liceità del trattamento dei dati sensibili

Il diritto del CDE affida alla normativa nazionale il compito di definire una protezione adeguata per l'utilizzo dei dati sensibili, mentre **il diritto dell'UE**, all'articolo 8 della direttiva sulla protezione dei dati personali, contiene un regime specifico per il trattamento di categorie di dati che rivelano l'origine razziale o etnica, le opinioni

140 CGUE, *cause riunite C-468/10 e C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, punti 30 e 32.

141 *Ibid*., punti 40, 44, 48 e 49.

142 Raccomandazione sulla profilazione, articolo 3.4, lettera b).

politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o informazioni sulla salute o sulla vita sessuale. In linea di principio il trattamento dei dati sensibili è vietato[143]. Tuttavia, esiste un elenco esaustivo e numerato delle deroghe previste a tale divieto, reperibile nell'articolo 8, paragrafi 2 e 3, della direttiva. Tali deroghe comprendono il consenso esplicito dell'interessato, gli interessi vitali di quest'ultimo, gli interessi legittimi altrui e l'interesse pubblico.

Contrariamente a quanto avviene per il trattamento dei dati non sensibili, un rapporto contrattuale con l'interessato non è visto come una base generale per il trattamento legittimo dei dati sensibili. Pertanto, se i dati sensibili devono essere trattati nel quadro di un contratto con l'interessato, l'utilizzo degli stessi richiede il consenso esplicito e a sé stante dell'interessato, oltre all'accettazione della stipula del contratto. Una richiesta esplicita da parte dell'interessato di prodotti o servizi che rivelino necessariamente i dati sensibili dovrebbe, tuttavia, essere considerata valida al pari del consenso esplicito.

Esempio: se, all'atto di prenotare un volo, un passeggero di una compagnia aerea chiede a detta compagnia di fornire una sedia a rotelle e cibo kosher, la compagnia può utilizzare questi dati anche se il passeggero non ha firmato una clausola di consenso supplementare dichiarando di accettare l'utilizzo dei suoi dati che rivelano informazioni sulla sua salute e sulla sua fede religiosa.

Consenso esplicito dell'interessato

La prima condizione perché sia lecito il trattamento dei dati, siano essi sensibili o non sensibili, è il consenso dell'interessato. Nel caso di dati sensibili, tale consenso deve essere esplicito. Tuttavia, la normativa nazionale può prevedere che il consenso all'utilizzo dei dati sensibili non costituisce una base giuridica sufficiente per consentirne il trattamento[144], per esempio quando, in casi eccezionali, tale trattamento comporti rischi inusuali per l'interessato.

In un caso specifico, perfino il consenso implicito è riconosciuto come base giuridica per il trattamento di dati sensibili: l'articolo 8, paragrafo 2, lettera e), della direttiva prevede che il trattamento non è proibito se riguarda dati resi manifestamente pubblici dall'interessato. Questa disposizione presuppone evidentemente che l'azione

143 Direttiva sulla protezione dei dati personali, articolo 8, paragrafo 1.

144 *Ibid.*, articolo 8, paragrafo 2, lettera a).

dell'interessato di rendere pubblici i propri dati debba essere interpretata come un consenso implicito dell'interessato all'utilizzo dei dati in questione.

Interessi vitali dell'interessato

Come nel caso dei dati non sensibili, i dati sensibili possono essere trattati in ragione degli interessi vitali dell'interessato[145].

Affinché il trattamento dei dati sensibili sia legittimo in base a quanto sopra, è necessario che si sia verificata l'impossibilità di sottoporre la questione all'interessato consentendogli di prendere una decisione in merito, perché per esempio l'interessato era incosciente o assente e non poteva essere contattato.

Interessi legittimi altrui

Come per i dati non sensibili, gli interessi legittimi altrui possono costituire la base per il trattamento dei dati sensibili. Tuttavia, per i dati sensibili e ai sensi dell'articolo 8, paragrafo 2, della direttiva sulla protezione dei dati personali questo si applica solo ai seguenti casi:

- quando il trattamento è necessario per salvaguardare l'interesse vitale di un'altra persona[146] e l'interessato è nell'incapacità fisica o giuridica di dare il proprio consenso;

- quando i dati sensibili sono pertinenti in materia di diritto del lavoro, come i dati sanitari nell'ambito di un posto di lavoro particolarmente pericoloso, o i dati sulle convinzioni religiose, come nell'ambito delle vacanze[147];

- quando fondazioni, associazioni o altri organismi che non perseguono scopi di lucro e rivestono carattere politico, filosofico, religioso o sindacale trattano i dati riguardanti i loro soci o sponsor o altre parti interessate (tali dati sono sensibili perché possono rivelare le convinzioni religiose o politiche degli individui interessati)[148];

145 *Ibid.*, articolo 8, paragrafo 2, lettera c).

146 *Ibid.*

147 *Ibid.,* articolo 8, paragrafo 2, lettera b).

148 *Ibid.,* articolo 8, paragrafo 2, lettera d).

- quando i dati sensibili sono utilizzati nell'ambito di un procedimento giudiziario dinanzi a un'autorità giudiziaria o amministrativa per costituire, esercitare o difendere un diritto per via giudiziaria[149].

- Inoltre, ai sensi dell'articolo 8, paragrafo 3, della direttiva sulla protezione dei dati personali, qualora i dati sanitari siano utilizzati a fini di diagnostica medica e della somministrazione di cure mediche da parte di operatori sanitari, la gestione di questi servizi è inclusa in questa deroga. A titolo di garanzia specifica, l'espressione "operatori sanitari" si riferisce solo a coloro che sono soggetti a specifici obblighi professionali di riservatezza.

Interesse pubblico

Inoltre, ai sensi dell'articolo 8, paragrafo 4, della direttiva sulla protezione dei dati personali, gli Stati membri possono introdurre ulteriori finalità per le quali i dati sensibili possono essere trattati, purché:

- il trattamento dei dati avvenga per motivi di interesse pubblico rilevante; e

- sia previsto dalla legislazione nazionale o da una decisione dell'autorità di controllo; e

- la legislazione nazionale o la decisione dell'autorità di controllo prevedano le opportune garanzie per proteggere in modo efficace gli interessi degli interessati[150].

Un esempio significativo riguarda i sistemi di cartelle cliniche elettroniche, la cui istituzione è prevista in molti Stati membri. Grazie a tali sistemi, i dati sanitari raccolti dagli operatori durante il trattamento di un paziente sono messi a disposizione di altri operatori sanitari che si occupano del paziente in questione su larga scala, di solito a livello nazionale.

Il Gruppo di lavoro articolo 29 ha concluso che l'istituzione di tali sistemi non potrebbe avvenire in base alle norme giuridiche vigenti che riguardano il trattamento dei dati sui pazienti ai sensi dell'articolo 8, paragrafo 3, della direttiva sulla protezione dei dati personali. Supponendo che l'esistenza di tali sistemi di cartelle

149 *Ibid.*, articolo 8, paragrafo 2, lettera e).

150 *Ibid.*, articolo 8, paragrafo 4.

cliniche elettroniche costituisca tuttavia un interesse pubblico rilevante, questa potrebbe basarsi sull'articolo 8, paragrafo 4, della direttiva, che richiede una base giuridica esplicita per la loro creazione e che contiene inoltre le garanzie necessarie per una gestione sicura del sistema[151].

4.2. Norme sulla sicurezza del trattamento

Punti salienti

- Le norme sulla sicurezza del trattamento implicano un obbligo del titolare del trattamento e del responsabile del trattamento di attuare misure tecniche e organizzative adeguate per prevenire ogni ingerenza non autorizzata nelle operazioni di trattamento dei dati.
- Il livello necessario di sicurezza dei dati è determinato da:
  - le caratteristiche di sicurezza disponibili sul mercato per ogni tipo specifico di trattamento;
  - i costi;
  - la sensibilità dei dati trattati.
- La sicurezza del trattamento dei dati è ulteriormente salvaguardata dall'obbligo generale di tutti i soggetti, titolari o responsabili del trattamento, di garantire che i dati rimangano riservati.

L'obbligo dei titolari e dei responsabili del trattamento di predisporre misure adeguate per garantire la sicurezza dei dati è, pertanto, previsto nel **diritto del CDE** nonché **nel diritto dell'UE in materia di protezione dei dati.**

4.2.1. Elementi di sicurezza dei dati

Conformemente alle disposizioni pertinenti contenute nel **diritto dell'UE:**

> *"Gli Stati membri dispongono che "il titolare del trattamento "deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla*

151 Gruppo di lavoro articolo 29 (2007), Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), WP 131, Bruxelles,15 febbraio 2007.

perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali"[152].

Una disposizione simile vige ai sensi del **diritto del CDE**:

"Idonee misure di sicurezza vengono adottate per la protezione dei dati a carattere personale registrati nelle collezioni automatizzate contro la distruzione accidentale o non autorizzata, o la perdita accidentale, nonché contro l'accesso, la modificazione o la diffusione non autorizzati"[153].

Spesso sono state elaborate anche norme industriali, nazionali e internazionali per il trattamento sicuro dei dati. Il marchio di certificazione europeo di tutela della privacy (EuroPriSe), per esempio, è un progetto eTEN (reti trans europee nel settore delle telecomunicazioni) dell'UE che ha valutato le possibilità di certificare prodotti, in particolare software, conformemente al diritto europeo in materia di protezione dei dati. L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) è stata istituita per accrescere la capacità dell'UE, dei suoi Stati membri e della comunità imprenditoriale, di prevenire, affrontare e rispondere ai problemi di sicurezza informatica e di rete[154]. L'ENISA pubblica regolarmente analisi delle attuali minacce alla sicurezza nonché consigli su come affrontarle.

La sicurezza dei dati non si ottiene solo mettendo in atto gli strumenti giusti, hardware e software, ma richiede anche adeguate norme organizzative interne. Tali norme interne dovrebbero includere idealmente i seguenti aspetti:

- trasmissione periodica a tutto il personale delle informazioni riguardanti le norme sulla sicurezza dei dati e i loro obblighi in base al diritto in materia di protezione dei dati, specialmente per quanto riguarda gli obblighi di riservatezza;

- distribuzione chiara delle responsabilità e delineazione netta delle competenze in tema di trattamento dei dati, specie in relazione alle decisioni di trattare i dati personali e di trasferirli a terzi;

152 Direttiva sulla protezione dei dati, articolo 17, paragrafo 1.

153 Convenzione n. 108, articolo 7.

154 Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004).

- utilizzo dei dati personali solo in osservanza delle istruzioni impartite dalla persona competente o secondo le norme generali vigenti;
- protezione dell'accesso alle sedi e all'hardware e al software del titolare del trattamento o del responsabile del trattamento, compresi i controlli relativi all'autorizzazione all'accesso;
- garanzia che le autorizzazioni all'accesso ai dati personali siano state assegnate dalla persona competente su richiesta della documentazione adeguata;
- protocolli automatizzati sull'accesso ai dati personali con mezzi elettronici e controlli regolari di tali protocolli da parte dell'ufficio di vigilanza interna;
- accurata documentazione per altre forme di divulgazione oltre all'accesso automatico ai dati, al fine di dimostrare che non ha avuto luogo alcuna trasmissione illegale di dati.

L'offerta di un'adeguata formazione e istruzione sulla sicurezza dei dati a tutti i membri del personale costituisce ugualmente un elemento importante delle precauzioni effettive in materia di sicurezza. Inoltre, è necessario attuare procedure di verifica intese a garantire che le misure adeguate non siano soltanto teoriche ma vengano attuate e funzionino concretamente (come gli audit interni o esterni).

Le misure volte a migliorare il livello di sicurezza di un titolare del trattamento o di un responsabile del trattamento prevedono l'intervento di responsabili della protezione dei dati personali, la formazione del personale in tema di sicurezza, audit regolari, test d'intrusione e marchi di qualità.

Esempio: nella causa *I. c. Finlandia*[155], la ricorrente non era stata in grado di dimostrare che altri dipendenti dell'ospedale per cui lavorava avevano avuto accesso alle sue cartelle cliniche sanitarie in modo illecito. La violazione del proprio diritto alla protezione dei dati, asserita dalla ricorrente, era stata pertanto respinta dai giudici nazionali. La Corte EDU ha concluso che vi era stata una violazione dell'articolo 8 della CEDU, poiché il sistema dei registri dell'ospedale per la gestione delle cartelle cliniche non consentiva di chiarire retroattivamente quale uso fosse stato fatto dei registri dei pazienti, dal momento che

155 Corte EDU, *I. c. Finlandia*, n. 20511/03, del 17 luglio 2008.

recava solamente le ultime cinque consultazioni più recenti e che tali informazioni venivano cancellate dopo il ritorno delle cartelle negli archivi. La Corte EDU ha ritenuto decisivo il fatto che il sistema dei registri in uso nell'ospedale fosse stato chiaramente in contrasto con gli obblighi legali previsti dalla normativa nazionale, aspetto che non aveva ricevuto la debita considerazione da parte dei giudici nazionali.

Notificazioni di violazioni di dati personali

Nel diritto di diversi paesi europei in materia di protezione dei dati è stato introdotto un nuovo strumento per affrontare le violazioni della sicurezza dei dati. Detto strumento consiste nell'obbligo per i fornitori di servizi di comunicazioni elettroniche di notificare le violazioni in materia di dati personali alle presunte vittime e alle autorità di controllo. Per i fornitori di servizi di telecomunicazione questo compito è obbligatorio in base al diritto dell'UE[156]. La finalità delle notificazioni di violazioni in materia di dati personali agli interessati è quella di evitare che sia recato pregiudizio: la notificazione di tali violazioni e delle loro possibili conseguenze riduce al minimo il rischio di conseguenze negative per gli interessati. In casi di negligenza grave, i fornitori possono anche essere sanzionati.

Sarà necessario definire preventivamente procedure interne per la gestione efficace e la comunicazione delle violazioni della sicurezza, poiché in genere le tempistiche per l'obbligo di comunicazione agli interessati e/o all'autorità di controllo, secondo la normativa nazionale, sono alquanto brevi.

4.2.2. Riservatezza

Ai sensi del diritto dell'UE, il trattamento sicuro dei dati è ulteriormente salvaguardato dall'obbligo generale di tutte le persone, titolari del trattamento o responsabili del trattamento, di garantire che i dati rimangano riservati.

156 Cfr. la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*), GU L 201 del 31.7.2002, articolo 4, paragrafo 3, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009.

Esempio: una dipendente di una compagnia assicurativa riceve una telefonata sul luogo di lavoro da qualcuno che le dice di essere un cliente e richiede informazioni relative al proprio contratto assicurativo.

L'obbligo di mantenere i dati del cliente riservati esige che la dipendente applichi perlomeno misure di sicurezza minime prima di divulgare i dati personali. Ciò potrebbe essere fatto, per esempio, proponendo di richiamare al numero di telefono riportato nel fascicolo del cliente.

L'articolo 16 della direttiva sulla protezione dei dati personali riguarda la riservatezza limitata al rapporto tra titolare del trattamento e responsabile del trattamento. Gli articoli 7 e 8 della direttiva stabiliscono se i titolari del trattamento debbano mantenere o meno i dati riservati, potendo o meno divulgarli a terzi.

L'obbligo di riservatezza non si estende alle situazioni in cui i dati sono portati a conoscenza di una persona in qualità di privato e non come dipendente di un titolare o di un responsabile del trattamento. In questo caso, l'articolo 16 della direttiva sulla protezione dei dati personali non si applica poiché, in effetti, l'utilizzo dei dati personali da parte di privati esula completamente dal campo di applicazione della direttiva nei casi laddove tale utilizzo rientri nella cosiddetta esenzione per l'esercizio di attività a carattere personale o domestico[157]. Tale esenzione riguarda l'utilizzo dei dati personali da parte di "una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico"[158]. In seguito alla sentenza della CGUE pronunciata nella causa *Bodil Lindqvist*[159], detta esenzione deve essere però interpretata in senso restrittivo, specialmente per quanto riguarda la divulgazione dei dati. In particolare, l'esenzione per l'esercizio di attività a carattere personale o domestico non si estende alla pubblicazione di dati personali a uso di un numero illimitato di destinatari su Internet (per maggiori dettagli sulla causa cfr. i paragrafi 2.1.2, 2.2, 2.3.1 e 6.1).

In base al diritto del CDE, l'obbligo di riservatezza è implicito nella nozione di sicurezza dei dati di cui all'articolo 7 della Convenzione n. 108, che verte sulla sicurezza dei dati.

Per i responsabili del trattamento, la riservatezza si traduce nel permesso di utilizzare i dati personali affidati loro dal titolare del trattamento solo in linea con le

157 Direttiva sulla protezione dei dati personali, articolo 3, paragrafo 2, secondo trattino.

158 *Ibid.*

159 CGUE, C-101/01, *Lindqvist*, 6 novembre 2003.

istruzioni impartite da quest'ultimo. Per i dipendenti di un titolare o di un responsabile del trattamento, la riservatezza implica l'utilizzo dei dati personali attenendosi esclusivamente alle istruzioni dei propri superiori competenti.

L'obbligo di riservatezza deve essere incluso in qualsiasi contratto stipulato tra i titolari del trattamento e i relativi responsabili. Inoltre, i titolari e i responsabili del trattamento dovranno adottare misure specifiche per far sì che i propri dipendenti siano subordinati a un obbligo giuridico di riservatezza, generalmente definito mediante l'inclusione di clausole di riservatezza nel contratto di lavoro del dipendente.

La violazione degli obblighi professionali di riservatezza è punibile ai sensi del diritto penale in molti Stati membri dell'UE e parti contraenti della Convenzione n. 108.

4.3. Norme sulla trasparenza del trattamento

Punti salienti

- Prima di avviare il trattamento dei dati personali, il titolare del trattamento deve quanto meno informare gli interessati circa l'identità del titolare del trattamento e la finalità del trattamento dei dati, a meno che l'interessato non sia già in possesso di queste informazioni.
- Qualora i dati siano raccolti da terzi, l'obbligo di fornire informazioni non si applica se:
  - il trattamento dei dati è previsto dalla legge; o
  - la fornitura di informazioni si rivela impossibile o richiederebbe uno sforzo sproporzionato.
- Prima di avviare il trattamento dei dati personali, il titolare del trattamento deve inoltre:
  - notificare all'autorità di controllo le operazioni di trattamento previste; o
  - far documentare internamente il trattamento da un responsabile della protezione dei dati personali indipendente, se la normativa nazionale prevede tali procedure.

Il principio di correttezza del trattamento esige la trasparenza dello stesso. **Il diritto del CDE** dispone, a questo proposito, che qualsiasi persona debba poter accertare l'esistenza di trattamenti dei dati, la loro finalità e il titolare del trattamento[160]. La

160 Convenzione n. 108, articolo 8, lettera a).

modalità di attuazione di quanto sopra è stabilita dal diritto nazionale. **Il diritto dell'UE** è più specifico, poiché garantisce la trasparenza per l'interessato attraverso l'obbligo posto in capo al titolare del trattamento di informare l'interessato stesso e per il pubblico in generale per mezzo di una notificazione.

Per entrambi i sistemi giuridici, le deroghe e le restrizioni derivanti dagli obblighi di trasparenza del titolare del trattamento possono essere contemplate nella normativa nazionale quando tali restrizioni costituiscono una misura necessaria per salvaguardare taluni interessi pubblici, la protezione dell'interessato oppure i diritti e le libertà altrui, fintanto che sia necessario in una società democratica[161]. Tali deroghe possono essere necessarie per esempio nell'ambito di indagini penali, ma possono essere giustificate anche in altre circostanze.

4.3.1. Informazione

In base al diritto del CDE e del diritto dell'UE, i titolari delle operazioni di trattamento sono obbligati a informare preventivamente l'interessato circa la finalità del trattamento[162]. Quest'obbligo non dipende da una richiesta dell'interessato ma dev'essere rispettato in modo proattivo dal titolare del trattamento, a prescindere dal fatto che l'interessato mostri o meno interesse per le informazioni.

Contenuto delle informazioni

Le informazioni devono comprendere la finalità del trattamento nonché l'identità e i recapiti del titolare del trattamento[163]. La direttiva sulla protezione dei dati personali richiede che siano fornite maggiori informazioni "nella misura in cui, in considerazione delle specifiche circostanze in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento leale nei confronti" dell'interessato. Gli articoli 10 e 11 della direttiva prevedono, tra l'altro, le categorie dei dati trattati e i destinatari di tali dati, nonché l'esistenza del diritto di accesso ai dati e del diritto di rettifica di questi ultimi. Qualora i dati siano raccolti dagli interessati, le informazioni dovrebbero chiarire se rispondere alle domande è obbligatorio o facoltativo nonché le possibili conseguenze di una mancata risposta[164].

161 *Ibid*., articolo 9, paragrafo 2; e direttiva sulla protezione dei dati personali, articolo 13, paragrafo 1.

162 Convenzione n. 108, articolo 8, lettera a); direttiva sulla protezione dei dati personali , articoli 10 e 11.

163 Convenzione n. 108, articolo 8, lettera a); direttiva sulla protezione dei dati personali, articolo 10, lettere a) e b).

164 Direttiva sulla protezione dei dati personali, articolo 10, lettera c).

Nell'ottica del **diritto del CDE**, la fornitura di tali informazioni può essere considerata una buona pratica secondo il principio di correttezza del trattamento dei dati e, in tale misura, è anche parte del diritto del CDE.

Il principio di correttezza del trattamento richiede che le informazioni siano di facile comprensione per l'interessato. Il linguaggio adoperato deve essere appropriato per i destinatari. Il livello e il tipo di linguaggio utilizzato devono differenziarsi in funzione del pubblico di riferimento, per esempio adulti o bambini, pubblico in generale o accademici esperti.

Alcuni interessati vorranno ricevere solo informazioni sintetiche circa la modalità e la motivazione del trattamento dei loro dati, mentre altri richiederanno una spiegazione dettagliata. Le modalità per bilanciare tale aspetto della correttezza delle informazioni sono trattate in un parere del Gruppo di lavoro articolo 29 che promuove l'idea delle cosiddette avvertenze a livelli multipli[165], che consentono all'interessato di decidere in merito al livello di dettaglio delle informazioni.

Tempistiche per la fornitura delle informazioni

La direttiva sulla protezione dei dati personali contiene disposizioni leggermente diverse relativamente alle tempistiche con cui le informazioni devono essere fornite, a seconda se i dati sono raccolti presso l'interessato (articolo 10) o presso terzi (articolo 11). Qualora i dati siano raccolti presso l'interessato, le informazioni devono essere fornite, al più tardi, al momento della raccolta. Nel caso in cui i dati siano raccolti presso terzi, le informazioni devono essere fornite, al più tardi, nel momento in cui il titolare del trattamento registra i dati o prima che i dati siano divulgati a terzi per la prima volta.

Deroghe all'obbligo d'informazione

In base al diritto dell'Unione esiste una deroga generale all'obbligo d'informare l'interessato se questi è già in possesso delle informazioni[166]. Ciò si riferisce alle situazioni in cui l'interessato, secondo le circostanze del caso, è già a conoscenza del fatto che i suoi dati saranno trattati per una certa finalità da un determinato titolare del trattamento.

165 Gruppo di lavoro articolo 29 (2004), Parere 10/2004 sulla maggiore armonizzazione della fornitura di informazioni, WP 100, Bruxelles, 25 novembre 2004.

166 Direttiva sulla protezione dei dati personali, articolo 10 e articolo 11, paragrafo 1.

L'articolo 11 della direttiva relativo all'obbligo d'informare l'interessato quando i dati non siano stati ottenuti dallo stesso stabilisce anche che non esiste un tale obbligo, in particolare in relazione al trattamento a scopi statistici o di ricerca storica o scientifica, qualora:

- la fornitura di tali informazioni risulti impossibile; o
- implichi uno sforzo sproporzionato; oppure
- la registrazione o la comunicazione dei dati sia espressamente prescritta per legge[167].

Solo l'articolo 11, paragrafo 2, della direttiva sulla protezione dei dati personali stabilisce che non vi è necessità di informare gli interessati circa le operazioni di trattamento se queste sono prescritte per legge. Data l'ipotesi giuridica generale che il diritto è conosciuto da chi vi è soggetto, si potrebbe sostenere che, quando i dati sono raccolti presso l'interessato ai sensi dell'articolo 10 della direttiva, lo stesso interessato è in possesso delle informazioni. Tuttavia, poiché la conoscenza del diritto è solo un'ipotesi, il principio della correttezza del trattamento richiederebbe, ai sensi dell'articolo 10, che l'interessato sia informato anche se il trattamento è prescritto per legge, in particolare perché informare l'interessato non è particolarmente oneroso quando i dati sono raccolti direttamente presso lo stesso.

Per quanto riguarda il diritto del CDE, la Convenzione n. 108 prevede esplicitamente delle deroghe all'articolo 8 ivi contenuto. Anche in questo caso, le deroghe di cui agli articoli 10 e 11 della direttiva sulla protezione dei dati personali possono essere interpretate come esempi di buona pratica per le deroghe ai sensi dell'articolo 9 della Convenzione n. 108.

Diverse modalità di fornitura delle informazioni

La modalità ideale per la fornitura delle informazioni sarebbe quella di rivolgersi a ogni singolo interessato, a voce o per iscritto. Se i dati sono raccolti presso l'interessato, la fornitura delle informazioni dovrebbe andare di pari passo con la raccolta. Soprattutto quando i dati sono raccolti presso terzi, tuttavia, date le evidenti difficoltà pratiche di raggiungere gli interessati personalmente, le informazioni possono essere fornite anche tramite un'adeguata pubblicazione.

167 *Ibid.*, considerando 40, e articolo 11, paragrafo 2.

Uno dei modi più efficaci per fornire le informazioni sarà quello di disporre di adeguate clausole informative sulla pagina iniziale del sito Internet del titolare del trattamento, come per esempio una politica sulla privacy relativa al sito Internet. Vi è tuttavia una parte considerevole della popolazione che non utilizza Internet e la politica d'informazione di una società o di un'autorità pubblica deve tenere conto di questo aspetto.

4.3.2. Notificazione

La normativa nazionale può obbligare i titolari del trattamento a notificare all'autorità di controllo competente le proprie operazioni di trattamento in modo che queste possano essere pubblicate. In alternativa, la normativa nazionale può prevedere che i titolari del trattamento facciano ricorso a un responsabile della protezione dei dati personali, cui è affidato in particolare il compito di tenere un registro delle operazioni di trattamento effettuate dal titolare del trattamento[168]. Questo registro interno deve essere messo a disposizione del pubblico su richiesta.

> Esempio: una notificazione e parimenti la documentazione di un responsabile della protezione dei dati personali interno devono descrivere le caratteristiche principali del trattamento in questione. Ciò includerà le informazioni sul titolare del trattamento, la finalità e la base giuridica del trattamento, le categorie dei dati trattati, i possibili destinatari terzi e se sono previsti flussi tranfrontalieri di dati nonché, in tal caso, quali.

La pubblicazione delle notificazioni da parte dell'autorità di controllo deve assumere la forma di un registro speciale. Per rispondere al suo obiettivo, l'accesso a questo registro deve essere facile e gratuito. Lo stesso vale per la documentazione tenuta da un responsabile della protezione dei dati personali di un titolare del trattamento.

Gli esoneri dagli obblighi di notificazione all'autorità di controllo competente o dall'impiego di un responsabile della protezione dei dati interno possono sussistere in virtù della normativa nazionale per le operazioni di trattamento che non siano tali da recare uno specifico pregiudizio agli interessati. Tali esoneri sono elencati nell'articolo 18, paragrafo 2, della direttiva sulla protezione dei dati personali[169].

168 *Ibid.*, articolo 18, paragrafo 2, secondo trattino.

169 *Ibid.*, articolo 18, paragrafo 2, primo trattino.

4.4. Regole per promuovere l'osservanza delle norme di protezione dei dati

Punti salienti

- Sviluppando il principio di responsabilità, la direttiva sulla protezione dei dati personali menziona diversi strumenti atti a promuovere l'osservanza delle previsioni normative in essa contenute:
  - controllo preliminare, da parte dell'autorità di controllo nazionale, delle operazioni di trattamento che si intendono effettuare;
  - responsabili della protezione dei dati personali che forniscono al titolare del trattamento particolari competenze nel campo della protezione dei dati;
  - codici di condotta che specificano le norme vigenti in materia di protezione dei dati da applicarsi in diversi settori della società, in particolare quello delle imprese.
- Nella raccomandazione sulla profilazione, il diritto del CDE propone strumenti simili per promuovere l'osservanza delle norme di protezione dei dati.

4.4.1. Controllo preliminare

Ai sensi dell'articolo 20 della direttiva sulla protezione dei dati personali, prima che il trattamento abbia inizio l'autorità di controllo deve controllare le operazioni di trattamento suscettibili di comportare rischi specifici per i diritti e le libertà degli interessati, a causa della finalità o delle circostanze del trattamento. La normativa nazionale deve stabilire quali operazioni di trattamento debbano essere sottoposte al controllo preliminare. Tale controllo può condurre al divieto di effettuare determinate operazioni di trattamento o all'ordine di modificare le caratteristiche delle operazioni di trattamento che ci si propone di svolgere. L'articolo 20 della direttiva mira a garantire che un trattamento inutilmente rischioso non abbia nemmeno inizio, poiché l'autorità di controllo ha il potere di proibire tali operazioni. Il requisito primario perché questo meccanismo sia efficace è che l'autorità di controllo venga effettivamente informata. Al fine di garantire che i titolari del trattamento adempiano al proprio obbligo di comunicazione, le autorità di controllo necessitano di poteri coercitivi, quali la capacità di sanzionare i titolari del trattamento.

Esempio: se una società svolge operazioni di trattamento che, ai sensi della normativa nazionale, sono soggette a controlli preliminari, questa società deve

presentare all'autorità di controllo una documentazione relativa alle operazioni di trattamento programmate. Alla società non è consentito avviare operazioni di trattamento prima di aver ricevuto un responso positivo dall'autorità di controllo.

In alcuni Stati membri la normativa nazionale prevede in alternativa che le operazioni di trattamento possano iniziare in caso di mancata risposta dall'autorità di controllo entro un certo termine, per esempio tre mesi.

4.4.2. Responsabili della protezione dei dati personali

La direttiva sulla protezione dei dati personali attribuisce alla normativa nazionale la possibilità di stabilire che i titolari del trattamento designino un soggetto che agisca in qualità di responsabile della protezione dei dati personali[170]. Il compito di tale responsabile è quello di garantire che i diritti e le libertà degli interessati non siano pregiudicati dalle operazioni di trattamento[171].

Esempio: in Germania, ai sensi della legge federale tedesca sulla protezione dei dati personali (*Bundesdatenschutzgesetz*), articolo 4f, punto 1, le società private sono tenute a nominare un responsabile della protezione dei dati personali interno qualora impieghino permanentemente 10 o più persone nel trattamento automatizzato dei dati personali.

Per poter raggiungere questo obiettivo la posizione del responsabile deve godere di una certa indipendenza all'interno dell'organizzazione del titolare del trattamento, come esplicitamente indicato nella direttiva. Rafforzare i diritti dei lavoratori per prevenire eventualità come il licenziamento ingiustificato sarebbe inoltre necessario al fine di far sì che le funzioni del responsabile siano espletate in modo efficace.

Per promuovere l'osservanza della normativa nazionale in materia di protezione dei dati, il concetto di responsabile interno della protezione dei dati personali è stato adottato anche in alcune raccomandazioni del CDE[172].

170 *Ibid.*, articolo 18, paragrafo 2, secondo trattino.

171 *Ibid.*

172 Cfr., per esempio, la raccomandazione sulla profilazione, articolo 8.3.

4.4.3. Codici di condotta

Per promuovere l'osservanza delle norme in materia di protezione dei dati, le imprese e altri settori possono delineare regole dettagliate che disciplinino le loro attività di trattamento usuali, codificando le migliori prassi. Le competenze degli operatori del settore possono favorire l'individuazione di soluzioni pratiche e, pertanto, di probabile applicazione. In questo senso, gli Stati membri e la Commissione europea sono invitati a promuovere l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri[173].

Al fine di garantire che tali codici di condotta siano rispettosi delle disposizioni nazionali adottate ai sensi della direttiva sulla protezione dei dati personali, gli Stati membri devono definire una procedura di valutazione dei codici. Di norma, questa procedura dovrebbe richiedere il coinvolgimento dell'autorità nazionale, delle associazioni di settore e di altri enti che rappresentano altre categorie di titolari del trattamento[174].

I progetti di codici comunitari e le modifiche o le proroghe di codici comunitari esistenti possono essere sottoposti alla valutazione del Gruppo di lavoro articolo 29. In seguito ad approvazione di quest'ultimo, la Commissione europea può provvedere a un'appropriata divulgazione di tali codici[175].

Esempio: la Federazione europea del marketing diretto (FEDMA) ha sviluppato un codice di condotta europeo per l'utilizzo dei dati personali nella vendita diretta. Il codice è stato presentato con successo al Gruppo di lavoro articolo 29 e, nel 2010, è stato integrato da un allegato relativo alle comunicazioni nel settore del marketing online[176].

173 Cfr. la direttiva sulla protezione dei dati personali, articolo 27, paragrafo 1.

174 *Ibid*., articolo 27, paragrafo 2.

175 *Ibid*., articolo 27, paragrafo 3.

176 Gruppo di lavoro articolo 29 (2010), *Parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto*, WP 174, Bruxelles, 13 luglio 2010.

5

I diritti degli interessati e la relativa attuazione

Unione europea	Argomenti trattati	Consiglio d'Europa
Diritto di accesso		
Direttiva sulla tutela dei dati, articolo 12 CGUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, 7 maggio 2009	**Diritto di accesso ai propri dati**	Convenzione n. 108, articolo 8, lettera b)
	Diritto di rettifica, cancellazione o blocco del trattamento dei dati	Convenzione n. 108, articolo 8, lettera c) Corte EDU, *Cemalettin Canli c. Turchia*, n. 22427/04, 18 novembre 2008 Corte EDU, *Segerstedt-Wiberg e altri c. Svezia*, n. 62332/00, 6 giugno 2006 Corte EDU, *Ciubotaru c. Moldova*, n. 27138/04, 27 aprile 2010
Diritto di opposizione		
Direttiva sulla tutela dei dati, articolo 14, primo comma, lettera a)	**Diritto di opposizione per motivi legittimi derivanti dalla situazione particolare dell'interessato**	Raccomandazione sulla profilazione, articolo 5.3

Direttiva sulla tutela dei dati, articolo 14, primo comma, lettera b)	**Diritto di opposizione all'ulteriore uso dei dati a fini di invio di materiale pubblicitario**	Raccomandazione sulla promozione commerciale diretta, articolo 4.1
Direttiva sulla tutela dei dati, articolo 15	**Diritto di opposizione a decisioni automatizzate**	Raccomandazione sulla profilazione, articolo 5.5
Controllo indipendente		
Carta, articolo 8, paragrafo 3 Direttiva sulla tutela dei dati, articolo 28 Regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, capo V CGUE, C-518/07, *Commissione europea c. Repubblica federale di Germania*, 9 marzo 2010 CGUE, C-614/10, *Commissione europea c. Repubblica austriaca*, 16 ottobre 2012 CGUE, C-288/12, *Commissione europea c. Ungheria*, 8 aprile 2014	**Autorità di controllo nazionali**	Convenzione n. 108, Protocollo addizionale, articolo 1
Mezzi di ricorso e sanzioni		
Direttiva sulla tutela dei dati, articolo 12	**Richiesta rivolta al titolare del trattamento**	Convenzione n. 108, articolo 8, lettera b)
Direttiva sulla tutela dei dati, articolo 28, paragrafo 4 Regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, articolo 32, paragrafo 2	**Domande presentate all'autorità di controllo**	Convenzione n. 108, Protocollo addizionale, articolo 1, paragrafo 2, lettera b)
Carta, articolo 47	**Giudici (in generale)**	CEDU, articolo 13
Direttiva sulla tutela dei dati, articolo 28, paragrafo 3	**Giudici nazionali**	Convenzione n. 108, Protocollo addizionale, articolo 1, paragrafo 4
TFUE, articolo 263, quarto comma Regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, articolo 32, paragrafo 1 TFUE, articolo 267	**CGUE**	
	Corte EDU	CEDU, articolo 34

Mezzi di ricorso e sanzioni		
Carta, articolo 47 Direttiva sulla tutela dei dati, articoli 22 e 23 CGUE, C-14/83, *Sabine von Colson e Elisabeth Kamann c. Land Nordrhein-Westfalen*, 10 aprile 1984 CGUE, C-152/84, *M.H. Marshall c. Southampton and South-West Hampshire Area Health Authority*, 26 febbraio 1986	**Per violazioni del diritto nazionale in materia di tutela dei dati**	CEDU, articolo 13 (solo per gli Stati membri del CDE) Convenzione n. 108, articolo 10 Corte EDU, *K.U. c. Finlandia*, n. 2872/02, 2 dicembre 2008 Corte EDU, *Biriuk c. Lituania*, n. 23373/03, 25 novembre 2008
Regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, articoli 34 e 49 CGUE, C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd*, 29 giugno 2010	**Per violazioni del diritto dell'UE da parte delle istituzioni e degli organismi dell'Unione**	

L'efficacia delle norme giuridiche in generale e dei diritti degli interessati in particolare dipende, in larga misura, dall'esistenza di meccanismi adeguati per la loro attuazione. Nell'ambito del diritto europeo in materia di protezione dei dati, la normativa nazionale deve dare all'interessato i mezzi per proteggere i propri dati, oltre a designare autorità di controllo indipendenti con il compito di assistere l'interessato nell'esercizio dei propri diritti e di vigilare sul trattamento dei dati personali. Inoltre, il diritto a un ricorso effettivo, sancito dalla CEDU e dalla Carta, esige che siano messi a disposizione di ognuno mezzi di ricorso giurisdizionali.

5.1. I diritti degli interessati

Punti salienti

- Ai sensi della normativa nazionale, ogni persona deve avere il diritto di chiedere a un titolare del trattamento informazioni sull'esistenza di un trattamento dei propri dati da parte di detto titolare.
- La normativa nazionale deve garantire agli interessati il diritto di:
  - accedere ai propri dati presso qualsiasi titolare del trattamento che li stia trattando;
  - fare rettificare i propri dati (o farne bloccare il trattamento, se del caso) da parte del titolare del trattamento che li stia trattando, se i dati sono inesatti;

  - fare cancellare i propri dati o farne bloccare il trattamento, se del caso, da parte del titolare del trattamento se questi li sta trattando illegalmente.
- Inoltre, gli interessati hanno diritto di opposizione nei confronti dei titolari del trattamento nel caso di:
  - decisioni automatizzate (fondate su dati personali trattati esclusivamente con mezzi automatizzati);
  - trattamento dei propri dati che incida significativamente sull'interessato, per motivi legittimi;
  - uso dei propri dati a fini di marketing diretto.

5.1.1. Diritto di accesso

Nell'ambito del diritto dell'Unione, l'articolo 12 della direttiva sulla protezione dei dati delinea gli elementi del diritto di accesso dell'interessato, compreso il diritto di ottenere dal titolare del trattamento "la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati", nonché "la rettifica, la cancellazione" o il blocco dei dati "il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati".

Questi stessi diritti sono previsti **nell'ambito della normativa del CDE** e devono essere garantiti dalla normativa nazionale (articolo 8 della Convenzione n. 108/1981 del CDE). In diverse raccomandazioni del CDE è usato il termine "accesso" e sono descritti i diversi aspetti del diritto di accesso, dei quali si propone l'adozione nell'ambito della normativa nazionale, alla stregua di quanto illustrato al paragrafo precedente.

Ai sensi dell'articolo 9 della Convenzione n. 108 e dell'articolo 13 della direttiva sulla protezione dei dati, l'obbligo dei titolari del trattamento di rispondere a una richiesta di accesso avanzata dall'interessato può essere limitato in caso di prevalenti interessi giuridici di altri. Interessi giuridici prevalenti possono riguardare interessi pubblici quali la sicurezza nazionale, la pubblica sicurezza e il perseguimento di reati penali nonché interessi privati più impellenti degli interessi della tutela dei dati. Qualsiasi esenzione o restrizione deve essere necessaria in una società democratica e proporzionata allo scopo perseguito. In casi del tutto eccezionali, per esempio a causa di prescrizioni mediche, la tutela dell'interessato può esigere di per sé una restrizione

della trasparenza connessa, in particolare, alla restrizione del diritto di accesso degli interessati.

Quando i dati sono trattati esclusivamente a fini statistici o di ricerca scientifica, la direttiva sulla protezione dei dati consente alla normativa nazionale di limitare i diritti di accesso; tuttavia devono sussistere adeguate garanzie giuridiche. In particolare, occorre garantire che nessuna misura o decisione relative a una determinata persona siano adottate nel contesto di questo tipo di trattamento di dati personali e che "non sussista manifestamente alcun rischio di pregiudizio alla vita privata" dell'interessato[177]. Disposizioni simili sono contenute nell'articolo 9, paragrafo 3, della Convenzione n. 108.

Il diritto di accesso ai propri dati

Ai sensi del diritto del CDE, il diritto di accesso ai propri dati è riconosciuto esplicitamente dall'articolo 8 della Convenzione n. 108. La CEDU ha stabilito più volte che esiste un diritto di accesso alle informazioni concernenti i propri dati personali trattati da altri e che questo diritto nasce dalla necessità di rispettare la vita privata[178]. Nella causa *Leander*[179], la CEDU ha concluso che, in talune circostanze, il diritto di accesso ai dati personali conservati da autorità pubbliche potrebbe tuttavia essere limitato.

Ai sensi del diritto dell'UE, il diritto di acceso ai propri dati è riconosciuto esplicitamente dall'articolo 12 della direttiva sulla protezione dei dati e, come diritto fondamentale, dall'articolo 8, paragrafo 2, della Carta.

L'articolo 12, lettera a), della direttiva dispone che gli Stati membri garantiscano a qualsiasi interessato il diritto di accesso ai propri dati personali. In particolare, qualsiasi interessato ha il diritto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di trattamenti di dati che lo riguardano e di essere informato almeno:

- sulle finalità del trattamento;
- sulle categorie di dati trattati;

177 Direttiva sulla protezione dei dati, articolo 13, paragrafo 2.

178 Corte EDU, *Gaskin c. Regno Unito*, n. 10454/83, 7 luglio 1989; Corte EDU, *Odièvre c. Francia* [GC], n. 42326/98, 13 febbraio 2003; Corte EDU, *K.H. e a. c. Slovacchia*, n. 32881/04, 28 aprile 2009; Corte EDU, *Godelli c. Italia*, n. 33783/09, 25 settembre 2012.

179 Corte EDU, *Leander c. Svezia*, n. 9248/81, 11 luglio 1985.

- sui dati che sono oggetto di trattamento;
- sui destinatari o sulle categorie di destinatari cui sono comunicati i dati;
- sull'origine, per quanto disponibile, dei dati oggetto di trattamento;
- nel caso delle decisioni automatizzate, sulla logica applicata nei trattamenti automatizzati dei dati.

La normativa nazionale può aggiungere informazioni a carico del titolare del trattamento, indicando per esempio la base giuridica che autorizza il trattamento di dati personali.

> Esempio: accedendo ai propri dati personali, una persona è in grado di stabilire se i dati siano esatti o meno. Pertanto, è indispensabile che l'interessato sia informato sulle categorie di dati trattati e sul contenuto degli stessi. Non è sufficiente quindi che un titolare del trattamento si limiti a comunicare genericamente all'interessato che è in corso il trattamento del suo nome, del suo indirizzo, della sua data di nascita e della sua sfera di interessi. Il titolare deve fornire all'interessato comunicazione dettagliata dei dati trattati ossia il "nome: N.N.; indirizzo: 1040 Vienna, Schwarzenbergplatz 11, Austria; data di nascita: 10.10.1974 e sfera di interessi (in base alla dichiarazione dell'interessato): musica classica". L'ultimo elemento contiene, inoltre, informazioni sull'origine dei dati.

La comunicazione all'interessato dei dati in corso di trattamento e di qualsiasi informazione disponibile sulla loro origine deve essere effettuata in modo intelligibile. Questo significa che il titolare del trattamento potrebbe essere tenuto a spiegare più dettagliatamente all'interessato quale sia l'oggetto del trattamento. Solitamente, per esempio, la semplice citazione di abbreviazioni tecniche o di termini medici in risposta a una richiesta di accesso non sono sufficienti, anche se sono conservati solo tali acronimi o termini.

L'informazione sull'origine dei dati trattati dal titolare del trattamento deve essere fornita in risposta a una richiesta di accesso nella misura in cui tale informazione è disponibile. Detta disposizione deve essere intesa alla luce dei principi di correttezza e di responsabilità. Un titolare del trattamento non può eliminare le informazioni sull'origine dei dati per essere esonerato dalla divulgazione delle stesse, né può ignorare la norma ordinaria e i requisiti previsti per la documentazione nel proprio

settore di attività. Normalmente, la mancata conservazione di documenti sull'origine dei dati trattati non consente al titolare del trattamento di ottemperare ai propri obblighi nell'ambito del diritto di accesso.

L'effettuazione di valutazioni automatizzate esige che sia illustrata la logica generale della stessa valutazione, compresi i criteri specifici presi in considerazione in sede di valutazione dell'interessato.

La direttiva non chiarisce se il diritto di accesso alle informazioni riguardi il passato e, in tal caso, quale periodo del passato. A tale proposito, come rilevato nella giurisprudenza della CGUE, il diritto di accesso ai propri dati non deve essere indebitamente ristretto da limiti temporali. Gli interessati devono avere anche una ragionevole possibilità di acquisire informazioni sulle operazioni di trattamento dei dati effettuate in passato.

Esempio: nella causa *Rijkeboer*[180], la CGUE è stata chiamata a statuire se, ai sensi dell'articolo 12, lettera a), della direttiva il diritto di accesso di una persona alle informazioni sui destinatari o sulle categorie di destinatari dei dati personali e sul contenuto dei dati comunicati possa essere limitato a un anno precedente la sua richiesta di accesso.

Al fine di stabilire se l'articolo 12, lettera a), della direttiva autorizzi una siffatta limitazione temporale, la Corte ha deciso di interpretare l'articolo alla luce degli obiettivi della direttiva, dichiarando in primo luogo che il diritto di accesso è necessario affinché l'interessato possa esercitare il diritto di ottenere dal titolare del trattamento la rettifica, la cancellazione o il blocco del trattamento dei suoi dati (articolo 12, lettera b)), o affinché egli notifichi tale rettifica, cancellazione o blocco ai terzi cui sono stati comunicati tali dati, ai sensi dell'articolo 12, lettera c). Il diritto di accesso è anche necessario per consentire all'interessato l'esercizio del diritto di opposizione al trattamento dei suoi dati personali (articolo 14) o il diritto di agire in giudizio nel caso in cui subisca un pregiudizio (articoli 22 e 23).

Per garantire l'effetto utile delle disposizioni succitate, la Corte ha statuito che "tale diritto deve necessariamente estendersi al passato. In caso contrario, infatti", l'interessato "non sarebbe in grado di esercitare efficacemente il suo

180 CGUE, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, 7 maggio 2009.

diritto a fare rettificare, cancellare" o bloccare il trattamento dei "dati ritenuti illeciti o non corretti nonché a procedere giurisdizionalmente ed ottenere il risarcimento del pregiudizio subìto".

Diritto alla rettifica, alla cancellazione e al blocco del trattamento dei dati

"Una persona deve godere del diritto d'accesso ai dati che la riguardano e che sono oggetto di trattamento, per poter verificare, in particolare, la loro esattezza e la liceità del trattamento"[181]. In linea con detti principi, la normativa nazionale deve garantire agli interessati il diritto di ottenere dal titolare del trattamento la rettifica, la cancellazione o il blocco del trattamento dei loro dati se ritengono che il trattamento degli stessi non sia conforme alle disposizioni della direttiva, in particolare a causa del carattere incompleto o inesatto dei dati[182].

Esempio: nella causa *Cemalettin Canli c. Turchia*[183], la Corte EDU ha constatato una violazione dell'articolo 8 della CEDU derivante dalla presentazione di un rapporto di polizia inesatto nel corso di un procedimento penale.

Il ricorrente era stato sottoposto a due procedimenti penali a causa della presunta appartenenza a organizzazioni illegali, ma non era mai stato condannato. Quando il ricorrente era stato nuovamente arrestato e accusato di un altro reato, la polizia aveva trasmesso al tribunale penale un rapporto intitolato "*modulo informativo su ulteriori reati*" nel quale il ricorrente risultava essere membro di due organizzazioni illegali. La richiesta del ricorrente concernente la modifica del rapporto e degli schedari della polizia era stata respinta. La Corte EDU ha considerato che le informazioni contenute nel rapporto di polizia rientrassero nell'ambito di applicazione dell'articolo 8 della CEDU, dato che anche le informazioni pubbliche rientrano nella sfera della "vita privata" quando sono sistematicamente raccolte e conservate in fascicoli dalle autorità. Inoltre, il rapporto di polizia era inesatto e la sua formulazione e trasmissione al tribunale penale non erano state conformi alla legge. La Corte EDU ha concluso asserendo la sussistenza di una violazione dell'articolo 8.

181 Direttiva sulla tutela dei dati, considerando 41.

182 *Ibid.*, articolo 12, lettera b).

183 Corte EDU, *Cemalettin Canli c. Turchia*, n. 22427/04, 18 novembre 2008, punti 33, 42 e 43; Corte EDU, *Dalea c. Francia*, n. 964/07, 2 febbraio 2010.

Esempio: nella causa *Segerstedt-Wiberg e altri c. Svezia*[184], i ricorrenti erano stati membri di alcuni partiti politici di matrice socialista e comunista e sospettavano che nei registri dei servizi segreti fossero state inserite informazioni sul loro conto. La Corte EDU ha stimato che la conservazione dei dati in questione avesse una base giuridica e perseguisse uno scopo legittimo. Per quanto riguarda alcuni ricorrenti, la Corte EDU ha dichiarato che la persistente conservazione dei dati costituiva un'ingerenza sproporzionata nelle loro vite private. Nel caso del sig. Schmid, ad esempio, le autorità avevano conservato informazioni secondo le quali nel 1969 egli aveva asseritamente invocato la resistenza violenta contro i controlli di polizia nel corso di manifestazioni. La Corte EDU ha rilevato che detta informazione non avrebbe potuto perseguire alcun interesse rilevante di sicurezza nazionale, in particolare data la sua natura storica, e ha concluso asserendo la sussistenza di una violazione dell'articolo 8 della CEDU per quattro ricorrenti su cinque.

In alcuni casi basterà semplicemente che l'interessato chieda la rettifica, per esempio, della grafia di un nome oppure il cambio di un indirizzo o di un numero di telefono. Tuttavia, se tali richieste sono correlate a questioni giuridiche, come l'identità giuridica dell'interessato o l'esatto luogo di residenza per il rilascio di documenti legali, le richieste di rettifica possono rivelarsi insufficienti e il titolare del trattamento può richiedere la prova della presunta inesattezza. Tali domande non devono imporre un irragionevole onere della prova sull'interessato, impedendogli dunque di ottenere la rettifica dei propri dati. La Corte EDU ha rilevato violazioni dell'articolo 8 della CEDU in diversi casi in cui il ricorrente non era stato in grado di contestare l'esattezza delle informazioni contenute in registri segreti[185].

Esempio: nella causa *Ciubotaru c. Moldova*[186], il ricorrente non aveva potuto modificare l'indicazione della propria origine etnica, contenuta nei registri ufficiali, da moldava a rumena, asseritamente a causa del fatto che non era riuscito a suffragare tale richiesta. La Corte EDU ha ritenuto accettabile che gli Stati richiedessero prove oggettive all'atto della registrazione dell'identità etnica di una persona. Quando tali richieste sono basate su motivi puramente soggettivi e non comprovati, le autorità potrebbero respingerle. Tuttavia, la richiesta del ricorrente si fondava su qualcosa di più di una mera percezione soggettiva della

184 Corte EDU, *Segerstedt-Wiberg e a. c. Svezia*, n. 62332/00, 6 giugno 2006, punti 89 e 90; cfr. anche, ad esempio, Corte EDU, *M.K. c. Francia*, n. 19522/09, 18 aprile 2013.

185 Corte EDU, *Rotaru c. Romania*, n. 28341/95, 4 maggio 2000.

186 Corte EDU, *Ciubotaru c. Moldova*, n. 27138/04, 27 aprile 2010, punti 51 e 59.

propria etnia: egli era stato in grado di dimostrare legami oggettivamente verificabili con il gruppo etnico rumeno quali la lingua, il nome, l'affinità ecc. Tuttavia, secondo il diritto nazionale, il ricorrente era obbligato a dimostrare che i suoi genitori erano appartenuti al gruppo etnico rumeno. Date le realtà storiche della Moldova, tale requisito aveva creato un ostacolo insormontabile alla registrazione di un'identità etnica diversa da quella registrata per i suoi genitori dalle autorità sovietiche. Impedendo al ricorrente di fare esaminare la sua domanda alla luce di prove oggettivamente verificabili, lo Stato non aveva ottemperato all'obbligo positivo di garantire al ricorrente l'effettivo rispetto della sua vita privata. La Corte ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Nel corso di una causa civile o di un procedimento dinanzi a un'autorità pubblica per stabilire l'esattezza o meno dei dati, l'interessato può richiedere l'inserimento di una voce o di una nota nel proprio fascicolo attestante la contestazione dell'esattezza dell'informazione inserita e l'attesa di una decisione ufficiale. Durante questo periodo, il titolare del trattamento non deve presentare i dati come certi o definitivi, specialmente a terzi.

La richiesta di un interessato di cancellazione o eliminazione dei propri dati è spesso fondata sull'asserzione che il trattamento di dati personali non ha una base legittima. Tali richieste vengono avanzate spesso nei casi in cui il consenso è stato revocato o quando alcuni dati non sono più necessari per le finalità della raccolta. L'onere della prova relativo alla legittimità del trattamento dei dati incombe sul titolare del trattamento, poiché questi è responsabile della legittimità del trattamento. Secondo il principio di responsabilità, il titolare del trattamento dev'essere in grado di dimostrare in ogni momento l'esistenza di una solida base giuridica per il trattamento di dati personali, pena l'interruzione di quest'ultimo.

Se il trattamento dei dati è contestato perché i dati sono asseritamente inesatti o trattati illecitamente, l'interessato, in conformità del principio di correttezza del trattamento, può chiedere il blocco del trattamento dei dati contestati. Questo non significa che i dati siano cancellati ma che il titolare del trattamento deve evitare di usarli nel periodo del relativo blocco. Ciò sarebbe particolarmente necessario nel caso in cui l'uso persistente di dati inesatti e conservati illecitamente danneggi l'interessato. Il diritto nazionale dovrebbe fornire indicazioni maggiormente dettagliate sull'insorgere dell'obbligo di procedere al blocco dell'uso dei dati e sulle modalità di adempimento.

Gli interessati, inoltre, hanno il diritto di ottenere dal titolare del trattamento la notifica a terzi di qualsiasi blocco, rettifica o cancellazione, qualora detti terzi abbiano ricevuto i dati prima di tali operazioni di trattamento. Poiché il titolare del trattamento dovrebbe avere documentato la divulgazione dei dati a terzi, dovrebbe essere possibile individuare i destinatari dei dati e richiedere la cancellazione. Tuttavia, se nel frattempo i dati sono stati pubblicati, per esempio su Internet, potrebbe rivelarsi impossibile cancellare i dati in ogni circostanza, poiché i destinatari dei dati potrebbero non essere reperibili. A norma della direttiva sulla protezione dei dati, è obbligatorio contattare i destinatari a fini di rettifica, cancellazione o blocco del trattamento dei dati "se non si dimostra che è impossibile o implica uno sforzo sproporzionato"[187].

5.1.2. Diritto di opposizione

Il diritto di opposizione include il diritto di opporsi alle decisioni individuali automatizzate, al trattamento dei dati a motivo della particolare situazione dell'interessato e a un ulteriore uso dei dati a fini di marketing diretto.

Diritto di opposizione a decisioni individuali automatizzate

Le decisioni automatizzate sono decisioni adottate usando dati personali trattati esclusivamente con mezzi automatici. Qualora sia probabile che tali decisioni abbiano un considerevole impatto sulle vite delle persone perché riguardano, ad esempio, l'affidabilità creditizia, il rendimento professionale, il comportamento o l'affidabilità, è necessaria una protezione particolare per evitare conseguenze inopportune. La direttiva sulla protezione dei dati prevede che le decisioni automatizzate non comportino questioni rilevanti per le persone e impone il diritto della persona a far riesaminare la decisione automatizzata[188].

Esempio: un importante esempio pratico di decisione automatizzata è il *credit scoring* (valutazione dello stato di affidabilità creditizia). Per accertare con rapidità l'affidabilità creditizia di un cliente futuro, taluni dati, quali la professione e la situazione familiare, vengono ottenuti dal cliente e combinati con i dati pertinenti disponibili da altre fonti, quali i sistemi di informazioni creditizie. Questi dati sono inseriti automaticamente in un algoritmo di valutazione, che calcola un valore generale rappresentativo dell'affidabilità creditizia del potenziale cliente.

187 Direttiva sulla protezionedei dati, articolo 12, lettera c, ultima parte della frase.

188 *Ibid.*, articolo 15, paragrafo 1.

Così, il dipendente dell'azienda può decidere in pochi secondi se l'interessato è accettabile o meno come cliente.

Tuttavia, secondo la direttiva, gli Stati membri devono disporre che una persona può essere sottoposta a una decisione individuale automatizzata quando gli interessi dell'interessato non sono in gioco, perché la decisione è a favore dell'interessato, o quando sono tutelati con altri mezzi appropriati[189]. Il diritto di opposizione nei confronti di decisioni automatizzate è garantito anche dal **diritto del CDE**, come si evince dalla raccomandazione sulla profilazione[190].

Diritto di opposizione a motivo della situazione particolare dell'interessato

Non esiste un diritto generale degli interessati di opporsi al trattamento dei propri dati[191]. L'articolo 14, lettera a), della direttiva sulla protezione dei dati, tuttavia, conferisce all'interessato i mezzi per presentare opposizione per motivi preminenti e legittimi derivanti dalla sua situazione particolare. Un diritto analogo è stato riconosciuto nella raccomandazione sulla profilazione[192] del CDE. Tali disposizioni mirano a conseguire un corretto equilibrio fra i diritti alla protezione dei dati dell'interessato e i diritti legittimi di altri al trattamento dei dati dell'interessato.

Esempio: una banca conserva per sette anni i dati sui propri clienti che non rispettano le scadenze di rimborso dei prestiti. Un cliente i cui dati sono conservati in questa banca dati richiede un altro prestito. Vengono effettuate la consultazione della banca dati e una valutazione della situazione finanziaria e al cliente viene rifiutato il prestito. Tuttavia, il cliente può opporsi alla registrazione dei propri dati personali nella banca dati e chiedere la cancellazione degli stessi se può dimostrare che il mancato rimborso era solo il risultato di un errore, corretto subito dopo che il cliente ne era venuto a conoscenza.

189 *Ibid.*, articolo 15, paragrafo 2.

190 Raccomandazione sulla profilazione, articolo 5.5.

191 Cfr. anche Corte EDU, *M.S. c. Svezia*, n. 20837/92, 27 agosto 1997, in cui i dati medici erano stati comunicati senza il consenso o la possibilità di opporsi; Corte EDU, *Leander c. Svezia*, n. 9248/81, 26 marzo 1987; oppure Corte EDU, *Mosley c. Regno Unito*, n. 48009/08, 10 maggio 2011.

192 Raccomandazione sulla profilazione, articolo 5.3.

Se un'opposizione viene accolta, i dati in questione non possono più essere trattati dal titolare del trattamento. Le operazioni di trattamento svolte sui dati dell'interessato prima dell'opposizione restano, tuttavia, legittime.

Diritto di opposizione all'ulteriore uso dei dati a fini di marketing diretto

L'articolo 14, lettera b), della direttiva sulla protezione dei dati prevede uno specifico diritto di opposizione all'uso dei dati a fini di marketing diretto. Tale diritto è sancito anche nella raccomandazione sul marketing diretto[193] del CDE. Questo tipo di opposizione deve essere sollevato prima che i dati siano messi a disposizione di terzi a fini di detto marketing. All'interessato, pertanto, deve essere data l'opportunità di opporsi prima che i dati siano trasmessi.

5.2. Controllo indipendente

Punti salienti

- Per garantire un'effettiva protezione dei dati devono essere create autorità di controllo indipendenti ai sensi della normativa nazionale.
- Le autorità di controllo nazionali devono agire in assoluta indipendenza, garantita dalla legge che le istituisce e ripresa nella specifica struttura organizzativa dell'autorità di controllo.
- Le autorità di controllo svolgono funzioni specifiche, fra cui:
  - vigilare e promuovere la protezione dei dati a livello nazionale;
  - esprimere pareri agli interessati e ai titolari del trattamento, nonché al governo e al pubblico in senso lato;
  - ricevere i ricorsi e assistere l'interessato in caso di presunte violazioni dei diritti in materia di protezione dei dati;
  - vigilare sui titolari e sui responsabili del trattamento;
  - intervenire, se del caso,

193 CDE, Comitato dei ministri (1985), raccomandazione Rec(85)20 agli Stati membri sulla protezione dei dati a carattere personale usati a fini di marketing diretto, 25 ottobre 1985, articolo 4.1.

  - avvertendo, ammonendo o persino sanzionando titolari e responsabili del trattamento,
  - ordinando la rettifica, il blocco del trattamento o la cancellazione dei dati,
  - imponendo un divieto sul trattamento;
- deferire questioni all'autorità giudiziaria.

La direttiva sulla protezione dei dati impone un controllo indipendente quale importante meccanismo per garantire un'effettiva protezione dei dati. La direttiva ha introdotto uno strumento di attuazione della protezione dei dati che, inizialmente, non esisteva nella Convenzione n. 108 o negli orientamenti dell'OCSE sulla tutela della vita privata.

Poiché il controllo indipendente si è dimostrato indispensabile per lo sviluppo di un'effettiva tutela dei dati, una nuova disposizione introdotta nelle revisionate Linee Guida OCSE sulla tutela della vita privata, adottate nel luglio 2013, sollecita i paesi membri a "istituire e mantenere autorità di controllo per la protezione della vita privata con la governance, le risorse e le competenze tecniche necessarie per esercitare effettivamente i loro poteri e per prendere decisioni su base obiettiva, imparziale e coerente"[194].

Nell'ambito del diritto del CDE, il Protocollo addizionale alla Convenzione n. 108 ha reso obbligatoria l'istituzione di autorità di controllo. L'articolo 1 di detto Protocollo definisce il quadro giuridico per le autorità di controllo indipendenti che le parti contraenti devono attuare nel proprio diritto interno. L'articolo descrive le funzioni e i poteri di tali autorità con formulazioni simili a quelle usate nella direttiva sulla tutela dei dati. In linea di principio, le autorità di controllo dovrebbero, pertanto, funzionare allo stesso modo nell'ambito del diritto dell'UE e del CDE.

Nel quadro del diritto dell'UE, le competenze e la struttura organizzativa delle autorità di controllo sono state definite dapprima nell'articolo 28, paragrafo 1, della direttiva sulla protezione dei dati. Il regolamento sulla protezione dei dati da parte delle istituzioni dell'UE[195] istituisce il GEPD quale autorità di controllo del trattamento dei

194 OCSE (2013), Orientamenti per la tutela della vita privata e i flussi transfrontalieri di dati personali, paragrafo 19, lettera c).

195 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, GU L 8 del 12.1.2001, articoli 41–48.

dati personali da parte degli organismi e delle istituzioni dell'Unione. Nel definire il ruolo e le responsabilità dell'autorità di controllo, il regolamento ha fatto tesoro dell'esperienza acquisita sin dalla promulgazione della direttiva sulla protezione dei dati.

L'indipendenza delle autorità di controllo è garantita dall'articolo 16, paragrafo 2, del TFUE e dall'articolo 8, paragrafo 3, della Carta. Quest'ultima disposizione considera specificamente il controllo da parte di un'autorità indipendente preposta a tale funzione come un elemento essenziale del diritto fondamentale alla protezione dei dati. Inoltre, la direttiva sulla protezione dei dati impone agli Stati membri di istituire autorità di controllo intese a sorvegliare l'applicazione della direttiva che siano pienamente indipendenti nell'esercizio delle loro funzioni[196]. Non è solo la legislazione in base alla quale è istituita l'autorità di controllo a dover contenere disposizioni atte a garantirne specificamente l'indipendenza, ma è anche la particolare struttura organizzativa dell'autorità stessa a dover dare prova di tale indipendenza.

Nel 2010 la CGUE ha esaminato per la prima volta la questione della portata del requisito relativo all'indipendenza delle autorità di controllo per la protezione dei dati[197]. Gli esempi che seguono ne illustrano il ragionamento.

Esempio: nella causa *Commissione europea c. Germania*[198], la Commissione europea aveva chiesto alla CGUE di dichiarare che la Germania aveva trasposto erroneamente il requisito secondo cui le autorità di controllo della protezione dei dati devono essere "pienamente indipendenti", venendo meno così agli obblighi a essa incombenti in virtù dell'articolo 28, paragrafo 1, della direttiva sulla tutela dei dati. Secondo la Commissione, il problema nasceva dal fatto che la Germania aveva sottoposto alla vigilanza dello Stato le autorità preposte ai controlli sul trattamento dei dati personali in settori diversi da quello pubblico nei vari Stati federali (*Länder*).

196 Direttiva sulla tutela dei dati, articolo 28, paragrafo 1, ultima frase; Protocollo addizionale alla Convenzione n. 108, articolo 1, paragrafo 3.

197 Cfr. FRA (2010), *Fundamental rights: challenges and achievements in 201*0 (Diritti fondamentali: sfide e risultati nel 2010), relazione annuale 2010, pag. 59. La FRA ha affrontato tale questione più approfonditamente nella relazione *Data protection in the European Union: the role of National Data Protection Authorities* (La protezione dei dati nell'Unione europea: il ruolo delle autorità di controllo nazionali), pubblicata nel maggio 2010.

198 CGUE, C-518/07, *Commissione europea c. Repubblica federale di Germania*, 9 marzo 2010, punto 27.

A giudizio della Corte, la valutazione della fondatezza del ricorso dipendeva dalla portata dell'esigenza di indipendenza contenuta in quella disposizione e, pertanto, dalla sua interpretazione.

La Corte ha sottolineato che i termini "pienamente indipendenti" di cui all'articolo 28, paragrafo 1, della direttiva devono essere interpretati in base al tenore letterale effettivo di quella disposizione nonché delle finalità e all'economia della direttiva sulla protezione dei dati[199]. La Corte ha evidenziato che le autorità di controllo sono "custodi" dei diritti correlati al trattamento di dati personali garantiti nella direttiva e che la loro designazione negli Stati membri è quindi considerata "un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali"[200]. La Corte ha concluso che "nello svolgimento delle loro funzioni, le autorità di controllo devono agire in modo obiettivo ed imparziale. A tale fine esse devono essere sottratte a qualsiasi influenza esterna, compresa quella, diretta o indiretta, dello Stato o dei *Länder*, e non solamente essere poste al riparo dall'influenza degli organismi controllati"[201].

La CGUE ha altresì rilevato che il significato dei termini "pienamente indipendenti" dovrebbe essere interpretato alla luce dell'indipendenza del GEPD, definita nel regolamento sulla protezione dei dati delle istituzioni dell'UE. Come sottolineato dalla Corte, l'articolo 44, paragrafo 2, di detto regolamento "esplicita questa nozione d'indipendenza aggiungendo che, nell'adempimento delle sue funzioni, il GEPD non sollecita né accetta istruzioni da alcuno". Ciò esclude il controllo statale su un'autorità di controllo per la protezione dei dati[202].

Di conseguenza, la CGUE ha statuito che le istituzioni tedesche preposte alla tutela dei dati, responsabili a livello di Stato federale del controllo del trattamento dei dati personali effettuato da organi non pubblici, non erano sufficientemente indipendenti perché sottoposte alla vigilanza dello Stato.

Esempio: nella causa *Commissione europea c. Austria*[203], la CGUE ha posto in evidenza problemi simili per quanto riguarda la posizione di taluni membri del personale dell'autorità di controllo austriaca (Commissione per la protezione dei

199 *Ibid.*, punti 17 e 29.

200 *Ibid.*, punto 23.

201 *Ibid.*, punto 25.

202 *Ibid.*, punto 27.

203 CGUE, C-614/10, *Commissione europea c. Repubblica austriaca*, 16 ottobre 2012, punti 59 e 63.

dati, DSK). In questa causa la Corte ha concluso che la normativa austriaca impediva all'autorità di controllo di esercitare le proprie funzioni in modo pienamente indipendente ai sensi della direttiva sulla protezione dei dati. L'indipendenza dell'autorità di controllo austriaca non era sufficientemente garantita, perché il personale della DSK è fornito dalla cancelleria federale, che controlla la stessa DSK e ha il diritto di essere informata in ogni momento dei suoi lavori.

Esempio: nella causa *Commissione europea c. Ungheria*[204], la CGUE ha sottolineato che "il requisito [...] secondo il quale deve essere garantito che ogni autorità di controllo sia pienamente indipendente nell'esercizio delle funzioni che le sono attribuite, implichi l'obbligo, per lo Stato membro interessato, di rispettare la durata del mandato di tale autorità fino al termine inizialmente previsto" e ha dichiarato che "l'Ungheria, ponendo anticipatamente fine al mandato dell'autorità di controllo per la protezione dei dati personali, è venuta meno agli obblighi ad essa incombenti in forza della direttiva 95/46/CE [...]".

La normativa nazionale definisce i poteri e le competenze delle autorità di controllo, fra cui[205]:

- fornire pareri ai titolari del trattamento dei dati e agli interessati su tutte le questioni inerenti alla tutela dei dati;
- svolgere attività ispettive sulle operazioni di trattamento e intervenire di conseguenza;
- rivolgere un avvertimento o un monito ai titolari del trattamento;
- ordinare la rettifica, il blocco del trattamento, la cancellazione o la distruzione dei dati;
- vietare un trattamento a titolo provvisorio o definitivo;
- deferire la questione all'autorità giudiziaria.

204 CGEU, C-288/12, *Commissione europea c. Ungheria,* 8 aprile 2014, punti 50 e 67.

205 Direttiva sulla tutela dei dati, articolo 28; cfr. inoltre la Convenzione n. 108, Protocollo addizionale, articolo 1.

Per poter esercitare le proprie funzioni, un'autorità di controllo deve avere accesso a tutti i dati personali e alle informazioni necessarie a fini d'indagine nonché a qualsiasi locale in cui un titolare del trattamento conservi informazioni rilevanti.

Esistono notevoli differenze fra le giurisdizioni nazionali in relazione ai procedimenti e all'effetto giuridico delle constatazioni delle autorità di controllo. Tali constatazioni possono tradursi in raccomandazioni da mediatore o in decisioni immediatamente esecutive. Pertanto, in sede di analisi dell'efficacia dei mezzi di ricorso disponibili in una giurisdizione, tali strumenti devono essere valutati nel loro contesto.

5.3. Mezzi di ricorso e sanzioni

Punti salienti

- A norma della Convenzione n. 108 e della direttiva sulla protezione dei dati, il diritto nazionale deve stabilire mezzi di ricorso e sanzioni appropriati contro le violazioni del diritto alla protezione dei dati.
  - Ai sensi del diritto dell'UE, il diritto a un ricorso efficace impone che la normativa nazionale preveda ricorsi giurisdizionali contro le violazioni dei diritti alla protezione dei dati, indipendentemente dalla possibilità di rivolgersi all'autorità di controllo.
  - La normativa nazionale deve prevedere sanzioni efficaci, equivalenti, proporzionali e dissuasive.
- Prima di adire l'autorità giudiziaria è fatto obbligo di rivolgersi al titolare del trattamento. La regolamentazione dell'eventuale obbligo di rivolgersi all'autorità di controllo prima di adire l'autorità giudiziaria è lasciata alla discrezionalità del diritto nazionale.
- In caso di violazioni della normativa sulla tutela dei dati, in ultima istanza e nel rispetto di talune condizioni, gli interessati possono adire la CEDU.
- Anche la CGUE può essere adita dagli interessati, ma solo in misura molto limitata.

I diritti nell'ambito della normativa sulla tutela dei dati possono essere esercitati solo dalla persona titolare di tali diritti; si tratterà di una persona che è, o almeno sostiene di essere, l'interessato. Tali persone possono essere rappresentate nell'esercizio dei loro diritti da soggetti che, secondo il diritto nazionale, soddisfano i requisiti necessari. I minori devono essere rappresentati dai genitori o dai tutori. Dinanzi all'autorità di controllo una persona può essere rappresentata anche da associazioni il cui scopo legittimo sia la promozione del diritto alla protezione dei dati personali.

5.3.1. Richieste rivolte al titolare del trattamento

I diritti menzionati al paragrafo 3.2 devono essere esercitati, *in primis*, nei confronti del titolare del trattamento. Rivolgersi direttamente all'autorità di controllo nazionale o a un'autorità giudiziaria non sarebbe utile, dato che l'autorità di controllo potrebbe solo consigliare di rivolgersi dapprima al titolare del trattamento e l'autorità giudiziaria giudicherebbe la domanda irricevibile. I requisiti formali per presentare una domanda giuridicamente valida a un titolare del trattamento, specie se debba essere una richiesta scritta o meno, dovrebbero essere disciplinati dal diritto nazionale.

L'ente cui la persona interessata si è rivolta considerandola come titolare del trattamento deve rispondere alla richiesta, anche se non è il titolare del trattamento. In ogni caso dev'essere fornita una risposta all'interessato entro i limiti di tempo fissati dal diritto nazionale, anche solo per comunicare che non vengono trattati dati riguardanti il richiedente. Conformemente all'articolo 12, lettera a), della direttiva sulla protezione dei dati, e all'articolo 8, lettera b), della Convenzione n. 108, la richiesta dev'essere trattata "senza ritardi eccessivi". Pertanto, il diritto nazionale dovrebbe stabilire un periodo di risposta sufficientemente breve ma che consenta al titolare del trattamento di gestire adeguatamente la richiesta.

Prima di rispondere alla richiesta, l'interlocutore cui la persona interessata si è rivolta considerandolo come titolare del trattamento deve accertare l'identità del richiedente per stabilire se sia effettivamente la persona che dichiara di essere ed evitare quindi una grave violazione della riservatezza. Laddove i requisiti per l'accertamento dell'identità non siano specificamente regolamentati dal diritto nazionale, devono essere definiti dal titolare del trattamento. Il principio di correttezza del trattamento esige, tuttavia, che i titolari del trattamento non prescrivano condizioni eccessivamente onerose per l'accertamento dell'identità (e dell'autenticità della richiesta, come illustrato al paragrafo 2.1.1).

Il diritto nazionale deve anche trattare la questione se i titolari del trattamento, prima di rispondere alle richieste, possano esigere o meno dal richiedente il pagamento di un corrispettivo: l'articolo 12, lettera a), della direttiva, e l'articolo 8, lettera b), della Convenzione n. 108, prevedono che la risposta alle richieste di accesso dev'essere data "senza [...] spese eccessiv(e)". In numerosi paesi europei il diritto nazionale prevede che le richieste ai sensi della legge sulla protezione dei dati devono ottenere risposta gratuitamente, fintanto che la risposta non comporti sforzi eccessivi; a loro volta, anche i titolari del trattamento sono solitamente tutelati dal diritto nazionale contro l'abuso del diritto di ottenere una risposta alle richieste.

Se la persona, l'istituzione o l'organo cui l'interessato si è rivolto considerandolo come titolare del trattamento non nega di essere il titolare del trattamento, entro il periodo prescritto dal diritto nazionale tale persona, istituzione o organo deve:

dare seguito alla richiesta e notificare al richiedente la modalità di trattamento della richiesta; oppure

informare il richiedente dei motivi per i quali la sua richiesta non sarà trattata.

5.3.2. Domande presentate all'autorità di controllo

Una persona che abbia presentato richiesta di accesso o un'opposizione al titolare del trattamento e non abbia ricevuto una risposta tempestiva e soddisfacente può rivolgersi all'autorità di controllo nazionale per la protezione dei dati con una domanda di assistenza. Nel corso del procedimento dinanzi all'autorità di controllo occorre chiarire se la persona, l'istituzione o l'organo cui il richiedente si è rivolto fossero effettivamente tenuti a rispondere alla richiesta e se la risposta sia stata corretta e sufficiente. L'autorità di controllo deve informare l'interessato dell'esito del procedimento relativo alla sua domanda[206]. Gli effetti giuridici dell'esito del procedimento dinanzi alle autorità di controllo nazionali dipendono dal diritto nazionale, in base al quale si chiarisce se le decisioni dell'autorità siano giuridicamente esecutive, nel senso che sono eseguibili da parte dell'autorità competente, o se occorra adire l'autorità giudiziaria qualora il titolare del trattamento non ottemperi alle decisioni (parere, monito ecc.) dell'autorità di controllo.

Nel caso in cui i diritti alla protezione dei dati garantiti dall'articolo 16 del TFUE siano asseritamente violati dalle istituzioni o dagli organismi dell'UE, l'interessato può presentare un reclamo al GEPD[207], l'autorità di controllo indipendente per la tutela dei dati istituita dal regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, che definisce le funzioni e i poteri del GEPD. In mancanza di risposta da parte di quest'ultimo entro sei mesi, il reclamo si considera respinto.

Avverso le decisioni di un'autorità di controllo nazionale dev'essere possibile ricorrere all'autorità giudiziaria. Ciò vale sia per l'interessato sia per i titolari del trattamento, in quanto parti di un procedimento dinanzi all'autorità di controllo.

206 Direttiva sulla protezionedei dati, articolo 28, paragrafo 4.

207 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, GU L 8 del 12.1.2001.

Esempio: il commissario all'informazione del Regno Unito ha emanato una decisione il 24 luglio 2013 invitando la polizia dell'Hertfordshire a sospendere l'uso di un sistema di riconoscimento delle targhe di immatricolazione a suo avviso illegittimo. I dati raccolti dalle videocamere erano conservati sia nelle banche dati della polizia locale sia in una banca dati centrale. Le fotografie delle targhe erano conservate per due anni, mentre quelle delle automobili per 90 giorni. Si è ritenuto che un uso talmente ampio di videocamere e di altre forme di sorveglianza non fosse proporzionato al problema che si intendeva risolvere.

5.3.3. Domanda presentata all'autorità giudiziaria

Secondo la direttiva sulla protezione dei dati, la persona che, ai sensi della normativa sulla tutela dei dati, abbia presentato domanda al titolare del trattamento e non sia soddisfatta della risposta ricevuta da quest'ultimo deve avere il diritto di adire un'autorità giudiziaria nazionale[208].

Spetta al diritto nazionale pronunciarsi sull'eventuale obbligo di rivolgersi all'autorità di controllo prima di adire l'autorità giudiziaria. Nella maggior parte dei casi, però, è vantaggioso per le persone che esercitano i propri diritti in materia di protezione dei dati rivolgersi dapprima all'autorità di controllo, dato che i procedimenti relativi alle domande di assistenza presso tale autorità dovrebbero essere non burocratici e gratuiti. Anche le misure contenute nella decisione dell'autorità di controllo (parere, monito ecc.) possono aiutare l'interessato a tutelare i propri diritti dinanzi all'autorità giudiziaria.

Secondo il diritto del CDE, le violazioni dei diritti alla tutela dei dati, asseritamente perpetrate a livello nazionale da una parte contraente della CEDU e costituenti nel contempo una violazione dell'articolo 8 della stessa CEDU, possono essere inoltre fatte valere dinanzi alla Corte EDU dopo aver esperito tutte le vie di ricorso nazionali. La richiesta di constatazione di una violazione dell'articolo 8 della CEDU dinanzi alla Corte EDU deve soddisfare anche altre condizioni di ricevibilità (articoli 34-37 CEDU)[209].

Benché possano essere dirette solo contro le parti contraenti, le domande presentate alla Corte EDU possono riguardare indirettamente anche azioni o omissioni di

208 Direttiva sulla protezione dei dati, articolo 22.

209 CEDU, articoli 34–37, disponibile all'indirizzo: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

privati, nella misura in cui un paese parte contraente non abbia adempiuto ai propri obblighi a norma della CEDU e non abbia garantito una protezione sufficiente contro le violazioni dei diritti alla protezione dei dati nel proprio ordinamento nazionale.

Esempi: nella causa *K. U. c. Finlandia*[210], il ricorrente, un minore, aveva denunciato che su un sito Internet di appuntamenti era stato pubblicato a suo nome un annuncio a sfondo sessuale. L'identità della persona che aveva pubblicato i dati non era stata rivelata dal fornitore di servizi a causa degli obblighi di riservatezza imposti dalla legge finlandese. Il ricorrente lamentava che la legge finlandese non prevedesse una protezione sufficiente contro tali azioni commesse da un privato che aveva indiscriminatamente inserito su Internet dati relativi al ricorrente. La Corte EDU ha stabilito che gli Stati non solo erano obbligati ad astenersi da ingerenze arbitrarie nella vita privata degli individui, ma erano anche soggetti a obblighi positivi, che comportano "l'adozione di misure atte a garantire il rispetto della vita privata anche nella sfera dei rapporti reciproci fra gli individui". Nel caso di specie, affinché il ricorrente fosse protetto all'atto pratico e in modo efficace s'imponeva che fossero presi provvedimenti reali per identificare e perseguire l'autore del reato. Tuttavia, tale protezione non era garantita dallo Stato e la Corte ha concluso asserendo una violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Köpke c. Germania*[211], la ricorrente era stata sospettata di furto sul luogo di lavoro e pertanto era stata sottoposta di nascosto a videosorveglianza. La Corte EDU ha concluso che nulla indicava che le autorità nazionali non avessero cercato un equo equilibrio, nell'ambito del loro margine di discrezionalità, fra il diritto della ricorrente al rispetto della propria vita privata di cui all'articolo 8 da una parte e, dall'altra, l'interesse del datore di lavoro alla protezione dei propri diritti di proprietà nonché l'interesse pubblico alla corretta amministrazione della giustizia. Pertanto, la domanda è stata dichiarata irricevibile.

Se la Corte EDU constata che uno Stato nonché parte contraente ha violato uno qualsiasi dei diritti sanciti dalla CEDU, detta parte è tenuta ad attuare la sentenza della Corte EDU. Le misure di esecuzione devono dapprima fare cessare la violazione e porre rimedio, per quanto possibile, alle conseguenze negative a carico del ricorrente. L'esecuzione delle sentenze può anche richiedere misure generali per

210 Corte EDU, *K.U. c. Finlandia*, n. 2872/02, 2 dicembre 2008.

211 Corte EDU, *Köpke c. Germania* (dec.), n. 420/07, 5 ottobre 2010.

prevenire violazioni simili a quelle constatate dalla Corte, attraverso modifiche legislative, pronunce giurisprudenziali o altre misure.

Se la Corte EDU constata che vi è stata una violazione della CEDU, l'articolo 41 della CEDU prevede che la Corte possa accordare un'equa soddisfazione alla parte lesa a spese dello Stato parte contraente.

Ai sensi del diritto dell'UE[212], in taluni casi le vittime di violazioni della legislazione nazionale in materia di tutela dei dati, che recepisce la normativa UE sulla tutela dei dati, possono adire la CGUE. Sono previsti due casi in cui un ricorso proposto da un interessato per violazione dei propri diritti alla protezione dei dati può sfociare in un procedimento dinanzi alla CGUE.

Nel primo caso, l'interessato deve essere stato vittima diretta di un atto amministrativo o di regolamentazione dell'UE che violi il suo diritto alla protezione dei dati. In virtù dell'articolo 263, quarto comma, del TFUE:

> *"Qualsiasi persona fisica o giuridica può proporre [...] un ricorso contro gli atti adottati nei suoi confronti o che la riguardano direttamente e individualmente, e contro gli atti regolamentari che la riguardano direttamente e che non comportano alcuna misura d'esecuzione".*

Pertanto, le vittime di un trattamento illecito dei propri dati da parte di un organismo dell'UE possono adire direttamente il Tribunale, che è l'organo della CGUE competente a giudicare le questioni trattate dal regolamento sulla protezione dei dati da parte delle istituzioni dell'UE. Esiste anche la possibilità di adire direttamente la CGUE qualora una disposizione del diritto dell'Unione abbia effetto direttamente sulla situazione giuridica di una persona.

Il secondo caso riguarda la competenza della CGUE a pronunciarsi in via pregiudiziale ai sensi dell'articolo 267 del TFUE (già art. 234 CE).

Gli interessati, nel corso dei procedimenti in ambito nazionale, possono domandare al giudice nazionale di chiedere chiarimenti alla Corte di giustizia sull'interpretazione dei trattati dell'UE nonché sull'interpretazione e la validità di taluni atti delle

212 UE (2007), Trattato di Lisbona che modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea, firmato a Lisbona il 13 dicembre 2007, GU C 306 del 17.12.2007. Cfr. altresì le versioni consolidate del trattato sull'Unione europea, GU C 326 del 26.10.2012, e del TFUE, GU C 326 del 26.10.2012.

istituzioni, degli organismi, degli uffici o delle agenzie dell'Unione. Tali chiarimenti sono noti come pronunce pregiudiziali. Non si tratta di un ricorso diretto a disposizione del denunciante, ma di un ricorso che consente ai giudici nazionali di garantire che la loro interpretazione del diritto dell'UE sia corretta.

Se una parte di un procedimento dinanzi ai giudici nazionali richiede il rinvio di una questione alla CGUE, solo i giudici nazionali di ultimo grado, contro le cui decisioni non è ammesso ricorso giurisdizionale, sono tenuti a uniformarsi alla pronuncia.

Esempio: nella causa *Kärntner Landesregierung e altri*[213], la Corte costituzionale austriaca ha trasmesso alla CGUE alcune domande sulla validità degli articoli 39 della direttiva 2006/24/CE (*direttiva sulla conservazione dei dati*) alla luce degli articoli 7, 9 e 11 della Carta e sulla compatibilità o meno di talune disposizioni della legge federale austriaca sulle telecomunicazioni, che recepisce la direttiva sulla conservazione dei dati, con aspetti della direttiva sulla tutela dei dati e del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE.

Il sig. Seitlinger, uno dei ricorrenti nel procedimento pendente dinanzi alla Corte costituzionale, ha dichiarato di usare il telefono, Internet e la posta elettronica sia sul lavoro sia nella vita privata. Di conseguenza, le informazioni che egli invia e riceve passano attraverso reti di telecomunicazione pubbliche. Ai sensi della legge austriaca sulle telecomunicazioni del 2003, il suo fornitore di servizi di telecomunicazione è obbligato, per legge, a raccogliere e a conservare i dati relativi all'uso della rete da parte del sig. Seitlinger. Questi ha realizzato che tale raccolta e conservazione dei suoi dati personali non erano in alcun modo necessarie ai fini tecnici di trasmettere le informazioni da A a B sulla rete. Né erano minimamente necessarie, in effetti, la raccolta e la conservazione di tali dati a fini di fatturazione. Il sig. Seitlinger non aveva certamente acconsentito a questo uso dei suoi dati personali. Il solo motivo della raccolta e della conservazione di tutti quei dati supplementari era la legge austriaca sulle telecomunicazioni del 2003.

Il sig. Seitlinger, pertanto, ha adito la Corte costituzionale austriaca sostenendo che gli obblighi di legge imposti al fornitore dei servizi di telecomunicazione violano i suoi diritti fondamentali ai sensi dell'articolo 8 della Carta.

213 CGUE, cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e a.*, 8 aprile 2014.

La CGUE rende una decisione solo sugli elementi costituitivi della domanda di pronuncia pregiudiziale a essa sottoposta. La decisione sulla causa principale resta di competenza del giudice nazionale.

In linea di principio, la Corte di giustizia deve rispondere alle domande che le vengono sottoposte. Non può rifiutare di pronunciarsi in via pregiudiziale adducendo che la risposta non sarebbe né pertinente né tempestiva per la soluzione della causa principale; tuttavia, può rifiutarsi qualora la domanda esuli dalla propria sfera di competenza.

Infine, se i diritti alla protezione dei dati sanciti dall'articolo 16 del TFUE sono asseritamente violati da un'istituzione o da un organismo dell'UE durante il trattamento di dati personali, l'interessato può adire il Tribunale (articolo 32, paragrafi 1 e 4, del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE). Lo stesso si applica alle decisioni del GEPD per le questioni relative a tali violazioni (articolo 32, paragrafo 3, del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE).

Il Tribunale è competente a emanare sentenze sulle questioni disciplinate dal regolamento sulla protezione dei dati da parte delle istituzioni dell'UE. Se invece una persona intende presentare ricorso quale membro del personale di un'istituzione o di un organismo dell'Unione, deve adire il Tribunale della funzione pubblica dell'Unione europea.

Esempio: la sentenza *Commissione europea c. The Bavarian Lager Co. Ltd*[214] illustra i ricorsi disponibili contro attività o decisioni delle istituzioni e degli organismi dell'UE rilevanti per la protezione dei dati.

La Bavarian Lager aveva richiesto alla Commissione europea l'accesso ai verbali completi di una riunione tenuta dalla Commissione asseritamente concernente questioni giuridiche rilevanti per tale società. La Commissione aveva respinto la richiesta di accesso della società per prevalenti interessi di protezione dei dati[215]. Contro tale decisione, la Bavarian Lager, in applicazione dell'articolo 32

214 CGUE, C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd*, 29 giugno 2010.

215 Per un'analisi della questione cfr.: GEPD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling (*Accesso pubblico a documenti contenenti dati personali dopo la sentenza Bavarian Lager), Bruxelles, FEPD, disponibile all'indirizzo: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, aveva proposto un ricorso dinanzi alla CGUE (più esattamente, dinanzi al Tribunale di primo grado, il predecessore del Tribunale). Nella decisione pronunciata nella causa T194/04, *Bavarian Lager c. Commissione*, il Tribunale di primo grado ha annullato la decisione con la quale la Commissione respingeva la richiesta di accesso. La Commissione europea ha impugnato tale decisione dinanzi alla Corte di giustizia la quale (riunita in grande sezione) ha emanato una sentenza di annullamento della sentenza del Tribunale di primo grado e di conferma del rigetto da parte della Commissione della richiesta di accesso.

5.3.4. Sanzioni

Nell'ambito del diritto del CDE, l'articolo 10 della Convenzione n. 108 prevede che ciascuna parte contraente debba definire le sanzioni e i ricorsi appropriati per le violazioni delle disposizioni di diritto nazionale che danno attuazione ai principi fondamentali della protezione dei dati enunciati nella stessa Convenzione[216].
Nell'ambito del diritto dell'UE, l'articolo 24 della direttiva sulla protezione dei dati dispone che gli Stati membri "adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva e in particolare stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione [...]".

Entrambi gli strumenti giuridici offrono agli Stati membri un ampio margine di discrezionalità nella scelta delle sanzioni e dei ricorsi appropriati; nessuno di essi contiene particolari orientamenti sulla natura o sul tipo di sanzioni appropriate né fornisce esempi di sanzioni.

Tuttavia:

> *"Benché gli Stati membri dell'UE godano di un margine di discrezionalità per determinare quali misure siano più appropriate per la salvaguardia dei diritti riconosciuti alle persone dal diritto dell'Unione, conformemente al principio di leale cooperazione sancito dall'articolo 4, paragrafo 3, del TUE, devono essere rispettati i requisiti minimi di efficacia, equivalenza, proporzionalità e dissuasività"*[217].

216 Corte EDU, *I. c. Finlandia*, n. 20511/03, 17 luglio 2008; Corte EDU, *K.U. c. Finlandia*, n. 2872/02, 2 dicembre 2008.

217 FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package (*Parere dell'Agenzia dell'Unione europea per i diritti fondamentali sulla proposta di un pacchetto di riforma della protezione dei dati), 2/2012, Vienna, 1 ottobre 2012, pag. 27.

La CGUE ha più volte ribadito che il diritto nazionale non è del tutto libero di imporre sanzioni.

Esempio: nella sentenza *Von Colson e Kamann c. Land Nordrhein-Westfalen*[218], la CGUE ha sottolineato che tutti gli Stati membri ai quali la direttiva si rivolge sono tenuti ad adottare, nel proprio ordinamento giuridico nazionale, tutti i provvedimenti necessari per garantire la piena efficacia della direttiva stessa, conformemente allo scopo che essa persegue. La Corte ha statuito che, benché spetti agli Stati membri scegliere i modi e i mezzi destinati a garantire l'attuazione di una direttiva, tale libertà nulla toglie agli obblighi loro imposti. In particolare, un ricorso giuridico efficace deve consentire alle persone di perseguire e applicare il diritto in questione fino al raggiungimento del suo effetto sostanziale. Ai fini di una tutela effettiva ed efficace, i mezzi di ricorso giuridici devono dare luogo a procedimenti penali e/o ad azioni di risarcimento che conducano a sanzioni con effetto dissuasivo.

Per quanto riguarda le sanzioni contro le violazioni del diritto dell'UE da parte delle istituzioni o degli organismi dell'Unione, a causa della speciale competenza del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, le sanzioni sono previste solo sotto forma di provvedimenti disciplinari. A norma dell'articolo 49 del regolamento, "il funzionario o altro agente delle Comunità europee che, volontariamente o per negligenza, non assolva agli obblighi previsti dal presente regolamento è passibile di provvedimenti disciplinari [...]".

218 CGUE, C-14/83, *Sabine von Kolson and Elisabeth Kamann c. Land Nordrhein-Westfalen*, 10 Aprile 1984.

6

Flussi transfrontalieri dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Flussi transfrontalieri dei dati		
Direttiva sulla protezione dei dati, articolo 25, paragrafo 1 CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003	**Definizione**	Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 1
Libera circolazione di dati		
Direttiva sulla protezione dei dati, articolo 1, paragrafo 2	**Fra gli Stati membri dell'UE**	
	Fra le parti contraenti della Convenzione n. 108	Convenzione n. 108, articolo 12, paragrafo 2
Direttiva sulla protezione dei dati, articolo 25	**Verso paesi terzi che garantiscono un livello adeguato di protezione dei dati**	Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 1
Direttiva sulla protezione dei dati, articolo 26, paragrafo 1	**Verso paesi terzi in casi specifici**	Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 2, lettera a)
Circolazione limitata di dati verso paesi terzi		
Direttiva sulla protezione dei dati, articolo 26, paragrafo 2 Direttiva sulla protezione dei dati, articolo 26, paragrafo 4	**Clausole contrattuali**	Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 2, lettera b) Guida alla redazione delle clausole contrattuali

Direttiva sulla protezione dei dati, articolo 26, paragrafo 2	Norme vincolanti d'impresa	
Esempi: Accordo PNR UE-USA Accordo SWIFT UE-USA	Accordi internazionali specifici	

La direttiva sulla protezione dei dati non si limita a prevedere la libera circolazione di dati fra gli Stati membri, ma contiene anche disposizioni sui requisiti da soddisfare per il trasferimento dei dati personali verso paesi terzi al di fuori dell'UE. Anche il CDE ha riconosciuto l'importanza delle norme di attuazione per i flussi transfrontalieri dei dati versi paesi terzi e nel 2001 ha adottato il Protocollo addizionale alla Convenzione n. 108. Detto Protocollo ha recepito i principali aspetti normativi sui flussi transfrontalieri dei dati dalle parti contraenti della Convenzione e dagli Stati membri dell'UE.

6.1. Natura dei flussi transfrontalieri dei dati

Punto saliente

- Il flusso transfrontaliero dei dati consiste nel trasferimento di dati personali verso un destinatario soggetto a una giurisdizione straniera.

L'articolo 2, paragrafo 1, del Protocollo addizionale alla Convenzione n. 108 descrive il flusso transfrontaliero dei dati come il trasferimento di dati personali verso un destinatario soggetto a una giurisdizione straniera. L'articolo 25, paragrafo 1, della direttiva sulla tutela dei dati regolamenta il "trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento [...]". Tale trasferimento di dati è consentito solo nel rispetto delle norme stabilite dall'articolo 2 del Protocollo addizionale alla Convenzione n. 108 e, per gli Stati membri dell'UE, anche dagli articoli 25 e 26 della direttiva sulla tutela dei dati.

Esempio: nella sentenza *Bodil Lindqvist*[219], la CGUE ha statuito che «l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio

219 CGUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, punti 27, 68 e 69.

indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce "un trattamento di dati personali interamente o parzialmente automatizzato" ai sensi dell'art. 3, n. 1, della direttiva 95/46».

La Corte ha poi sottolineato che la direttiva contiene anche norme specifiche che mirano a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso paesi terzi.

Tuttavia, tenuto conto, da una parte, dello sviluppo di Internet all'epoca della redazione della direttiva e, dall'altra, della mancanza nella stessa di criteri applicabili all'uso di Internet, «non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di "trasferimenti verso un paese terzo di dati personali" l'inserimento [...] di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli».

Altrimenti, qualora la direttiva "venisse interpretata nel senso che si configura un trasferimento verso un paese terzo di dati personali ogni volta che dati personali vengono caricati su una pagina Internet, tale trasferimento sarebbe necessariamente un trasferimento verso tutti i paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet. Il regime speciale previsto [dalla direttiva] diverrebbe quindi necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale. Infatti, non appena la Commissione constatasse [...] che un solo paese terzo non garantisce un livello di protezione adeguato, gli Stati membri sarebbero tenuti ad impedire qualsiasi immissione su Internet di dati personali".

Il principio secondo cui la semplice pubblicazione di dati (personali) non dev'essere considerata un flusso transfrontaliero dei dati si applica anche ai registri pubblici online o ai mezzi di comunicazione di massa, quali giornali (elettronici) e televisione. Solo la comunicazione diretta a destinatari specifici può rientrare nella nozione di "flusso transfrontaliero dei dati".

6.2. Libera circolazione di dati fra gli Stati membri o fra le parti contraenti

Punto saliente

- Il trasferimento di dati personali verso un altro Stato membro dello Spazio economico europeo o di un'altra parte contraente della Convenzione n. 108 dev'essere libero da restrizioni.

Ai sensi dell'articolo 12, paragrafo 2, della Convenzione n. 108, **nell'ambito del diritto del CDE** dev'essere garantita la libera circolazione dei dati personali fra le parti contraenti della Convenzione. La legislazione nazionale non può limitare il trasferimento di dati personali verso una parte contraente tranne nei casi in cui:

- lo imponga la natura specifica dei dati[220]; o
- la restrizione sia necessaria per evitare l'aggiramento di disposizioni giuridiche nazionali sul flusso transfrontaliero dei dati verso parti terze[221].

Ai sensi del diritto dell'UE, le restrizioni o i divieti alla libera circolazione dei dati fra Stati membri per motivi connessi alla tutela dei dati sono proibiti dall'articolo 1, paragrafo 2, della direttiva sulla tutela dei dati. La zona della libera circolazione di dati è stata ampliata dall'accordo sullo Spazio economico europeo (SEE)[222], che introduce Islanda, Liechtenstein e Norvegia nel mercato interno.

Esempio: se un'affiliata di un gruppo d'imprese internazionale, con sede in diversi Stati membri dell'UE, fra cui Slovenia e Francia, trasferisce dati personali dalla Slovenia alla Francia, tale flusso di dati non dev'essere limitato o vietato dal diritto nazionale sloveno.

Tuttavia, se la medesima affiliata slovena intende trasferire gli stessi dati personali alla società madre negli Stati Uniti, in quanto esportatore di dati deve

220 Convenzione n. 108, articolo 12, paragrafo 3, lettera a).

221 *Ibid.*, articolo 12, paragrafo 3, lettera b).

222 Decisione del Consiglio e della Commissione, del 13 dicembre 1993, relativa alla conclusione dell'accordo sullo Spazio economico europeo tra le Comunità europee, i loro Stati membri e la Repubblica d'Austria, la Repubblica di Finlandia, la Repubblica d'Islanda, il Principato del Liechtenstein, il Regno di Norvegia, il Regno di Svezia e la Confederazione elvetica, GU L 1 del 3.1.1994.

rispettare le procedure stabilite dal diritto sloveno per il flusso transfrontaliero dei dati verso paesi terzi senza un'adeguata protezione dei dati, a meno che la società madre non abbia aderito ai principi di approdo sicuro in materia di riservatezza, un codice di condotta volontario relativo all'offerta di un adeguato livello di protezione dei dati (cfr. il paragrafo 6.3.1).

I flussi transfrontalieri di dati verso Stati membri del SEE per scopi che esulano dall'ambito del mercato interno, quali indagini su reati, non sono tuttavia soggetti alle disposizioni della direttiva sulla protezione dei dati e, pertanto, non sono coperti dal principio della libera circolazione dei dati. Per quanto riguarda il diritto del CDE, tutti gli ambiti rientrano nella sfera di applicazione della Convenzione n. 108 e del Protocollo addizionale della stessa, sebbene le parti contraenti possano prevedere esenzioni. Tutti i membri del SEE sono anche parti contraenti della Convenzione n. 108.

6.3. Libera circolazione di dati verso paesi terzi

Punto saliente

- Il trasferimento di dati personali verso paesi terzi è libero da restrizioni nell'ambito del diritto nazionale sulla protezione dei dati se:
  - è stata accertata l'adeguatezza della protezione dei dati presso il destinatario o
  - risulta necessario per interessi specifici dell'interessato o per prevalenti interessi legittimi altrui, in particolare per interessi pubblici rilevanti.
- Adeguatezza della protezione dei dati in un paese terzo significa che i principi fondamentali della protezione dei dati siano stati effettivamente introdotti nel diritto nazionale di detto paese.
- Ai sensi del diritto dell'UE, l'adeguatezza della protezione dei dati in un paese terzo è valutata dalla Commissione europea. Ai sensi del diritto del CDE, le modalità di valutazione dell'adeguatezza sono disciplinate dalla legislazione nazionale.

6.3.1. Libera circolazione di dati in caso di tutela adeguata

Secondo il diritto del CDE, la legislazione nazionale può consentire la libera circolazione di dati verso Stati non contraenti se lo Stato o l'organizzazione destinatari assicurano un livello di protezione adeguato per il trasferimento di dati in questione[223]. La legislazione nazionale stabilisce le modalità di valutazione del livello di protezione dei dati in un paese straniero e le persone preposte a detta valutazione.

Nell'ambito del diritto dell'UE, la libera circolazione dei dati verso paesi terzi con un adeguato livello di protezione di detti dati è prevista dall'articolo 25, paragrafo 1, della direttiva sulla protezione dei dati. Il requisito dell'adeguatezza piuttosto che dell'equivalenza rende possibile il rispetto di diverse vie attraverso cui garantire la protezione dei dati. A norma dell'articolo 25, paragrafo 6, della direttiva, la Commissione europea è competente a valutare il livello di protezione dei dati in paesi stranieri attraverso decisioni di adeguatezza e consultazioni relative alla stessa valutazione con il Gruppo di lavoro articolo 29 per la protezione dei dati che ha contribuito in modo sostanziale all'interpretazione degli articoli 25 e 26[224].

Una decisione di adeguatezza da parte della Commissione europea è vincolante. Se la Commissione europea pubblica una decisione di adeguatezza per un determinato paese sulla *Gazzetta ufficiale dell'Unione europea*, tutti gli Stati membri del SEE e i relativi organismi sono tenuti a ottemperare alla decisione, nel senso che i dati possono circolare verso quel paese senza procedure di verifica o di autorizzazione presso le autorità nazionali[225].

La Commissione europea può altresì valutare alcuni elementi del sistema giuridico di un paese o limitarsi a singoli punti. La Commissione ha emesso, per esempio, una decisione di adeguatezza per quanto riguarda soltanto il diritto commerciale privato

223 Convenzione n. 108, Protocollo addizionale, articolo 2, paragrafo 1.

224 Cfr., per esempio, Gruppo di lavoro articolo 29 (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers* (Documento di lavoro sui trasferimenti di dati personali verso paesi terzi: applicazione dell'articolo 26, paragrafo 2, della direttiva UE sulla tutela dei dati alle norme vincolanti d'impresa per le trasmissioni internazionali di dati), WP 74, Bruxelles, 3 giugno 2003; e Gruppo di lavoro articolo 29 (2005), *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995*, WP 114, Bruxelles, 25 novembre 2005.

225 Per un elenco sempre aggiornato dei paesi beneficiari di una decisione di adeguatezza, cfr. la pagina iniziale della Commissione europea, Direzione generale per la Giustizia, disponibile all'indirizzo: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

del Canada[226]. Esistono anche diverse decisioni di adeguatezza per i trasferimenti basati su accordi conclusi fra l'UE e Stati stranieri. Tali decisioni riguardano esclusivamente un solo tipo di trasferimento di dati, quale la trasmissione dei codici di prenotazione da parte delle compagnie aeree alle autorità straniere preposte ai controlli di frontiera nei casi in cui la compagnia aerea operi partendo dall'UE e dirigendosi verso alcune destinazioni extra-europee (cfr. il paragrafo 6.4.3). Una prassi più recente nel trasferimento di dati basata su accordi speciali fra l'UE e paesi terzi elimina in genere l'esigenza di decisioni di adeguatezza, presumendosi che l'accordo stesso offra un adeguato livello di protezione dei dati[227].

Una delle più importanti decisioni di adeguatezza non riguarda in realtà un insieme di disposizioni giuridiche[228], ma norme molto simili a un codice di condotta note come principi di approdo sicuro in materia di riservatezza. Tali principi sono stati messi a punto tra l'UE e gli Stati Uniti per le imprese commerciali statunitensi. La conformità ai principi di approdo sicuro si acquisisce mediante un impegno volontario, assunto tramite una dichiarazione dinanzi al dipartimento per il Commercio statunitense e documentato in un elenco pubblicato dallo stesso dipartimento. Poiché uno degli elementi più importanti dell'adeguatezza è dato dall'effettiva attuazione della tutela dei dati, l'accordo sull'approdo sicuro prevede anche un certo livello di supervisione statale: possono aderire ai principi di approdo sicuro solo le imprese soggette alla vigilanza della Commissione federale per il commercio degli USA.

6.3.2. Libera circolazione di dati in casi specifici

Ai sensi del diritto del CDE, l'articolo 2, paragrafo 2, del Protocollo addizionale alla Convenzione n. 108 consente il trasferimento di dati personali verso paesi terzi nei

226 Decisione 2002/2/CE della Commissione, del 20 dicembre 2001, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act), GU L 2 del 4.1.2002.

227 Ad esempio, l'Accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna (GU L 215 dell'11.8.2012, pagg. 5–14) o l'Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi, GU L 8 del 13.1.2010, pagg. 11-16.

228 Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, GU L 215 del 25.8.2000.

quali non è garantito un adeguato livello di protezione, nella misura in cui il trasferimento sia previsto dal diritto interno e sia necessario per:

- interessi specifici dell'interessato; o
- quando prevalgono interessi legittimi altrui, in particolare interessi pubblici rilevanti.

Ai sensi del diritto dell'UE, l'articolo 26, paragrafo 1, della direttiva sulla protezione dei dati contiene disposizioni simili a quelle del Protocollo addizionale alla Convenzione n. 108.

Ai sensi della direttiva, gli interessi dell'interessato possono giustificare la libera circolazione dei dati verso un paese terzo se è soddisfatta almeno una delle seguenti condizioni:

- l'interessato ha espresso il proprio consenso inequivocabile al trasferimento dei dati;
- l'interessato ha stipulato – o si accinge a stipulare – un contratto che richieda chiaramente il trasferimento dei dati verso un destinatario all'estero;
- è stato concluso un contratto fra il titolare del trattamento e un terzo nell'interesse dell'interessato;
- il trasferimento è necessario per la salvaguardia dell'interesse vitale dell'interessato;
- il trasferimento avviene a partire da un registro pubblico, ossia si è in presenza di un caso di interessi prevalenti della popolazione in generale che consiste nel fatto di poter accedere a informazioni conservate in registri pubblici.

Gli interessi legittimi altrui possono giustificare la libera circolazione transfrontaliera di dati[229]:

229 Direttiva sulla tutela dei dati, articolo 26, paragrafo 1, lettera d).

- per la salvaguardia di un interesse pubblico rilevante, diverso dalla sicurezza nazionale o pubblica, dato che questi settori non sono coperti dalla direttiva sulla tutela dei dati; oppure

- per rivendicare, esercitare o difendere un diritto per via giudiziaria.

I casi succitati devono essere intesi come deroghe dalla regola secondo la quale il libero trasferimento di dati verso altri paesi richiede un adeguato livello di protezione dei dati nel paese destinatario. Le deroghe devono sempre essere interpretate in senso restrittivo. Questo aspetto è stato sottolineato più volte dal Gruppo di lavoro articolo 29 nel quadro dell'articolo 26, paragrafo 1, della direttiva sulla protezione dei dati, in particolare se il consenso è la base presunta per il trasferimento di dati[230]. Il Gruppo di lavoro articolo 29 ha concluso che le norme generali sull'importanza giuridica del consenso si applicano anche all'articolo 26, paragrafo 1, della direttiva. Se nell'ambito dei rapporti di lavoro, per esempio, non è chiaro se il consenso dato dai dipendenti sia effettivamente un consenso libero, allora i trasferimenti di dati non possono essere fondati sull'articolo 26, paragrafo 1, lettera a), della direttiva. In tali casi, si applica l'articolo 26, paragrafo 2, che impone alle autorità di controllo nazionali di autorizzare i trasferimenti di dati.

6.4. Circolazione limitata di dati verso paesi terzi

Punti salienti

- Prima di trasferire i dati verso paesi terzi che non garantiscono un adeguato livello di protezione dei dati, il titolare del trattamento può essere tenuto a sottoporre il flusso di dati in questione all'esame delle autorità di controllo.

- Durante questo esame, il titolare del trattamento che desidera trasferire i dati deve dimostrare due punti:

  - l'esistenza di una base giuridica per il trasferimento di dati verso il destinatario; e

  - la presenza di misure atte a garantire un'adeguata tutela dei dati presso il destinatario.

230 Cfr., in particolare, Gruppo di lavoro articolo 29 (2005), *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995*, WP 114, Bruxelles, 25 novembre 2005.

- Le misure volte ad accertare l'esistenza di un'adeguata tutela dei dati presso il destinatario possono includere:
  - clausole contrattuali fra il titolare del trattamento che trasferisce i dati e il destinatario straniero dei dati; o
  - norme vincolanti d'impresa, applicabili di solito per i trasferimenti di dati nell'ambito di un gruppo multinazionale di imprese.
- I trasferimenti di dati verso autorità straniere possono essere disciplinati anche da un accordo internazionale speciale.

La direttiva sulla protezione dei dati e il Protocollo addizionale alla Convenzione n. 108 consentono alla legislazione nazionale di definire regimi per i flussi transfrontalieri dei dati verso paesi terzi che non garantiscono un adeguato livello di tutela degli stessi, a condizione che il titolare del trattamento abbia stipulato accordi speciali per assicurare l'esistenza di adeguate garanzie di tutela dei dati presso il destinatario e possa dimostrarlo a un'autorità competente. Questo requisito è menzionato esplicitamente solo nel Protocollo addizionale alla Convenzione n. 108, ma il soddisfacimento dello stesso è considerato prassi normale anche nell'ambito della direttiva sulla protezione dei dati.

6.4.1. Clausole contrattuali

Sia il **diritto del CDE** sia **quello dell'UE** citano le clausole contrattuali stipulate fra il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo come possibile mezzo per garantire un livello sufficiente di protezione dei dati presso il destinatario.

A **livello di Unione**, la Commissione europea, con l'ausilio del Gruppo di lavoro articolo 29, ha elaborato clausole contrattuali tipo ufficialmente certificate da una decisione della Commissione come prova di un'adeguata protezione dei dati[231]. Poiché le decisioni della Commissione sono vincolanti in ogni loro parte negli Stati membri, le autorità nazionali di controllo dei flussi transfrontalieri di dati devono riconoscere la validità di tali clausole contrattuali tipo nei propri procedimenti[232]. Pertanto, se il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo concordano e sottoscrivono tali clausole, l'autorità di controllo dovrebbe avere una prova sufficiente dell'esistenza di garanzie adeguate.

231 Direttiva sulla protezione dei dati, articolo 26, paragrafo 4.

232 TFUE, articolo 288.

L'esistenza di clausole contrattuali tipo nel quadro giuridico dell'UE non vieta ai titolari del trattamento di formulare altre clausole contrattuali *ad hoc*. Queste, tuttavia, dovrebbero garantire il medesimo livello di tutela offerto dalle clausole contrattuali tipo. Le caratteristiche più importanti di dette clausole sono:

- la presenza di una clausola relativa a una terza parte beneficiaria che consenta agli interessati di esercitare diritti contrattuali anche se non sono parte del contratto;

- il destinatario o l'importatore dei dati accetta, in caso di controversia, di essere sottoposto ai procedimenti dell'autorità di controllo nazionale e/o dei tribunali del titolare del trattamento che trasferisce i dati .

Attualmente, un titolare del trattamento che intenda trasferire dati personali ad altro titolare del trattamento può scegliere tra due set di clausole tipo[233]. Per i trasferimenti da titolare del trattamento a responsabile del trattamento esiste un unico set di clausole contrattuali tipo[234].

Ai sensi **del diritto del CDE**, il comitato consultivo della Convenzione n. 108 ha elaborato una guida sulla redazione di clausole contrattuali[235].

233 La serie I è contenuta nell'allegato alla decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE, GU L 181 del 4.7.2001; la serie II è contenuta nell'allegato alla decisione 2004/915/CE della Commissione, del 27 dicembre 2004, che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi, GU L 385 del 29.12.2004.

234 Decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, GU L 39 del 12.2.2010.

235 CDE, comitato consultivo della Convenzione n. 108 (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data* (Guida alla redazione di clausole contrattuali che disciplinano la tutela dei dati durante il trasferimento di dati personali verso parti terze che non garantiscono un adeguato livello di tutela dei dati).

6.4.2. Norme vincolanti d'impresa

Molto spesso le norme vincolanti d'impresa (BCR) multilaterali coinvolgono contemporaneamente diverse autorità di controllo europee[236]. Affinché siano approvate, il progetto relativo alle BCR dev'essere trasmesso unitamente ai moduli di domanda standardizzati all'autorità capofila[237], individuabile nel modello di domanda standardizzato. Quest'autorità informa poi tutte le autorità di controllo dei paesi membri del SEE in cui sono stabiliti gli affiliati del gruppo, sebbene la loro partecipazione al processo di valutazione delle BCR sia facoltativa. Pur non essendo obbligatorio, tutte le autorità di controllo interessate dovrebbero inserire i risultati della valutazione nelle proprie procedure formali di autorizzazione.

6.4.3. Accordi internazionali specifici

L'UE ha concluso accordi specifici per i due tipi di trasferimenti di dati indicati di seguito.

Codice di prenotazione (Passenger Name Record)

I dati relativi ai codici di prenotazione (PNR) sono raccolti dai vettori aerei durante il processo di prenotazione e includono nomi, indirizzi, dati delle carte di credito e numeri di posto dei passeggeri. Ai sensi della normativa statunitense, le compagnie aeree sono obbligate a rendere disponibili tali dati al dipartimento per la Sicurezza interna prima della partenza dei passeggeri. Questo vale per i voli in arrivo, in partenza o in transito negli Stati Uniti.

236 Il contenuto e la struttura delle norme vincolanti d'impresa adeguate sono illustrati nei documenti del Gruppo di lavoro articolo 29 (2008), *Working document setting up a framework for the structure of Binding Corporate Rules* (Documento di lavoro che istituisce un quadro per la struttura delle norme vincolanti d'impresa), WP 154, Bruxelles, 24 giugno 2008, e *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules (*Documento di lavoro che stabilisce uno schema di elementi e principi da riscontrare nelle norme vincolanti d'impresa*)*, WP 153, Bruxelles, 24 giugno 2008.

237 Gruppo di lavoro articolo 29 (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* (Raccomandazione 1/2007 sulla domanda tipo per l'approvazione di norme vincolanti d'impresa per il trasferimento di dati personali), WP 133, Bruxelles, 10 gennaio 2007.

Allo scopo di garantire adeguata protezione ai dati PNR, conformemente a quanto stabilito dalla direttiva 95/46/CE, è stato adottato, nel 2004, un "pacchetto PNR"[238] che prevedeva l'adeguatezza del trattamento dei dati effettuato dal dipartimento per la sicurezza interna degli Stati Uniti (US Department of Homeland Security - DHS).

A seguito dell'annullamento del pacchetto PNR da parte della Corte di giustizia[239], sono stati sottoscritti due diversi accordi con un duplice scopo : in primo luogo fornire una corretta base giuridica per il trasferimento di dati PNR alle autorità statunitensi e in secondo luogo creare i presupposti per un'adeguata tutela dei dati nel paese destinatario.

Il primo accordo sulla condivisione e la gestione dei dati fra i paesi dell'UE e gli Stati Uniti, sottoscritto nel 2007, presentava diverse lacune ed è stato sostituito, nel 2012, da un nuovo accordo per garantire una migliore certezza del diritto[240]. Il nuovo accordo contiene importanti miglioramenti, in quanto limita e chiarisce i fini per i quali le informazioni possono essere usate, come gravi reati di natura transnazionale e terrorismo, individua i tempi di conservazione dei dati che, comunque, dopo sei mesi, devono essere spersonalizzati e mascherati. Inoltre, in caso di utilizzo non conforme dei propri dati, tutti hanno il diritto di ricorrere per via amministrativa e giudiziaria conformemente alla normativa degli Stati Uniti nonché di accedere ai propri dati PNR e, nel caso in cui le informazioni siano inesatte, di chiederne la rettifica, inclusa la possibilità di cancellazione, al dipartimento per la Sicurezza interna.

L'accordo è entrato in vigore il 1° luglio 2012 e resterà in vigore per sette anni, fino al 2019.

238 Decisione del Consiglio 2004/496/EC del 17 Maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti e Decisione dalla Commissione 2004/535/EC del 14 Maggio relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti *United States' Bureau of Customs and Border Protection*.

239 CGUE, cause riunite C-317/04 e C-318/04, *Parlamento europeo c. Consiglio dell'Unione europea*, 30 maggio 2006, punti 57, 58 e 59 con cui la Corte ha stabilito che sia la decisione di adeguatezza sia l'accordo riguardano trattamenti di dati che sono esclusi dall'ambito di applicazione della direttiva.

240 Decisione 2012/472/UE del Consiglio, del 26 aprile 2012, relativa alla conclusione dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, GU L 215 dell'11.8.2012, pag. 4. Il testo dell'accordo è allegato alla decisione, GU L 215 dell'11.8.2012, pagg. 5-14.

Nel dicembre 2011 il Consiglio dell'Unione europea ha approvato anche la conclusione di un nuovo accordo UE-Australia sul trattamento e sul trasferimento dei dati PNR[241]. Detto accordo rappresenta un ulteriore passo avanti nell'agendadell'Unione, che prevede un approccio globale per l'uso dei dati PNR [242], l'istituzione di un regime in materia di PNR nell'UE[243] e la negoziazione di accordi con paesi terzi[244].

Dati di messaggistica finanziaria

La Society for Worldwide Interbank Financial Telecommunication (SWIFT), con sede in Belgio, è l'ente responsabile del trattamento della maggior parte dei trasferimenti mondiali di denaro dalle banche europee. La società operava con un "mirror" center negli Stati Uniti e alla stessa era stato richiesto dal dipartimento del Tesoro statunitense di dare accesso ai dati a fini di indagini sul terrorismo[245].

Dal punto di vista dell'UE non sussisteva una base giuridica sufficiente per rendere accessibili tali dati (disponibili negli Stati Uniti solo perché uno dei centri per il trattamento dei dati di SWIFT era ubicato in tale paese).

241 Decisione 2012/381/UE del Consiglio, del 13 dicembre 2011, relativa alla conclusione dell'accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record — PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, GU L 186 del 14.7.2012, pag. 3. Il testo dell'accordo, che ha sostituito un precedente accordo del 2008, è allegato alla decisione, GU L 186 del 14.7.2012, pagg. 4–16.

242 Cfr., in particolare, la Comunicazione della Commissione del 21 settembre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi, COM(2010) 492 def., Bruxelles, 21 settembre 2010 sulla quale vedi anche Gruppo di lavoro articolo 29 (2010), *Parere 7/2010 concernente la comunicazione della Commissione europea sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record,* PNR*) verso paesi terzi*, WP 178, Bruxelles, 12 novembre 2010.

243 Proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM(2011) 32 def., Bruxelles, 2 febbraio 2011. Nell'aprile 2011 il Parlamento europeo ha chiesto alla FRA di emanare un parere su questa proposta e sulla conformità della stessa con la Carta dei diritti fondamentali dell'Unione europea. Cfr. FRA (2011), *Opinion 1/2011 – Passenger Name Record (Parere 1/2011 – Codici di prenotazione)*, Vienna, 14 giugno 2011.

244 L'UE sta attualmente negoziando un nuovo accordo in materia di PNR con il Canada che sostituirà quello del 2006 tuttora in vigore.

245 Cfr., al riguardo, Gruppo di lavoro articolo 29 (2011), *Parere 14/2011 sulle questioni di protezione dei dati legate alla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo*, WP 186, Bruxelles, 13 giugno 2011; Gruppo di lavoro articolo 29 (2006), *Parere 10/2006 sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT)*, WP 128, Bruxelles, 22 novembre 2006; Commissione belga per la protezione della vita privata (*Commission de la protection de la vie privée*) (2008), *Control and recommendation procedure initiated with respect to the company SWIFT scrl* (Procedura di controllo e raccomandazione avviata nei confronti della società SWIFT), decisione del 9 dicembre 2008.

Nel 2010 è stato concluso un accordo specifico tra l'UE e gli Stati Uniti, noto come accordo SWIFT, volto a fornire la necessaria base giuridica e a garantire un'adeguata tutela dei dati[246].

Ai sensi dell'accordo, i dati finanziari conservati dalla SWIFT continuano ad essere forniti al dipartimento del Tesoro statunitense a fini di prevenzione, indagine, accertamento o azione penale nei confronti del terrorismo o del suo finanziamento. Detto dipartimento può richiedere dati finanziari alla SWIFT, purché la richiesta:

- individui il più chiaramente possibile i dati finanziari;
- motivi espressamente la necessità dei dati;
- sia quanto più possibile precisa onde ridurre al minimo la quantità di dati richiesti;
- non richieda dati relativi all'area unica dei pagamenti in euro (SEPA).

Europol deve ricevere una copia di ciascuna richiesta avanzata dal dipartimento del Tesoro statunitense e verificare se i principi dell'accordo SWIFT siano rispettati o meno[247]. In caso affermativo, la SWIFT deve fornire i dati finanziari direttamente al suddetto dipartimento, che deve conservarli in un ambiente fisico sicuro in cui possano essere consultati solo da analisti che indagano sul terrorismo o sul relativo finanziamento. I dati finanziari non devono essere collegati con nessun'altra banca dati. In generale, i dati finanziari ricevuti dalla SWIFT sono cancellati dopo un periodo massimo di cinque anni successivi alla ricezione degli stessi. I dati finanziari rilevanti per indagini o procedimenti specifici possono essere conservati per tutto il periodo in cui sono necessari per tali indagini o procedimenti.

Il dipartimento del Tesoro statunitense può trasferire informazioni estratte dai dati forniti dalla SWIFT a specifiche autorità di contrasto, di pubblica sicurezza o antiterrorismooperanti all'interno o all'esterno degli Stati Uniti solo a fini di prevenzione, indagine, accertamento o azione penale nei confronti del terrorismo e del suo

246 Decisione 2010/412/UE del Consiglio, del 13 luglio 2010, relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi, GU L 195 del 27.7.2010, pagg. 3 e 4. Il testo dell'accordo è allegato alla decisione, GU L 195 del 27.7.2010, pagg. 5-14.

247 L'Autorità comune di controllo su Europol ha effettuato delle verifiche sull'attività svolta da Europol in tale ambito, i cui esiti sono disponibili all'indirizzo: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

finanziamento. Se il trasferimento in uscita di dati finanziari interessa un cittadino o una persona residente in uno Stato membro dell'UE, qualsiasi condivisione dei dati con le autorità di un paese terzo è soggetta al consenso preventivo delle autorità competenti dello Stato membro interessato. Possono essere previste eccezioni nei casi in cui la condivisione dei dati sia essenziale per la prevenzione di una minaccia immediata e grave alla sicurezza pubblica.

Controllori indipendenti, fra cui una personalità nominata dalla Commissione europea, monitorano il rispetto dei principi dell'accordo SWIFT.

Gli interessati hanno il diritto di ottenere conferma dall'autorità di protezione dei dati competente dell'UE che i loro diritti alla protezione dei dati personali siano stati rispettati. Gli interessati hanno anche il diritto di rettifica, cancellazione o blocco del trattamento dei propri dati raccolti e conservati dal dipartimento del Tesoro statunitense nell'ambito dell'accordo SWIFT. Tuttavia, i diritti di accesso degli interessati possono essere soggetti a talune limitazioni. Quando l'accesso viene rifiutato, gli interessati devono essere informati per iscritto di tale rifiuto e del loro diritto di ricorrere per via amministrativa e giudiziaria negli Stati Uniti.

L'accordo SWIFT ha una validità quinquennale e scadrà ad agosto 2015. Sarà prorogato automaticamente per periodi successivi di un anno, salvo il caso in cui, almeno sei mesi prima, una parte comunichi all'altra la propria intenzione di non prorogare l'accordo.

7

La protezione dei dati nel contesto della pubblica sicurezza e della giustizia penale

Unione europea	Argomenti trattati	Consiglio d'Europa
	In generale	Convenzione n. 108
	Polizia	Raccomandazione sull'uso dei dati personali in ambito di polizia
		Corte EDU, *B.B. c. Francia*, n. 5335/06, 17 dicembre 2009
		Corte EDU, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008
		Corte EDU, *Vetter c. Francia*, n. 59842/00, 31 maggio 2005
	Criminalità informatica	Convenzione sulla lotta contro la criminalità informatica
La protezione dei dati nel contesto della cooperazione transfrontaliera delle autorità di polizia e giudiziarie		
Decisione quadro sulla protezione dei dati	In generale	Convenzione n. 108
		Raccomandazione sull'uso dei dati personali in ambito di polizia
Decisione di Prüm	Per dati particolari: impronte digitali, DNA, teppismo ecc.	Convenzione n. 108
		Raccomandazione sull'uso dei dati personali in ambito di polizia
Decisione Europol	Da parte di agenzie specifiche	Convenzione n. 108
Decisione Eurojust		Raccomandazione sull'uso dei dati personali in ambito di polizia
Regolamento Frontex		

Decisione Schengen II Regolamento VIS Regolamento Eurodac Decisione SID	**Da sistemi specifici di informazione comune**	Convenzione n. 108 Raccomandazione sull'uso dei dati personali in ambito di polizia Corte EDU, *Dalea c. Francia*, n. 964/07, 2 febbraio 2010

Al fine di raggiungere un equilibrio fra gli interessi dell'individuo in materia di protezione dei dati e gli interessi della società nella raccolta degli stessi per combattere la criminalità e garantire la sicurezza nazionale e pubblica, il CDE e l'UE hanno adottato specifici strumenti giuridici.

7.1. Il diritto del CDE sulla protezione dei dati nell'ambito della pubblica sicurezza e della giustizia penale

Punti salienti

- La Convenzione n. 108 e la raccomandazione del CDE relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza riguardano la protezione dei dati in tutti gli aspetti delle attività di polizia.
- La Convenzione sulla lotta contro la criminalità informatica (*Convenzione di Budapest*) è uno strumento giuridico internazionale vincolante che concerne i reati commessi contro o per mezzo delle reti di comunicazione elettronica.

A livello europeo, la Convenzione n. 108 copre tutti i settori del trattamento dei dati personali e le disposizioni in essa contenute mirano a regolamentare il trattamento dei dati personali in generale. Di conseguenza, la Convenzione n. 108 si applica alla protezione dei dati in materia di pubblica sicurezza e giustizia penale, sebbene le parti contraenti possano limitarne l'applicazione.

I compiti giuridici delle autorità di pubblica sicurezza e giustizia penale impongono spesso il trattamento di dati personali, che può avere notevoli conseguenze per le persone interessate. La raccomandazione sull'uso dei dati personali nell'ambito della pubblica sicurezza, adottata dal CDE nel 1987, contiene raccomandazioni alle parti

contraenti sull'applicazione dei principi della Convenzione n. 108 nel contesto del trattamento di dati personali da parte delle autorità di polizia[248].

7.1.1. La raccomandazione sull'uso dei dati personali nell'ambito della pubblica sicurezza

Secondo giurisprudenza costante della Corte EDU, l'archiviazione e la conservazione di dati personali da parte della polizia o delle autorità nazionali di pubblica sicurezza costituiscono un'ingerenza ai sensi dell'articolo 8, paragrafo 1, della CEDU. Numerose sentenze della Corte EDU riguardano la giustificazione di tali ingerenze[249].

Esempio: nella causa *B.B. c. Francia*[250], la Corte EDU ha statuito che l'inserimento in una banca dati giudiziaria nazionale di una persona condannata per reati sessuali rientrava nell'ambito di applicazione dell'articolo 8 della CEDU. Tuttavia, poiché erano state attuate garanzie sufficienti per la protezione dei dati, fra cui il diritto dell'interessato di richiedere la cancellazione dei dati, la durata limitata della conservazione dei dati e l'accesso limitato agli stessi, era stato raggiunto un giusto equilibrio fra gli opposti interessi privati e pubblici in questione. La Corte EDU ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Esempio: nella causa *S. e Marper c. Regno Unito*[251], entrambi i ricorrenti erano stati accusati di aver commesso reati, ma non erano stati condannati. Tuttavia, le impronte digitali, i profili del DNA e i campioni di cellule dei ricorrenti erano custoditi e conservati dalla polizia. La conservazione a tempo indeterminato di dati biometrici era autorizzata per legge qualora una persona fosse sospettata di aver commesso un reato, anche se la stessa veniva successivamente assolta o prosciolta. La Corte EDU ha statuito che la conservazione generale e indiscriminata di dati personali, illimitata nel tempo e nel cui ambito le persone assolte avevano solo limitate possibilità di richiedere la cancellazione, costituiva un'ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata. La Corte ha concluso asserendo una violazione dell'articolo 8 della CEDU.

248 CDE, Comitato dei ministri (1987), Raccomandazione N. R (87) 15 agli Stati membri che disciplina l'uso di dati personali nell'ambito della pubblica sicurezza, 17 settembre 1987.

249 Cfr., ad esempio, Corte EDU, *Leander c. Svezia*, n. 9248/81, 26 marzo 1987; Corte EDU, *M.M. c. Regno Unito*, n. 24029/07, 13 novembre 2012; Corte EDU, *M.K. c. Francia*, n. 19522/09, 18 aprile 2013.

250 Corte EDU, *B.B. c. Francia*, n. 5335/06, 17 dicembre 2009.

251 Corte EDU, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008, punti 119 e 125.

Molte altre sentenze della Corte EDU riguardano la giustificazione dell'interferenza mediante sorveglianza con il diritto alla protezione dei dati.

Esempio: nella causa *Allan c. Regno Unito*[252], le conversazioni private di un detenuto con un amico nella sala visite del carcere e con un codetenuto in una cella erano state registrate in segreto dalle autorità. La Corte EDU ha statuito che l'uso di dispositivi di audioregistrazione e videoregistrazione nella cella del ricorrente, nella sala visite del carcere e su un codetenuto costituisse violazione del diritto del ricorrente alla vita privata. Poiché nel momento in cui si erano verificati i fatti non esisteva un sistema legale per regolamentare l'uso di dispositivi di registrazione in segreto da parte della polizia, detta ingerenza non era conforme alla legge. La Corte EDU ha concluso asserendo l'esistenza di una violazione dell'articolo 8 della CEDU.

Esempio: nella causa *Klass e altri c. Germania*[253], i ricorrenti sostenevano che diversi atti legislativi tedeschi che autorizzavano la sorveglianza in segreto della posta, della corrispondenza e delle telecomunicazioni violassero l'articolo 8 della CEDU, in particolare perché la persona interessata non era stata informata delle misure di sorveglianza e, al termine di tali misure, non poteva adire i tribunali. La Corte EDU ha statuito che il rischio di sorveglianza interferiva necessariamente con la libertà di comunicazione fra gli utenti di servizi postali e di telecomunicazione. Tuttavia, ha anche constatato che erano state attuate garanzie sufficienti contro eventuali abusi. La legislazione tedesca era giustificata nel ritenere che tali misure sono necessarie in una società democratica nell'interesse della sicurezza nazionale e ai fini della prevenzione di disordini o di reati. La Corte EDU ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Poiché il trattamento di dati personali da parte delle autorità di polizia può avere conseguenze rilevanti per gli interessati, sono particolarmente necessarie norme dettagliate sulla protezione dei dati ai fini della tenuta di banche dati in questo settore. La raccomandazione del CDE sull'uso dei dati personali in ambito di pubblica sicurezza ha cercato di affrontare la questione fornendo orientamenti sulle modalità di raccolta dei dati per le attività di polizia; sulle modalità di tenuta degli archivi di dati in questo settore e sulle persone che dovrebbero essere autorizzate ad accedere a tali archivi, comprese le condizioni per il trasferimento dei dati ad autorità di polizia straniere; sulle modalità di esercizio dei diritti alla protezione dei dati da parte

252 Corte EDU, *Allan c. Regno Unito*, n. 48539/99, 5 novembre 2002.

253 Corte EDU, *Klass e a. c. Germania*, n. 5029/71, 6 settembre 1978.

degli interessati; infine, sulle modalità di attuazione del controllo da parte di autorità indipendenti. Anche l'obbligo di garantire un'adeguata sicurezza dei dati è stato considerato.

La raccomandazione non consente una raccolta illimitata e indiscriminata di dati da parte delle autorità di polizia, ma limita la raccolta di dati personali da parte di dette autorità a quanto necessario per la prevenzione di un pericolo concreto o per la repressione di un reato specifico. Ogni ulteriore raccolta di dati dovrebbe basarsi su una legislazione nazionale specifica. Il trattamento di dati sensibili dovrebbe essere limitato a quanto assolutamente necessario nel contesto di una particolare indagine.

Quando i dati personali sono raccolti all'insaputa dell'interessato, quest'ultimo dovrebbe esserne informato non appena la divulgazione dei dati non arrechi più pregiudizio alle indagini. Anche la raccolta di dati attraverso dispositivi tecnici di sorveglianza o altri mezzi automatizzati dovrebbe essere basata su disposizioni giuridiche specifiche.

Esempio: nella causa *Vetter c. Francia*[254], alcuni testimoni anonimi avevano accusato il ricorrente di omicidio. Poiché il ricorrente si recava regolarmente a casa di un amico, la polizia aveva installato in quest'abitazione dei dispositivi di ascolto dietro autorizzazione del giudice inquirente. Sulla base delle conversazioni registrate, il ricorrente veniva arrestato e processato per omicidio. Lo stesso richiedeva quindi che la registrazione fosse dichiarata inammissibile come prova, sostenendo in particolare che non era prevista dalla legge. Per la Corte EDU, il punto in questione consisteva nel chiarire se l'uso di dispositivi di ascolto fosse "conforme alla legge" o meno. Le intercettazioni in luoghi privati non rientravano manifestamente nell'ambito di applicazione degli articoli 100 e segg. del codice di procedura penale, poiché tali disposizioni riguardavano l'intercettazione di linee telefoniche. L'articolo 81 del codice non indicava con ragionevole chiarezza la portata o le modalità di esercizio della discrezionalità da parte delle autorità nell'autorizzare il controllo di conversazioni private. Di conseguenza, il ricorrente non aveva goduto del livello minimo di protezione spettante ai cittadini nell'ambito dello Stato di diritto in una società democratica. La Corte ha concluso asserendo che vi era stata una violazione dell'articolo 8 della CEDU.

254 Corte EDU, *Vetter c. Francia*, n. 59842/00, 31 maggio 2005.

La raccomandazione conclude affermando che, all'atto di conservare dati personali, bisognerebbe operare una chiara distinzione fra i dati amministrativi e i dati di polizia; fra le diverse categorie di interessati, quali sospettati, detenuti, vittime e testimoni; e fra i dati basati su fatti reali e quelli basati su sospetti o deduzioni.

I dati acquisiti dalla polizia dovrebbero essere strettamente limitati nello scopo, cosa che incide sulla comunicazione di tali dati a terzi: il trasferimento o la comunicazione di tali dati in ambito di polizia dovrebbero essere regolamentati in base alla presenza o meno di un interesse legittimo alla condivisione delle informazioni. Il trasferimento o la comunicazione di tali dati al di fuori dell'ambito di polizia dovrebbero essere consentiti solo qualora sussista un chiaro obbligo legale o autorizzazione. Il trasferimento o la comunicazione a livello internazionale dovrebbero essere limitati alle autorità di polizia straniere ed essere basati su disposizioni giuridiche specifiche, possibilmente accordi internazionali, a meno che non siano necessari per prevenire un pericolo grave e imminente.

Il trattamento di dati personali da parte della polizia deve essere oggetto di un controllo indipendente per garantire il rispetto della normativa nazionale in materia di protezione dei dati. Gli interessati devono godere di tutti i diritti di accesso sanciti dalla Convenzione n. 108. Se i diritti di accesso degli interessati sono stati limitati in applicazione dell'articolo 9 della Convenzione n. 108 nell'interesse di specifiche indagini di polizia, la normativa nazionale deve garantire all'interessato il diritto di ricorrere all'autorità di controllo nazionale competente per la protezione dei dati o a un altro organo indipendente.

7.1.2. La Convenzione di Budapest sulla lotta contro la criminalità informatica

Poiché le attività criminali si avvalgono sempre più dei sistemi elettronici di trattamento dei dati e comportano conseguenze per gli stessi, per affrontare tale sfida sono necessarie nuove disposizioni giuridiche in ambito penale. Il CDE, pertanto, ha adottato uno strumento giuridico internazionale, la Convenzione sulla lotta contro la criminalità informatica – nota anche come Convenzione di Budapest – per affrontare la questione dei crimini commessi contro e per mezzo delle reti elettroniche[255]. La suddetta Convenzione è aperta all'adesione anche degli Stati non membri del CDE. A metà 2013, quattro Stati non membri del CDE – Australia, Repubblica dominicana,

255 Consiglio d'Europa, Comitato dei ministri (2001), Convenzione sulla criminalità informatica, STCE n. 185, Budapest, 23 novembre 2001, entrata in vigore il 1° luglio 2004.

Giappone e Stati Uniti – hanno aderito alla Convenzione e altri 12 paesi non membri l'hanno firmata o sono stati invitati ad aderirvi.

La Convenzione sulla lotta contro la criminalità informatica resta il trattato internazionale più autorevole in materia di violazioni di diritto commesse su Internet o altre reti informatiche. Impone alle parti di aggiornare e di armonizzare le rispettive leggi penali contro la pirateria e altre violazioni della sicurezza, fra cui il diritto d'autore, la frode informatica, la pedopornografia e altre attività informatiche illecite. La Convenzione prevede inoltre poteri procedurali che riguardano la ricerca sulle reti informatiche e l'intercettazione delle comunicazioni nel contesto della lotta contro la criminalità informatica. Infine, rende possibile un'effettiva cooperazione internazionale. Un Protocollo addizionale alla Convenzione riguarda l'incriminazione di atti di propaganda di natura razzista e xenofoba sulle reti informatiche.

Benché, sostanzialmente, non sia uno strumento volto a promuovere la protezione dei dati, la Convenzione considera alla stregua di reati attività che potrebbero violare i diritti dell'interessato alla protezione dei propri dati. Essa inoltre obbliga le parti contraenti, in sede di attuazione della Convenzione, a prevedere un'adeguata protezione dei diritti umani e delle libertà, compresi i diritti sanciti dalla CEDU, come il diritto alla protezione dei dati[256].

7.2. Il diritto dell'UE sulla protezione dei dati nell'ambito della pubblica sicurezza e della giustizia penale

Punti salienti

- A livello di UE, la protezione dei dati in ambito di pubblica sicurezza e giustizia penale è regolamentata solo in termini di cooperazione transfrontaliera delle autorità di polizia e giudiziarie.
- Esistono speciali regimi di protezione dei dati per l'Ufficio europeo di polizia (Europol) e l'Unità europea di cooperazione giudiziaria (Eurojust), organismi dell'Unione che sostengono e promuovono l'applicazione della legge a livello transfrontaliero.

256 *Ibid.*, articolo 15, paragrafo 1.

- Esistono specifici regimi di protezione dei dati anche per i sistemi d'informazione comune istituiti a livello di UE per lo scambio transfrontaliero d'informazioni fra le autorità competenti. Esempi importanti sono costituiti da Schengen II, dal Sistema d'informazione visti (VIS) e da Eurodac, un sistema centralizzato contenente i dati relativi alle impronte digitali di cittadini di paesi terzi che presentano domanda di asilo in uno degli Stati membri dell'UE.

La direttiva sulla tutela dei dati non si applica nel settore della pubblica sicurezza e della giustizia penale. Il paragrafo 7.2.1 descrive gli strumenti giuridici più importanti in questo campo.

7.2.1. La decisione quadro sulla protezione dei dati

La decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (*decisione quadro sulla protezione dei dati*)[257] mira a garantire la protezione dei dati personali delle persone fisiche quando tali dati sono trattati ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati o dell'attuazione di sanzioni penali. Ad agire per conto degli Stati membri o dell'UE sono le autorità competenti negli ambiti della polizia e della giustizia penale, ossia agenzie o organismi dell'UE nonché autorità degli Stati membri[258]. L'ambito di applicazione della decisione quadro si limita a garantire la protezione dei dati nella cooperazione transfrontaliera fra dette autorità, senza estendersi alla sicurezza nazionale.

Le decisione quadro sulla protezione dei dati si basa, in larga misura, sui principi e sulle definizioni contenute nella Convenzione n. 108 e nella direttiva sulla tutela dei dati.

I dati devono essere usati solo da un'autorità competente ed esclusivamente per i fini per i quali sono stati trasmessi o messi a disposizione. Lo Stato membro che li riceve deve rispettare qualsiasi restrizione sullo scambio dei dati prevista dalla legge dello Stato membro che li trasmette. Tuttavia, l'uso dei dati per scopi diversi da parte dello Stato destinatario è consentito a determinate condizioni. La registrazione e documentazione delle trasmissioni costituiscono un obbligo specifico delle autorità competenti al fine di contribuire a chiarire le responsabilità in seguito a denunce. L'ulteriore trasferimento di dati ricevuti nel corso della cooperazione transfrontaliera

257 Consiglio dell'Unione europea (2008), Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (*decisione quadro sulla protezione dei dati*), GU L 350 del 30.12.2008.

258 *Ibid.*, articolo 2, lettera h).

verso parti terze richiede il consenso dello Stato membro dal quale i dati provengono, sebbene siano previste eccezioni in casi urgenti.

Le autorità competenti devono adottare le misure di sicurezza necessarie per proteggere i dati personali contro qualsiasi forma di trattamento illegale.

Ogni Stato membro deve garantire che almeno una se non più autorità di controllo nazionali indipendenti siano incaricate di fornirgli consulenza e sorvegliare l'applicazione delle disposizioni adottate conformemente alla decisione quadro sulla protezione dei dati. Inoltre, chiunque può rivolgersi alle autorità di controllo con un'istanza relativa alla tutela dei propri diritti e libertà personali per quanto riguarda il trattamento dei dati personali da parte delle autorità competenti.

L'interessato ha il diritto di essere informato in merito al trattamento dei propri dati personali e ha il diritto di accesso, rettifica, cancellazione e blocco del trattamento. Quando l'esercizio di questo diritto è negato per motivi preminenti, l'interessato deve avere il diritto di ricorrere alla competente autorità di controllo nazionale e/o di adire l'autorità giudiziaria. Se una persona subisce un danno cagionato da una violazione della legislazione nazionale di attuazione della decisione quadro sulla protezione dei dati, detta persona ha il diritto di ottenere il risarcimento da parte del titolare del trattamento[259]. In generale, gli interessati hanno il diritto di accesso a mezzi di ricorso per qualsiasi violazione dei loro diritti garantiti dalla legislazione nazionale di attuazione della decisione quadro sulla protezione dei dati[260].

La Commissione europea ha proposto una riforma che consiste nell'adozione di un regolamento generale sulla protezione dei dati[261] e di una direttiva generale sulla tutela dei dati[262]. La nuova direttiva sostituirà l'attuale decisione quadro sulla protezione dei dati e applicherà i principi e le norme generali relativi alla cooperazione giudiziaria e di polizia in materia penale.

259 *Ibid.*, articolo 19.

260 *Ibid.*, articolo 20.

261 Commissione europea (2012), *Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM(2012) 11 final, Bruxelles, 25 gennaio 2012.

262 Commissione europea (2012), *Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (direttiva generale sulla tutela dei dati)*, COM(2012) 10 final, Bruxelles, 25 gennaio 2012.

7.2.2. Strumenti giuridici più specifici sulla protezione dei dati nel settore della cooperazione transfrontaliera in materia di pubblica sicurezza e applicazione della legge

Oltre a quanto previsto dalla decisione quadro sulla protezione dei dati, lo scambio di informazioni conservate dagli Stati membri in settori specifici è disciplinato da una serie di strumenti giuridici, quali la decisione quadro 2009/315/GAI del Consiglio relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario e la decisione del Consiglio concernente le modalità di cooperazione tra le unità di informazione finanziaria degli Stati membri per quanto riguarda lo scambio di informazioni[263].

Occorre evidenziare che la cooperazione transfrontaliera[264] fra le autorità competenti comporta in misura sempre crescente lo scambio di dati sull'immigrazione. Questa sfera del diritto non rientra nel settore della pubblica sicurezza e della giustizia penale ma, sotto diversi aspetti, è rilevante per l'attività della polizia e delle autorità giudiziarie. Lo stesso dicasi per i dati relativi alle merci importate nell'UE o da questa esportate. L'eliminazione dei controlli di frontiera interna nell'Unione ha determinato un aumento del rischio di frodi, costringendo gli Stati membri a intensificare la cooperazione, in particolare rafforzando lo scambio transfrontaliero di informazioni, per accertare e perseguire in modo più efficace le violazioni del diritto doganale nazionale e dell'UE.

La decisione di Prüm

Un importante esempio di cooperazione transfrontaliera istituzionalizzata mediante lo scambio di dati tenuti a livello nazionale è la decisione 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (*decisione di Prüm*), che nel 2008 ha

263 Consiglio dell'Unione europea (2009), Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario, GU L 93 del 7.04.2009; Consiglio dell'Unione europea (2000), Decisione 2000/642/GAI del Consiglio, del 17 ottobre 2000, concernente le modalità di cooperazione tra le unità di informazione finanziaria degli Stati membri per quanto riguarda lo scambio di informazioni, GU L 271 del 24.10.2000.

264 Commissione europea (2012), Comunicazione della Commissione al Parlamento europeo e al Consiglio – Rafforzare la cooperazione in materia di applicazione della legge nell'UE: il modello europeo di scambio di informazioni (EIXM), COM(2012) 735 final, Bruxelles, 7 dicembre 2012.

integrato nel diritto dell'UE il trattato di Prüm[265], un accordo internazionale di cooperazione di polizia firmato nel 2005 da Austria, Belgio, Francia, Germania, Lussemburgo, Paesi Bassi e Spagna[266].

Lo scopo della decisione di Prüm è quello di agevolare agli Stati membri il compito di migliorare la condivisione delle informazioni ai fini della prevenzione e della lotta contro la criminalità in tre settori: terrorismo, criminalità transfrontaliera e migrazione irregolare. A tal fine, la decisione contiene disposizioni per quanto riguarda:

- l'accesso automatizzato a profili DNA, ai dati relativi alle impronte digitali e a taluni dati nazionali di immatricolazione dei veicoli;
- la trasmissione dei dati in relazione a eventi di rilievo a dimensione transfrontaliera;
- la trasmissione delle informazioni per prevenire reati terroristici;
- altre misure per potenziare la cooperazione di polizia transfrontaliera.

Le banche dati messe a disposizione nell'ambito della decisione di Prüm sono regolamentate interamente dalla normativa nazionale, ma lo scambio di dati è disciplinato specificamente dalla stessa decisione e, più di recente, dalla decisione quadro sulla protezione dei dati. Gli organi competenti per il controllo di tali flussi di dati sono le autorità di controllo nazionali per la protezione dei dati.

7.2.3. Protezione dei dati presso Europol ed Eurojust

Europol

Europol, l'agenzia dell'UE preposta alla attività di contrasto, ha la sede centrale all'Aia e dispone di unità nazionali Europol (UNE) in ciascuno Stato membro. L'ufficio Europol è stato istituito nel 1998; il suo attuale status giuridico come istituzione dell'UE

265 Consiglio dell'Unione europea (2008), Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.8.2008.

266 Trattato tra il Regno del Belgio, la Repubblica federale di Germania, il Regno di Spagna, la Repubblica francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria, relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale, disponibile all'indirizzo: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

è basato sulla decisione del Consiglio che istituisce l'Ufficio europeo di polizia (*decisione Europol*)[267]. Il mandato di Europol è quello di sostenere le attività di prevenzione e d'indagine sulla criminalità organizzata, sul terrorismo e su altre forme gravi di criminalità, elencate nell'allegato alla decisione Europol, che interessino due o più Stati membri.

Per conseguire i propri obiettivi, Europol ha creato il sistema d'informazione Europol, che mette a disposizione degli Stati membri una banca dati per lo scambio di informazioni e *intelligence* in materia penale attraverso le rispettive UNE. Il sistema d'informazione Europol può essere usato per rendere disponibili dati che riguardino persone sospettate di aver commesso un reato di competenza di Europol o che sono state condannate per un siffatto reato o persone riguardo alle quali vi siano indicazioni concrete per ritenere che possano commettere tali reati. Europol e le UNE possono inserire dati direttamente nel sistema d'informazione Europol ed estrarli dallo stesso. Solo la parte che ha inserito i dati nel sistema può modificarli, rettificarli o cancellarli.

Se necessario per lo svolgimento dei propri compiti, Europol può conservare, modificare e utilizzare dati relativi a reati in archivi di lavoro a fini di analisi. Detti archivi sono a disposizione a fini di raccolta, trattamento o uso di dati a sostegno di concrete indagini penali condotte da Europol unitamente agli Stati membri dell'UE.

In risposta ai nuovi sviluppi, il 1° gennaio 2013 è stato istituito presso Europol il Centro europeo per la lotta alla criminalità informatica[268], che funge da centro dell'UE per le informazioni sulla criminalità informatica, contribuendo a velocizzare le risposte in caso di reati online, sviluppando e mobilitando capacità di analisi tecnica forense digitale e delineando le migliori pratiche sulle indagini concernenti la criminalità informatica. Il Centro si focalizza su reati informatici:

- commessi da gruppi organizzati per generare ingenti profitti da attività criminali come la frode online;

267 Consiglio dell'Unione europea (2009), Decisione del Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol), GU L 121 del 15.5.2009. Cfr. anche la proposta di regolamento della Commissione che prevede un quadro giuridico per un nuovo Europol che sostituisce e succede all'Ufficio Europol istituito con decisione 2009/371/GAI del Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol) e all'Accademia CEPOL istituita con decisione 2005/681/GAI del Consiglio che istituisce l'Accademia europea di polizia (CEPOL), COM(2013) 173 final.

268 Cfr. anche GEPD (2012), *Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione europea al Consiglio e al Parlamento europeo sull'istituzione di un Centro europeo per la lotta alla criminalità informatica*, Bruxelles, 29 giugno 2012.

- che recano gravi danni alla vittima, come lo sfruttamento sessuale dei minori online;

- che colpiscono i sistemi d'informazione e le infrastrutture critiche dell'UE.

Il regime di protezione dei dati che governa le attività di Europol è stato potenziato. Le decisione Europol prevede, all'articolo 27, che trovano applicazione i principi della Convenzione n. 108 e della raccomandazione sull'uso dei dati nell'ambito della pubblica sicurezza relativamente al trattamento dei dati automatizzati e non automatizzati. La trasmissione di dati fra Europol e gli Stati membri deve rispettare anche le norme di cui alla decisione quadro sulla protezione dei dati.

Per garantire il rispetto del diritto applicabile in materia di protezione dei dati e, in particolare, che i diritti delle persone non siano violati dal trattamento dei dati personali, un organo indipendente, l'autorità di controllo comune di Europol, segue e controlla le attività di Europol[269]. Ogni persona ha diritto di accesso a qualsiasi dato personale che Europol possa detenere sul suo conto, nonché il diritto di richiedere che tali dati personali siano controllati, rettificati o cancellati. Se una persona non è soddisfatta della decisione di Europol sull'esercizio di detti diritti, può presentare ricorso al comitato ricorsi dell'autorità di controllo comune.

Se gli è stato recato pregiudizio per errori di diritto o di fatto in dati conservati o trattati presso Europol, il soggetto danneggiato può però promuovere un'azione di risarcimento solo dinanzi al tribunale competente dello Stato membro nel quale si è verificato l'evento all'origine del danno[270]. Europol risarcirà lo Stato membro se il danno deriva dal mancato rispetto dei propri obblighi giuridici.

Eurojust

Eurojust, istituito nel 2002, è un organismo dell'UE con sede all'Aia, che promuove la cooperazione giudiziaria nell'ambito di indagini e azioni penali in merito a gravi

269 Decisione Europol, articolo 34.

270 *Ibid*., articolo 52.

forme di criminalità che interessino almeno due Stati membri[271]. Eurojust ha il compito di:

- stimolare e migliorare il coordinamento delle indagini e delle azioni penali tra le autorità nazionali competenti dei vari Stati membri;
- agevolare l'esecuzione di richieste e decisioni relative alla cooperazione giudiziaria.

Le funzioni di Eurojust sono esercitate dai membri nazionali. Ogni Stato membro delega un giudice o un pubblico ministero presso Eurojust, il cui status è soggetto alla legge nazionale ed è dotato delle competenze necessarie per svolgere i compiti necessari a stimolare e migliorare la cooperazione giudiziaria. Inoltre, i membri nazionali agiscono congiuntamente come collegio per svolgere compiti speciali nell'ambito del mandato di Eurojust.

Eurojust può trattare dati personali nella misura necessaria a conseguire i propri obiettivi. Ciò si limita, tuttavia, al trattamento di specifiche informazioni concernenti persone sospettate di aver commesso, partecipato o essere state condannate per un reato che rientra nella sfera di competenza di Eurojust. Eurojust può anche trattare talune informazioni concernenti testimoni o vittime di reati sottoposti alla propria competenza[272]. In casi eccezionali e per un periodo di tempo limitato, Eurojust può trattare una maggiore quantità di dati personali relativi alle circostanze di un reato qualora detti dati abbiano rilievo immediato per le indagini in corso. Nell'ambito della propria competenza, Eurojust può cooperare con altre istituzioni, organismi e agenzie dell'Unione e scambiare con questi dati personali, oltre a cooperare e scambiare dati personali con paesi terzi e altre organizzazioni.

Con riguardo alla protezione dei dati, Eurojust deve garantire un livello di protezione almeno equivalente a quello garantito dai principi di cui alla Convenzione n. 108 del

271 Consiglio dell'Unione europea (2002), decisione 2002/187/GAI del Consiglio, del 28 febbraio 2002, che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità, GU L 63 del 6.03.2002; Consiglio dell'Unione europea (2003), decisione 2003/659/GAI del Consiglio, del 18 giugno 2003, che modifica la decisione 2002/187/GAI, che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità, GU L 44 del 15.05.2009; Consiglio dell'Unione europea (2009), 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, GU L 138 del 4.6.2009 (*decisioni Eurojust*).

272 Versione consolidata della decisione 2002/187/GAI del Consiglio come modificata dalla decisione 2003/659/GAI del Consiglio e dalla decisione 2009/426/GAI del Consiglio, articolo 15, paragrafo 2.

CDE e successive modifiche. Nei casi di scambio di dati, occorre osservare norme e restrizioni specifiche attuate in un accordo di cooperazione o in un accordo operativo, conformemente alle decisioni del Consiglio su Eurojust e alle disposizioni del regolamento interno dell'Eurojust relative al trattamento e alla protezione dei dati personali[273].

In seno a Eurojust è stata istituita un'autorità di controllo comune indipendente con il compito di monitorare il trattamento dei dati personali da parte di Eurojust. Le persone possono rivolgersi all'autorità di controllo se non sono soddisfatte della risposta di Eurojust a una richiesta di accesso, rettifica, blocco del trattamento o cancellazione di dati personali. In caso di trattamento illecito di dati personali, Eurojust, conformemente al diritto nazionale dello Stato membro in cui ha sede, ossia i Paesi Bassi, è responsabile di qualsiasi pregiudizio cagionato all'interessato.

7.2.4. Protezione dei dati nei sistemi d'informazione comune a livello di UE

Oltre allo scambio di dati fra Stati membri e alla creazione di autorità dell'Unione specializzate nella lotta contro la criminalità transfrontaliera, a livello di UE sono stati istituiti diversi sistemi d'informazione comune che fungono da piattaforma per lo scambio di dati fra le autorità nazionali e dell'UE competenti per fini specifici di contrasto, compresa la legislazione in materia di immigrazione e dogane. Alcuni di questi sistemi sono stati sviluppati a partire da accordi multilaterali, successivamente integrati da strumenti e sistemi giuridici dell'UE, quali il Sistema d'Informazione Schengen, il Sistema d'informazione visti, Eurodac, Eurosur o il Sistema informativo doganale.

L'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA)[274], istituita nel 2012, è responsabile della gestione operativa a lungo termine del Sistema d'Informazione Schengen di seconda generazione (SIS II), del Sistema d'informazione visti (VIS) e di Eurodac. Il compito principale di eu-LISA è quello di garantire un esercizio efficace, sicuro e continuo

273 Disposizioni del regolamento interno dell'Eurojust relative al trattamento e alla protezione dei dati personali, GU C 68 del 19 marzo 2005, pag. 1.

274 Regolamento (UE) n. 1077/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, GU L 286 dell'1.11.2011.

dei sistemi IT. L'Agenzia è anche responsabile dell'adozione di misure necessarie a garantire la sicurezza dei sistemi e dei dati.

Il Sistema d'Informazione Schengen

Nel 1985 diversi Stati membri dell'allora Comunità europea sono entrati a far parte dell'accordo stipulato fra gli Stati dell'Unione economica del Benelux, la Germania e la Francia per l'eliminazione graduale dei controlli alle frontiere comuni (*accordo Schengen*), con l'intento di creare uno spazio per la libera circolazione delle persone, esente da controlli di frontiera nel territorio Schengen[275]. Per controbilanciare le minacce alla sicurezza pubblica che potevano derivare dall'apertura delle frontiere interne, sono stati stabiliti controlli di frontiera rafforzati presso le frontiere esterne dello spazio Schengen nonché una stretta cooperazione fra le autorità di polizia e le autorità giudiziarie nazionali.

A seguito dell'adesione di altri Stati all'accordo Schengen, il relativo sistema è stato integrato in via definitiva nel quadro giuridico dell'UE con il trattato di Amsterdam[276]. L'attuazione di questa decisione è avvenuta nel 1999. La versione più recente del Sistema d'Informazione Schengen, il cosiddetto SIS II, è divenuta operativa il 9 aprile 2013; attualmente riguarda tutti gli Stati membri dell'UE più Islanda, Liechtenstein, Norvegia e Svizzera[277]. Anche Europol ed Eurojust hanno accesso a SIS II.

SIS II è costituito da un sistema centrale (SIS-C), da un sistema nazionale (SIS-N) in ciascuno Stato membro e da un'infrastruttura di comunicazione fra il sistema centrale e i sistemi nazionali. Il SIS-C contiene taluni dati inseriti dagli Stati membri su persone e oggetti ed è usato dalle autorità nazionali preposte ai controlli di frontiera, dalle autorità di polizia, dalle autorità doganali, dalle autorità competenti al rilascio dei visti e dalle autorità giudiziarie nello spazio Schengen. Ogni Stato membro gestisce una copia nazionale del SIS-C, nota come Sistema d'Informazione Schengen

275 Accordo fra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, GU L 239 del 22.9.2000.

276 Comunità europee (1997), Trattato di Amsterdam che modifica il trattato sull'Unione europea, i trattati che istituiscono le Comunità europee e alcuni atti connessi, GU C 340 del 10.11.1997.

277 Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (*SIS II*), GU L 381 del 28.12.2006, e Consiglio dell'Unione europea (2007), decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (*SIS II*), GU L 205 del 7.8.2007.

nazionale (SIS-N), costantemente aggiornata, aggiornando così il SIS-C. Il SIS-N viene consultato e produce una segnalazione in almeno uno dei seguenti casi:

- la persona non ha il diritto d'ingresso o di soggiorno nel territorio Schengen; o
- la persona o l'oggetto sono ricercati da autorità giudiziarie o da autorità preposte all'applicazione della legge; o
- la persona è stata segnalata come scomparsa; o
- beni quali banconote, automobili, veicoli commerciali, armi e documenti d'identità sono stati denunciati come beni rubati o smarriti.

In caso di segnalazione, le attività di follow-up devono essere avviate attraverso i Sistemi d'Informazione Schengen nazionali.

Il SIS II dispone di nuove funzionalità, fra cui la possibilità di inserire dati biometrici, quali impronte digitali e fotografie; nuove categorie di segnalazioni, quali imbarcazioni, aeromobili, container o mezzi di pagamento rubati; migliori segnalazioni su persone e oggetti; copie dei mandati d'arresto europei (MAE) relativi a persone ricercate a fini di arresto, consegna o estradizione.

La decisione 2007/533/GAI del Consiglio sull'istituzione, l'esercizio e l'uso del Sistema d'Informazione Schengen di seconda generazione (decisione Schengen II) integra la Convenzione n. 108: "I dati personali trattati in applicazione della presente decisione sono protetti a norma della convenzione del Consiglio d'Europa" n. 108[278]. Quando l'uso di dati personali da parte delle autorità nazionali di polizia avviene in applicazione della decisione Schengen II, le disposizioni della Convenzione n. 108 e della raccomandazione sull'uso dei dati personali nell'ambito della pubblica sicurezza devono essere attuate nella legislazione nazionale.

L'autorità di controllo nazionale competente in ciascuno Stato membro controlla il sistema SIS-N interno, in particolare verificando la qualità dei dati che lo Stato membro inserisce nel SIS-C attraverso il proprio SIS-N. L'autorità di controllo nazionale deve provvedere che venga svolta una verifica delle operazioni di trattamento dei dati nel proprio SIS-N-almeno ogni quattro anni. Le autorità di controllo nazionali e

278 Consiglio dell'Unione europea (2007), decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), GU L 205 del 7.8.2007, articolo 57.

il GEPD cooperano e garantiscono il controllo coordinato del SIS II, mentre il GEPD è responsabile per la supervisione del C-SIS. . A fini di trasparenza, ogni due anni deve essere trasmessa al Parlamento europeo, al Consiglio e all'eu-LISA una relazione congiunta sulle attività svolte.

I diritti di accesso delle persone al SIS II possono essere esercitati in ogni Stato membro, dato che ogni SIS-N è una copia esatta del SIS-C.

Esempio: nella causa *Dalea c. Francia*[279], al ricorrente era stato negato un visto per entrare in Francia poiché le autorità francesi avevano segnalato al Sistema d'Informazione Schengen la necessità di negargli l'ingresso. Il ricorrente aveva chiesto, senza esito positivo, l'acceso e la rettifica o la cancellazione dei dati alla Commissione francese per la protezione dei dati e, in ultima istanza, al Consiglio di Stato. La Corte EDU ha statuito che l'inserimento del ricorrente nel Sistema d'Informazione Schengen era stato conforme alla legge e aveva perseguito lo scopo legittimo di tutelare la sicurezza nazionale. Poiché il ricorrente non aveva dimostrato quale danno avesse effettivamente subito a causa del negato ingresso nello spazio Schengen, e poiché erano state attuate misure sufficienti per tutelarlo da decisioni arbitrarie, l'ingerenza con il suo diritto al rispetto della vita privata era stata proporzionata. Pertanto, il ricorso del ricorrente ai sensi dell'articolo 8 è stato dichiarato irricevibile.

Il Sistema d'informazione visti

Il Sistema d'informazione visti (VIS), anch'esso gestito da eu-LISA, è stato sviluppato per sostenere l'attuazione di una politica comune dell'UE in materia di visti[280]. Il Sistema VIS consente agli Stati Schengen di scambiarsi informazioni sui visti mediante un sistema che collega i consolati degli Stati Schengen ubicati in paesi extra-UE con i punti di attraversamento delle frontiere esterne di tutti gli Stati Schengen. Il Sistema VIS tratta dati concernenti le domande di visti relativi a soggiorni di breve durata per l'ingresso o il transito attraverso lo spazio Schengen. Il Sistema VIS

279 Corte EDU, *Dalea c. Francia* (dec.), n. 964/07, 2 febbraio 2010.

280 Consiglio dell'Unione europea (2004), decisione del Consiglio dell'8 giugno 2004 che istituisce il sistema di informazione visti (VIS), GU L 213 del 15.06.2004; regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, GU L 218 del 13.8.2008 (*regolamento VIS*); Consiglio dell'Unione europea (2008), decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 218 del 13.8.2008.

consente alle autorità di frontiera di verificare, con l'aiuto di dati biometrici, se la persona che presenta un visto sia il legittimo titolare o meno e di identificare le persone prive di documenti o in possesso di documenti falsi.

Ai sensi del regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il Sistema d'informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (*regolamento VIS*), solo i dati sul richiedente, sui suoi visti, fotografie, impronte digitali, collegamenti con precedenti richieste di visto ed i dati relativi alle richieste di visto delle persone che lo accompagnano possono essere registrati nel VIS[281]. L'accesso al VIS per inserire, modificare o cancellare dati è limitato esclusivamente alle autorità degli Stati membri competenti per il rilascio dei visti, mentre l'accesso a fini di consultazione dei dati è previsto sia per le autorità competenti per il rilascio dei visti sia per le autorità competenti per i controlli ai punti di attraversamento delle frontiere esterne, per i controlli in materia di immigrazione e di richieste di asilo. A determinate condizioni, le autorità nazionali competenti per la pubblica sicurezza ed Europol possono chiedere l'accesso ai dati registrati nel VIS ai fini della prevenzione, dell'individuazione e d'indagine su reati di terrorismo e altri reati gravi[282].

Eurodac

Il termine Eurodac si riferisce a dattilogrammi o impronte digitali. Si tratta di un sistema centralizzato contenente dati relativi alle impronte digitali di cittadini di paesi terzi che presentano domanda di asilo in uno degli Stati membri dell'UE[283]. Il sistema è operativo da gennaio 2003 con lo scopo di contribuire alla determinazione dello Stato membro competente per l'esame di una domanda specifica di asilo ai sensi del regolamento (CE) n. 343/2003 del Consiglio, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda d'asilo

281 Articolo 5 del regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, GU L 218 del 13.8.2008 (*regolamento VIS*).

282 Consiglio dell'Unione europea (2008), decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 218 del 13.8.2008.

283 Regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino, GU L 316 del 15.12.2000; regolamento (CE) n. 407/2002 del Consiglio, del 28 febbraio 2002, che definisce talune modalità di applicazione del regolamento (CE) n. 2725/2000 che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino, GU L 62 del 5.3.2002 (*regolamenti Eurodac*).

presentata in uno degli Stati membri da un cittadino di un paese terzo (*regolamento Dublino II*)[284]. I dati personali contenuti in Eurodac possono essere usati solo al fine di facilitare l'applicazione del regolamento Dublino II; ogni altro uso è soggetto a sanzioni.

Eurodac comprende un'unità centrale, gestita da eu-LISA, che conserva e confronta le impronte digitali, nonché un sistema per la trasmissione elettronica dei dati fra gli Stati membri e la banca dati centrale. Gli Stati membri rilevano e trasmettono le impronte digitali di ciascun cittadino extra-UE o di un apolide di età maggiore di 14 anni che richieda asilo nel loro territorio o che sia fermato per attraversamento non autorizzato della loro frontiera esterna. Gli Stati membri possono anche rilevare e trasmettere le impronte digitali di cittadini extra-UE o di apolidi soggiornanti nel loro territorio senza permesso.

I dati relativi alle impronte digitali sono conservati nella banca dati Eurodac solo in formato pseudonimizzato. In caso di corrispondenza, lo pseudonimo è comunicato al secondo Stato membro, unitamente al nome del primo Stato membro che ha trasmesso i suddetti dati,. Il secondo Stato membro si rivolgerà poi al primo Stato membro perché, a norma del regolamento Dublino II, tale primo Stato membro è responsabile del trattamento della domanda di asilo.

I dati personali archiviati in Eurodac e relativi ai richiedenti asilo sono conservati per 10 anni dalla data di rilevamento delle impronte digitali, a meno che l'interessato non ottenga la cittadinanza di uno Stato membro dell'UE. In tal caso, i dati devono essere cancellati immediatamente. I dati relativi agli stranieri fermati per attraversamento non autorizzato della frontiera esterna sono conservati per due anni e devono essere cancellati immediatamente se l'interessato ottiene un permesso di soggiorno, lascia il territorio dell'Unione o acquisisce la cittadinanza di uno Stato membro.

Oltre a tutti gli Stati membri dell'UE, anche Islanda, Norvegia, Liechtenstein e Svizzera applicano Eurodac sulla base di accordi internazionali.

284 Regolamento (CE) n. 343/2003 del Consiglio, del 18 febbraio 2003, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda d'asilo presentata in uno degli Stati membri da un cittadino di un paese terzo, GU L 50 del 25.2.2003 (*regolamento Dublino II*).

Eurosur

Il sistema europeo di sorveglianza delle frontiere (*Eurosur*)[285] è volto a migliorare il controllo delle frontiere esterne Schengen al fine di individuare, prevenire e combattere l'immigrazione irregolare e la criminalità transfrontaliera. Il sistema serve a rafforzare lo scambio di informazioni e la cooperazione operativa fra i centri di coordinamento nazionale e Frontex, l'Agenzia UE per lo sviluppo e l'applicazione del nuovo concetto di gestione integrata delle frontiere[286]. Gli obiettivi generali di Eurosur sono:

- ridurre il numero di migranti irregolari che entrano nell'UE in modo clandestino;
- ridurre il numero di decessi di migranti irregolari salvando più vite in mare;
- aumentare la sicurezza interna dell'UE nel suo insieme contribuendo a prevenire la criminalità transfrontaliera[287].

Eurosur è divenuto operativo il 2 dicembre 2013 in tutti gli Stati membri con frontiere esterne e lo sarà a partire dal 1 dicembre 2014 negli altri Stati. Il regolamento si applica alla sorveglianza delle frontiere terrestri, marittime esterne e aeree degli Stati membri.

285 Regolamento (UE) n. 1052/2013 del Parlamento europeo e del Consiglio, del 22 ottobre 2013, che istituisce il sistema europeo di sorveglianza delle frontiere (Eurosur), GU L 295 del 6.11.2013.

286 Regolamento (UE) n. 1168/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, recante modifica del regolamento (CE) n. 2007/2004 del Consiglio che istituisce un'Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea, GU L 394 del 22.11.2011 (*regolamento Frontex*).

287 Cfr. anche Commissione europea (2008), Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Esame della creazione di un sistema europeo di sorveglianza delle frontiere (EUROSUR), COM(2008) 68 definitivo, Bruxelles, 13 febbraio 2008; Commissione europea (2011), Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur) [*Valutazione d'impatto che accompagna la proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un sistema europeo di sorveglianza delle frontiere (EUROSUR)*], documento di lavoro dei servizi della Commissione, SEC(2011) 1536 final, Bruxelles,12 dicembre 2011, pag. 18.

Il Sistema informativo doganale

Un altro importante sistema d'informazione comune attuato a livello di UE è il Sistema informativo doganale (SID)[288]. Nel corso della creazione del mercato interno, tutti i controlli e le formalità concernenti le merci circolanti nel territorio dell'UE sono stati aboliti. Il maggiore rischio di frode che ne è derivato è stato controbilanciato da una più intensa cooperazione fra le amministrazioni doganali degli Stati membri. Lo scopo del SID è quello di sostenere gli Stati membri nella prevenzione, nell'indagine e nel perseguimento di gravi violazioni delle leggi nazionali e dell'UE in materia doganale e agricola.

Le informazioni contenute nel SID comprendono dati personali con riferimento a merci, mezzi di trasporto, imprese, persone, articoli e denaro bloccati, sequestrati o confiscati. Queste informazioni possono essere utilizzate unicamente a fini di osservazione e di rendiconto, di controlli specifici e di analisi strategica o operativa concernenti persone sospettate di violazione delle disposizioni doganali.

L'accesso al SID è concesso alle autorità nazionali doganali, fiscali, agricole, sanitarie pubbliche e di polizia nonché a Europol e a Eurojust.

Il trattamento di dati personali dev'essere effettuato nel rispetto delle norme specifiche di cui al Regolamento n. 515/97 e alla Convenzione SID[289] nonché delle disposizioni della direttiva sulla tutela dei dati, del regolamento sulla protezione dei dati da parte delle istituzioni dell'UE, della Convenzione n. 108 e della raccomandazione sull'uso dei dati personali nell'ambito della pubblica sicurezza. Il GEPD è responsabile del controllo di conformità del SID con il regolamento (CE) n 45/2001 e convoca almeno una volta all'anno una riunione con tutte le autorità nazionali di controllo per la protezione dei dati, competenti per le questioni di controllo relative al SID.

288 Consiglio dell'Unione europea (1995), Atto del Consiglio, del 26 luglio 1995, che elabora la convenzione sull'uso dell'informatica nel settore doganale, GU C 316 del 27.11.1995, modificato dal Consiglio dell'Unione europea (2009), Regolamento (CE) n. 515/97 del Consiglio del 13 marzo 1997 relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola e Decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale, GU L 323 del 10.12.2009 (*decisione SID*).

289 *Ibid.*

8

Altre norme europee specifiche in materia di protezione dei dati

Unione europea	Argomenti trattati	Consiglio d'Europa
Direttiva sulla protezione dei dati Direttiva relativa alla vita privata e alle comunicazioni elettroniche	Comunicazioni elettroniche	Convenzione n. 108 Raccomandazione sui servizi di telecomunicazione
Direttiva sulla protezione dei dati, articolo 8, paragrafo 2, lettera b)	Rapporti di lavoro	Convenzione n. 108 Raccomandazione in materia di rapporti di lavoro
		Corte EDU, *Copland c. Regno Unito*, n. 62617/00, 3 aprile 2007
Direttiva sulla protezione dei dati, articolo 8, paragrafo 3	Dati sanitari	Convenzione n. 108 Raccomandazione sui dati sanitari
		Corte EDU, *Z. c. Finlandia*, n. 22009/93, 25 febbraio 1997
Direttiva sulle sperimentazioni cliniche	Sperimentazioni cliniche	
Direttiva sulla protezione dei dati, articolo 6, paragrafo 1, lettere b) ed e), e articolo 13, paragrafo 2	Statistiche	Convenzione n. 108 Raccomandazione sui dati statistici
Regolamento (CE) n. 223/2009 relativo alle statistiche europee CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008	Statistiche ufficiali	Convenzione n. 108 Raccomandazione sui dati statistici

Direttiva 2004/39/CE relativa ai mercati degli strumenti finanziari Regolamento (UE) n. 648/2012 sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni Regolamento (CE) n. 1060/2009 relativo alle agenzie di rating del credito Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno	**Dati finanziari**	Convenzione n. 108 Raccomandazione 90(19) sulla protezione dei dati personali utilizzati a fini di pagamento e di altre operazioni connesse Corte EDU, *Michaud c. Francia*, n. 12323/11, 6 dicembre 2012

In diverse circostanze, a livello europeo, sono stati adottati strumenti giuridici particolari che applicano con maggior precisione le regole generali della Convenzione n. 108 o della direttiva sulla protezione dei dati a situazioni specifiche.

8.1. Comunicazioni elettroniche

Punti salienti

- La raccomandazione del CDE del 1995 contiene regole specifiche sulla protezione dei dati nel settore delle telecomunicazioni, con particolare riguardo ai servizi telefonici.
- Il trattamento dei dati personali relativi alla prestazione di servizi di comunicazione a livello di UE è regolamentato nella direttiva e-privacy.
- La riservatezza delle comunicazioni elettroniche non si limita al contenuto di una comunicazione, ma si estende anche ai dati relativi al traffico, quali le informazioni su chi ha comunicato con chi, quando e per quanto tempo, nonché ai dati relativi all'ubicazione, come il luogo dal quale sono stati comunicati i dati.

Le reti di comunicazione hanno un maggiore potenziale di ingerenza ingiustificata nella sfera personale degli utenti, poiché comportano ulteriori possibilità tecniche di ascoltare e controllare le comunicazioni effettuate attraverso tali reti. Di conseguenza, si è ritenuto necessario adottare specifiche norme sulla protezione dei dati per fare fronte ai rischi specifici corsi dagli utenti dei servizi di comunicazione.

Nel 1995 il CDE ha emanato una raccomandazione relativa alla protezione dei dati nel settore delle telecomunicazioni, con particolare riguardo ai servizi telefonici[290].

290 CDE, Comitato dei ministri (1995), Raccomandazione N. R (95) 4 agli Stati membri sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici, 7 febbraio 1995.

Secondo questa raccomandazione, i dati personali nel contesto delle telecomunicazioni dovrebbero essere raccolti e trattati unicamente ai fini della connessione di un utente alla rete e della fornitura di un determinato servizio di telecomunicazione nonché per la fatturazione e la verifica del pagamento, per assicurare un'installazione tecnica ottimale e lo sviluppo della rete e del servizio.

Particolare attenzione è stata dedicata anche all'uso delle reti di comunicazione per l'invio di messaggi di marketing diretto. In generale, tali messaggi non possono essere inviati nei confronti di un abbonato che abbia espresso il desiderio di non ricevere messaggi pubblicitari. I dispositivi di chiamata automatica per la trasmissione di messaggi preregistrati di natura pubblicitaria possono essere usati soltanto se gli abbonati hanno accordato il proprio consenso esplicito. La legislazione nazionale deve prevedere norme specifiche in questo settore.

Per quanto riguarda il **quadro giuridico dell'UE**, dopo un primo tentativo nel 1997, nel 2002 è stata adottata la direttiva relativa alla vita privata e alle comunicazioni elettroniche, modificata poi nel 2009 al fine di integrare e specificare le disposizioni della direttiva sulla protezione dei dati nel settore delle telecomunicazioni[291]. L'applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche è limitata ai servizi di comunicazione nelle reti elettroniche pubbliche.

La direttiva relativa alla vita privata e alle comunicazioni elettroniche distingue tre categorie principali di dati generati nel corso di una comunicazione:

- i dati che costituiscono il contenuto dei messaggi inviati durante la comunicazione: si tratta di dati strettamente riservati;

- i dati necessari per stabilire e mantenere la comunicazione, i cosiddetti dati relativi al traffico, quali informazioni sugli interlocutori, sul momento e sulla durata della comunicazione;

291 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, GU L 201 del 31.7.2002 (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*), modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009.

- fra i dati relativi al traffico figurano dati specificamente connessi all'ubicazione del dispositivo di comunicazione, i cosiddetti dati relativi all'ubicazione; tali dati riguardano al contempo l'ubicazione degli utenti dei dispositivi di comunicazione e assumono particolare rilievo per quanto concerne gli utenti di dispositivi di comunicazione mobile.

I dati relativi al traffico possono essere usati dal fornitore di servizi solo ai fini della fatturazione e della fornitura tecnica del servizio. Con il consenso dell'interessato, tuttavia, questi dati possono essere divulgati ad altri titolari del trattamento che offrono servizi a valore aggiunto, quali la fornitura di informazioni, in base all'ubicazione dell'utente, sulla stazione della metropolitana o sulla farmacia più vicine o sulle previsioni del tempo per quell'ubicazione.

Altre forme di accesso ai dati relativi alle comunicazioni realizzate su reti elettroniche, fra cui l'accesso a fini di indagine su reati, devono soddisfare, ai sensi dell'articolo 15 della direttiva e-privacy, i requisiti della giustificazione di un'ingerenza con il diritto alla protezione dei dati sancito dall'articolo 8, paragrafo 2, della CEDU e confermato dalla Carta agli articoli 8 e 52.

Gli emendamenti apportati nel 2009 alla direttiva relativa alla vita privata e alle comunicazioni elettroniche[292] hanno introdotto quanto segue:

- le restrizioni all'invio di messaggi di posta elettronica a fini di marketing diretto sono state estese agli SMS, ai servizi di messaggeria multimediali e ad altri tipi di applicazioni simili; i messaggi di posta elettronica a fini di promozione commerciale sono vietati a meno che non sia stato ottenuto il consenso preventivo. Senza tale consenso, possono essere contattati con messaggi di posta elettronica a fini di promozione commerciale solo i clienti già acquisiti, qualora abbiano messo a disposizione il proprio indirizzo di posta elettronica e non abbiano obiezioni;

- è stato imposto agli Stati membri l'obbligo di prevedere mezzi di ricorso contro le violazioni del divieto di inviare comunicazioni indesiderate[293];

292 Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009.

293 Cfr. la direttiva modificata, articolo 13.

- l'inserimento di marcatori ("cookies"), software che controlla e registra le azioni di un utente informatico, non è più consentito senza il consenso dell'utente stesso. La legislazione nazionale dovrebbe disciplinare in maniera più dettagliata le modalità di espressione e di acquisizione del consenso per garantire una protezione sufficiente[294].

In caso di violazione dei dati a motivo di un accesso non autorizzato, di perdita o di distruzione di dati, l'autorità di controllo competente deve esserne informata immediatamente. Gli abbonati devono essere informati qualora tale violazione dei dati possa arrecare loro un possibile danno[295].

La direttiva sulla conservazione dei dati (invalidata il 8 aprile 2014)[296] obbligava i fornitori di servizi di comunicazione a tenere a disposizione i dati relativi al traffico, nello specifico ai fini della repressione di reati gravi, per un periodo di almeno sei mesi, ma non superiore a 24 mesi, indipendentemente dal fatto che il fornitore di servizi avesse ancora necessità di conservare tali dati a fini di fatturazione o di fornitura tecnica del servizio.

Gli Stati membri dell'UE designano autorità pubbliche indipendenti responsabili del controllo della sicurezza dei dati conservati.

La conservazione di dati relativi alle telecomunicazioni interferisce chiaramente con il diritto alla protezione dei dati[297]. La giustificazione o meno di tale ingerenza è stata oggetto di diversi procedimenti giudiziari negli Stati membri dell'UE[298].

---

294 Cfr. *ibid.,* articolo 5; cfr. anche Gruppo di lavoro articolo 29 (2012), *Parere 04/2012 relativo all'esenzione dal consenso per l'uso di cookie*, WP 194, Bruxelles, 7 giugno 2012.

295 Cfr. anche Gruppo di lavoro articolo 29 (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (Documento di lavoro 01/2011 sull'attuale quadro dell'UE in materia di violazioni dei dati personali e raccomandazioni sui futuri sviluppi politici), WP 184, Bruxelles, 5 aprile 2011.

296 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006.

297 GEPD (2011), *Parere del 31 maggio 2011 sulla relazione di valutazione relativa all'applicazione della direttiva sulla conservazione di dati (direttiva 2006/24/CE) presentata dalla Commissione al Consiglio e al Parlamento europeo*, 31 maggio 2011.

298 Germania, Corte costituzionale federale (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 marzo 2010; Romania, Corte costituzionale federale (*Curtea Constituțională a României*), n. 1258, 8 ottobre 2009; Repubblica ceca, Corte costituzionale (*Ústavní soud České republiky*), 94/2011 Coll., 22 marzo 2011.

Esempio: nelle cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e a.,* la CGUE ha dichiarato invalida la direttiva sulla conservazione dei dati. Secondo la Corte, "l'ingerenza vasta e particolarmente grave di tale direttiva nei diritti fondamentali in parola non è sufficientemente regolamentata in modo da essere effettivamente limitata allo stretto necessario"[299].

Una questione cruciale nel contesto delle comunicazioni elettroniche è costituita dall'ingerenza da parte delle autorità pubbliche. I mezzi di sorveglianza o di intercettazione delle comunicazioni, quali dispositivi di ascolto o di intercettazione, sono autorizzati solo se sono previsti dalla legge e costituiscono una misura necessaria in una società democratica nell'interesse della tutela della sicurezza nazionale, della pubblica sicurezza, degli interessi monetari dello Stato o della repressione di reati, oppure ancora della protezione dell'interessato o dei diritti e delle libertà di altri.

Esempio: nella causa *Malone c. Regno Unito*[300], il ricorrente era stato accusato di una serie di reati in materia di ricettazione. Durante il processo era emersa l'intercettazione di una conversazione telefonica del ricorrente sulla base di un mandato emesso dal Segretario di Stato a uso del ministero dell'Interno. Anche se le modalità di intercettazione della comunicazione del ricorrente erano conformi al diritto nazionale, la Corte EDU ha constatato che non vi erano norme giuridiche sulla portata e sulle modalità di esercizio della discrezionalità goduta dalle autorità pubbliche in questo settore e che pertanto l'ingerenza derivante dall'esistenza della pratica in questione non era 'conforme alla legge'. La Corte ha statuito che vi era stata una violazione dell'articolo 8 della CEDU.

8.2. Dati relativi al rapporto di lavoro

Punti salienti

- La raccomandazione del CDE sul trattamento dei dati in ambito lavorativo contiene norme specifiche sulla protezione dei dati nei rapporti di lavoro.
- Nella direttiva sulla protezione dei dati, i rapporti di lavoro sono specificamente richiamati solo nel contesto del trattamento dei dati sensibili.

299 CGUE, cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e a.,*8 aprile 2014, punto 65.

300 Corte EDU, *Malone c. Regno Unito*, n. 8691/79, 2 agosto 1984.

- La validità del consenso, che deve essere libero, come base giuridica per il trattamento dei dati relativi ai dipendenti può essere opinabile, dato lo squilibrio economico esistente fra il datore di lavoro e il dipendente. Le circostanze del consenso devono essere valutate attentamente.

Nell'UE non è previsto uno specifico quadro giuridico che disciplini il trattamento di dati personali nel contesto dei rapporti di lavoro. Nella direttiva sulla protezione dei dati, i rapporti di lavoro sono specificamente richiamati soltanto nell'articolo 8, paragrafo 2, concernente il trattamento dei dati sensibili. Per quanto riguarda il CDE, la raccomandazione sul trattamento dei dati in ambito lavorativo è stata emanata nel 1989 ed è attualmente in fase di aggiornamento[301].

Un'indagine sui problemi più comuni relativi alla protezione dei dati e specifici del contesto lavorativo è reperibile in un documento di lavoro del Gruppo di lavoro articolo 29[302]. Il Gruppo di lavoro ha analizzato l'importanza del consenso come fondamento giuridico per il trattamento dei dati in ambito lavorativo[303], rilevando che lo squilibrio economico fra il datore di lavoro che chiede il consenso e il dipendente che dà il consenso solleva spesso dubbi sul fatto che il consenso sia stato espresso liberamente. Le circostanze nelle quali è richiesto il consenso, pertanto, dovrebbero essere considerate attentamente in sede di valutazione della validità del consenso in ambito lavorativo.

Un problema comune concernente la protezione dei dati in quello che attualmente è il tipico ambito lavorativo riguarda la definizione della legittimitàdel controllo delle comunicazioni elettroniche dei dipendenti sul luogo di lavoro. Si sostiene spesso che questo problema è facilmente risolvibile vietando l'uso privato dei mezzi di comunicazione sul luogo di lavoro. Tale divieto generale, tuttavia, potrebbe rivelarsi sproporzionato e irrealistico. La sentenza della Corte EDU illustrata di seguito assume particolare rilievo in questo contesto.

301 Consiglio d'Europa, Comitato dei ministri (1989), raccomandazione N. R (89) 2 agli Stati membri sull'uso dei dati personali per scopi di lavoro, 18 gennaio 1989. Cfr. altresì Comitato consultivo sulla Convenzione n. 108, Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation (*Studio sulla raccomandazione R (89) 2 sull'uso dei dati personali per scopi di lavoro e per avanzare proposte per la revisione della suddetta raccomandazione*), 9 settembre 2011.

302 Gruppo di lavoro articolo 29 (2001), *Parere 8/2001 sul trattamento dei dati personali nell'ambito dell'occupazione*, WP 48, Bruxelles, 13 settembre 2001.

303 Gruppo di lavoro articolo 29 (2005), *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995*, WP 114, Bruxelles, 25 novembre 2005.

Esempio: nella causa *Copland c. Regno Unito*[304], l'uso del telefono, della posta elettronica e di Internet da parte di una dipendente di un college è stato controllato in segreto per accertare se questa stesse facendo un uso eccessivo delle strutture del college per scopi personali. La Corte EDU ha statuito che le telefonate dal luogo di lavoro ricadevano negli ambiti concettuali di vita privata e di corrispondenza. Pertanto, le telefonate e i messaggi di posta elettronica inviati dal luogo di lavoro, così come le informazioni derivanti dal monitoraggio dell'uso personale di Internet, erano protetti ai sensi dell'articolo 8 della CEDU. Nel caso della ricorrente, non esistevano disposizioni in merito alle circostanze nelle quali i datori di lavoro potevano controllare l'uso del telefono, della posta elettronica e di Internet da parte dei dipendenti. Pertanto, l'ingerenza non era conforme alla legge. La Corte ha concluso che vi era stata una violazione dell'articolo 8 della CEDU.

Ai sensi della raccomandazione del CDE relativa alla protezione dei dati utilizzati per scopi di lavoro, i dati personali raccolti per scopi lavorativi dovrebbero essere ottenuti direttamente dal singolo dipendente.

I dati personali raccolti a fini di assunzione devono essere limitati alle informazioni necessarie per valutare l'idoneità dei candidati e le loro prospettive di carriera.

La raccomandazione menziona specificamente anche i dati raccolti a fini di valutazione relativi alla produttività o al potenziale dei singoli dipendenti. Tali dati valutativi, in forza dei principi di correttezza del trattamento dei dati personali e di esattezza dei dati stessi, devono basarsi su valutazioni eque e imparziali e non devono essere formulati in modo da risultare offensivi.

Un aspetto specifico del diritto in materia di protezione dei dati nel rapporto di lavoro riguarda il ruolo dei rappresentanti dei lavoratori. Tali rappresentanti possono venire in possesso dei dati personali dei dipendenti solo nella misura in cui ciò sia necessario per consentire loro di rappresentare gli interessi dei lavoratori.

I dati personali sensibili raccolti per scopi di lavoro possono essere trattati solo in casi particolari e nel rispetto delle garanzie stabilite dalla legislazione nazionale. I datori di lavoro possono chiedere ai dipendenti o ai candidati informazioni sul loro stato di salute e possono sottoporli a esame medico soltanto se necessario per accertarne l'idoneità all'impiego, per soddisfare esigenze di medicina preventiva o

304 Corte EDU, *Copland c. Regno Unito*, n. 62617/00, 3 aprile 2007.

per consentire il riconoscimento delle prestazioni sociali. I dati relativi alla salute non possono essere raccolti da fonti diverse dal dipendente interessato, tranne quando sia stato acquisito il suo consenso esplicito e informato o quando lo preveda la normativa nazionale.

Secondo la raccomandazione in materia di rapporti di lavoro, i dipendenti dovrebbero essere informati sulla finalità del trattamento dei loro dati personali, sulla tipologia di dati personali conservati, sui soggetti ai quali i dati sono comunicati in via regolare nonché sulla finalità e sul fondamento giuridico di tali comunicazioni. I datori di lavoro dovrebbero, inoltre, informare i lavoratori in anticipo sull'introduzione o la modifica di sistemi automatizzati per il trattamento dei dati personali o per il controllo dei movimenti o della produttività dei lavoratori.

I lavoratori devono avere il diritto di accesso ai propri dati relativi al rapporto di lavoro nonché il diritto di rettifica o cancellazione. In caso di trattamento di dati valutativi, i lavoratori devono inoltre avere il diritto di contestare tale valutazione. Tuttavia, questi diritti possono essere temporaneamente limitati in caso di indagini interne. Se a un lavoratore sono negati l'accesso, la rettifica o la cancellazione di dati personali relativi al rapporto di lavoro, la legislazione nazionale deve prevedere procedure idonee per contestare tale rifiuto.

8.3. Dati sanitari

Punto saliente

- I dati sanitari sono dati sensibili e pertanto godono di una protezione specifica.

I dati personali concernenti lo stato di salute dell'interessato sono qualificati dati sensibili ai sensi dell'articolo 8, paragrafo 1, della direttiva sulla protezione dei dati e dell'articolo 6 della Convenzione n. 108. A loro volta, i dati sanitari sono soggetti a un regime di trattamento più rigoroso rispetto ai dati non sensibili.

Esempio: nella causa *Z. c. Finlandia*[305], l'ex marito della ricorrente, che aveva contratto il virus dell'HIV, aveva commesso una serie di reati di natura sessuale. Successivamente era stato accusato di omicidio colposo per avere esposto consapevolmente le sue vittime al rischio di infezione da HIV. Il giudice nazionale aveva disposto un periodo di riservatezza di 10 anni per la sentenza integrale e i documenti relativi alla causa, malgrado la ricorrente avesse chiesto la concessione di un periodo di riservatezza più lungo. La corte d'appello aveva respinto tale richiesta con una sentenza nella quale apparivano i nomi completi della ricorrente e dell'ex marito. La Corte EDU ha statuito che l'ingerenza non era da ritenersi necessaria in una società democratica, dal momento che la protezione dei dati sanitari è di fondamentale importanza per il godimento del diritto al rispetto della vita privata e familiare, in particolare per quanto riguarda le informazioni sulle infezioni da HIV, data la stigmatizzazione di questa condizione in numerose società. Pertanto, la Corte ha concluso che il fatto di consentire l'accesso all'identità e alla condizione sanitaria della ricorrente, descritte nella sentenza della corte d'appello, dopo un periodo di soli 10 anni dalla sua pronuncia costituiva una violazione dell'articolo 8 della CEDU.

L'articolo 8, paragrafo 3, della direttiva sulla protezione dei dati consente il trattamento dei dati sanitari quando ciò sia necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura. Il trattamento è autorizzato, tuttavia, solo quando è effettuato da un operatore professionista in campo sanitario soggetto al segreto professionale o da un'altra persona parimente soggetta a un obbligo di segretezza equivalente[306].

La raccomandazione del CDE relativa alla protezione dei dati sanitari del 1997 applica in modo più dettagliato i principi della Convenzione n. 108 al trattamento di dati personali in questo ambito[307]. Le norme proposte sono in linea con quelle della direttiva sulla protezione dei dati per quanto riguarda gli scopi legittimi del trattamento dei dati sanitari, il necessario obbligo del segreto professionale per le persone che utilizzino dati relativi alla salute e i diritti degli interessati alla trasparenza e all'accesso, alla rettifica e alla cancellazione. Inoltre, i dati sanitari trattati legittimamente da ope-

305 Corte EDU, *Z. c. Finlandia*, n. 22009/93, 25 febbraio 1997, punti 94 e 112; cfr. anche Corte EDU, *M.S. c. Svezia*, n. 20837/92, 27 agosto 1997; Corte EDU, *L.L. c. Francia*, n. 7508/02, 10 ottobre 2006; Corte EDU, *I. c. Finlandia*, n. 20511/03, 17 luglio 2008; Corte EDU, *K.H. e a. c. Slovacchia*, n. 32881/04, 28 aprile 2009; Corte EDU, *Szuluk c. Regno Unito*, n. 36936/05, 2 giugno 2009.

306 Cfr. anche Corte EDU, *Biriuk c. Lituania*, n. 23373/03, 25 novembre 2008.

307 CDE, Comitato dei ministri (1997), Raccomandazione N. R (97) 5 agli Stati membri relativa alla protezione dei dati sanitari, 13 febbraio 1997.

ratori sanitari professionisti non possono essere trasmessi alle autorità di contrasto a meno che non siano previste "sufficienti garanzie per impedire una divulgazione non coerente con il rispetto della vita privata sancito dall'articolo 8 della CEDU"[308].

Inoltre, la raccomandazione contiene disposizioni specifiche sui dati sanitari di nascituri e incapaci nonché sul trattamento di dati genetici. Si riconosce espressamente che la ricerca scientifica giustifica la conservazione dei dati per un periodo superiore a quello necessario, sebbene in tal caso sia richiesta di solito l'anonimizzazione. L'articolo 12 della raccomandazione propone regole dettagliate per i casi in cui i ricercatori necessitino di dati personali e i dati anonimizzati risultino insufficienti.

La pseudonimizzazione può rappresentare uno strumento appropriato per soddisfare le esigenze scientifiche e tutelare, nel contempo, gli interessi dei pazienti. Il concetto di pseudonimizzazione nel contesto della protezione dei dati è illustrato in modo più dettagliato nel paragrafo 2.1.3.

A livello nazionale ed europeo si è discusso ampiamente di iniziative concernenti la conservazione in cartelle cliniche elettroniche dei dati relativi ai trattamenti sanitari di pazienti[309]. Un aspetto specifico legato all'esistenza di sistemi nazionali di cartelle cliniche elettroniche è costituito dalla loro disponibilità oltre confine; si tratta di un tema particolarmente interessante a livello di UE nell'ambito dell'assistenza sanitaria transfrontaliera[310].

Un'altra questione oggetto di discussione ai fini della formulazione di nuove disposizioni è rappresentata dalle sperimentazioni cliniche, ossia dalla sperimentazione di nuovi farmaci su pazienti in un ambiente di ricerca documentato. Anche questo tema incide notevolmente sulla protezione dei dati. Le sperimentazioni cliniche su prodotti medicinali per uso umano sono disciplinate dalla direttiva 2001/20/CE del Parlamento europeo e del Consiglio, del 4 aprile 2001, concernente il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri relative all'applicazione della buona pratica clinica nell'esecuzione della

308 Corte EDU, *Avilkina e a. c. Russia*, n. 1585/09, 6 giugno 2013, punto 53 (non definitiva).

309 Gruppo di lavoro articolo 29 (2007), *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, WP 131, Bruxelles, 15 febbraio 2007.

310 Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, GU L 88 del 4.4.2011.

sperimentazione clinica di medicinali ad uso umano (*direttiva sulle sperimentazioni cliniche*)[311]. Nel dicembre 2012 la Commissione europea ha proposto un regolamento che dovrebbe sostituire la direttiva sulle sperimentazioni cliniche allo scopo di renderle più uniformi ed efficienti[312].

A livello di UE restano pendenti molte altre iniziative legislative e di altro genere per quanto riguarda i dati personali nel settore della sanità[313].

8.4. Trattamento di dati personali a fini statistici

Punti salienti

- I dati raccolti a fini statistici non possono essere usati per nessun altro scopo.
- I dati raccolti legittimamente per qualsiasi scopo possono essere successivamente utilizzati a fini statistici, purché la legislazione nazionale preveda adeguate garanzie che siano rispettate dagli utenti. A tal fine, dovrebbero essere previste in particolare l'anonimizzazione o la pseudonimizzazione dei dati prima della trasmissione a terzi.

Nella direttiva sulla protezione dei dati, il trattamento di dati a fini statistici è menzionato nel contesto di possibile deroghe dai principi della protezione dei dati. Ai sensi dell'articolo 6, paragrafo 1, lettera b), della direttiva, la legislazione nazionale può derogare al principio di limitazione della finalità per consentire l'uso ulteriore dei dati a fini statistici, ma la legislazione nazionale deve prevedere anche tutte le garanzie necessarie. L'articolo 13, paragrafo 2, della direttiva consente alla legislazione nazionale di prevedere restrizioni dei diritti di accesso se i dati sono trattati esclusivamente a fini statistici; anche in tal caso la legislazione nazionale deve prevedere garanzie adeguate. In questo contesto, la direttiva sulla protezione dei dati

311 Direttiva 2001/20/CE del Parlamento europeo e del Consiglio, del 4 aprile 2001, concernente il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri relative all'applicazione della buona pratica clinica nell'esecuzione della sperimentazione clinica di medicinali ad uso umano, GU L 121 dell'1.5.2001.

312 Commissione europea (2012), Proposta di regolamento del Parlamento europeo e del Consiglio concernente la sperimentazione clinica di medicinali per uso umano, e che abroga la direttiva 2001/20/CE, COM(2012) 369 final, Bruxelles, 17 luglio 2012.

313 GEPD (2013), *Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione concernente il piano d'azione «Sanità elettronica» 2012-2020 — una sanità innovativa per il 21esimo secolo*, Bruxelles, 27 marzo 2013.

impone un requisito specifico, ossia che nessuno dei dati acquisiti o creati nel corso della ricerca statistica sia utilizzato per decisioni concrete riguardanti gli interessati.

Sebbene i dati legittimamente raccolti da un titolare del trattamento per qualsiasi scopo possano essere riutilizzati da quest'ultimo per fini statistici – le cosiddette statistiche secondarie – tali dati dovrebbero, a seconda del contesto, essere anonimizzati o pseudonimizzati prima di essere trasmessi a terzi per fini statistici, a meno che l'interessato vi acconsenta o tale trasmissione sia specificamente prevista dalla legislazione nazionale. Ciò deriva dall'obbligo di attuare garanzie appropriate di cui all'articolo 6, paragrafo 1, lettera b), della direttiva sulla protezione dei dati.

Rispetto all'uso di dati a fini statistici, rivestono massima importanza le statistiche ufficiali, condotte dagli istituti statistici nazionali e dell'UE alla luce del diritto nazionale e dell'UE sulle statistiche ufficiali. In virtù di tali disposizioni, i cittadini e le imprese sono di solito obbligati a comunicare dati alle autorità statistiche. I funzionari degli istituti statistici sono vincolati da specifici obblighi di segreto professionale che vengono scrupolosamente osservati, dal momento che risultano essenziali per assicurare un elevato livello di fiducia dei cittadini in quanto necessario affinché i dati siano messi a disposizione delle autorità statistiche.

Il regolamento (CE) n. 223/2009 sulle statistiche europee (*regolamento sulle statistiche europee*) contiene disposizioni essenziali per la protezione dei dati nelle statistiche ufficiali; pertanto, può essere considerato rilevante anche per quanto riguarda le disposizioni sulle statistiche ufficiali a livello nazionale[314]. Il regolamento ribadisce il principio secondo il quale le operazioni statistiche ufficiali necessitano di una base giuridica sufficientemente precisa[315].

Esempio: nella causa *Huber c. Bundesrepublik Deutschland*[316], la CGUE ha rilevato che la raccolta e la conservazione di dati personali da parte di un'autorità

314 Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunità europee, GU L 87 del 31.3.2009.

315 Questo principio dev'essere ulteriormente specificato nel codice di buone pratiche dell'Eurostat che, conformemente all'articolo 11 del regolamento sulle statistiche europee, fornirà orientamenti sulla compilazione di statistiche ufficiali, compreso l'uso ponderato dei dati personali; disponibile all'indirizzo: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

316 CGUE, C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008; cfr., in particolare, punto 68.

a fini statistici non costituivano di per sé un motivo sufficiente per considerare legittimo il trattamento. Anche la legge che prevedeva il trattamento dei dati personali doveva soddisfare il requisito di necessità, il che non era avvenuto nel caso specifico.

Nel 1997 è stata emanata in seno al CDE la raccomandazione sui dati statistici concernente la realizzazione di statistiche nei settori pubblico e privato[317]. La raccomandazione ha introdotto alcuni principi che coincidono con le norme cardine della direttiva sulla protezione dei dati di cui sopra. Norme più dettagliate sono previste per le questioni seguenti.

Mentre i dati raccolti da un titolare del trattamento a fini statistici non possono essere usati per nessun altro scopo, i dati raccolti per scopi non statistici sono utilizzabili ulteriormente a fini statistici. La raccomandazione sui dati statistici consente anche la comunicazione dei dati a terzi se ciò avviene solo per fini statistici. In tali casi, le parti dovrebbero concordare e formalizzare per iscritto la portata dell'ulteriore uso legittimo a fini statistici. Poiché tali previsioni non possono sostituire il consenso dell'interessato, si deve ritenere che la legislazione nazionale debba prevedere ulteriori garanzie appropriate per minimizzare i rischi di abuso di dati personali, quali l'obbligo di anonimizzare o pseudonimizzare i dati prima della trasmissione.

Chi si occupa di ricerca statistica in via professionale dovrebbe essere vincolato da speciali obblighi di segreto professionale – come accade per le statistiche ufficiali – ai sensi della legislazione nazionale. Questo dovrebbe valere anche per gli intervistatori, se impegnati nella raccolta dei dati presso gli interessati o altre persone.

Se un'indagine statistica che si avvale di dati personali non è prescritta dalla legge, gli interessati dovrebbero acconsentire all'uso dei loro dati per renderla legittima o dovrebbero almeno avere la possibilità di opporvisi. Se i dati personali sono raccolti a fini statistici dagli intervistatori, questi ultimi devono essere chiaramente informati circa l'obbligatorietà o meno della comunicazione dei dati ai sensi della legislazione nazionale. I dati sensibili non dovrebbero mai essere raccolti secondo modalità tali da consentire l'identificazione della persona, a meno che ciò sia esplicitamente autorizzato dal diritto nazionale.

Quando un'indagine statistica non può essere realizzata sulla base di dati anonimizzati, e sono effettivamente necessari dati personali, i dati raccolti per quello scopo

317 CDE, Comitato dei ministri (1997), Raccomandazione N. R (97) 18 agli Stati membri relativa alla protezione dei dati personali raccolti e trattati per scopi statistici, 30 settembre 1997.

dovrebbero essere resi anonimi il prima possibile. I risultati dell'indagine statistica non devono, per lo meno, consentire l'identificazione di alcun interessato, a meno che ciò non presenti manifestamente alcun rischio.

Dopo la conclusione dell'analisi statistica, i dati personali usati dovrebbero essere cancellati o resi anonimi. In tal caso, la raccomandazione sui dati statistici propone di conservare i dati identificativi separatamente dagli altri dati personali. Ciò significa, per esempio, che i dati dovrebbero essere pseudonimizzati e la chiave di cifratura o l'elenco con i sinonimi identificativi dovrebbero essere conservati separatamente dai dati pseudonimizzati.

8.5. Dati finanziari

Punti salienti

- Benché i dati finanziari non siano dati sensibili ai sensi della Convenzione n. 108 o della direttiva sulla protezione dei dati, il loro trattamento necessita di particolari garanzie per garantirne l'esattezza e la sicurezza.
- I sistemi di pagamento elettronico necessitano di una protezione integrata dei dati elaborati, la cosiddetta tutela della vita privata fin dalla progettazione.
- In questo settore particolari problemi di protezione dei dati derivano dall'esigenza di attuare appropriati meccanismi di autenticazione.

Esempio: nella causa *Michaud c. Francia*[318], il ricorrente, un avvocato francese, ha contestato l'obbligo impostogli dalla legge francese di comunicare eventuali sospetti su possibili attività di riciclaggio di denaro da parte dei clienti. La Corte EDU ha osservato che l'imposizione agli avvocati dell'obbligo di comunicare alle autorità amministrative informazioni sul conto di un'altra persona ottenute attraverso scambi con tale persona costituiva un'ingerenza nel diritto degli avvocati al rispetto della propria corrispondenza e vita privata ai sensi dell'articolo 8 della CEDU, poiché l'ambito di tale diritto si estendeva alle attività di natura professionale o commerciale. Tuttavia, l'ingerenza era conforme alla legge e perseguiva un obiettivo legittimo, ossia la prevenzione di disordini e di

318 Corte EDU, *Michaud c. Francia*, n. 12323/11, 6 dicembre 2012; cfr. anche Corte EDU, *Niemietz c. Germania*, n. 13710/88, 16 dicembre 1992, punto 29, e Corte EDU, *Halford c. Regno Unito*, n. 20605/92, 25 giugno 1997, punto 42.

reati. Poiché gli avvocati erano soggetti all'obbligo di comunicare sospetti solo in circostanze molto limitate, la Corte EDU ha statuito che l'obbligo era proporzionato, concludendo che non vi era stata alcuna violazione dell'articolo 8.

Con la raccomandazione Rec (90) 19 del 1990, il CDE ha proposto un'applicazione al contesto dei pagamenti del quadro giuridico generale in materia di protezione dei dati, contenuto nella Convenzione n. 108[319]. Questa raccomandazione chiarisce la portata della raccolta e dell'uso legittimi dei dati in questo ambito, specialmente mediante carte di pagamento, e propone ai legislatori nazionali disposizioni dettagliate sui limiti della comunicazione a terzi dei dati relativi a pagamenti, sui limiti temporali della conservazione dei dati, sulla trasparenza, sulla sicurezza dei dati e sui flussi transfrontalieri degli stessi nonché, infine, in materia di controllo e di mezzi di ricorso. Le soluzioni proposte corrispondono a quanto previsto successivamente in via generale a livello dell'UE attraverso la direttiva sulla protezione dei dati.

È in fase di formulazione una serie di strumenti giuridici volti a regolamentare i mercati degli strumenti finanziari nonché le attività degli enti creditizi e delle imprese d'investimento[320], mentre altri strumenti giuridici contribuiscono alle attività di contrasto dell'abuso di informazioni privilegiate e della manipolazione dei mercati[321]. Le questioni più critiche in questi settori, in quanto incidono sulla protezione dei dati, sono:

- la conservazione di registrazioni sulle operazioni finanziarie;

319 CDE, Comitato dei ministri (1990), Raccomandazione n. R (90) 19 relativa alla protezione dei dati personali utilizzati a fini di pagamento e di altre operazioni connesse, 13 settembre 1990.

320 Commissione europea (2011), *Proposta di direttiva del Parlamento europeo e del Consiglio relativa ai mercati degli strumenti finanziari che abroga la direttiva 2004/39/CE del Parlamento europeo e del Consiglio*, COM(2011) 656 definitivo, Bruxelles, 20 ottobre 2011; Commissione europea (2011), *Proposta di regolamento del Parlamento europeo e del Consiglio sui mercati degli strumenti finanziari e che modifica il regolamento [EMIR] sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni*, COM(2011) 652 definitivo, Bruxelles, 20 ottobre 2011; Commissione europea (2011), *Proposta di direttiva del Parlamento europeo e del Consiglio sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e che modifica la direttiva 2002/87/CE del Parlamento europeo e del Consiglio relativa alla vigilanza supplementare sugli enti creditizi, sulle imprese di assicurazione e sulle imprese di investimento appartenenti ad un conglomerato finanziario*, COM(2011) 453 definitivo, Bruxelles, 20 luglio 2011.

321 Commissione europea (2011), Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato), COM(2011) 651 definitivo, Bruxelles, 20 ottobre 2011; Commissione europea (2011), Proposta di direttiva del Parlamento europeo e del Consiglio relativa alle sanzioni penali in caso di abuso di informazioni privilegiate e di manipolazione del mercato, COM(2011) 654 definitivo, Bruxelles, 20 ottobre 2011.

- il trasferimento di dati personali verso paesi terzi;
- la registrazione di conversazioni telefoniche o di comunicazioni elettroniche, compreso il potere delle autorità competenti di richiedere le registrazioni dei dati telefonici e dei dati relativi al traffico;
- la divulgazione di informazioni personali, compresa la pubblicazione di sanzioni;
- i poteri di controllo e di indagine delle autorità competenti, comprese le ispezioni in loco e l'ingresso in locali privati per il sequestro di documenti;
- i meccanismi per la comunicazione di violazioni, vale a dire regimi di denuncia di irregolarità (*whistleblowing*);
- la cooperazione fra le autorità competenti degli Stati membri e l'Autorità europea degli strumenti finanziari e dei mercati (ESMA).

In questi settori sono affrontate specificamente anche altre questioni, fra cui la raccolta di dati sulla condizione finanziaria degli interessati[322] o sui pagamenti transfrontalieri attraverso bonifici bancari, che inevitabilmente comportano la creazione di flussi di dati personali[323].

322 Regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito, GU L 302 del 17.11.2009; Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio recante modifica del regolamento (CE) n. 1060/2009 relativo alle agenzie di rating del credito*, COM(2010) 289 definitivo, Bruxelles, 2 giugno 2010.

323 Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE, GU L 319 del 5.12.2007.

Approfondimenti

Capitolo 1

Araceli Mangas, M. (a cura di) (2008), *Carta de los derechos fundamentales de la Unión Europea* (La Carta dei diritti fondamentali dell'Unione europea), Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit* (Il diritto fondamentale alla protezione dei dati tra libertà e sicurezza), Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection* (Introduzione alla protezione dei dati), Bruxelles, disponibile all'indirizzo: http://www.edri.org/files/paper06_datap.pdf.

Frowein, J. e Peukert, W. (2009), *Europäische Menschenrechtskonvention* (La Convenzione europea dei diritti dell'uomo), Berlino, N. P. Engel Verlag.

Grabenwarter, C. e Pabel, K. (2012), *Europäische Menschenrechtskonvention* (La Convenzione europea dei diritti dell'uomo), Monaco, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. e Bates, E. (2009), *Law of the European Convention on Human Rights* (La giurisprudenza sulla Convenzione europea dei diritti dell'uomo), Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union* (La Carta dei diritti fondamentali dell'Unione europea), Monaco, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union* (La Carta dei diritti fondamentali dell'Unione europea), Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights* (Cause, documenti e commentari sulla Convenzione europea dei diritti dell'uomo), Oxford, Oxford University Press.

Nowak, M., Januszewski, K. e Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights* (I diritti umani per tutti. Manuale viennese sui diritti umani), Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. e Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme* (La Carta dei diritti fondamentali dell'Unione europea e la Convenzione europea dei diritti dell'uomo), Bruxelles, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?' ("La direttiva UE sulla tutela dei dati – situazione statica o dinamica?"), *Neue Juristische Wochenschrift*, n. 5, pagg. 281–288.

Warren, S. e Brandeis, L. (1890), 'The right to privacy' ("Il diritto alla vita privata"), *Harvard Law Review,* vol. 4, n. 5, pagg. 193–220, disponibile all'indirizzo: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Capitolo 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law* (La protezione dei dati: guida pratica al diritto del Regno Unito e dell'Unione europea), Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea* (Vita privata e protezione dei dati nell'Unione europea), Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel* (La protezione dei dati a carattere personale), Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht* (La protezione dei dati nel diritto europeo), Baden-Baden, Nomos.

Morgan, R. e Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance* (Strategia di protezione dei dati: attuazione delle norme in materia), Londra, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization' ("Le promesse non mantenute sulla vita privata: risposte al sorprendente fallimento dell'anonimizzazione"), *UCLA Law Review*, vol. 57, n. 6, pagg. 1701–1777.

Tinnefeld, M., Buchner, B. e Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht* (Introduzione al diritto alla protezione dei dati: la protezione dei dati e la libertà d'informazione in un'ottica europea), Monaco, Oldenbourg Wissenschaftsverlag.

Ufficio del commissario all'informazione del Regno Unito (2012), *Anonymisation: managing data protection risk. Code of practice* (Anonimizzazione: la gestione del rischio connesso alla protezione dei dati. Codice di buone prassi), disponibile all'indirizzo: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

Capitoli 3 - 5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' ("La direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati") in: Grabitz, E., Hilf, M. e Nettesheim, M. (a cura di), *Das Recht der Europäischen Union* (Il diritto dell'Unione europea), Band IV, A. 30, Monaco, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales* (La protezione dei dati personali), Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne* (La protezione dei dati personali nell'Unione europea), Saarbrücken, Éditions universitaires européennes.

Dammann, U. e Simitis, S. (1997), *EG-Datenschutzrichtlinie* (La direttiva UE sulla tutela dei dati), Baden-Baden, Nomos.

FRA (Agenzia dell'Unione europea per i diritti fondamentali) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)* [La protezione dei dati nell'Unione europea: il ruolo delle autorità di controllo nazionali (Rafforzare l'architettura dei diritti fondamentali nell'UE, seconda parte)], Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea (Ufficio pubblicazioni).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition) [Elaborazione di indicatori per la protezione, il rispetto e la promozione dei diritti del minore nell'Unione europea (edizione per conferenza)], Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities* (Accesso alla giustizia in Europa: una panoramica delle sfide e delle opportunità), Lussemburgo, Ufficio delle pubblicazioni.

Simitis, S. (2011), *Bundesdatenschutzgesetz* (Legge federale sulla protezione dei dati), Baden-Baden, Nomos.

Ufficio del commissario all'informazione del Regno Unito, *Privacy Impact Assessment* (Valutazione dell'impatto sulla vita privata), disponibile all'indirizzo: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment .

Capitolo 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. e Nouwt, S. (2009), *Reinventing data protection?* (Reinventare la protezione dei dati?), Berlino, Springer.

Kuner, C. (2007), *European data protection law* (Diritto europeo in materia di protezione dei dati), Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law* (Regolamentazione dei flussi transfrontalieri dei dati e legge sulla riservatezza dei dati), Oxford, Oxford University Press.

Capitolo 7

Europol (2012), *Data Protection at Europol* (La protezione dei dati presso Europol), Lussemburgo, Ufficio delle pubblicazioni, disponibile all'indirizzo : https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime* (La protezione dei dati presso Eurojust: un regime solido, efficace e ad hoc), l'Aia, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cyber crime* (La protezione dei dati presso Europol come risorsa nella lotta contro la criminalità informatica), ERA Forum, vol. 13, n. 3, pagg. 381–395.

Gutwirth, S., Poullet, Y. e De Hert, P. (2010), *Data protection in a profiled world* (La protezione dei dati in un mondo caratterizzato dalla profilazione), Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. e Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* (Computer, vita privata e protezione dei dati: una questione di scelta), Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, (Distruggere la democrazia per difenderla? La direttiva sulla conservazione dei dati, lo stato di sorveglianza e il nostro ecosistema costituzionale), *European Law Review*, vol. 36, n. 5, pagg. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon* (Il ruolo del Parlamento europeo nella conclusione degli accordi transatlantici sul trasferimento dei dati personali dopo Lisbona), Centre for the Law of External Relations, documenti di lavoro CLEER 2013/2, disponibile all'indirizzo: http://www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Capitolo 8

Büllesbach, A., Gijrath, S., Poullet, Y. e Hacon, R. (2010), *Concise European IT law* (Compendio sul diritto europeo in materia di tecnologie dell'informazione), Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. e Poullet, Y. (2012), *European data protection: In good health?* (La protezione dei dati in Europa: funziona?), Dordrecht, Springer.

Gutwirth, S., Poullet, Y. e De Hert, P. (2010), *Data protection in a profiled world* (La protezione dei dati in un mondo caratterizzato dalla profilazione), Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. e Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* (Computer, vita privata e protezione dei dati: una questione di scelta), Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem (Distruggere la democrazia per difenderla? La direttiva sulla conservazione dei dati, lo stato di sorveglianza e il nostro ecosistema costituzionale), *European Law Review*, vol. 36, n. 5, pagg. 722–776.

Rosemary, J. e Hamilton, A. (2012), *Data protection law and practice* (La protezione dei dati: diritto e prassi), Londra, Sweet & Maxwell.

Giurisprudenza

Selezione della giurisprudenza della Corte europea dei diritti dell'uomo

Accesso ai dati personali

Gaskin c. Regno Unito, n. 10454/83, 7 luglio 1989
Godelli c. Italia, n. 33783/09, 25 settembre 2012
K.H. e a. c. Slovacchia, n. 32881/04, 28 aprile 2009
Leander c. Svezia, n. 9248/81, 26 marzo 1987
Odièvre c. Francia [GC], n. 42326/98, 13 febbraio 2003

Equilibrio tra protezione dei dati e libertà di espressione

Axel Springer AG c. Germania [GC], n. 39954/08, 7 febbraio 2012
Von Hannover c. Germania, n. 59320/00, 24 giugno 2004
Von Hannover c. Germania (n. 2) [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012

Sfide della protezione dei dati online

K.U. c. Finlandia, n. 2872/02, 2 dicembre 2008

Corrispondenza

Amann c. Svizzera [GC], n. 27798/95, 16 febbraio 2000
Bernh Larsen Holding AS e a. c. Norvegia, n. 24117/08, 14 marzo 2013
Cemalettin Canli c. Turchia, n. 22427/04, 18 novembre 2008

Dalea c. Francia, n. 964/07, 2 febbraio 2010
Gaskin c. Regno Unito, n. 10454/83, 7 luglio 1989
Haralambie c. Romania, n. 21737/03, 27 ottobre 2009
Khelili c. Svizzera, n. 16188/07, 18 ottobre 2011
Leander c. Svezia, n. 9248/81, 26 marzo 1987
Malone c. Regno Unito, n. 8691/79, 2 agosto 1984
McMichael c. Regno Unito, n. 16424/90, 24 febbraio 1995
M.G. c. Regno Unito, n. 39393/98, 24 settembre 2002
Rotaru c. Romania [GC], n. 28341/95, 4 maggio 2000
S. e Marper c. Regno Unito, nn. 30562/04 e 30566/04, 4 dicembre 2008
Shimovolos c. Russia, n. 30194/09, 21 giugno 2011
Turek c. Slovacchia, n. 57986/00, 14 febbraio 2006

Banche dati dei casellari giudiziari

B.B. c. Francia, n. 5335/06, 17 dicembre 2009
M.M. c. Regno Unito, n. 24029/07, 13 novembre 2012

Banche dati sul DNA

S. e Marper c. Regno Unito, nn. 30562/04 e 30566/04, 4 dicembre 2008

Dati GPS

Uzun c. Germania, n. 35623/05, 2 settembre 2010

Dati sanitari

Biriuk c. Lituania, n. 36909/02, 25 novembre 2008
I. c. Finlandia, n. 20511/03, 17 luglio 2008
L.L. c. Francia, n. 7508/02, 10 ottobre 2006
M.S. c. Svezia, n. 20837/92, 27 agosto 1997
Szuluk c. Regno Unito, n. 36936/05, 2 giugno 2009
Z. c. Finlandia, n. 22009/93, 25 febbraio 1997

Identità

Ciubotaru c. Moldova, n. 27138/04, 27 aprile 2010
Godelli c. Italia, n. 33783/09, 25 settembre 2012
Odièvre c. Francia [GC], n. 42326/98, 13 febbraio 2003

Informazioni sulle attività professionali

Michaud c. Francia, n. 12323/11, 6 dicembre 2012
Niemietz c. Germania, n. 13710/88, 16 dicembre 1992

Intercettazione delle comunicazioni

Amann c. Svizzera [GC], n. 27798/95, 16 febbraio 2000
Copland c. Regno Unito, n. 62617/00, 3 aprile 2007
Cotlet c. Romania, n. 38565/97, 3 giugno 2003
Kruslin c. Francia, n. 11801/85, 24 aprile 1990
Lambert c. Francia, n. 23618/94, 24 agosto 1998
Liberty e a. c. Regno Unito, n. 58243/00, 1 luglio 2008
Malone c. Regno Unito, n. 8691/79, 2 agosto 1984
Halford c. Regno Unito, n. 20605/92, 25 giugno 1997
Szuluk c. Regno Unito, n. 36936/05, 2 giugno 2009

Obblighi per i soggetti interessati

B.B. c. Francia, n. 5335/06, 17 dicembre 2009
I. c. Finlandia, n. 20511/03, 17 luglio 2008
Mosley c. Regno Unito, n. 48009/08, 10 maggio 2011

Fotografie

Sciacca c. Italia, n. 50774/99, 11 gennaio 2005
Von Hannover c. Germania, n. 59320/00, 24 giugno 2004

Diritto all'oblio

Segerstedt-Wiberg e a. c. Svezia, n. 62332/00, 6 giugno 2006

Diritto di opposizione

Leander c. Svezia, n. 9248/81, 26 marzo 1987
Mosley c. Regno Unito, n. 48009/08, 10 maggio 2011
M.S. c. Svezia, n. 20837, 27 agosto 1997
Rotaru c. Romania [GC], n. 28341/95, 4 maggio 2000

Categorie di dati sensibili

I. c. Finlandia, n. 20511/03, 17 luglio 2008
Michaud c. Francia, n. 12323/11, 6 dicembre 2012
S. e Marper c. Regno Unito, nn. 30562/04 e 30566/04, 4 dicembre 2008

Sorveglianza e attuazione (ruolo dei diversi attori comprese le autorità di controllo)

I. c. Finlandia, n. 20511/03, 17 luglio 2008
K.U. c. Finlandia, n. 2872/02, 2 dicembre 2008
Von Hannover c. Germania, n. 59320/00, 24 giugno 2004
Von Hannover c. Germania (n. 2) [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012

Metodi di sorveglianza

Allan c. Regno Unito, n. 48539/99, 5 novembre 2002
Associazione "21 Décembre 1989" e a. c. Romania, nn. 33810/07 e 18817/08, 24 maggio 2011
Bykov c. Russia [GC], n. 4378/02, 10 marzo 2009
Kennedy c. Regno Unito, n. 26839/05, 18 maggio 2010
Klass e a. c. Germania, n. 5029/71, 6 settembre 1978
Rotaru c. Romania [GC], n. 28341/95, 4 maggio 2000
Taylor-Sabori c. Regno Unito, n. 47114/99, 22 ottobre 2002
Uzun c. Germania, n. 35623/05, 2 settembre 2010
Vetter c. Francia, n. 59842/00, 31 maggio 2005

Videosorveglianza

Köpke c. Germania, n. 420/07, 5 ottobre 2010
Peck c. Regno Unito, n. 44647/98, 28 gennaio 2003

Campionatura di voci

P.G. e J.H. c. Regno Unito, n. 44787/98, 25 settembre 2001
Wisse c. Francia, n. 71611/01, 20 dicembre 2005

Selezione della giurisprudenza della Corte di giustizia dell'Unione europea

Giurisprudenza concernente la direttiva sulla tutela dei dati

C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*, 16 dicembre 2008
[Concetto di "attività giornalistiche" ai sensi dell'articolo 9 della direttiva sulla tutela dei dati]

Cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010
[Proporzionalità dell'obbligo legale di pubblicare dati personali relativi ai beneficiari di determinati fondi agricoli dell'UE]

C-101/01, *Bodil Lindqvist*, 6 novembre 2003
[Legittimità della pubblicazione di dati su Internet da parte di un privato sulla vita privata altrui]

C-131/12, *Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja González*, domanda di pronuncia pregiudiziale proposta dall'*Audiencia Nacional* (Spagna) il 9 marzo 2012, 25 maggio 2012, pendente
[Obblighi dei fornitori di motori di ricerca di astenersi, su richiesta dell'interessato, dal mostrare dati personali nei risultati di ricerca]

C-270/11, *Commissione europea c. Regno di Svezia*, 30 maggio 2013
[Imposizione di una sanzione per mancata attuazione di una direttiva]

C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 gennaio 2008
[Obbligo dei fornitori di accesso Internet di divulgare l'identità degli utilizzatori di programmi di scambio di archivi denominati KaZaA alle associazioni per la tutela della proprietà intellettuale]

C-288/12, *Commissione europea c. Ungheria*, 8 aprile 2014
[Legittimità della rimozione dall'incarico del commissario nazionale delegato per la protezione dei dati]

C-291/12, *Michael Schwarz c. Stadt Bochum*, conclusioni dell'avvocato generale, 13 giugno 2013
[Violazione del diritto primario dell'UE da parte del regolamento (CE) n. 2252/2004 che prevede la memorizzazione delle impronte digitali nel passaporto]

C-360/10, *SABAM c. Netlog N.V.*, 16 febbraio 2012
[Obbligo dei fornitori di reti sociali di prevenire l'uso illecito di opere musicali e audiovisive da parte degli utenti di tali reti]

Cause riunite C-465/00, C-138/01 e C-139/01, *Rechnungshof c. Österreichischer Rundfunk e a. e Neukomm e Lauermann c. Österreichischer Rundfunk*, 20 maggio 2003
[Proporzionalità dell'obbligo legale di pubblicare dati personali concernenti la retribuzione dei dipendenti di determinate categorie di enti pubblici]

Cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011
[Corretta attuazione dell'articolo 7, lettera f), della direttiva sulla tutela dei dati – "legittimi interessi altrui" – nel diritto nazionale]

C-518/07, *Commissione europea c. Repubblica federale di Germania*, 9 marzo 2010
[Indipendenza di un'autorità di controllo nazionale]

C-524/06, *Huber c. Bundesrepublik Deutschland*, 16 dicembre 2008
[Legittimità della ritenzione di dati relativi a stranieri in un registro statistico]

C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, 5 maggio 2011
[Necessità di un rinnovo del consenso]

C-553/07, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, 7 maggio 2009
[Diritto di accesso dell'interessato]

CGUE, cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e a.*, 8 aprile 2014
[Violazione del diritto primario dell'UE da parte della direttiva sulla conservazione dei dati]

C-614/10, *Commissione europea c. Repubblica d'Austria*, 16 ottobre 2012
[Indipendenza di un'autorità di controllo nazionale]

Giurisprudenza concernente il regolamento sulla protezione dei dati da parte delle istituzioni dell'UE

C-28/08 P, *Commissione europea c. The Bavarian Lager Co. Ltd.*, 29 giugno 2010
[Accesso ai documenti]

C-41/00 P, *Interporc Im- und Export GmbH c. Commissione delle Comunità europee*, 6 marzo 2003
[Accesso ai documenti]

F-35/10 P, *Dimitrios Pachtitis c. Commissione europea ed EPSO*, 15 giugno 2010
[Uso dei dati personali nell'ambito del lavoro dipendente presso le istituzioni dell'UE]

F-46/09, *V c. Parlamento europeo*, 5 luglio 2011
[Uso dei dati personali nell'ambito del lavoro dipendente presso le istituzioni dell'UE]

Elenco della giurisprudenza

Giuriprudenza della Corte di giustizia dell'Unione europea

Giuriprudenza della Corte europea dei diritti dell'uomo

Giuriprudenza dei tribunal nazionali

Agenzia dell'Unione europea per i diritti fondamentali
Corte europea dei diritti dell'uomo – Consiglio d'Europa

Manuale sul diritto europeo in materia di protezione dei dati

2014 — 211 p. — 14,8 × 21 cm

ISBN 978-92-871-9951-5 (CdE)
ISBN 978-92-9239-335-9 (FRA)
doi:10.2811/54588

Numerose informazioni sull'Agenzia dell'Unione europea per i diritti fondamentali sono disponibili su Internet. È possibile accedervi attraverso il sito Internet della FRA (fra.europa.eu).

Ulteriori informazioni sul Consiglio d'Europa sono disponibili sul sito hub.coe.int.

Ulteriori informazioni sulla Corte europea dei diritti dell'uomo sono disponibili sul sito web della Corte: echr.coe.int. Il portale di ricerca HUDOC consente di accedere alle sentenze e decisioni in inglese e/o francese, le traduzioni in altre lingue, riassunti, comunicati stampa e altre informazioni sul lavoro della Corte.

10.2811/54588 TK-01-13-772-IT-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Il rapido sviluppo delle tecnologie dell'informazione e della comunicazione (TIC) rileva il crescente bisogno di una solida protezione dei dati personali – un diritto sancito sia dagli strumenti dell'Unione europea (UE) sia dagli atti giuridici del Consiglio d'Europa (CDE). I progressi tecnologici ampliano, per esempio, le frontiere del controllo, dell'intercettazione delle comunicazioni e dell'archiviazione dei dati, che pongono sfide significative al diritto alla protezione dei dati. Il presente manuale mira ad accrescere le conoscenze dei professionisti del settore legale non specializzati nel settore della protezione dei dati relativamente a quest'area del diritto, presentando una panoramica dei quadri giuridici applicabili dell'Unione europea e del Consiglio d'Europa. Il manuale illustra la giurisprudenza fondamentale sintetizzando le sentenze cardine della Corte europea dei diritti dell'uomo (Corte EDU) e della Corte di giustizia dell'Unione europea (CGUE); in assenza di una siffatta giurisprudenza, contiene esempi pratici connessi a casi ipotetici. In sintesi, il presente manuale contribuisce a garantire un vigoroso e determinato rispetto del diritto alla protezione dei dati.

AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI
Schwarzenbergplatz 11 – 1040 Vienna - Austria
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

CONSIGLIO D'EUROPA
CORTE EUROPEA DEI DIRITTI DELL'UOMO
67075 Strasburgo Cedex - Francia
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Ufficio delle pubblicazioni
ISBN 978-92-871-9951-5 (CDE)
ISBN 978-92-9239-335-9 (FRA)
ISBN 978-92-9239-335-9
9 789292 393359