Diritto, Economia e Tecnologie della Privacy

Anno VI, Numero 3, 2015

Istituto Italiano Privacy

Diritto, Economia e Tecnologie della Privacy

Rivista quadrimestrale dell'Istituto Italiano per la Privacy e la valorizzazione dei dati

Diritto, Economia e Tecnologie della Privacy

Anno VI, n. 3, 2015
Registrazione al Tribunale di Arezzo n. 1P/10RS del 26 ottobre 2010
Rivista quadrimestrale

Provider: Aruba S.p.A., P.zza Garibaldi 8 – 52010 Soci (AR). Autorizzazione Ministero delle Comunicazioni n. 473. Server collocati in Via Sergio Ramelli, 8 – 52100 Arezzo (AR).
Stampa: Daniele Mosera, via Giulio Pittarelli, 23, 00166, Roma.

Segreteria di redazione:
e-mail: rivista@istitutoprivacy.it

Direzione e redazione: Piazza di San Salvatore in Lauro, 13, 00186, Roma; Direttore responsabile: Giovanni Crea

Proprietà della rivista: Istituto Italiano per la Privacy e la valorizzazione dei dati. Consiglio di Amministrazione dell'Istituto Italiano per la Privacy e la valorizzazione dei dati: Luca Bolognini – Presidente; Diego Fulco – Direttore; Pietro Paganini – Segretario Generale.

Editore: Istituto Italiano per la Privacy e la valorizzazione dei dati, Piazza di San Salvatore in Lauro, 13, 00186, Roma
www.istitutoitalianoprivacy.it
info@istitutoitalianoprivacy.org
tel.: +39 06 97842491
fax: +39 06 23328983

Condizioni economiche

- singolo numero: € 25,00
- abbonamento annuale (tre numeri): € 70,00 (L'abbonamento decorre dal mese di gennaio di ciascun anno. La sottoscrizione dell'abbonamento nel corso dell'anno dà diritto a ricevere i numeri arretrati). Il pagamento può essere effettuato mediante versamento bancario sul conto intestato a Istituto Italiano per la Privacy e la valorizzazione dei dati – IBAN – IT55V0310450120000000821176 (Deutsche Bank)

INDICE

Editoriale

Nuove prospettive del trattamento dei contenuti nel quadro della *data economy*

GIOVANNI CREA

Con la diffusione delle ICT, la produzione di contenuti rappresentativi di realtà ed esperienze è divenuta un'attività costante dell'uomo che, nel tempo, si è estesa alle macchine e, da ultimo, agli elementi dell'ambiente (*things*). Le logiche della *data economy* hanno altresì evidenziato come il trattamento dei suddetti contenuti sia divenuto una funzione pressoché inevitabile in relazione alla capacità di determinare delle «utilità»[1]; sotto questo aspetto, gli addetti ai lavori, ricorrendo a un parallelismo con il petrolio – *data is the new oil of the digital economy*[2] – hanno osservato come i *big data*, alla stregua di questa risorsa, a poco servono se non vengono 'raffinati'. Un tale processo appare poi indispensabile in un'economia postfordista, dal profilo sempre più digitale, in cui le imprese, secondo i casi, perseguono scopi di sopravvivenza ovvero di espansione (anche fino a raggiungere un potere di mercato). La *data economy* – e, più in generale, l'economia digitale – ha radici in quella "nuova economia" che, a partire dall'esperienza della fornitura dei primi servizi internet – si pensi all'accesso a internet, al servizio di *hosting*, alla corrispondenza elettronica – si è poi evoluta con l'affermazione di piattaforme di intermediazione di cui i servizi di ricerca in rete, i *social media* e i siti che facilitano scambi e condivisione sono tra gli esempi più noti. Questi stessi esempi descrivono un modello aziendale il cui valore è derivato dal trattamento di contenuti informativi e conoscitivi, e può essere impiegato sia per la creazione di servizi

[1] Il trattamento dei contenuti è praticamente inevitabile dal momento della generazione degli stessi, specie se lo si riconduce a quell'ampia accezione fornita dalla disciplina del trattamento dei dati personali.

[2] È il titolo di un articolo apparso sulla rivista Wired nel luglio 2014 e reperibile all'indirizzo http://www.wired.com/2014/07/data-new-oil-digital-economy/

innovativi (ad esempio, "Sreet view" di Google) sia per la misurazione di fenomeni sociali[3] sia, ancora, come leva di scambio sui versanti pubblicitari[4] (una piattaforma *social* verosimilmente cercherebbe di sfruttare il profilo dei propri utenti per scopi di raccolta pubblicitaria).

L'economia digitale sta attraversando una fase caratterizzata da questioni e sfide di notevole portata legate all'avvento delle piattaforme in internet, la cui natura 'multiversante' e transfrontaliera implica una più complessa strutturazione della filiera di generazione del valore. In relazione a tale complessità, la regolamentazione dei processi di trattamento è tutt'altro che scontata; condizione, questa, che non esclude nuove riflessioni sul bilanciamento tra la necessità del trattamento dei contenuti da un lato – nella misura in cui esso si riconduce a un'iniziativa economica e al suo contributo alla crescita dell'economia digitale – e, dall'altro, i diritti individuali e gli obiettivi di interesse generale sui quali il trattamento medesimo può avere effetto. Sappiamo, al riguardo, che le piattaforme in rete sono sottoposte alle norme dell'UE che ne disciplinano i comportamenti – tra i quali il trattamento dei contenuti è un esempio rilevante – con riferimento ai profili della concorrenza, dei diritti dei consumatori, della protezione dei dati, dei diritti di proprietà, della responsabilità extracontrattuale. Ma non va nemmeno sottaciuto come nell'economia digitale trovino applicazione teorie, paradigmi e istanze – la "coda

[3] Cfr. F. GIANNOTTI, *Big data e social mining. I dati, a saperli ascoltare, raccontano storie*, in AA.VV., *Misurare l'innovazione digitale. Gli indicatori di successo delle politiche di innovazione territoriale Venezia*, Ed. Cà Foscari, 2015, 49-61. L'autore richiama un noto studio che ha dimostrato come, nel caso dei motori di ricerca, l'ipotesi di correlazione tra le interrogazioni riguardanti il fenomeno dell'influenza e il numero di individui che hanno effettivamente avuto sintomi influenzali, si sia rivelata utile per prevedere, nel breve periodo, l'incidenza di tale fenomeno. In tal modo, gli operatori sanitari possono fronteggiare con maggiore efficacia le epidemie stagionali.

[4] Cfr. E. PEDEMONTE, *Google, Facebook, i nuovi monopoli e gli ideologi della Silicon Valley*, in *Scientific journal on digital cultures*, vol 1, n. 2, 2016, 27-34. A. PASSONI, *Economia delle piattaforme e architettura digitale delle scelte. Appunti sull'alternativa cooperativa*, reperibile all'indirizzo http://archiviomarini.sp.unipi.it/688/

lunga"[5] (legge di Pareto), le utilizzazioni libere, l'*open access* – che stanno influenzando i concetti di privacy e proprietà (intellettuale e industriale). Così come il modello della condivisione (*sharing*), oltre a prefigurare un allentamento dei regimi di protezione della conoscenza – con l'adozione di sistemi di *commons*, se non di *open* access – per ricreare condizioni di apertura, sta modificando i ruoli della domanda e dell'offerta; sotto quest'ultimo aspetto vanno segnalate le esperienze di collaborazione tra imprese e consumatori nella progettazione di nuovi prodotti, ma anche la tendenza dei consumatori (tradizionalmente riconosciuti come parte debole) a svolgere, sia pure occasionalmente, la funzione di prestazione di servizi avvalendosi di piattaforme in rete. Scenari, questi, che delineano un rafforzamento della posizione dei consumatori (*empowerment*) anche sul piano del controllo del trattamento dei contenuti che li riguardano.

D'altro canto, va osservato che le pratiche che stanno emergendo da questi e altri mutamenti non sono facilmente collocabili nelle tradizionali categorie giuridiche. Un punto, questo, che introduce questioni legate sia all'applicazione effettiva delle norme, di cui la Commissione europea non fa mistero[6], sia al controllo dei contenuti da parte dei titolari, e che forse richiede un ripensamento sugli schemi normativi più adeguati per regolare i nuovi modelli di produzione; il che, in altre parole, significa valutare la prospettiva di un'architettura normativa che non costituisca una barriera predefinita alla circolazione delle conoscenze, e che tuttavia possa garantire a

[5] L'espressione "coda lunga" (*long tail*), adottata da Chris Anderson, giornalista e direttore di *Wired USA* dal 2001 al 2012, si ispira a un modello statistico, noto come "legge di Pareto", in cui la gran parte di una popolazione si distribuisce in un numero elevato di classi (o segmenti), sicché ogni classe ha una numerosità bassa. In economia, la *long tail* descrive, tra gli altri fenomeni, anche quello della frammentazione della domanda che ha segnato il passaggio dall'economia di massa, caratteristica del periodo 'fordista', a un'economia fondata sulla differenziazione del prodotto. Dal lato della produzione, il predetto fenomeno implica la capacità dei processi produttivi di realizzare una varietà di modelli, ciascuno destinato alle necessità di pochi consumatori. L'integrazione delle ICT nei processi produttivi ha introdotto elementi di flessibilità nella direzione di una maggiore differenziazione.

[6] Questione che emerge in COMMISSIONE EUROPEA, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, comunicazione com(2016) 288, 25 maggio 2016.

proprietari e interessati strumenti tecnici (oltre che diritti) attraverso i quali proteggere, nei limiti stabiliti dalle stesse norme, i contenuti che li riguardano da trattamenti non autorizzati ovvero controllare i processi di trattamento a cui detti contenuti possono essere sottoposti. Un tale approccio riposa su principi di autodeterminazione – la libertà dei proprietari di stabilire se e in che misura condividere i propri contenuti – e di "*protection by design*"[7] derivato dall'analogo principio adottato nell'ambito della disciplina del trattamento dei dati personali. Quest'ultimo profilo, trasposto sul piano digitale, rimanda al concetto del "codice informatico" di Lessig che il giurista statunitense ha introdotto per indicare il trasferimento nel software delle regole di protezione (*code as law*), e di cui non mancano esempi in tal senso; dalle tecnologie di tipo *Digital Rights Management*, impiegate per la protezione di contenuti digitali coperti da un diritto di proprietà, alle *privacy enhancing technologies*, che, seguendo l'approccio *privacy by design*, sono progettate per inibire *ex ante* il *tracking* occulto dei dati personali e, più in generale, per impedire trattamenti illegittimi, alle tecnologie di protezione delle banche dati[8].

E, anzi, a ben vedere, nell'ecosistema digitale il *code* è una misura tecnica che abilita la facoltà di autodeterminazione dei titolari dei contenuti, e che, in tal modo, va oltre quel meccanismo giuridico fondato sull'autorizzazione preventiva (*opt in*) che, in particolare sul fronte della privacy, ha sempre rappresentato una pietra miliare della disciplina europea.

[7] Nella sua forma generale questo principio può essere esplicitato con riguardo all'adozione di misure tecniche (software) progettate per proteggere i contenuti da trattamenti non autorizzati ovvero per svolgere trattamenti conformi alle regole.

[8] Sul punto, sia consentito un rinvio a G. CREA, *la protezione dei minori in rete nelle prospettive dell'analisi del comportamento e della tutela tecnologica*, in *Diritto ed economia dei mezzi di comunicazione*, n. 3, 2011, 51-71.

Contributi

I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro

Marianna Quaranta*

SOMMARIO: 1. Premesse. – 2. Il dato biometrico ed i sistemi biometrici. – 3. Il trattamento e l'archiviazione del dato biometrico nel documento di lavoro europeo. – 4. La normativa di riferimento e le prescrizioni del Garante. – 5. L'uso della tecnologia RFID. – 6. La notificazione del trattamento e la verifica preliminare. – 7. Le linee guida del Garante e considerazioni conclusive

1. Premesse.

Il rapido sviluppo delle tecnologie biometriche negli ultimi anni e l'estensione della loro applicazione ne ha reso necessaria un'attenta analisi sotto l'aspetto della tutela dei dati personali. L'uso generalizzato e incontrollato della biometria, infatti, ha da sempre sollevato preoccupazioni in relazione alla tutela dei diritti e delle libertà fondamentali degli individui, in quanto si tratta di dati "particolari" che riguardano le caratteristiche comportamentali e fisiologiche di un individuo e sono tali da consentirne l'identificazione univoca.

Attualmente, si ricorre al trattamento di dati biometrici nelle procedure automatizzate di autenticazione/verifica e di identificazione per il controllo dell'accesso ad aree, tanto fisiche quanto virtuali, che per peculiarità proprie risultano particolarmente sensibili[1].

---

* Avvocato del foro di Napoli specializzato in diritto societario e *data protection*. Membro della commissione Privacy e Security del Consiglio dell'Ordine degli Avvocati di Napoli.

[1] Le implicazioni e i problemi derivanti dall'utilizzo delle tecniche biometriche in rapporto ai diritti dell'individuo sono state dibattute in diverse sedi tra quelle di maggior rilievo si citano: per l'Unione europea il Working party art. 29;

2. Il dato biometrico ed i sistemi biometrici.

Per quel che concerne l'UE, il Gruppo di lavoro dei garanti europei Working party art. 29 ha adottato il 1° agosto 2003 il "documento di lavoro sulla biometria" (doc. n. 12168/02/it wp80) in cui, venivano formulate delle raccomandazioni in forma di linee-guida per l'industria e gli utenti, allo scopo di contribuire ad un'omogenea ed efficace applicazione delle norme nazionali rispetto alla direttiva 46/95/CE in materia di sistemi biometrici. In mancanza di una definizione univoca, è condivisibile quella espressa dal Gruppo dei garanti europei nel documento del 1 agosto 2003 succitato dove si chiarisce che "*i dati biometrici possono sempre essere considerati come informazioni concernenti una persona fisica in quanto sono dati che, per la loro stessa natura, forniscono indicazioni su una determinata persona*". Per sistemi biometrici si intendono le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo. Si possono distinguere due categorie principali di tecniche biometriche a seconda che vengano utilizzati dati stabili o dati comportamentali dinamici.

Esistono, in primo luogo, tecniche di tipo fisico e fisiologico che misurano le caratteristiche fisiologiche di una persona. Esse comprendono: la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA7, l'analisi dei pori della pelle ecc.

In secondo luogo, esistono tecniche di tipo comportamentale che misurano il comportamento di una persona. Esse comprendono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura ecc. La raccolta di campioni biometrici, i cosiddetti dati biometrici (ad esempio, l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione della

l'OCSE/OECD (Organisation for economic co-operation and development); l'ICAO (International Civil Aviation Organization).

voce), viene effettuata nel corso della cosiddetta fase di "iscrizione"/o *enrollment*, utilizzando un sensore specifico per ogni tipo di elemento biometrico. Il sistema biometrico estrae dai dati biometrici i tratti specifici dell'utilizzatore necessari per elaborare un "modello" biometrico.

Il modello o anche t*emplate* è una riduzione strutturata di un'immagine biometrica, ossia la misura biometrica registrata di un individuo. Tale modello, presentato in forma digitale, viene trattato ed archiviato e non l'elemento biometrico in se stesso.

3. Il trattamento e l'archiviazione del dato biometrico nel documento di lavoro europeo.

Nell'ambito dell'identificazione biometrica, la persona è generalmente identificabile in quanto i dati biometrici sono utilizzati per l'identificazione o l'autenticazione/verifica non solo per distinguere la persona interessata da tutte le altre, ma anche per l'identificazione specifica. In linea generale, si riconosce il rischio che dati biometrici ottenuti da tracce fisiche lasciate da un individuo a sua insaputa (come ad esempio, le impronte digitali) siano riutilizzati per finalità incompatibili, è relativamente inferiore se i dati, invece di essere memorizzati in basi di dati centralizzate, restano con la persona stessa senza essere accessibili a terzi. Sul punto, il Gruppo di lavoro europeo ha inteso sottolineare come i dati biometrici debbano essere trattati e soprattutto rilevati in modo leale. A tal fine, il responsabile del trattamento deve informare correttamente la persona interessata: in particolare, deve essere resa la definizione esatta della finalità del trattamento e l'identità del responsabile (che spesso coinciderà con la persona che gestisce il sistema biometrico o che applica la tecnica biometrica). Poiché l'archiviazione centralizzata dei dati biometrici aumenta il rischio che tali dati vengano utilizzati come chiave per collegare basi di dati distinte ed ottenere così profili dettagliati delle abitudini della persona interessata, come meglio si chiarirà nel prosieguo, essa è stata esclusa dal Garante con diversi provvedimenti tanto nel settore pubblico quanto in quello privato.

La questione della finalità compatibile solleva, inoltre, il problema dell'interoperabilità di sistemi diversi che utilizzano la biometria. La normalizzazione necessaria per conseguire l'interoperabilità potrebbe favorire una maggiore interconnessione fra le basi di dati. Alcuni sistemi biometrici quali il riconoscimento a distanza del volto, la rilevazione delle impronte digitali, la registrazione della voce presentano maggiori rischi da questo punto di vista. Pertanto, diventa cruciale la predisposizione di idonee misure di sicurezza.

Sul punto, conformemente all'articolo 17 della direttiva 95/46/CE il responsabile del trattamento deve attuare le misure tecniche ed organizzative appropriate in tema di sicurezza al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla 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. Le misure di sicurezza vanno adottate quando i dati biometrici sono sottoposti a trattamento (archiviazione, trasmissione, estrazione delle caratteristiche e confronto ecc.) ed in particolare, se il responsabile del trattamento trasmette tali dati via internet. Le misure di sicurezza possono prevedere, ad esempio, la cifratura dei modelli e la protezione delle chiavi di cifratura oltre al controllo ed alla protezione dell'accesso, rendendo così virtualmente impossibile la ricostruzione dei dati originali a partire dai modelli.

4. La normativa di riferimento e le prescrizioni del Garante.

L'elemento biometrico, inteso come aspetto della identità fisica dell'uomo, non trova esplicita tutela se non con riferimento ai parametri costituzionali della salute e dell'integrità fisica e nel divieto di trattamenti sanitari obbligatori (art. 32 Cost.).

Specifici richiami si rinvengono nel Codice della privacy che disciplina il trattamento di dati biometrici con un regime di maggiore severità rispetto al trattamento di meri dati personali. Nel caso in cui il dato biometrico che si intende trattare non abbia carattere di dato sensibile, trova, infatti, applicazione l'art. 17 del Codice relativo ai trattamenti che presentano rischi specifici per i diritti e le libertà

fondamentali e per la dignità dell'interessato e pertanto, salvo quanto si dirà al punto 6, è d'obbligo procedere alla verifica preliminare per verificare il rispetto dei principi di necessità, liceità, finalità e pertinenza. Deve, quindi, essere valutata la liceità del sistema, unitamente ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice). L'utilizzo di dati biometrici risulta infatti, giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati. Il trattamento poi risulta lecito e proporzionato[2], sempreché siano adottati gli accorgimenti e le misure di sicurezza idonee a preservare il tipo di trattamento effettuato quali la memorizzazione del modello su una *smart card* destinata a restare nell'esclusiva disponibilità dell'interessato.

Rispetto alla liceità del trattamento, il titolare deve rilasciare sempre un'informativa agli interessati, conformemente all'articolo 13 del Codice. Inoltre, per i soggetti privati, è necessario acquisire il consenso del singolo interessato, che deve essere "specifico" e "libero". Il consenso, infatti, è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto e se sono state rese all'interessato tutte le informazioni previste all'articolo 13 del Codice.

Il titolare del trattamento dovrà somministrare un'informativa scritta completa degli elementi previsti dal Codice; inoltre, nella informativa si dovrà indicare un sistema alternativo di identificazione che deve essere chiaramente evidenziato. Tutti i trattamenti debbono essere eseguiti con adeguate misure di sicurezza in tutto il processo biometrico, dalla fase di *enrollment*, alla fase di esercizio. Nel caso di dati biometrici che abbiano qualità di dati sensibili o giudiziari si incorre, inoltre, negli obblighi di adozione di misure ulteriori di protezione, che prevedono anche l'uso di tecniche crittografiche qualora si tratti di dati genetici. I dati personali necessari per realizzare

[2] Ad esempio con il provvedimento n. 38 del 31 gennaio 2013, il Garante ha bocciato ritenendo sproporzionato e, quindi, inammissibile il sistema di trattamento di dati personali la richiesta del Comune di Boscoreale manifestava l'intenzione di "utilizzare la tecnologia relativa alla rilevazione dell'impronta digitale per il controllo delle presenze del personale" al fine di "evitare il ripetersi di fenomeni di abusi derivanti da un uso improprio del tesserino magnetico".

il modello possono essere trattati esclusivamente durante la fase di raccolta, mentre quelli memorizzati debbono essere accessibili solo al personale preposto nel rispetto delle misure di sicurezza.

Con riferimento alle modalità di archiviazione delle informazioni adottate si è detto che la memorizzazione dei *template* – peraltro, protetti da sistemi di crittografia e cifratura dei dati – avviene sulle sole *smart card* poste nell'esclusiva disponibilità degli interessati. Mentre per quel che riguarda la conservazione dei dati relativi ovvero (gli accessi effettuati con l'uso del sistema di rilevazione di tipo biometrico) alla card è associato un numero di serie che consente solo indirettamente di risalire all'anagrafica dell'interessato, ovvero, ai suoi dati identificativi. La conservazione (del dato) del passaggio della sequenza numerica che identifica la card (assolutamente non riconducibile al *template* dell'impronta) potrebbe aversi per un periodo non superiore a 7 giorni e poi verrebbe cancellata dal sistema automaticamente con la sovrascrittura.

Gli ulteriori dati personali (non biometrici) relativi alle operazioni di verifica per l'accesso degli utenti/clienti, salvo il rispetto di specifiche disposizioni normative eventualmente applicabili, vengono già conservati per il periodo di tempo strettamente necessario al perseguimento degli scopi per i quali i medesimi dati sono stati raccolti e successivamente trattati (di solito per la durata del rapporto contrattuale in essere).

5. L'uso della tecnologia RFID.

Per quanto concerne l'utilizzo della tecnologia RFID essa è ammessa, se dal confronto tra le prescrizioni di legge (Raccomandazione della Commissione europea del 12 maggio 2009 e Quadro per la valutazione dell'impatto delle applicazioni RFID sulla protezione della vita privata e dei dati) e quanto relazionato dal fornitore del sistema, non emergono rischi evidenti per i dati personali, né per la salute degli utenti. Difatti, da un lato, le modalità d'uso della tessera non debbano divergere da quelle delle tradizionali smart card, dall'altro la ridotta distanza operativa di lettura (5 cm) attraverso canali cifrati di comunicazione deve risultare in grado di

impedire l'acquisizione (anche inconsapevole) dei dati contenuti nella tessera da parte di soggetti estranei al trattamento. La smart card, poi lo si ribadisce, deve poter essere letta solo dai lettori presenti nel sistema da implementare presso la struttura.

Per quanto concerne, poi, la riconoscibilità della card rilasciata agli utenti essa deve essere priva di indicazioni immediatamente riferibili agli stessi, essendo, a tal fine, attribuito solo un codice individuale a ciascun interessato, anche nell'ottica della prevenzione di eventuali utilizzi impropri dei dati biometrici contenuti nelle tessere eventualmente smarrite o sottratte. In ogni caso, nell'ipotesi di smarrimento o furto, le card devono essere immediatamente disattivate, adottando tutte le idonee misure affinché vengano immediatamente inibite tutte le funzioni connesse all'uso della tessera elettronica, fornendo in pari tempo agli interessati adeguate istruzioni sulla corretta custodia della tessera e sugli adempimenti connessi ad un'eventuale perdita di disponibilità di quest'ultima.

6. La notificazione del trattamento e la verifica preliminare.

Il trattamento dei dati biometrici ai sensi dell'art. 37 del Codice, comma 1, lett. a) va notificato secondo la procedura informatizzata prevista e l'iscrizione negli appositi registri. Per valutare la correttezza del trattamento biometrico effettuato, uno step necessario era costituito dalla cosiddetta verifica preliminare di cui all'art. 17 del Codice.

Recentemente, il Garante, avendo dato numerose direttive sul trattamento dei dati biometrici e per deflazionare il numero delle richieste di verifica preliminare, ha adottato il provvedimento di autorizzazione n. 513 del 12 novembre 2014, con cui l'Autorità ha fornito una compiuta compilazione delle prescrizioni e previsto casi di esonero dalla verifica preliminare succitata a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici idonei a raggiungere gli obiettivi di sicurezza individuati nel rispetto dei presupposti di legittimità contenuti nel Codice. In particolare, i titolari sono esonerati dall'obbligo di presentare istanza di verifica preliminare se: – le

caratteristiche biometriche[3] consistono nell'impronta digitale o nell'emissione vocale[4]; – la cancellazione dei dati biometrici grezzi ha luogo immediatamente dopo la loro trasformazione in campioni o in modelli biometrici; – i dispositivi per l'acquisizione iniziale (enrollment) e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi oppure integrati nei sistemi informatici che li utilizzano, siano essi postazioni di enrollment ovvero postazioni di lavoro o sistemi server protetti con autenticazione biometrica; – le trasmissioni di dati tra i dispositivi di acquisizione e i sistemi informatici sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati; – il supporto, rilasciato in un unico esemplare[5], è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso ai sistemi informatici, è restituito e distrutto con procedura formalizzata. È sempre esclusa la realizzazione di archivi biometrici centralizzati. Infine, deve essere predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo, altresì, la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione deve essere conservata ed aggiornata dal titolare del trattamento, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

[3] Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

[4] Nel caso di utilizzo dell'emissione vocale, tale caratteristica è utilizzata esclusivamente in combinazione con altri fattori di autenticazione e con accorgimenti che escludano i rischi di utilizzo fraudolento di eventuali registrazioni della voce (prevedendo, per esempio, la ripetizione da parte dell'interessato di parole o frasi proposte nel corso della procedura di riconoscimento).

[5] Nel caso in cui i riferimenti biometrici siano conservati in modalità sicura su supporti portatili (*smart card* o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno level 3. L'area di memoria in cui sono conservati i dati biometrici deve essere resa accessibile ai soli lettori autorizzati e protetta da accessi non autorizzati.

7. Le linee guida del Garante e considerazioni conclusive.

Anche con riferimento al trattamento dei dati biometrici dei lavoratori, il Garante con le linee guida del 2006 ha ribadito che l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. L'utilizzo di dati biometrici, infatti, può essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili[6]", considerata la natura delle attività ivi svolte. Difatti, in base al principio di necessità[7], il titolare del trattamento è tenuto ad accertare se la finalità perseguita possa essere realizzata senza utilizzare dati biometrici o comunque conformandosi al principio di proporzionalità del trattamento[8]. In un caso, il Garante ha ammesso il trattamento per finalità di accertamento della presenza in servizio dei dipendenti in ragione delle peculiarità del trattamento strettamente connesso a quel particolare contesto lavorativo[9]. È, invece, sempre esclusa la centralizzazione in una banca

---

[6] Appartengono a tale ambito, in particolare: • le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche mansioni che comportano la necessità di trattare informazioni riservate e applicazioni critiche; • le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità è ristretta a un numero circoscritto di addetti; • le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato; • l'utilizzo di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza onde scongiurare infortuni e danni a cose o persone.

[7] In tal senso, recentemente cfr. provvedimento 22 ottobre 2015, n. 4430740, su Rilevazione delle presenze dei dipendenti di un Comune tramite un sistema biometrico basato sul trattamento di impronte digitali.

[8] Cfr. artt. 3e 11 del Codice: si vedano, ad esempio, Provvedimento 31 gennaio 2013, n. 38, doc. web n. 2304669 nei confronti di un comune e Provvedimenti 30 maggio 2013, nn. 261 e 262 e 1° agosto 2013, n. 384, doc. web nn. 2502951, 2503101 e 2578547 nei confronti di alcuni istituti scolastici. In giurisprudenza cfr. Trib. Prato, 19 settembre 2011, n. 964. In generale cfr. le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 7.1).

[9] Provvedimento 10 gennaio 2013, n. 4, doc. web n. 2354574 nei confronti di una società a partecipazione pubblica.

dati delle informazioni personali. I sistemi informativi devono essere, infatti, configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In sintesi, è possibile affermare che il trattamento di dati biometrici in ambito lavorativo è ammesso solo in casi eccezionali laddove vi sia esigenza di accedere ad aree riservate e sempre nel rispetto dei principi di liceità, proporzionalità, necessità e non eccedenza. Ogni uso diverso è sanzionato specie ove si consideri che la normativa, descritta deve essere letta anche alla luce del sistema delle tutele poste a protezione del lavoratore.

La videosorveglianza sui luoghi di lavoro tra pronunce della S.C., statuto dei lavoratori e normative sulla riservatezza dei dati personali

ROBERTO ARCELLA*

SOMMARIO: 1. La videosorveglianza nei luoghi di lavoro: premessa. – 2. L'attività del Garante per la protezione dei dati personali. – 3. Il punto della giurisprudenza: l'interpretazione dell'art. 4 dello Statuto dei lavoratori.

1. La videosorveglianza nei luoghi di lavoro: premessa.

La videosorveglianza, prezioso strumento di tutela dei beni aziendali e della sicurezza, è già da qualche decennio al centro di dibattiti giuridici, per quanto costituisca argomento "giovane" in relazione all'epoca in cui le tecnologie ne hanno consentito una certa diffusione. Basti pensare che, allorquando l'art. 4 dello Statuto dei Lavoratori se ne occupò (1970), i sistemi di videoripresa avevano una limitatissima diffusione attesi gli elevati costi che implicavano, in guisa tale che la norma in esame poteva in qualche modo considerarsi di concreta applicazione solo per determinate categorie di soggetti datoriali particolarmente organizzati.

Il tema riveste oggi una rilevanza certamente maggiore che allora, avuto riguardo alla diffusa utilizzazione di tali strumenti, alla relativa facilità di installazione, ai bassissimi costi, alla notevole possibilità di mimetizzazione degli stessi all'interno degli ambienti ed infine alla concreta ed agevole possibilità di immediata propagazione elettronica delle immagini stesse attraverso la rete internet (ragione questa che ha indotto il Garante a dedicare un apposito paragrafo nel Provvedimento generale dell'aprile 2010, che impone la misura della cifratura dei dati

* Avvocato del Foro di Napoli, componente della Commissione Privacy e Security del Consiglio dell'Ordine degli Avvocati di Napoli, componente del Gruppo di Lavoro della Fondazione Italiana per l'Innovazione Forense (Consiglio Nazionale Forense), socio fondatore del Centro Studi Processo Telematico.

relativamente alle immagini trasferite su reti pubbliche di comunicazione[1]). Nella stessa direzione si è mossa la Giurisprudenza della S.C. (Cass. Civ. 3^ sez. penale, sent. 22611 dell'11 giugno 2012), che ha offerto una lettura più equilibrata dell'art. 4 dello Statuto dei lavoratori, evidenziando che se che l'obiettivo del legislatore è quello di tutelare il diritto alla riservatezza dei lavoratori, nel caso in cui tutti i dipendenti abbiano prestato il loro consenso all'installazione delle telecamere non vi è alcuna violazione del diritto alla riservatezza.

[1] Il par. 3.3.1 del provvedimento generale ora citato, infatti, prevede che "…la trasmissione 16 E non a caso si tratta di materia analizzata sotto molteplici profili, che vanno (ovviamente) dalla tutela della riservatezza ai sensi del d.lgs. 30 giugno 2003, n. 196 - essendosene ripetutamente occupato il Garante - alla utilizzabilità delle immagini raccolte con tali sistemi in ambito processualpenalistico. Parallelamente, alla luce delle accresciute esigenze di sicurezza in certi ambiti lavorativi, considerati obiettivi particolarmente sensibili della criminalità comune (tabaccherie, farmacie, distributori di benzina, gioiellerie), nel corso del 2012 si è assistito anche ad una rilettura ministeriale e giurisprudenziale dell'art. 4 dello Statuto dei lavoratori che, senza negare il diritto alla riservatezza dei dipendenti, ha alleggerito le procedure di cui all'art. 4 comma 2 e le responsabilità del datore di lavoro: in particolare, la nota del Ministero del Lavoro e delle Politiche Sociali, Direzione generale per l'attività ispettiva prot. 37/0007162 del 16 aprile 2012 ha semplificato notevolmente la procedura di rilascio dell'autorizzazione prevista dall'art. 4, comma 2, per l'installazione di impianti di videosorveglianza, per imprese medie e piccole in cui sussistono serie esigenze di tutela dell'incolumità dei lavoratori. La nota indica, esemplificativamente, le tabaccherie, farmacie, distributori di benzina, gioiellerie, ma risulta evidentemente applicabile a qualsiasi esercizio commerciale per il quale possa esistere un rischio per la tutela dell'incolumità dei dipendenti a causa dell'elevato rischio di rapina. La procedura semplificata consente alla DPL – senza necessità di sopralluogo – di rilasciare l'autorizzazione sulla base: (a) della documentazione allegata da parte del datore di lavoro che indichi il numero di telecamere, il posizionamento, l'angolo visuale, la planimetria dei locali e le caratteristiche tecniche dell'impianto richiedente (b) di autodichiarazioni attestanti l'impegno all'osservanza della normativa vigente ed a non usare i dati per finalità, ad esempio, di controllo o disciplinari. tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs)".

Vale la pena sottolineare anche che, in parte motiva, tale pronuncia afferma, in maniera più che condivisibile, che il consenso unanime dei dipendenti costituisce una misura di tutela del diritto alla riservatezza maggiore rispetto all'accordo con i sindacati o all'autorizzazione della Direzione provinciale del lavoro prescritti dall'art. 4, comma 2 S.L.

2. L'attività del Garante per la protezione dei dati personali.

Anche il Garante Privacy (com'è ovvio) ha dovuto ripetutamente occuparsi dell'argomento, sia con provvedimenti generali (il ricordato Provv. 8 aprile 2010, in Gazzetta Ufficiale n. 99 del 29 aprile 2010) che abbracciano un po' tutto il campo dello "scibile" in materia di captazione di immagini (dalle videoriprese in ambito di lavoro agli ospedali e luoghi di cura; dagli istituti scolastici al trasporto pubblico, dalla sicurezza urbana, al deposito dei rifiuti, dai dispositivi per la rilevazione delle infrazioni al codice della strada alla videosorveglianza in ambito condominiale), nonché con una serie di pronunce nelle quali la costante è rappresentata dal rilievo di illiceità del trattamento di dati personali effettuato mediante i sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970[2].

Particolarmente interessante è il caso affrontato nel provvedimento del 4 aprile 2013 (Registro dei provvedimenti n. 164 del 4 aprile 2013) nel quale si è esaminata la fattispecie relativa un sistema di videosorveglianza installato presso la sede di una società (che occupa 158 dipendenti e si estende per una superficie di circa 7550 18 mq) "per finalità di tutela dei beni aziendali" composto di diciannove telecamere, quindici delle quali sono "celate all'interno di rilevatori di fumo ed all'interno di segnali luminosi delle uscite di emergenza e sono tutte collegate ad un registratore digitale": qui il Garante ha ravvisato d'un colpo solo la violazione del principio di liceità (art. 11,

[2] Cfr. [doc. web n. 2691507], Sistemi di videosorveglianza installati presso esercizi commerciali e diritti dei lavoratori - 12 settembre 2013) Registro dei provvedimenti n. 397 del 12 settembre 2013; [doc. web n. 1810223], Prescrizioni per il corretto impiego di un sistema di videosorveglianza all'interno di un hotel – 14 aprile 2011, Registro dei provvedimenti n. 142 del 14 aprile 2011.

comma 1, lett. a), del Codice), essendo il trattamento effettuato in violazione del diritto alla riservatezza e della dignità dei lavoratori (art. 2 del Codice) nonché in violazione degli artt. 114 del Codice e 4, l. n. 300/1970; del principio di correttezza, di cui all'art. 11, comma 1, lett. a), del Codice, tenuto conto del carattere occulto dell'attività di videosorveglianza effettuata mediante larga parte delle telecamere, oltre che dell'art. 13 del Codice, non essendo stata resa ai lavoratori interessati alcuna informativa né individualizzata, né nelle forme semplificate prescritte nel menzionato provvedimento dell'8 aprile 2010 – secondo cui "il supporto con l'informativa deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze […] e deve avere un formato ed un posizionamento tale da essere chiaramente visibile…". Vale la pena rilevare, però, che nel ricordato caso il Garante non ha disposto la cancellazione delle immagini, autorizzando espressamente il titolare del trattamento alla loro conservazione per metterle a disposizione delle autorità competenti e degli interessati, facultati pertanto all'esercizio dei diritti previsti dall'art. 7 del Codice.

Degne di particolare nota sono, poi, le pronunce della Corte di Cassazione penale, tra le quali quella qui in commento (Cass. Pen 12/7/2013 n. 30177), che si occupano del tema della videosorveglianza come "prova" nel processo penale sia in rapporto alla norma ex art. 266 cod. proc. pen. (in tema di "intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione") ed al conseguente eventuale divieto di utilizzo ex art. 191 cod. proc. pen.

La pronunzia si occupa, in particolare, del caso di alcuni dipendenti delle Poste Italiane, tratti a giudizio con la contestazione (*inter alia*) di truffa aggravata relativa all'utilizzo di badge non autorizzati o di «passaggio» di mano di cartellini segna presenze da 19 un dipendente all'altro in guisa tale da far risultare presente ad una certa ora sul luogo di lavoro dei dipendenti che erano in realtà assenti o ritardatari (condotta criminosa che era stata fatta oggetto di riprese videoregistrate). La censura delle difese degli imputati si incentrava sulla deduzione che le videoriprese erano state effettuate in violazione dell'art. 266 cod. proc. pen in quanto avvenute "in luogo provato ed in assenza di autorizzazione del Giudice". Secondo le difese, gli ambiti

in cui erano state effettuate le riprese "andavano ritenuti quali luoghi di privata dimora, in quanto luoghi utilizzati per lo svolgimento di manifestazione della vita privata (come l'attività professionale) di chi lo occupava, anche in ragione della durata del rapporto tra il luogo e persona che vi operava", e, ancora, che nel caso di specie era certamente operante il divieto dell'art. 4 dello Statuto dei Lavoratori, ovvero il divieto assoluto di controllo a distanza dei lavoratori, divieto che si pone nei confronti di qualsiasi soggetto e non soltanto del datore di lavoro. In estrema sintesi, l'interessante pronuncia, che respinge il rilievo difensivo, afferma tre principi di fondo: a) che le "videoriprese" oggetto del processo non potevano qualificarsi come "intercettazioni" soggette alla disciplina ex art. 266 del codice di rito in quanto aventi ad oggetto "comportamenti non comunicativi" ed andavano quindi ritenute "prove atipiche"; b) che il luogo delle riprese non poteva qualificasi come "privato"; c) che il richiamo all'art. 4 dello Statuto dei Lavoratori non era pertinente, trattandosi di una disposizione mirata e limitata al divieto di controllo della attività lavorativa in quanto tale ovvero al divieto di controllo della corretta esecuzione della ordinaria prestazione del lavoratore subordinato, ma che non impedisce, invece, i controlli destinati alla difesa dell'impresa rispetto a specifiche condotte illecite del lavoratore o, comunque, a tutela del patrimonio aziendale[3] , conseguente piena utilizzabilità ai fini della prova di reati anche delle videoregistrazioni effettuate direttamente dal datore di lavoro, destinatario del citato divieto, laddove agisca non per il controllo della prestazione lavorativa ma per specifici casi di tutela dell'azienda rispetto a specifici illeciti.

Al di là dell'ultimo principio – che pare invero di applicazione piuttosto scivolosa se rapportato alle pronunce del Garante, apparendo assai difficile discriminare il momento (lecito) dell'inizio del trattamento dei dati videoregistrati (necessariamente anteriore all'inizio dell'attività illecita che si vuol comprovare) e quello in cui devono avere invece concreta e reale applicazione le prescrizioni del Codice e del Provvedimento Generale del 2010 – la pronuncia fa riaffiorare l'attualità del tema del tutela dei luoghi "privati", già oggetto di importanti riflessioni dottrinarie e giurisprudenziali, tra le

[3] *Ex multis*, Cass. Civ. Sez. Lav., Sentenza n. 2722 del 23/02/2012, Rv. 621115. 20

quali si segnala Cass. Pen., sez. VI, 10/1/2003 n. 3443, che rovesciava letteralmente l'opposto orientamento della IV sezione (sentenza 16/3/2000 "Viskovic").

L'argomento è di interesse fondamentale ai fini ermeneutici di tutta la disciplina in materia di privacy dacché riguarda la nozione di "domicilio" ai fini della tutela costituzionale ex art. 14, perché – com'è noto – secondo la dottrina costituzionalistica maggioritaria la norma costituzionale rinvia per "presupposizione"[4] alla definizione elaborata dal diritto penale, senza fornire elementi concettuali suscettibili di delinearne un contenuto nuovo[5]. In entrambi i casi si dibatteva di una videoripresa eseguita a fini investigativi nella toilette di un locale pubblico. La pronuncia del 2003, con una evidente forzatura della ratio ispiratrice della tutela penale, esclude la configurabilità del privato domicilio in base ad un criterio temporale, rappresentato dal grado di stabilità di permanenza: "Relativamente, invero, all'eccezione di inutilizzabilità delle intercettazioni audiovisive, deve senz'altro escludersi che il bagno di un locale pubblico, pur soddisfacendo, ove adoperato in modo conforme (e non è il caso di specie) alla sua normale destinazione, a legittime esigenze di carattere privato, possa considerarsi, per gli avventori che ne facciano occasionalmente uso, luogo di privata dimora ai fini della problematica in esame, posto che la nozione di "luogo di privata dimora"; di cui agli artt. 614 cp. e 266 cpp., postula il requisito, inconfigurabile nella specie, di un soggiorno che, per quanto breve, abbia comunque una certa durata, tate a far ritenere ragionevolmente apprezzabile l'esplicazione di vita privata che vi si svolge (cfr. Cass. V sent. n. 35947 cc. 04.06.2001)".

In senso diametralmente opposto, invece, la sentenza "Viskovic": qui, secondo la Corte di legittimità, "la tutela costituzionale si riferisce non solo alle private dimore e ai luoghi che, pur non costituendo dimora, consentono una sia pur temporanea ed esclusiva disponibilità dello spazio ma anche ai luoghi nei quali è temporaneamente garantita un'area di intimità e di riservatezza. Il principio che accomuna la

[4] S. ROMANO, *Principi di diritto Costituzionale Generale*, Giuffrè, 1947, p. 94.
[5] P. BARILE – E. CHELI, (voce) *Domicilio (libertà di)*, in *Enc. Dir.*, vol. XIII, Giuffrè, 1964, 862 ss.

privata dimora, i locali di uno stabilimento o di un'associazione o di un partito a questi luoghi è l'esistenza dello *jus excludendi alios* più ampio di quella prevista dal previgente art. 614 cod. pen. ed in particolare che essa finisca per coprire "tutti i luoghi, siano o meno di dimora, in cui può aver luogo il conflitto di interessi che essa regola. Se così è "domicilio", nella accezione costituzionale……è qualunque luogo di cui si disponga a titolo privato, anche se non si tratta di privata dimora" [6]. Da tali pronunce, ed in particolare da quella del 2000, certamente più articolata e condivisibile, possono dunque trarsi ampi spunti interpretativi ai fini dell'applicazione della normativa in materia di tutela della riservatezza ai fini civilistici e lavoristici.

Ancora più nel dettaglio delle distinzioni, la sentenza del 2013 qui in commento, con particolare chiarezza esemplificativa esclude che la tutela della riservatezza garantita al privato domicilio possa estendersi a luoghi quali "l'atrio di un ufficio così come tutte le sue parti comuni e le stanze "collettive" (uffici *open space*) [che] non sono[7], affatto la estensione di un domicilio privato, in modo non dissimile dalle parti comuni di un condominio di edificio, non essendovi affatto la possibilità per singoli soggetti di fruirne con una pienezza corrispondente a quella di fruizione del domicilio".

3. Il punto della giurisprudenza: l'interpretazione dell'art.4 dello Statuto dei lavoratori.

Altra questione recentemente esaminata in giurisprudenza attiene all'interpretazione dell'art. 4 S.L.[8]. In particolare, il Consiglio di Stato

[6] Cassazione Penale, sez. VI, 10/01/2003 n. 3443.

[7] Cassazione Penale, sez. IV, 16/03/2000, n. 7063.

[8] nella parte in cui si prevede che «*impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le*

(sez. VI , 05/06/2015 n. 2773) si è occupato di individuare i limiti ed identificare i parametri cui deve attenersi l'autorità amministrativa nel disporre l'eventuale deroga all'utilizzo degli impianti di videosorveglianza sui luoghi di lavoro in relazione alle esigenze organizzative dell'azienda e di tutela dei beni aziendali (nella specie, si trattava in particolare di impianti collocati all'interno di un Ipermercato al fine di contrastare fenomeni di taccheggi e furti.

Risultava nella specie impugnato il provvedimento con cui il Direttore generale delle relazioni industriali e dei rapporti di lavoro del Ministero del lavoro e delle politiche sociali n. 191 del 21 novembre 2012, disponeva la parziale riforma dell'autorizzazione della Direzione territoriale del lavoro di Como che aveva riconosciuto la regolarità del posizionamento di telecamere, finalizzate alla prevenzione ed alla repressione di furti e taccheggi nel grande centro commerciale della Ipercoop di Cantù, escludendo tuttavia la possibilità che la visione, consentita attraverso dette telecamere, fosse effettuata dal direttore del medesimo centro. Il TAR Lombardia aveva accolto il ricorso annullando quest'ultima disposizione, con ripristino della disciplina, dettata per la tipologia di controllo di cui trattasi nella prima autorizzazione.

Il CdS perviene, invece, ad opposte conclusioni, rilevando anzitutto, in punto di fatto, che la vicenda in esame riguardava non la prima installazione, ma la risistemazione di un sistema di videosorveglianza, per il quale nel 2006 era stato raggiunto il prescritto accordo – ex art. 4, secondo comma del citato Statuto dei Lavoratori – fra l'Azienda e le rappresentanze sindacali. Nell'accordo si faceva riferimento alla collocazione delle apparecchiature in un "*locale non accessibile ad altri, che non siano il Direttore e il*

rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale».

Responsabile della sicurezza, che comunque di norma non vi operano".

Il nucleo centrale della decisione risiede nella valutazione di due contrapposti principi: pur non essendo consentito infatti, a norma dell'art. 4 dello Statuto dei lavoratori, l'uso di sistemi di controllo a distanza, a fini di vigilanza sull'attività lavorativa, è assolutamente ragionevole contemperare il diritto dei lavoratori, a non essere in tal modo controllati, con le esigenze del datore di lavoro e della collettività, per la protezione e la sicurezza nei luoghi di lavoro. Il punto di coordinamento fra i principi sopra enunciati – osservano i Giudici del CdS – va ravvisato nella "*proporzionalità delle misure adottate, rispetto alla compressione dei diritti fondamentali dei lavoratori, da valutare secondo limiti di ragionevolezza*". È, infatti, realtà innegabile, secondo il CdS, «*che con il mezzo della videosorveglianza si possano non solo contrastare i taccheggi e le rapine (in corrispondenza ad una effettiva "esigenza organizzativa e produttiva"), ma anche, benché non intenzionalmente, trattare dati personali. La voce e l'immagine delle persone riprese non possono infatti non considerarsi informazioni riferite alle persone stesse, in base alla normativa sia nazionale (d.lgs. n. 196 del 2003, cit.) che comunitaria (Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995; cfr. anche Corte giust. UE, IV, 11 dicembre 2014, causa C - 212/13, secondo cui l'art. 3, par. 2, secondo trattino, della direttiva 95/46/CE, sulla tutela delle persone fisiche riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, va interpretato nel senso che l'utilizzo di un sistema di videocamera, che porta a una registrazione video delle persone immagazzinata in un dispositivo di registrazione continua quale un disco duro, installato da una persona fisica sulla sua abitazione familiare per proteggere i beni, la salute e la vita dei proprietari, e che sorveglia parimenti lo spazio pubblico, non costituisce un trattamento dei dati, effettuato per l'esercizio di attività a carattere esclusivamente personale o domestico ai sensi di quella disposizione).*

È in quest'ambito e per questi effetti che si impone l'esigenza di un controllo, che risulti rispettoso - come è nella ratio della norma, considerato il carattere generale del precetto di cui al primo comma

dell'art. 4 - del divieto di controllo a distanza dell'attività dei lavoratori.

Così, sia nel provvedimento sopra citato che in altri successivi, il Garante per la protezione dei dati personali ha ribadito che la videosorveglianza - autorizzabile solo per ragioni di sicurezza e di tutela del patrimonio aziendale - deve essere utilizzata nel rispetto del divieto di controllo a distanza dell'attività lavorativa, in conformità al principio generale, enunciato nel primo comma dell'art. 4 dello Statuto dei lavoratori.

Il tema investe dunque il rispetto della predetta norma, affinché gli impianti in questione non siano surrettiziamente utilizzati, oltre che per il contrasto del taccheggio e della rapina, per una finalità di controllo a distanza dell'attività dei lavoratori, essendo tale controllo vietato dalla norma generale (che non vieta al datore di lavoro di vigilare sulla condotta lavorativa dei dipendenti, ma esclude che la vigilanza possa avvenire a distanza con siffatti mezzi, che si presumono sleali o comunque eccessivamente intrusivi) ».

La decisione in commento, quindi, si colloca dichiaratamente nel filone della sopra ricordata Cass., lav., 23 febbraio 2012, n. 2722 in materia di controllo della posta elettronica aziendale effettuato dal datore di lavoro quando però diretto ad accertare non l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma, una condotta illecita del lavoratore, dannosa per l'azienda. A lume di tale pronuncia, infatti, l'utilizzo degli strumenti di controllo offerti dalle moderne tecnologie è ammissibile quando emergano indizi giustificativi di un'indagine a carico del lavoratore, per questioni che esulano dallo stretto ambito del rapporto di lavoro; ma si ribadisce al tempo stesso il divieto, di cui all'art. 4, primo comma, della legge n. 300 del 1970, quando si tratti solo di "*verificare l'esatto adempimento, da parte del lavoratore, delle obbligazioni nascenti dal rapporto di lavoro*".

Sulla necessità di una privacy policy aziendale

GIANLUCA BOZZELLI [*]

SOMMARIO: 1. Premessa. – 2. L'adozione di una privacy policy. – 3. Segue: l'adozione di un regolamento privacy.

1. Premessa

Un piano per la sicurezza *privacy* aziendale e l'adozione delle misure minime di sicurezza, secondo la normativa italiana sul trattamento dei dati personali (decreto legislativo 30 giugno 2003 n. 196), consentono agli imprenditori di essere idoneamente adempienti agli obblighi di legge, sia sotto l'aspetto formale, che sotto quello sostanziale e tecnico. La consulenza in questo campo assume la forma duplice, teorico giuridica e tecnico pratica. La prima si realizza attraverso la predisposizione di regolamenti e documentazioni, risultato di studio ed elaborazione da parte dei professionisti della normativa e delle principali pronunce giurisprudenziali sul punto; la seconda si basa su interventi tecnici sui sistemi informatici, destinati a mettere in sicurezza i sistemi operativi aziendali.

L'organizzazione interna, il controllo dei flussi di dati e la protezione degli archivi e delle banche dati non rappresentano esclusivamente l'adempimento dell'obbligo di legge, ma portano grandi vantaggi sostanziali a qualsiasi tipo di struttura aziendale. Non solo quindi consentono di evitare le sanzioni amministrative, civili e penali, previste dal Codice privacy, ma anche di meglio razionalizzare il lavoro, la distribuzione degli incarichi all'interno dell'impresa, eventualmente esternalizzando una serie di attività che richiedono grande impegno, ampia specializzazione e costante aggiornamento, assorbendo anche più di un'unità lavorativa.

[*] Avvocato, Vice Coordinatore della Commissione Privacy e Security del Tribunale di Napoli.

2. L'adozione di una privacy policy.

In chiave prospettica appare l'enorme importanza da parte delle imprese di dotarsi di una propria privacy policy aziendale, che può scongiurare il timore ed il rischio di sanzioni penali anche in relazione alle responsabilità derivanti dalla legge sulla responsabilità delle persone giuridiche (d.lgs. 8 giugno 2001, n. 231 e dalla legge 16 marzo 2006, n. 146). Una tale regolamentazione – elaborata da un professionista del settore, conoscitore tanto della normativa privacy, quanto di quella lavoristica e penale *in parte qua* – consentirà di ottemperare agli obblighi di legge, prevenendo infrazioni ed abusi, ma anche di difendersi dalle contestazioni che ragionevolmente si possa prevedere vengano sollevate, dai lavoratori – da un canto – e dalle pubbliche autorità – dall'altro. Per fare solo qualche esempio, si potrà evitare di incorrere nell'errore dell'azienda che, non avendo ben illustrato alla magistratura in che modo l'abuso (o non corretto utilizzo) degli strumenti informatici aziendali e l'impiego di software non licenziati abbiano danneggiato l'attività (prima che la reputazione) aziendale ed infranto gli obblighi di regolamentazione interna: evitando di vedersi concludere il procedimento di impugnazione del licenziamento irrogato, con la conferma dell'illegittimità anche in sede di legittimità.

Nel caso esaminato dalla Cassazione con la sentenza n. 22353 del 2 novembre 2015, l'imprenditore ha visto rigettare il ricorso avverso la decisione di conferma del giudice d'appello, in quanto "*Come già rilevato in relazione a fattispecie analoga da questa Corte nella sentenza n. 6222 del 18/3/2014, le allegazioni della società ricorrente non valgono a dimostrare che, contrariamente a quanto affermato dal giudice di appello, l'addebito mosso al dipendente riguardi infrazioni disciplinari diverse e più gravi rispetto alla fattispecie, contemplata dal contratto collettivo (richiamato nella lettera di contestazione), di uso improprio di strumenti aziendali*".

L'azienda contestava che il comportamento del lavoratore fosse recidivo, ma "*Il riferimento a precedenti informazioni e preavvisi (cioè a disposizioni del datore di lavoro in ordine all'uso del computer aziendale) non prospetta invero una violazione di distinti*

obblighi contrattuali, rilevando solo ai fini della valutazione della gravità dell'inadempimento".

Errata – sotto tale profilo o non completa – appare anche la lettera di contestazione dell'addebito, che "*non indica, quanto alla presenza di programmi coperti da copyright, la violazione di limiti posti all'utilizzazione degli stessi, con conseguenti profili di responsabilità per l'azienda. Inoltre, il fatto che la condotta sia stata reiterata non esorbita dalla previsione dell'"utilizzo improprio*", *locuzione che può intendersi anche come riferita ad un impiego protratto nel tempo*".
Con ogni probabilità, un regolamento *privacy* dettagliato ed integrato con il regolamento 231/2001 avrebbe consentito di fornire alla magistratura un quadro più chiaro delle responsabilità del lavoratore, accettate e riconosciute mediante sottoscrizione del regolamento stesso, e di quelle dell'imprenditore, per il caso di utilizzo di programmi coperti da *copyright*.

3. *Segue*: l'adozione di un regolamento privacy.

Un dettagliato regolamento privacy aziendale consentirà di invocare i criteri applicati dal Tribunale di Milano sez. VI con la sentenza del 4 febbraio 2014[1] e richiedere il risarcimento del danno patrimoniale e non patrimoniale alla banca in caso di furto con *phishing* delle credenziali aziendali, poiché *"nel rapporto contrattuale di home banking, la banca ha la veste di contraente qualificato, che, non ignaro delle modalità di frode mediante phishing da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza"*.

L'esperto privacy aziendale potrà sfruttare al meglio le ricadute della recente pronuncia della Corte di giustizia UE, 13 maggio 2014, n.131[2], grande sezione in tema di diritto all'oblio (sentenza Google),

[1] In *Responsabilità Civile e Previdenza*, 2015, fasc. 3, pagg. 911 segg. con nota di R. FRAU, *Home banking, captazione di credenziali di accesso dei clienti tramite phishing e responsabilità della banca*.

[2] S. RICCI**,** *Le ricadute penali della sentenza della corte di giustizia europea sul diritto all'oblio - the impact on criminal law of the european court of justice decision on the right to oblivion,* in *Cassazione Penale,* fasc.3, 2015, pag. 1247.

secondo la quale l'interessato può rivolgersi direttamente a *Google* (e successivamente al Garante o all'Autorità Giudiziaria) per esercitare la propria opposizione al trattamento di dati personali; tanto in caso di trattamento originariamente illecito, quanto in caso di trattamento lecito del sito di provenienza, ma i dati appaiano inadeguati, non pertinenti (o non più pertinenti), od eccessivi rispetto alle finalità e oppure al tempo trascorso. Il punto centrale della questione – all'attenzione del professionista – sarà pertanto la valutazione e l'individuazione dei parametri per considerare l'adeguatezza e la pertinenza delle informazioni trattate.

L'impresa, ben consigliata sotto il profilo della riservatezza, e dotata di un valido regolamento e di un buon consulente *privacy* – come detto esperto anche della materia del lavoro – , probabilmente farà buon uso dei principi applicati dalla Corte d'Appello di Milano con la sentenza del 4/8/2015 n. 755[3], conscio che è possibile sottoporre il lavoratore a controllo da parte di investigatore privato in considerazione della peculiarità dell'attività svolta da questi (in quel caso consistente in buona parte in attività ispettive da svolgersi fuori sede) "*così che il ricorso all'agenzia investigativa da parte del datore di lavoro per un periodo di circa due mesi […] era quindi necessitato ai fini dell'accertamento di eventuali illeciti – connessi al sospettato utilizzo dell'istituto delle trasferte per assentarsi dal servizio – e, come tale, diversamente da quanto ritenuto dal tribunale, ricompreso nella giurisprudenza di legittimità che lo valuta ammissibile (cfr. tra le recenti: Cass. 26 novembre 2014 n. 25162)*".

In epoca di *job act* (in Italia pare che si concorra a rendere incomprensibile l'attività politica ricorrendo sempre più di frequente alle terminologie straniere), con la pubblicazione in Gazzetta Ufficiale n. 221 del 23 settembre scorso (suppl. ordinario n. 53), è entrato in vigore il decreto legislativo n. 151 del 14 settembre 2015, recante «*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014 n. 183*». L'intervento riformatore dell'articolo 4 SDL (Statuto dei Lavoratori l. 300/1970)

[3] In Banca dati *De Jure* Giuffrè.

prende coscienza del dibattito giurisprudenziale sorto attorno alla casistica dei controllo c.d. "difensivi" [4]. La Suprema Corte ha, infatti, recentemente confermato che le garanzie poste in materia di divieto di controlli a distanza dal comma 2 dell'art. 4 SDL si applicano ai controlli difensivi, volti ad accertare comportamenti illeciti dei lavoratori "*quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso*", stabilendo che sono legittimi quei controlli diretti ad accertare comportamenti illeciti del lavoratore e lesivi del patrimonio aziendale (Cassazione sentenza 17 febbraio 2015 n. 3122. e sentenza 23 febbraio 2012 n. 2722). L'esperto privacy aziendale saprà far buon uso della norma modificata, il cui scopo rimane quello di contemperare il diritto del lavoratore a non vedersi sottoposto ad un controllo a distanza nello svolgimento delle proprie attività nel luogo di lavoro, con la confermata esigenza datoriale di una corretta ed insindacabile organizzazione interna del lavoro e della produzione, "*individuando una precisa procedura esecutiva e gli stessi soggetti partecipi*" (Cassazione Civile sentenza 01 ottobre 2012 n. 16622).

Ancora, l'esperto professionista potrà prevedere il diritto/obbligo da parte del datore di lavoro di accedere alle *password* di protezione delle corrispondenze dei lavoratori utilizzate ai fini dello svolgimento dell'attività lavorativa, potendo invocare così scriminanti, circostanze comprovanti l'assenza di dolo e il consenso dell'avente diritto. Consentirà altresì di invocare la giurisprudenza di merito più liberista (Tribunale di Milano sent. 10 maggio 2002), secondo cui la generalizzata applicazione del principio di segretezza non potrebbe mai prevalere "*nel momento in cui il lavoratore utilizzi lo strumento per fini privati (ossia extra lavorativi), atteso che giammai un sollecito (o, al massimo, semplicemente tollerato ma non certo favorito) di uno strumento di lavoro può far attribuire a chi questo illecito commette diritti di sorta*". Oppure legittimerà l'invocazione dei principi fissati dalla Suprema Corte secondo cui "*ai fini*

[4] *Inter cetera*, cfr. G. SARACINO, *I controlli a distanza sui lavoratori dopo i decreti attuativi del Jobs Act*, 8/10/2015, in *www.altalex.com* e P. RAUSEI, *Jobs Act, controlli a distanza: cosa cambia per i datori di lavoro*, 9/7/2015 in *www.ipsoa.it*.

dell'operatività del diritto d'utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori ex art. 4 Statuto dei Lavoratori è necessario che il controllo riguardi (direttamente o indirettamente)l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito di applicazione della norma e controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate" (Cassazione sentenza 3 aprile 2002 n.4746).

Una politica di *privacy* resa nota potrebbe evidenziare l'obbligo del controllo cui i datori debbono procedere in virtù di una chiara disposizione inserita nell'allegato B) del Codice *privacy*[5], che prescrive i trattamenti effettuati con strumenti elettronici: "*Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale*".

La prescrizione dell'allegato tecnico al Codice *privacy* prevede infatti l'obbligo di controlli effettuati sul sistema informatico non solo come controlli difensivi ma come verifiche obbligate dal monitoraggio tecnologico dei trattamenti effettuati con strumenti elettronici. Sebbene raccolte, le risultanze delle attività di controllo potranno essere utilizzate certamente ai fini della sua della soppressione di comportamenti di rilevanza penale, ma anche ai fini disciplinari e della responsabilità civile, anche in assenza della procedura di cui all'art. 4 comma 2 SDL, purché si tratti di controllo condotto *ex post*, che accerti condotte illecite commesse dal dipendente sulla base di dati occasionalmente acquisiti nell'ambito di controlli eseguiti con finalità di aggiornamento dei sistemi informatici.

Il Garante ha ribadito, con le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (Deliberazione n. 53 del 23 novembre 2006) "l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che "*deve avere cognizioni*

[5] "*Disciplinare tecnico in materia di misure minime di sicurezza*".

in materia di protezione dei dati personali e ricevere una formazione adeguata. In assenza di un'adeguata formazione degli addetti al trattamento dei dati personali il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito" e nelle Linee guida del Garante per posta elettronica e internet (Deliberazione n. 13 del 1° marzo 2007) "*la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9)*".

Una corretta politica sulla tutela dei dati personali deve essere pertanto accompagnata da una completo ed articolato programma di informazione, ma anche di formazione aziendale, al fine di formare validi incaricati del trattamento dei dati personali in ambito aziendale. L'importanza della privacy policy aziendale e la necessità della presenza di un esperto consulente aziendale si fa ancora più evidente alla luce delle novità legislative, tanto interne quanto comunitarie.

Documenti di lavoro, comunicazioni ai sindacati e cartellini identificativi

CARMINE MAZZOCCHI [*]

SOMMARIO: 1. Premesse. – 2. I documenti di lavoro. – 3. Le comunicazioni ai sindacati in tema di lavoro straordinario. – 4. I cartellini identificativi.

1. Premesse.

Il Titolo VIII del Codice della privacy disciplina i trattamenti finalizzati alla gestione ed al trattamento dei dati personali in materia di previdenza e lavoro ed è evidentemente teso a tutelare la riservatezza del lavoratore in ogni aspetto della sua vita, non solo lavorativa. In tale ottica, occorre ricordare la particolare attenzione che il datore di lavoro deve osservare nella compilazione dei c.d. "documenti di lavoro", quali i cedolini e le buste paga, nell'indicazione delle eventuali ore di straordinario e la relativa comunicazioni sindacali, nonché nella stampa e distribuzione dei cartellini identificativi dei singoli dipendenti.

2. I documenti di lavoro.

Partendo dai cedolini e dalle buste paga occorre rilevare che un primo aspetto riguarda la compilazione, la conservazione e la consegna e le relative cautele da adottare, o meglio, che andrebbero adottate a tutela della riservatezza del lavoratore. Già con parere del 31.12.98 il Garante ebbe a precisare che "*Per i dati la cui inclusione nel cedolino dello stipendio appaia necessaria nell'interesse del dipendente, andrebbero adottate, ai sensi dell'art. 15 della legge n. 675/1996, opportune cautele a tutela della riservatezza che possono consistere, ad esempio, nel piegare e spillare il cedolino,*

[*] Avvocato, Membro della Commissione Privacy e security del Tribunale di Napoli.

nell'imbustarlo o nell'apporvi una copertura delle parti più significative che non riguardino dati di comune conoscenza (generalità, ufficio di appartenenza, ecc.), ovvero nell'introdurre una cd. "distanza di cortesia" agli sportelli. [1]

È pacifico, precisava il Garante, che i dati presenti nel cedolino dello stipendio dei dipendenti rientrano certamente nella nozione di "dato personale" contenuta nella legge n. 675/1996 in quanto collegati a persone fisiche individuate o individuabili. Alcuni di essi possono avere natura "sensibile" (sussidi di cura, indennità missione handicappati, iscrizione al sindacato, ecc.) o rendono opportune maggiori cautele (multe disciplinari, pignoramenti per alimenti o tasse, ecc.). Il cedolino è destinato ad essere consegnato, di regola, nelle mani dell'interessato. Ciononostante, si concorda con la necessità di adottare le opportune misure volte a tutelare la riservatezza dei dipendenti per fare in modo che i dati contenuti nel "cedolino" non siano immediatamente accessibili ad altre persone rimanendo conoscibili dai soli incaricati del trattamento che li devono necessariamente utilizzare per la gestione del rapporto di lavoro. Il dipendente ha ovviamente interesse a poter verificare nel modo più semplice possibile le voci relative a ritenute ed emolumenti. Ciò non preclude al datore di lavoro la possibilità di eliminare dai cedolini determinati particolari relativi a situazioni strettamente personali o familiari (es., la causa del pignoramento, la ragione del sussidio, la sigla del sindacato). Nelle amministrazioni dotate di un efficiente sistema informativo si potrebbero poi configurare ulteriori modalità basate sulla riduzione al minimo dei dati contenuti nel cedolino e sulla possibilità per il dipendente di accedere facilmente, con l'uso di una password, a tutte le informazioni che riguardano lo stipendio.

Occorre rilevare che i documenti in oggetto non hanno rilievo nel solo ambito lavorativo, ma vengono spesso utilizzati anche per attività diverse ed estranee al rapporto d'impiego. Si pensi, ad esempio, all'accesso al credito mediante presentazione della busta paga, o anche alle richieste di sgravi fiscali o riduzioni di tariffe. È, inoltre, frequente che il lavoratore subisca provvedimenti esecutivi con addebito o, più semplicemente, potrebbe avere predisposto dei pagamenti volontari

[1] Provv. del Garante per la protezione dei dati personali doc. web. 39324.

come ad esempio il versamento periodico di somme a favore del coniuge separato o il pagamento di quote sindacali.

Ciò premesso il Garante, si è più volte dovuto occupare di casi inerenti le varie indicazioni e voci contenute nei cedolini e nelle buste paga. Un caso emblematico ha riguardato un ricorso presentato da un pensionato INPS il quale contestava l'utilizzo nel cedolino di pensione mensile dell'espressione "pignoramento". Sosteneva, infatti, il ricorrente che, ai sensi degli artt. 7 e 8 del D.Lgs. n. 196/2003 recante il Codice in materia di protezione dei dati personali, il titolare del trattamento avrebbe potuto utilizzare, in luogo della citata voce "pignoramento", espressioni più generiche. L'istituto resistente replicava facendo presente che il cedolino dei pensionati riportava genericamente l'esistenza di una trattenuta per pignoramento, senza mai indicare la causa del pignoramento. Il Garante accoglieva il ricorso ed ordinava all'istituto di previdenza resistente di modificare la dicitura "*pignoramento*" utilizzando nei termini predetti una diversa espressione o codice che, pur rendendo enucleabile la ritenuta e lasciando identificabile la porzione di retribuzione "disponibile" a garanzia del credito, non la descriva specificamente[2].

Con la citata decisione il Garante ha affermato che la dicitura 'pignoramento' non può figurare sulla busta-paga confermando un indirizzo consolidato.

La dicitura "pignoramento" apposta sulla busta-paga a motivazione di una ritenuta operata sullo stipendio contrasta con i principi posti a tutela della riservatezza dei dati personali, in quanto rende chiaramente conoscibile a terzi delicati aspetti della vita privata del lavoratore. Le finalità di documentazione e trasparenza nel rapporto fra datore di lavoro e dipendente possono essere soddisfatte mediante l'utilizzazione di diverse dizioni o codici identificativi che rendano enucleabile la ritenuta senza descriverla specificamente.[3]

[2] Provv. Garante per la protezione dei dati personali del 31.10.07 doc. web. 1459297.

[3] Provv. Garante per la protezione dei dati personali del 19.02.02, doc. web 1063659.

Analoghe decisioni hanno riguardato specifiche voci che, ove inserite in busta paga, possono rivelare delicati aspetti relativi a peculiari rapporti familiari o a determinati provvedimenti giudiziari e sempre il Garante si è dichiarato favorevole ad evitare formule troppo esplicite (si pensi, oltre che alla specifica causale del pignoramento, alla superflua indicazione della sigla identificativa del sindacato destinatario della ritenuta sindacale, ovvero alla dicitura : alimenti al coniuge).

Altro spinoso problema riguarda i lavoratori che appartengono alla categoria delle "persone svantaggiate" prevista dall'art. 4 della L. 381/91 (*"Disciplina delle cooperative sociali"*) e che comprende, tra gli altri, *"gli invalidi fisici, psichici e sensoriali, gli ex degenti di ospedali psichiatrici, anche giudiziari, i soggetti in trattamento psichiatrico, i tossicodipendenti, gli alcolisti, i minori in età lavorativa in situazioni di difficoltà familiare, le persone detenute o internate negli istituti penitenziari, i condannati e gli internati ammessi alle misure alternative alla detenzione e al lavoro all'esterno"* .

Anche su questo punto il Garante si è pronunciato prescrivendo l'adozione, nel prospetto di paga di diciture o codici sostitutivi rispetto alla locuzione *"lavoratore svantaggiato"* utilizzata, vietando al contempo l'ulteriore trattamento di tale informazione nel prospetto medesimo (doc. web. 1640331) in quanto tale indicazione risulterebbe ultronea rispetto agli elementi che devono, di regola, essere menzionati nel prospetto di paga, atteso che il documento è suscettibile di circolazione al di fuori dello stretto contesto lavorativo con conseguente conoscibilità delle informazioni ivi contenute da parte di terzi. A nulla sono valse, nel caso di specie, le difese della resistente, secondo cui l'indicazione nel prospetto di paga del riferimento legislativo afferente la condizione di "*persona svantaggiata"* discenderebbe direttamente dal quadro normativo vigente. Infatti, il Garante ha precisato che, diversamente da quanto sostenuto dalla resistente, l'art. 4 della legge 8 novembre 1991, n. 381 si limita a prevedere le agevolazioni che devono essere riconosciute in capo ai soggetti ivi indicati (con talune eccezioni), senza tuttavia contemplare la necessaria indicazione, in sede di compilazione del prospetto di paga, dell'appartenenza di questi ultimi alla categoria

delle *"persone svantaggiate"* e che tale indicazione non risulta necessaria neanche alla luce di quanto previsto dall'art. 1 della legge 5 gennaio 1953, n. 4, che individua gli elementi che debbono essere indicati nel prospetto di paga da consegnare al lavoratore (segnatamente: nome; cognome; qualifica professionale; periodo di riferimento della retribuzione; assegni familiari; altri elementi che compongono la retribuzione; singole trattenute).

Pertanto, la finalità di rendere edotto il lavoratore, in forma chiara e puntuale, degli elementi che compongono la propria retribuzione possono essere ugualmente perseguite avvalendosi di modalità alternative all'indicazione, nel prospetto di paga, della condizione di *"lavoratore svantaggiato"*, ad esempio, attraverso l'adozione di codici sostitutivi[4]. Sul punto, si è più volte espresso il Garante, affermando che "il trattamento dei dati idonei a rivelare la finalità della ritenuta nel cedolino è, in termini generali, lecito e correlato alle finalità del trattamento, che è volto anzitutto a documentare al lavoratore le diverse voci relative alle competenze e alle trattenute anche per permettere una verifica agevole circa l'esatta corresponsione della retribuzione"[5]. Ha però precisato che le causali "sensibili" di cui sopra vanno apposte sulla busta-paga nel rispetto dei principi posti a tutela della riservatezza dei dati personali e che pertanto le finalità di documentazione e trasparenza nel rapporto fra datore di lavoro e dipendente devono essere soddisfatte mediante l'utilizzazione di diverse dizioni o codici identificativi che rendano enucleabile la ritenuta senza descriverla specificamente.

Si può, quindi, affermare che tutte le ulteriori indicazioni o diciture inserite nei documenti di lavoro possono sicuramente diffondere dati riservati meritevoli di tutela perché ineriscono la sfera personale del lavoratore atteso che il cedolino dello stipendio può essere esibito o prodotto a terzi. In questi casi, fermo restando quanto sopra indicato circa la necessità di evitare l'indicazione della specifica causale, la

[4] Cfr. Provv. del Garante per la protezione dei dati personali del 31.10.07, doc. web n. 1459297; Provv. del Garante per la protezione dei dati personali del 19.02.02, doc. web n. 1063659).

[5] Decisione del Garante per la protezione dei dati personali del 19.02.02 doc. web n. 1063659.

cautela da adottare deve tuttavia permettere di individuare la predetta parte di retribuzione. Pertanto, adottando le cautele indicate, gli interessati potranno appurare unicamente il livello stipendiale ovvero, per mutui e finanziamenti conseguenti anche a c.d. cessioni del quinto dello stipendio, potranno identificare la porzione di retribuzione "disponibile" a garanzia del credito, ma non avranno accesso anche a tutte le causali delle varie voci.

Concludendo, si può affermare che le finalità di documentazione e di trasparenza, laddove vengano in considerazione, possono essere ugualmente perseguite, nel rispetto del principio di pertinenza e non eccedenza delle informazioni trattate mediante l'utilizzo di diciture meno specifiche che rendano ugualmente comprensibile la voce (a puro titolo di esempio: "altre trattenute"), oppure di idonei codici identificativi tenendo peraltro presente che tali indicazioni possono essere peraltro oggetto di eventuali richieste di chiarimenti rivolte dal lavoratore agli uffici amministrativi dell'ente.

3. Le comunicazioni ai sindacati in tema di lavoro straordinario.

La disciplina del lavoro straordinario è contenuta nell'art. 2108 comma 1 cod. civ., che dispone: « In caso di prolungamento dell'orario normale, il prestatore di lavoro deve essere compensato per le ore straordinarie con un aumento di retribuzione rispetto a quella dovuta per il lavoro ordinario». Nella normativa attuale non viene definito esplicitamente il limite massimo della durata del lavoro giornaliero, bensì solo di quello settimanale e viene posto un limite massimo all'orario di lavoro giornaliero pari a 12 ore complessive, derivanti da un vincolo da rispettare per ogni giorno di lavoro diventano una media riferita a un periodo di 4 mesi.

I vari C.C.N.L. – diversi per ogni settore di attività – trattano specificatamente questo argomento, pertanto non esiste una regola unica e spesso sono migliorativi rispetto alla legge, prevedendo ancora la volontarietà del lavoratore al lavoro straordinario ed il monte ore annuo effettuabile. In ogni caso è previsto che il datore di lavoro comunichi lo straordinario effettuato alle OO.SS., ai fini di evitare abusi diretti ed indiretti nei confronti dei lavoratori, sulla «misura e

consistenza degli straordinari» ed al fine di condizionarne il ricorso aziendale una volta superata una certa soglia.

La sezione lavoro della Cassazione, con la sentenza n. 7347 del 17 aprile 2004 ha affermato la sussistenza di "comportamento antisindacale" nel rifiuto di un'azienda di adempiere all'obbligo contrattuale pattuito in ordine al diritto di comunicazione alle RSA degli straordinari dei dipendenti in quanto, dal fatto oggettivo della mancata conoscenza dei dati sullo straordinario, conseguiva indiscutibilmente per il sindacato un impedimento o quantomeno una limitazione in ordine alla capacità decisionale del medesimo o delle sue strutture introaziendali di assumere – in fase successiva o nel momento più opportuno e consapevolmente – la determinazione di contrastare l'eventuale sistematica violazione del superamento del monte ore da parte dell'azienda. Ritenuto quindi pacifico che i sindacati hanno diritto di ricevere le comunicazioni in ordine allo straordinario eseguito e che la violazione di tale obbligo concretizza comportamenti antisindacali suscettibili di sanzione ex art. 28 st. lav., a questo punto deve considerarsi la problematica nell'ambito del codice sulla privacy. In tale ambito la tendenza è parzialmente limitativa in quanto si deve ritenere vietata la trasmissione ai sindacati dei nominativi dei lavoratori che effettuano ore di straordinario; pertanto le comunicazioni sulle ore di lavoro straordinario del dipendente devono essere inoltrate in forma anonima.

Sul punto, il Garante sulla Privacy ha chiarito che con le comunicazioni dei nominativi si commetterebbe un'illecita intromissione nella sfera privata del soggetto e che, quindi, le informazioni attinenti al lavoro straordinario debbano essere trasmesse alle organizzazioni sindacali senza specificare nome e cognome dei lavoratori cui i dati si riferiscono. È di tutta evidenza, dunque, come l'acquisizione dei nominativi non soltanto è superflua, ma potrebbe anche arrecare seri danni qualora se ne facesse un uso improprio, contrario ai principi a tutela e fondamento della privacy del lavoratore, il quale, in caso di violazione della propria riservatezza, può rivolgersi al Garante privacy avanzando richiesta di interruzioni delle divulgazioni illecite dei dati. Al riguardo anche la Giurisprudenza di merito si è da tempo espressa aderendo all'orientamento richiamato affermando che "*Non integra gli estremi della condotta antisindacale*

il comportamento del datore di lavoro il quale rifiuta di comunicare al sindacato i dati relativi all'effettuazione del lavoro straordinario da parte dei dipendenti in assenza di un consenso di questi ultimi reso ai sensi della l. 31 dicembre 1996 n. 675, sul trattamento dei dati personali"[6].

La Sezione lavoro della Cassazione, con sentenza n. 7347/2004 ha ulteriormente chiarito che «è esclusiva prerogativa del singolo dipendente la pretesa al rispetto del tetto contrattuale previsto», confermando l'orientamento che esclude in linea di massima la configurabilità di un comportamento antisindacale in caso di lesione di prerogative individuali, salvo che non sussista appunto l'intento del datore di lavoro di frustrare la libertà e l'attività sindacale.

Il recentissimo provvedimento del Garante n. 431, del 20.12.2012 ha definitivamente chiarito che le pubbliche amministrazioni, in assenza di disposizioni normative o di specifiche clausole contenute in contratti collettivi, non possono comunicare le ore di straordinario svolte da un dipendente indicando anche il nome e il cognome dello stesso. Le comunicazioni vanno fatte in forma anonima o aggregata.

Ancor più di recente, lo stesso Garante ha vietato di affiggere in bacheca l'elenco nominativo dei lavoratori che avevano eseguito ore di lavoro straordinario, vietando altresì la trasmissione del predetto elenco ai sindacati[7]. Tale pubblicazione, così come la comunicazione ai sindacati, viola l'articolo 11 del codice della privacy, secondo cui i dati personali oggetto di trattamento debbono essere non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, e viola anche l'art. 19 comma 3, del codice che prevede che la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione di tali dati da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Concludendo, sul punto possiamo affermare che sicuramente le OO.SS. conservano il diritto a ricevere la comunicazione delle ore di straordinario effettivamente svolte, ma che tale comunicazione deve avvenire in forma anonima.

[6] Pret. Roma, decreto 25 ottobre 1997.
[7] Provv. Garante per la Protezione dei dati personali, n. 358 del 18.07.13.

4. I cartellini identificativi.

Numerose norme contrattuali e organizzative impongono al personale (del settore privato o di quello pubblico), a contatto con l'utenza, di appuntare sul vestito o sulla divisa un cartellino identificativo contenente vari dati personali: tutto ciò al fine di realizzare una maggiore responsabilizzazione dei lavoratori verso il pubblico, agevolando quest'ultimo nell'identificazione del personale con cui è entrato in contatto e quindi – se del caso – consentendogli di tutelarsi in modo adeguato. Le finalità perseguite, di mera trasparenza e correttezza nel contatto con il pubblico o i clienti, inevitabilmente hanno portato problemi di armonizzazione alla legislazione sulla *privacy* atteso che le informazioni contenute nei cartellini identificativi e, grazie ad essi, possono essere diffuse in modo indifferenziato.

Il TU sulla sicurezza sul lavoro, al punto 3. dell'art. 20, prevede *che i lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto.*

Il successivo art. 26, trattando degli obblighi connessi ai contratti d'appalto o d'opera o di somministrazione, prevede al punto 8 che, *nell'ambito dello svolgimento di attività in regime di appalto o subappalto, il personale occupato dall'impresa appaltatrice o subappaltatrice deve essere munito di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro.*

Come è facile immaginare dalla semplice lettura delle succitate disposizioni, l'indicazione di dati sensibili su un cartellino identificativo, ha creato non pochi problemi dal punto di vista della privacy del lavoratore. Appare, infatti, eccessivo indicare sul cartellino identificativo del dipendente dati anagrafici o generalità complete del lavoratore.

Il Ministero del Lavoro, con circolare n. 29/2006, aveva già precisato che "*i dati contenuti nella tessera di riconoscimento devono consentire l'inequivoco e immediato riconoscimento del lavoratore interessato e pertanto, oltre alla fotografia, deve essere riportato in modo leggibile almeno il nome, il cognome e la data di nascita. La tessera inoltre deve indicare il nome o la ragione sociale dell'impresa datrice di lavoro*".

Con interpello n. 41/2008 al Ministero**,** *la ANIE – Federazione nazionale imprese elettrotecniche ed elettroniche,* atteso l'art. 36 *bis*, comma 3, del D.L. n. 223/2006 (conv. da L. n. 248/2006) dispone che: "*nell'ambito dei cantieri edili i datori di lavoro debbono munire, a decorrere dal 1° ottobre 2006, il personale occupato di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. I lavoratori sono tenuti ad esporre detta tessera di riconoscimento*", chiedeva chiarimenti in merito ai dati da riportare sul tesserino di riconoscimento per il personale occupato nei cantieri edili nel rispetto del Codice in materia di protezione dei dati personali, tenuto conto che, ai sensi della normativa in materia di *privacy* (D.Lgs. n. 196/2003), i dati personali trattati devono essere pertinenti e non eccedenti rispetto alla finalità perseguita, anche se derivanti da obblighi di legge. In particolare, l'ANIE, sulla scorta dei concetti di "*pertinenza*" e "*non eccedenza*" di cui all'art. 11 del Codice in materia di protezione dei dati personali, chiedeva se – rispetto alle finalità generali perseguite e all'esigenza che i dati riportati su detta tessera consentano l'identificazione del lavoratore – l'indicazione della data di nascita non risultasse eccessiva, risultando sufficiente l'indicazione degli altri elementi indicati dalla circolare n. 29/2006 (fotografia, nome e cognome del lavoratore, nome o ragione sociale del datore di lavoro). La Direzione del Ministero non riteneva di dover aderire a questa interpretazione sostenendo che la tutela del diritto alla riservatezza può, da parte del Legislatore, subire una limitazione (proporzionale) a fronte del disvalore e della pericolosità sociale di talune condotte che si vogliono combattere e reprimere, proprio a salvaguardia di concorrenti e superiori valori e garanzie costituzionali.

In definitiva, la tutela del diritto alla riservatezza può essere graduata ad opera del Legislatore in rapporto ad un'esigenza concreta

purché costituzionalmente protetta. La maggiore o minore limitazione alla tutela del diritto alla riservatezza sarà costituzionalmente fondata se posta in relazione con la maggiore o minore gravità attribuita dal Legislatore ad illeciti diversi individuati secondo scelte di politica legislativa. In questo senso, gli strumenti di cui all'art. 36 *bis* cit. rispondono tutti in modo costituzionalmente adeguato agli intenti programmatici del Legislatore e di cui al comma 1 dello stesso articolo ("*al fine di garantire la tutela della salute e la sicurezza dei lavoratori nei settori dell'edilizia, nonché al fine di contrastare il fenomeno del lavoro sommerso ed irregolare*…)"; e tutto ciò nel rispetto dei principi inderogabili sanciti dagli artt. 2, 32, 35 e 41 comma 2, Cost.

Pertanto, la indicazione contenuta nella circolare ministeriale – che, peraltro, ha solamente esplicitato il concetto di "*generalità del lavoratore*" senza apportare alcuna indebita integrazione concettuale e terminologica del precetto legislativo – risulta essere sotto ogni profilo, formale e sostanziale, rispettosa del principio del trattamento dei soli dati personali che siano pertinenti e non eccedenti rispetto alle finalità per cui sono raccolti e trattati[8]. Oltre a ciò, si consideri anche la necessità di leggere la norma *de quo* in correlazione con quanto sancito dal successivo comma 4: *"i datori di lavoro con meno di dieci dipendenti possono assolvere all'obbligo di cui al comma 3 mediante annotazione, su apposito registro di cantiere vidimato dalla Direzione provinciale del lavoro territorialmente competente da tenersi sul luogo di lavoro, degli estremi del personale giornalmente impiegato nei lavori*".

Il Registro di cantiere di cui all'art. 36 *bis*, comma 4, del D.L. n. 223/2006 – vidimato dalla competente D.P.L. e da tenersi sul luogo di lavoro – è strutturato sul modello del "vecchio" libro di matricola. Infatti sullo stesso dovranno essere trascritti gli estremi (*id est* i dati anagrafici) del personale giornalmente impiegato in cantiere e ciò al fine di soddisfare, se pur in altro modo, il contenuto precettivo di cui al precedente comma 3 dell'art. 36 *bis*. Il Ministero del lavoro ha, quindi, previsto un sistema di graduazione degli interessi e degli scopi perseguiti ed ha ritenuto prevalente sul diritto alla riservatezza quello

[8] Vedi art. 11, comma 1, lett. d) del D.Lgs. n. 196/2003.

alla individuazione e repressione di condotte lesive della salute e della sicurezza dei lavoratori nei settori dell'edilizia, così come il contrasto del fenomeno del lavoro sommerso e irregolare. Ovviamente in materia di riservatezza la competenza spetta al Garante che, con parere dell'11 gennaio 2001, (doc. web n. 30991) ha chiarito che le disposizioni degli artt. 20 e 27, commi 3 e 4, della legge n. 675/1996 consentono, rispettivamente nel settore del lavoro privato e in quello pubblico, la diffusione di dati personali solo a precise condizioni, al di là dell'ipotesi dell'espresso consenso dell'interessato; in particolare, mentre i soggetti privati possono diffondere i dati personali in adempimento di un obbligo previsto da una legge, da un regolamento o dalla normativa comunitaria, i soggetti pubblici possono far ciò solo ove previsto da una norma di legge o di regolamento.

Con specifico riferimento ai trattamenti connessi all'impiego, da parte dei lavoratori, dei cartellini identificativi sul posto di lavoro, il cui obbligo di utilizzazione trova fondamento, a seconda del settore lavorativo privato o pubblico, in accordi aziendali, in regolamenti aziendali o in atti amministrativi d'organizzazione adottati a livello nazionale o locale, deve comunque trovare applicazione l'art. 9 della legge n. 675/1996 e, segnatamente, il principio di pertinenza e non eccedenza, sicché, in assenza di specifiche norme di legge o di regolamento che ne prescrivano analiticamente il contenuto, da detti cartellini debbono essere espunti tutti quei dati personali dei lavoratori che risultino non pertinenti o inutilmente eccedenti rispetto alle finalità di responsabilizzare maggiormente il personale o di fornire agli utenti una conoscenza sufficiente degli operatori con cui entrano in rapporto, ben potendosi, a seconda dei casi, limitare le indicazioni a un semplice codice identificativo ovvero al solo nome e/o ruolo professionale. Inoltre, è importante ricordare che, senza consenso del lavoratore titolare non si possono comunicare o pubblicare informazioni personali (foto, curricula). Il datore di lavoro può chiedere al dipendente di esporre un cartellino che lo renda identificabile per ragioni di trasparenza e di verifica del corretto funzionamento dell'azienda o dell'ufficio pubblico; tuttavia i dati riportati nella parte del cartellino visibile al pubblico devono essere pertinenti e non eccedenti rispetto alla finalità perseguita e la loro diffusione deve rispettare determinate condizioni. Qualora non vi

siano precise disposizioni di legge o di regolamento che prescrivano il contenuto dei cartellini identificativi, non è giustificabile che sia imposta la diffusione di "elementi identificativi personali non pertinenti ed inutilmente eccedenti rispetto alle finalità di responsabilizzare maggiormente il personale e di fornire agli utenti una conoscenza sufficiente degli operatori con cui entrano in rapporto".

Con parere espresso in data 11 dicembre 2000 il Garante ha precisato che non risulta di alcuna utilità che appaiano sul cartellino (o sulla parte del cartellino agevolmente visibile da chiunque) dati personali quali quelli identificativi delle generalità e di quelli anagrafici, a differenza dell'immagine fotografica, della definizione del ruolo professionale svolto ed eventualmente di un nome, numero o sigla identificativi, che già da soli possono permettere un agevole esercizio da parte dell'utente o del cliente dei loro diritti. In applicazione quindi del principio di pertinenza e di non eccedenza, appare ingiustificabile la compressione della riservatezza personale nei limiti suddetti. Ad analoghe conclusioni deve giungersi anche in riferimento al settore pubblico e non solo ovviamente in riferimento a rapporti di lavoro che siano stati integralmente "privatizzati". In alcuni atti amministrativi di natura organizzativa o con funzioni di indirizzo, sia a livello nazionale che a livello locale, si prescrive, al fine di una maggiore trasparenza e responsabilità soprattutto alla luce dei principi della legge 241/1990, che alcune strutture della pubblica amministrazione o i concessionari pubblici prevedano l'adozione da parte del loro personale di cartellini identificativi personali. Anche in questo caso, specie in assenza di precise disposizioni di legge o di regolamento che prescrivano puntualmente il contenuto dei cartellini identificativi, appare non giustificabile che amministrazioni pubbliche o concessionari pubblici impongano la diffusione di elementi identificativi personali non pertinenti ed inutilmente eccedenti rispetto alle finalità di responsabilizzare maggiormente il personale e di fornire agli utenti una conoscenza sufficiente degli operatori con cui entrano in rapporto.

Ancora una volta, quindi, il Garante ha chiarito che la diffusione di dati sensibili può essere superata solo dalla sussistenza di leggi specifiche che la impongano; in mancanza, deve essere condizionata e

subordinata ai concetti di "*pertinenza*" e "*non eccedenza*" di cui all'art. 11 del Codice in materia di protezione dei dati personali.

Provvedimenti del Garante

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor" – 22 ottobre 2015

in *G.U.* n. 271 del 20 novembre 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Visto l'art. 25, paragrafi nn. 1, 2 e 6 della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, ai sensi del quale i dati personali possono essere trasferiti in un paese non appartenente all'Unione europea qualora venga constatato dalla Commissione europea che il paese terzo garantisce un livello di protezione adeguato ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Considerato, altresì, che gli Stati membri europei devono adottare le misure necessarie per conformarsi alle decisioni della Commissione, rese ai sensi del paragrafo n. 6 del citato art. 25 della direttiva;

Vista la decisione del 26 luglio 2000 n. 2000/520/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) adottata dalla Commissione europea, ai sensi delle disposizioni sopra citate, secondo la quale i "Principi di approdo sicuro in materia di riservatezza" allegati alla medesima decisione, applicati in conformità agli orientamenti forniti da talune "Domande più frequenti" (FAQ) parimenti allegate, garantiscono un

livello adeguato di protezione dei dati personali trasferiti dalla Unione europea ad organizzazioni aventi sede negli Stati Uniti d'America sulla base della documentazione pubblicata dal Dipartimento del commercio statunitense ivi menzionata;

Visto il decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito "Codice") ed in particolare l'art. 44, comma 1, lett. b), ove è previsto che il trasferimento di dati personali diretto verso un paese non appartenente all'Unione europea è consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, individuate dall'Autorità anche con le suddette decisioni della Commissione europea;

Tenuto conto che questa Autorità il 10 ottobre 2001 con la deliberazione n. 36 (pubblicata sulla Gazzetta Ufficiale del 26 novembre n. 275 – Suppl. Ordinario n. 250, doc. web. n. 30939) ha autorizzato, ai sensi dell'art. 44, comma 1, lett. b) (già art. 28, comma 4, lett. g) della legge 31 dicembre 1996, n. 675), i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati nel rispetto dei "Principi di approdo sicuro in materia di riservatezza", applicati in conformità alle "Domande più frequenti" (FAQ) e all'ulteriore documentazione allegata alla decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE (c.d. regime di "Approdo sicuro", di seguito "Safe Harbor");

Considerato che la Corte di giustizia dell'Unione Europea (di seguito "Corte di giustizia") si è pronunciata il 6 ottobre 2015 in ordine alla causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner, dichiarando invalida la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE con la quale era stato ritenuto adeguato il livello di protezione dei dati personali garantito dagli Stati Uniti d'America nel contesto del c.d. regime di "Safe Harbor";

Preso atto, inoltre, delle osservazioni formulate dal Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46/CE, di seguito "Gruppo ex art. 29", nello "Statement of the Article 29 Working Party" del 16 ottobre 2015, in merito agli effetti della sentenza della Corte di

giustizia sui trasferimenti dei dati effettuati, in virtù della decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE, dal territorio dell'Unione europea verso gli Stati Uniti d'America;

Tenuto conto che il Garante ha reso l'autorizzazione di cui alla deliberazione n. 36 sulla base della decisione della Commissione in ordine all'adeguatezza del livello di protezione ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona offerto dal regime di "Safe Harbor" e che, pertanto, a seguito dell'emanazione della sentenza della Corte di giustizia sopra citata è venuto meno il presupposto di legittimità dei trasferimenti di dati personali posti in essere dal territorio nazionale verso le organizzazioni aventi sede negli Stati Uniti d'America che hanno aderito a tale regime;

Rilevato che i trasferimenti dei dati personali verso un paese non appartenente all'Unione europea possono essere effettuati sulla base anche di ulteriori presupposti di liceità, così come previsto negli artt. 43 ("Trasferimenti consentiti in Paesi terzi") e 44 ("Altri trasferimenti consentiti") del Codice;

Rilevato, con riferimento all'art. 43, che i dati in questione possono essere trasferiti sulla base di una delle deroghe di cui al comma 1 del citato articolo e, in particolare, qualora gli interessati abbiano espresso liberamente il loro consenso specifico e informato (cfr. lett. a));

Rilevato, altresì, con riferimento all'art. 44, che tali trasferimenti possano essere effettuati mediante l'utilizzo delle clausole contrattuali tipo (c.d. standard contractual clauses) di cui alle autorizzazioni rese, ex art. 44, comma 1, lett. b) del Codice, dal Garante il 10 ottobre 2001, con deliberazione n. 35 (doc. web. n. 42156), il 9 giugno 2005, con deliberazione n. 12 (doc. web. n. 1214121) e il 27 maggio 2010, con deliberazione n. 35 (doc. web n. 1728496, al riguardo si veda anche il successivo Provvedimento del Garante del 15 novembre 2012, doc. web. n. 2191156); o altrimenti in ragione dell'avvenuta adozione, nell'ambito di società appartenenti a un medesimo gruppo, delle regole di condotta di cui all'art. 44, comma 1, lett. a) del Codice, denominate Binding Corporate Rules (c.d. "Bcr", cfr. in ordine alle "Bcr for Controller", fra gli altri, i documenti del "Gruppo ex art. 29",

WP 74 del 3 giugno 2003, WP 108 del 14 aprile 2005 e WP 153 del 24 giugno 2008; mentre, per quanto riguarda le "Bcr for Processor", i documenti WP 195 del 6 giugno 2012 e WP 204 del 19 aprile 2013); o qualora vengano autorizzati dal Garante, ai sensi dell'art. 44, comma 1, lett. a) del Codice, sulla base di adeguate garanzie per i diritti dell'interessato individuate dal medesimo anche in relazione a garanzie prestate con un contratto;

Ritenuto che, in ogni caso, alla luce delle considerazioni contenute nella predetta sentenza della Corte di giustizia, la protezione del diritto fondamentale al rispetto della vita privata a livello europeo richiede che deroghe e limitazioni alla protezione dei dati personali trovino applicazione solo nella misura in cui le stesse siano strettamente necessarie (cfr. Corte di giustizia dell'Unione europea causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner, paragrafo n. 92 e cause riunite C-293/12 and C-594/12, Digital Rights Ireland and Others) e che, ai sensi dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea, ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati deve aver diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel medesimo articolo;

Ritenuta la necessità, per le ragioni sopra esposte, di disporre la caducazione dell'autorizzazione adottata con la deliberazione del Garante n. 36 del 10 ottobre 2001 e per l'effetto di vietare i trasferimenti di dati ivi descritti; tutto ciò nei termini di cui al seguente dispositivo;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

TUTTO CIÓ PREMESSO IL GARANTE

1) dispone la caducazione dell'autorizzazione adottata dal Garante in data 10 ottobre 2001 con deliberazione n. 36 e per l'effetto vieta, ai sensi degli artt. 154, comma 1, lett. d) e 45 del Codice, ai soggetti

esportatori di trasferire, sulla base di tale delibera e dei presupposti indicati nella medesima, i dati personali dal territorio dello Stato verso gli Stati Uniti d'America;

2) si riserva, ai sensi dell'art. 154, comma 1, lettere da a) a d) del Codice, di svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, i provvedimenti previsti dal Codice;

3) dispone la trasmissione del presente provvedimento all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 22 ottobre 2015

IL PRESIDENTE
Soro

RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Costituzione di una banca dati relativa a morosità intenzionali della clientela del settore telefonico (S.I.Mo.I.Tel) – 8 ottobre 2015

in *G. U.* n. 257 del 4 novembre 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

Visto il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice");

Esaminata la richiesta presentata da Assotelecomunicazioni (di seguito, ASSTEL) relativa all'istituzione di una banca dati interoperatore contenente informazioni relative alle morosità nel settore della telefonia;

Visti gli esiti della consultazione pubblica indetta con delibera n. 154 del 27 marzo 2014 (reperibile sul sito istituzionale del Garante http://www.garanteprivacy.it, doc. web n. 3041680) sullo schema di provvedimento recante "Costituzione di una banca dati dei clienti morosi nell'ambito dei servizi di comunicazione elettronica";

Viste in particolare le osservazioni pervenute da alcune associazioni di consumatori rappresentative degli interessi degli utenti dei servizi telefonici;

Considerati gli esiti dei successivi incontri, anche di carattere tecnico, intercorsi tra questa Autorità e i rappresentanti delle associazioni dei consumatori, ASSTEL e gli operatori di telefonia che hanno inteso partecipare;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore la dott.ssa Giovanna Bianchi Clerici;

PREMESSO

1. Richiesta di ASSTEL.

ASSTEL, quale associazione di categoria che rappresenta le imprese della tecnologia dell'informazione esercenti servizi di telecomunicazione fissa e mobile, ha rappresentato l'intenzione degli operatori di comunicazione elettronica di "procedere (…) alla sottoscrizione di un accordo interoperatore per l'istituzione di una Banca dati finalizzata alla verifica dell'affidabilità e della puntualità nei pagamenti nel settore dei servizi di comunicazione elettronica" (c.d. SIT- Sistema Informatico Integrato). Tale banca dati, secondo quanto sostenuto da ASSTEL, permetterebbe agli operatori di settore di condividere le informazioni sui comportamenti debitori, in particolare dei clienti degli operatori telefonici, consentendo all'operatore ricevente di conoscere, in occasione della presentazione di una richiesta di instaurazione di un rapporto contrattuale da parte di un nuovo cliente, eventuali posizioni di indebitamento nei confronti di altri operatori.

Secondo ASSTEL, la costituzione del SIT, resa ancora più urgente dall'intervenuto processo di liberalizzazione avviato in Italia anche nel settore della telefonia, si renderebbe necessaria per assicurare l'ordinato sviluppo del mercato telefonico, attesa l'impossibilità di effettuare verifiche sulle eventuali morosità pregresse. Il perdurare di tale situazione – secondo i dati forniti da ASSTEL – produrrebbe un forte incremento delle perdite registrate dagli operatori, anche in conseguenza delle nuove offerte contrattuali, che propongono forme di contratto "post pagato" associate alla vendita a rate di terminali telefonici e di prodotti "ad alto valore tecnologico e ad alti costi, messi a disposizione della clientela con schemi di pagamento dilazionato"; l'aumento dei comportamenti insolventi, secondo quanto asserito da ASSTEL, rischierebbe di incidere negativamente non solo sugli operatori, ma anche sugli altri utenti che, pur adempiendo regolarmente alle obbligazioni, vedrebbero ridotta o resa meno

conveniente la possibilità di accedere a forme di contratto "post pagato".

2. L'istruttoria svolta.

All'esito dell'attività istruttoria relativa alla suddetta istanza, l'Autorità aveva predisposto uno schema di provvedimento che delineava i contorni di un'ipotetica banca dati. Tale provvedimento, con delibera n. 154 del 27 marzo 2014, è stato posto in consultazione pubblica sul sito dell'Autorità. Preso atto della rilevanza e della complessità delle osservazioni ricevute, l'Ufficio ha ritenuto di doversi incontrare con le Parti coinvolte dalle misure prescritte nel provvedimento (associazioni a tutela dei consumatori e operatori telefonici, inclusa ASSTEL quale associazione di categoria), per valutare le eventuali modifiche ed integrazioni da apportare allo schema proposto.

Nel corso degli incontri, che hanno avuto luogo tra dicembre 2014 e giugno 2015, è emersa la necessità di una rilevante rivisitazione della natura e delle caratteristiche della banca dati rispetto a quella proposta nello schema di provvedimento oggetto di consultazione. In particolare, le Parti, condividendo l'orientamento espresso negli anni dal Garante circa il pericolo insito nella proliferazione delle cd. black list (sul punto v. paragrafo 3 del presente provvedimento), hanno convenuto di definire diversamente l'ambito soggettivo e oggettivo della banca dati stessa.

3. Quadro normativo ed orientamenti del Garante in materia di "black list".

Nel corso degli anni, il tema della costituzione di banche dati settoriali contenenti dati relativi a inadempimenti o ritardati pagamenti degli utenti ha formato oggetto di valutazione da parte del Garante italiano e del Gruppo di lavoro dei Garanti europei previsto dall'art. 29 della direttiva 95/46/CE. In particolare, quest'ultimo ha adottato un parere il 3 ottobre 2002 "Documento di lavoro sulle liste nere" (WP65), con il quale, nel rappresentare la necessità di stabilire in questo ambito

criteri, indirizzi o direttrici d'intervento comuni tra gli Stati membri, ha evidenziato che per la creazione di tali archivi in specifici settori economici occorre mantenere un equilibrio tra "l'interesse legittimo del responsabile del trattamento di sapere se chi richiede un credito sia registrato per mancati pagamenti" e le conseguenze negative che tale trattamento può comportare per l'interessato (v. cit. Parere WP65, p. 4).

Il processo di liberalizzazione introdotto in Italia con il recepimento di alcune direttive europee ha mutato il quadro in particolare nei settori delle telecomunicazioni e dell'energia elettrica e del gas (c.d. utilities), che hanno dovuto adattarsi alla nascita di un mercato concorrenziale, che ha reso indispensabile aumentare l'offerta di servizi (specie quelli tecnologicamente più avanzati) e, al contempo, ridurre i prezzi al dettaglio.

Con specifico riferimento al settore delle comunicazioni elettroniche, il processo di liberalizzazione è stato avviato a livello europeo con il c.d. "pacchetto delle direttive comunitarie del 2002", modificato e integrato a più riprese dal legislatore comunitario (Direttive 2002/19/CE, 2002/20/CE e 2002/21/CE, modificate e integrate dalla Direttiva 2009/140/CE del Parlamento europeo e del Consiglio; Direttive 2002/22/CE, 2002/58/CE, modificate dalla Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 e dalla Direttiva 2009/140/CE del 25 novembre 2009 del Parlamento europeo e del Consiglio) e recepito nell'ordinamento italiano con il d.lg. 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche), da ultimo modificato dal d.lg. 28 maggio 2012, n. 70.

Il nuovo quadro normativo ha profondamente mutato il settore delle comunicazioni elettroniche, il ruolo rivestito dai relativi operatori ed il rapporto contrattuale che li lega ai propri clienti.

Il descritto processo di liberalizzazione, ha comportato, tuttavia, anche un aumento di morosità intenzionali da parte di chi agisce con la precisa volontà di usufruire dei servizi offerti dagli operatori telefonici, senza procedere ai relativi pagamenti.

In considerazione di ciò, il legislatore ha iniziato ad ammettere la possibilità di costituire banche dati di clienti inadempienti nei settori sopra descritti, ad iniziare da quello del gas e dell'energia elettrica (legge 13 agosto 2010, n. 129, art. 1-bis – di conversione in legge, con modificazioni, del d.l. 8 luglio 2010, n. 105, recante Misure urgenti in materia di energia).

Successivamente, lo stesso legislatore è intervenuto anche nel settore della telefonia stabilendo che "possono avere accesso" ai Sistemi di informazione creditizia (Sic) anche soggetti diversi da quelli specificamente menzionati dal codice deontologico di settore, tra cui i fornitori di servizi di comunicazione elettronica e di servizi interattivi associati, "di cui al comma 5 dell'art. 30-ter del decreto legislativo 13 agosto 2010, n. 141 (art. 6-bis del d.l. 13 agosto 2011, n. 138; convertito con modificazioni dalla legge 14 settembre 2011, n. 148)".

Al riguardo, l'Autorità pur ribadendo che, in linea di principio, sia opportuno evitare una proliferazione indiscriminata di archivi settoriali nei più diversi ambiti economici, che causerebbe un diffuso e potenzialmente pericoloso trattamento di dati degli interessati, ritiene che, con specifico riferimento alle morosità intenzionali della clientela nel settore della telefonia, possa prevedersi la costituzione di una banca dati. Ciò muovendo dalla considerazione riconosciuta dal legislatore che definisce questo settore "di preminente interesse generale" (art. 3, comma 2, Codice delle comunicazioni elettroniche) e di "pubblica utilità" (legge 14 novembre 1995, n. 481 recante Norme per la concorrenza e la regolazione dei servizi di pubblica utilità. Istituzione delle Autorità di regolazione dei servizi di pubblica utilità); dalla peculiare tipologia dei servizi offerti in tale ambito; dalla natura regolamentata di questo mercato – soprattutto a seguito del descritto processo di liberalizzazione – per il quale è prevista una specifica e rigida normativa comunitaria e nazionale all'interno della quale gli operatori sono tenuti ad operare; dall'attività di controllo e di regolazione effettuata in tali mercati dalle Autorità di settore.

4. Denominazione della banca dati relativa a morosità intenzionali della clientela nel settore telefonico; partecipanti e gestore della banca dati.

Considerato quanto sopra esposto, la banca dati finalizzata alla prevenzione delle morosità intenzionali della clientela titolare di contratti per la fornitura di servizi di telefonia fissa e mobile post-pagata, acquisterà la denominazione di "Sistema informativo sulle morosità intenzionali nel settore della telefonia" (di seguito, S.I.Mo.I.Tel.).

Il "gestore" del S.I.Mo.I.Tel. è il soggetto privato titolare del trattamento dei dati personali registrati nel sistema e che lo gestisce stabilendone anche le modalità di funzionamento e di utilizzazione nel rispetto delle misure prescritte dal presente provvedimento.

I "partecipanti" al S.I.Mo.I.Tel. sono esclusivamente operatori di telefonia fissa o mobile, titolari del trattamento dei dati personali degli interessati, raccolti in relazione a rapporti di fornitura dei servizi di telefonia fissa e mobile che, in virtù di un accordo con il gestore della banca dati, partecipano al relativo sistema e possono utilizzare i dati in esso contenuti, obbligandosi a comunicare al gestore i predetti dati in un quadro di reciprocità con gli altri partecipanti.

5. Ambito soggettivo: interessati del trattamento.

Come noto, l'art. 40 del d.l. 6 dicembre 2011, n. 201 (convertito, con modificazioni, in legge 22 dicembre 2011, n. 214) ha apportato significative modifiche alla disciplina del Codice, espungendo dalla nozione di "dato personale" e di "interessato" le persone giuridiche, gli enti e le associazioni (v. art. 4, comma 1, lett. b) e i) dello stesso Codice). Peraltro, le disposizioni contenute nel capo 1 del titolo X del Codice che riguardano i "contraenti", continuano a trovare applicazione anche alle persone giuridiche, enti ed associazioni (in senso conforme v. anche: provv. 20 settembre, doc. web n. 2094932). Poiché il trattamento dei dati oggetto del presente provvedimento verte sulla medesima platea di soggetti previsti dal citato titolo X, ne consegue che il medesimo provvedimento troverà applicazione anche

alle persone giuridiche, enti, associazioni. Si conferma l'applicabilità delle disposizioni in materia di protezione dei dati personali anche alle ditte individuali e ai liberi professionisti, in qualità di interessati (v. parere 25 giugno 2015, doc. web n. 4169267; provv. 23 ottobre 2014, doc. web n. 3676822; parere 9 febbraio 2012, doc. web n. 1876517).

6. Finalità, necessita e proporzionalità.

Il trattamento dei dati personali contenuti nel S.I.Mo.I.Tel. sarà effettuato dal gestore e dai partecipanti esclusivamente per verificare l'eventuale presenza di morosità intenzionali, dovendosi intendere per tali i mancati pagamenti non dovuti a circostanze impreviste e contingenti, ma ad una precisa volontà del soggetto.

L'accesso al S.I.Mo.I.Tel. sarà consentito al partecipante esclusivamente in caso di formale richiesta di instaurazione di un rapporto contrattuale o di un contratto già in essere per la fornitura di servizi di telefonia. Il trattamento dei dati dovrà avvenire nel rispetto dei principi di necessità, liceità, correttezza, qualità dei dati e proporzionalità (artt. 3 e 11 del Codice). In particolare, i sistemi informativi e i programmi informatici dovranno essere configurati, sin dall'origine, in modo da ridurre al minimo l'utilizzo delle informazioni relative agli interessati (art. 3 del Codice); inoltre, i dati personali raccolti dovranno essere pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d), del Codice).

7. Informativa.

Al momento della stipula del contratto, il partecipante fornirà all'interessato l'informativa ai sensi dell'art. 13 del Codice, anche con riguardo al trattamento dei dati personali effettuato nell'ambito del S.I.Mo.I.Tel. L'informativa, nel descrivere le finalità e modalità del trattamento, dovrà recare, in modo chiaro e preciso, anche le seguenti indicazioni:

− estremi identificativi e caratteristiche del S.I.Mo.I.Tel., quale soggetto cui sono comunicati i dati, denominazione e sede del gestore;
− soggetti partecipanti eventualmente indicati per categoria;

− i tempi di conservazione dei dati.

L'informativa sarà fornita agli interessati individualmente e per iscritto e, se inserita in un modulo utilizzato dal partecipante, sarà evidenziata e collocata in modo autonomo e unitario in parti distinte da quelle relative ad altre finalità del trattamento effettuato dal medesimo partecipante.

In caso di contratti stipulati telefonicamente o telematicamente, la stessa sarà resa avvalendosi di modalità in grado di consentire la dimostrazione dell'avvenuto adempimento dell'obbligo di informativa (ad es. registrazione della telefonata).
In ogni caso il testo dell'informativa dovrà essere pubblicato da ciascun partecipante sul proprio sito web.

Il partecipante, inoltre, fornirà l'informativa anche sul trattamento dei dati effettuato dal gestore il quale, a sua volta, renderà una più dettagliata informativa sui medesimi trattamenti attraverso il proprio sito web.

8. Bilanciamento di interessi.

Poiché il sistema che si intende realizzare avrà ad oggetto esclusivamente informazioni negative, si tratta di verificare – per garantirne l'effettiva utilità – se il trattamento dei dati personali degli interessati, ai sensi dell'art. 24 del Codice, possa basarsi su un presupposto equipollente al consenso.

Nonostante i rischi a cui possono essere esposti i diritti degli interessati in ragione della costituzione del S.I.Mo.I.Tel., deve comunque essere considerato che la normativa sulle liberalizzazioni nel settore dei servizi di comunicazione elettronica garantisce ai consumatori la possibilità di transitare con facilità da un operatore all'altro per ottenere servizi migliori a costi più contenuti, sicché lo scambio di informazioni riguardanti gli inadempimenti può risultare assai rilevante per la corretta gestione del rapporto contrattuale, in quanto necessario per valutare e contenere situazioni di morosità intenzionali che, ove non circoscritte, nel lungo periodo, andrebbero ad incidere non solo sugli stessi operatori, ma anche sugli altri

interessati, i quali potrebbero essere costretti a sopportare costi ulteriori, altrimenti non dovuti.
Ciò premesso, nel fare applicazione dell'istituto del bilanciamento di interessi di cui all'art. 24, comma 1, lett. g), del Codice, si deve ritenere che il trattamento delle informazioni relative alle morosità intenzionali effettuato nell'ambito del sistema che si intende realizzare, possa essere effettuato anche in assenza del consenso degli interessati, potendosi valutare come prevalente l'interesse -non solo degli operatori, ma anche degli interessati regolarmente adempienti- al corretto funzionamento di un sistema volto a favorire l'esatta gestione dei rapporti contrattuali alle migliori condizioni praticabili sul mercato.

9. Requisiti per l'iscrizione nel S.I.Mo.I.Tel.

L'interessato sarà iscritto nel S.I.Mo.I.Tel. al contemporaneo verificarsi dei seguenti presupposti:

− recesso dal contratto ad iniziativa di una delle parti esercitato da non meno di tre mesi;

− importo insoluto per ogni singolo operatore di non meno di 150 (centocinquanta) euro;

− presenza di fatture non pagate nei primi sei mesi successivi alla stipula del contratto;

− assenza di altri rapporti contrattuali post-pagati, attivi e regolari nei pagamenti con lo stesso operatore;

− assenza di formali reclami/contestazioni, istanze di conciliazioni o comunque istanze di definizione di controversie dinanzi agli organi competenti inoltrate dal cliente;

− invio a cura del partecipante all'interessato, almeno trenta giorni solari antecedenti all'iscrizione nel S.I.Mo.I.Tel., della comunicazione di preavviso di imminente iscrizione.

Il preavviso sarà inviato con comunicazione scritta tracciabile (a titolo esemplificativo, raccomandata A/R con avviso di ricevimento, posta

elettronica certificata) e comprovante la data e le modalità utilizzate per l'invio.

10. Requisiti e categorie di dati.

Il trattamento effettuato nell'ambito del S.I.Mo.I.Tel. avrà ad oggetto solo le informazioni di carattere negativo connesse all'inadempimento intenzionale dell'interessato verso i partecipanti.

Il trattamento non potrà riguardare dati sensibili e giudiziari, né comportare l'uso di tecniche o di sistemi automatizzati di credit scoring.

Nel S.I.Mo.I.Tel. potranno essere trattate le seguenti categorie di dati, che il gestore indicherà in un elenco reso agevolmente disponibile sul proprio sito, da comunicare anche agli interessati su eventuale loro richiesta:

− dati anagrafici, codice fiscale o partita Iva;

− importo totale della morosità per ogni singolo operatore telefonico;

− data di inizio del contratto;

− data di recesso dal contratto;

− data di inserimento nel S.I.Mo.I.Tel.;

− numero di fatture non pagate;

− partecipante che ha comunicato al S.I.Mo.I.Tel. i dati personali relativi alla morosità intenzionale;

− data e modalità di inoltro del preavviso;

− indicazione esplicita (ad es. con flag su check box) alla data di inserimento dei dati dell'interessato nel S.I.Mo.I.Tel., di assenza di reclami/contestazioni, istanze di conciliazioni e di definizione di controversie dinanzi agli organi competenti inoltrate dal cliente.

11. Modalità di raccolta, registrazione dei dati ed esito dell'accesso al S.I.Mo.I.Tel. a cura dei partecipanti.

Il partecipante dovrà adottare idonee procedure di verifica per garantire la correttezza e l'esattezza dei dati comunicati al gestore e risponderà tempestivamente alle richieste di verifica di quest'ultimo, anche a seguito dell'esercizio dei diritti da parte dell'interessato ai sensi dell'art. 7 del Codice, così da garantire, in tale ultimo caso, il rispetto dei termini previsti dall'art. 146, comma 2, del Codice.

Eventuali operazioni di cancellazione, integrazione, aggiornamento o modificazione dei dati registrati nel S.I.Mo.I.Tel. dovranno essere effettuate direttamente dal partecipante che li ha comunicati, se tecnicamente possibile, ovvero dal gestore, su richiesta del medesimo partecipante o d'intesa con esso, anche a seguito dell'esercizio dei diritti da parte dell'interessato o in attuazione di un provvedimento emesso dall'autorità giudiziaria o dal Garante.

In caso di rifiuto di una richiesta volta ad instaurare un rapporto contrattuale, il partecipante, ove abbia consultato il S.I.Mo.I.Tel., sarà tenuto a comunicare all'interessato tale circostanza.

L'esito dell'interrogazione al S.I.Mo.I.Tel. da parte dei partecipanti avverrà con modalità a "semaforo":

− verde: soggetto non presente nel S.I.Mo.I.Tel.;

− rosso: soggetto presente per segnalazioni di morosità intenzionali effettuate da uno o più operatori.

12. Utilizzazione dei dati.

Il S.I.Mo.I.Tel. sarà accessibile solo da un numero limitato di responsabili e di incaricati del trattamento designati per iscritto dai partecipanti e/o dal gestore del sistema (artt. 4, comma 1, lett. g) e h), 29 e 30 del Codice).

Non sarà consentito l'accesso al S.I.Mo.I.Tel. da parte di terzi, fatte salve le richieste provenienti da organi giudiziari e dalle Forze dell'ordine.

13. Esercizio dei diritti da parte degli interessati.

In relazione ai dati personali registrati nel S.I.Mo.I.Tel., gli interessati potranno esercitare i loro diritti secondo le modalità stabilite dagli artt. 7 e ss. del Codice, sia presso i partecipanti che li hanno comunicati, sia presso il gestore.

Nella richiesta con la quale eserciterà i propri diritti, l'interessato dovrà indicare il proprio codice fiscale e/o la partita Iva, al fine di agevolare la ricerca dei dati che lo riguardano.

Il partecipante che risulti destinatario di una richiesta ai sensi dell'art. 7 del Codice riguardo alle informazioni registrate nel S.I.Mo.I.Tel. dovrà fornire riscontro all'interessato nei termini previsti dall'art. 146, commi 2 e 3, del Codice. Ove la richiesta sia rivolta al gestore, anch'esso provvederà nei medesimi termini, consultando, se necessario, il partecipante.

Qualora si rendesse necessario svolgere ulteriori verifiche con il partecipante, il gestore informerà l'interessato di tale circostanza entro quindici giorni, indicando, per la risposta, un nuovo termine, che comunque non sarà superiore a quindici giorni.

14. Tempi di conservazione.

I dati contenuti nel S.I.Mo.I.Tel. saranno conservati per 36 (trentasei mesi) dalla data di recesso dal contratto in caso di inadempimenti non regolarizzati.

Al termine del periodo deve essere prevista la cancellazione automatica dell'informazione.

Diversamente, la cancellazione del nominativo dell'interessato dal S.I.Mo.I.Tel. avverrà entro 7 (sette) giorni lavorativi nei casi di seguito indicati:

− ricezione da parte del partecipante di una comunicazione inviata dal cliente di regolarizzazione del debito accompagnata dalla prova dell'avvenuto pagamento;

− avvenuto pagamento del debito − comprovato dalla registrazione dell'incasso sui sistemi dell'operatore unitamente al successivo abbinamento dell'incasso al nominativo dell'interessato − in mancanza di invio di una comunicazione di regolarizzazione del debito da parte del cliente;

− definizione di un accordo tra le Parti che stabilisca un piano di rientro rateizzato.

15. Misure di sicurezza.

Il gestore e i partecipanti adottano le misure tecniche, logiche, informatiche, procedurali, fisiche ed organizzative idonee a garantire la sicurezza, l'integrità e la riservatezza dei dati personali contenuti nel S.I.Mo.I.Tel. in conformità alla disciplina in materia di protezione dei dati personali (artt. 31 e ss. del Codice).

La banca dati dovrà essere separata, logicamente e fisicamente, da eventuali altre banche dati del gestore.

Il gestore adotterà adeguate misure di sicurezza al fine di garantire il corretto e regolare funzionamento del sistema, nonché il controllo degli accessi, secondo le modalità previste dall'Allegato B. al Codice (Disciplinare tecnico in materia di misure minime di sicurezza).

Tutti gli accessi al sistema, da parte del gestore e dei partecipanti, saranno registrati e memorizzati per verificarne la legittimità.

Le interrogazioni dovranno sempre riferirsi a singoli interessati e non saranno in nessun caso consentite interrogazioni massive della banca dati da parte dei partecipanti.

Le informazioni così ottenute non potranno essere in alcun modo conservate o memorizzate dai partecipanti per usi successivi.

I partecipanti non potranno creare una propria copia, nemmeno parziale, della banca dati.

16. Notificazione del trattamento.

Resta fermo l'obbligo per il gestore di notificare al Garante il trattamento dei dati secondo le modalità previste dall'art. 37, comma 1, lett. f), del Codice.

17. Comunicazioni al Garante.

17.1. Una volta che gli operatori telefonici avranno individuato il soggetto cui affidare – in qualità di autonomo titolare del trattamento – la gestione del S.I.Mo.I.Tel.:

a) comunicheranno all'Autorità gli estremi identificativi e l'ubicazione della banca dati;

b) invieranno all'Autorità, almeno tre mesi prima dell'effettiva messa in opera del sistema, copia dell'accordo che verrà sottoscritto dalle parti per la costituzione della banca dati, al fine di valutarne la conformità alle prescrizioni contenute nel presente provvedimento.

17.2. Entro 15 giorni dalla data di sottoscrizione dell'accordo di cui alla precedente lett. b), il gestore provvederà ad inviare al Garante l'elenco dei partecipanti che hanno formalizzato la sottoscrizione; parimenti provvederà all'invio al Garante dei nominativi dei successivi eventuali partecipanti.

17.3. Il gestore comunicherà a questa Autorità la messa in opera del S.I.Mo.I.Tel. almeno 15 giorni prima del relativo avvio.

18. Fase di prima applicazione.

18.1. In relazione ai rapporti già pendenti alla data di pubblicazione del presente provvedimento in Gazzetta Ufficiale ed entro 60 giorni da tale pubblicazione, ciascun partecipante informerà gli interessati, ai sensi dell'art. 13 del Codice, attraverso un messaggio breve e in stile colloquiale (inserito sul proprio sito web ed agevolmente accessibile, nonché in luoghi dove i partecipanti esercitano la loro attività, in particolare, con affissioni in bacheche o locali, avvisi e cartelli agli sportelli dedicati alla clientela), in ordine al trattamento dei dati

personali effettuato nell'ambito del S.I.Mo.I.Tel. L'informativa, avrà ad oggetto:

− gli estremi identificativi e le caratteristiche generali del S.I.Mo.I.Tel., quale soggetto cui sono comunicati i dati ed indicazioni della denominazione e della sede del gestore, ove già individuato. Qualora alla data sopra indicata (60 giorni dalla pubblicazione in G.U.) il gestore non fosse stato ancora individuato, i partecipanti integreranno l'informativa resa con tale indicazione appena possibile;

− i soggetti partecipanti eventualmente indicati per categoria;

− i tempi di conservazione dei dati;

Il completamento dell'informativa, con tutti gli elementi previsti dall'art. 13 del Codice e da rendere mediante elaborazione di un testo articolato, sarà effettuato, senza oneri per gli interessati, sul sito web di ciascun partecipante.

In relazione ai rapporti contrattuali stipulati successivamente alla data di pubblicazione in Gazzetta Ufficiale, l'informativa sarà fornita agli interessati secondo le modalità individuate al paragrafo 7. del presente provvedimento.

18.2. Decorsi 120 giorni dalla data di pubblicazione in Gazzetta Ufficiale del presente provvedimento, i partecipanti potranno iniziare ad inserire nel S.I.Mo.I.Tel. i dati relativi ai clienti i cui contratti sono stati oggetto del recesso di cui al paragrafo 9.

TUTTO CIÒ PREMESSO, IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. c), del Codice prescrive ai titolari del trattamento (partecipanti e gestore del S.I.Mo.I.Tel.), quali misure necessarie, quelle indicate in motivazione ai paragrafi 7.; da 9. a 12.; 14; 17. e 18.;

2. ai sensi dell'art. 24, comma 1, lett. g) del Codice, ritiene che il trattamento dei dati personali nell'ambito del S.I.Mo.I.Tel. possa essere effettuato dai partecipanti e dal gestore della banca dati anche senza il consenso degli interessati, purché nei limiti e alle condizioni indicate in motivazione;

3. ai sensi dell'art. 143, comma 2, del Codice, dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia– Ufficio pubblicazione leggi e decreti, affinché venga pubblicato nella Gazzetta Ufficiale della Repubblica Italiana.

La violazione delle misure prescritte nel presente provvedimento, ferme restando le sanzioni amministrative, civili e penali previste dalla normativa vigente, sarà sanzionata nei termini previsti dall'art. 162, comma 2-ter, del Codice.

Roma, 8 ottobre 2015

IL PRESIDENTE
Soro

IL RELATORE
Bianca Clerici

IL SEGRETARIO GENERALE
Busia

Giurisprudenza

CORTE DI GIUSTIZIA UE, Terza Sezione, sentenza 1° ottobre 2015, causa C-230/14

Rinvio pregiudiziale – Tutela delle persone fisiche con riguardo al trattamento dei dati personali – Direttiva 95/46/CE – Articoli 4, paragrafo 1, e 28, paragrafi 1, 3 e 6 – Responsabile del trattamento formalmente stabilito in uno Stato membro – Violazione del diritto alla protezione dei dati personali con riguardo alle persone fisiche in un altro Stato membro – Determinazione del diritto applicabile e dell'autorità di controllo competente – Esercizio dei poteri dell'autorità di controllo – Potere sanzionatorio

Sentenza

1. La domanda di pronuncia pregiudiziale verte sull'interpretazione degli articoli 4, paragrafo 1, lettera a), e 28, paragrafi 1, 3 e 6, della 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 (GU L 281, pag. 31).

2. Tale domanda è stata presentata nell'ambito di una controversia tra la Weltimmo s. r. o. (in prosieguo: la «Weltimmo»), società la cui sede è in Slovacchia, e la Nemzeti Adatvédelmi és Információszabadság Hatóság (autorità nazionale incaricata della protezione dei dati e della libertà dell'informazione; in prosieguo: l'«autorità ungherese di controllo») in merito a un'ammenda comminata da quest'ultima per violazione della legge n. CXII del 2011 sul diritto di autodeterminazione in materia di informazione e sulla libertà di informazione (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény; in prosieguo: la «legge sull'informazione»), che ha recepito la direttiva 95/46 nel diritto ungherese.

Contesto normativo
Il diritto dell'Unione

3. I considerando 3, 18 e 19 della direttiva 95/46 enunciano quanto segue:
«(3) considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo [26 TFUE], è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona;
(...)
(18) considerando che, onde evitare che una persona venga privata della tutela cui ha diritto in forza della presente direttiva, è necessario che qualsiasi trattamento di dati personali effettuato nella Comunità rispetti la legislazione di uno degli Stati membri; che, a questo proposito, è opportuno assoggettare i trattamenti effettuati da una persona che opera sotto l'autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato;
(19) considerando che lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile; che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo; che quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, in particolare per mezzo di filiali, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi».
4. L'articolo 2 della direttiva 95/46 così prevede:
«Ai fini della presente direttiva si intende per:
(...)
b) "trattamento di dati personali ['feldolgozása']" (trattamento ["feldolgozás"]): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, 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»;
(...)».
5. L'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 così dispone:
«1.Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:
a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile».
6. Ai termini dell'articolo 28, paragrafi 1, 3 e 6, della direttiva 95/46:
«1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri.
Tali autorità sono pienamente indipendenti nell'esercizio delle loro funzioni.
(...)
3. Ogni autorità di controllo dispone in particolare:
– di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo,
– di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;

– del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È ammesso il ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.
(...)
6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.
Le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile».

Il diritto ungherese

7. L'articolo 2, paragrafo 1, della legge sull'informazione così prevede:
«Rientrano nell'ambito di applicazione della presente legge tutte le operazioni di trattamento ed elaborazione dei dati effettuate in territorio ungherese con riguardo a dati di persone fisiche, dati di interesse pubblico o dati accessibili per motivi di interesse pubblico».
8. L'articolo 3, paragrafi 10 e 17, de la legge sull'informazione contiene le seguenti definizioni:
«10. "trattamento dei dati" ("adatkezelés"): ogni operazione o insieme di operazioni realizzate relativamente ai dati, a prescindere dalla procedura impiegata, in particolare la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'impiego, la richiesta, la trasmissione, la pubblicazione, il raffronto o l'interconnessione, il congelamento, la cancellazione o la distruzione, nonché il divieto di altre forme di impiego dei dati, la ricezione di fotografie, suoni o immagini o la registrazione di caratteristiche fisiche necessarie per l'identificazione delle persone (ad esempio, impronte digitali o del palmo della mano, campioni di DNA o immagini dell'iride);

(...)
17. "elaborazione dei dati" ["adatfeldolgozás"]: l'esecuzione di compiti tecnici in relazione alle operazioni di trattamento dei dati, a prescindere dal metodo e dallo strumento impiegato per lo svolgimento delle operazioni, nonché il luogo di esecuzione delle stesse, sempre che i suddetti compiti vengano eseguiti in relazione ai dati».

Procedimento principale e questioni pregiudiziali

9. La Weltimmo, che ha sede in Slovacchia, gestisce un sito Internet di annunci immobiliari riguardanti beni situati in Ungheria. Nell'ambito di tale attività, essa tratta i dati personali degli inserzionisti. Gli annunci sono gratuiti per un mese, trascorso il quale diventano a pagamento. Allo scadere del periodo gratuito molti inserzionisti hanno inviato un messaggio di posta elettronica chiedendo la cancellazione dei propri annunci e dei propri dati personali. La Weltimmo, però, non ha cancellato tali dati e ha fatturato i servizi forniti. A fronte del mancato pagamento delle fatture, la ricorrente ha trasmesso ad alcune agenzie di recupero crediti i dati personali degli inserzionisti coinvolti.
10. In seguito ai reclami presentati dagli inserzionisti, l'autorità ungherese di controllo si è dichiarata competente ex articolo 2, paragrafo 1, della legge sull'informazione, ritenendo che la raccolta dei dati in questione era avvenuta in territorio ungherese e costituiva un'operazione di trattamento ed elaborazione dei dati con riguardo a persone fisiche. Ritenendo che la Weltimmo avesse violato la legge sull'informazione, tale autorità di controllo ha imposto a detta società un'ammenda di dieci milioni di fiorini ungheresi (HUF) (circa 32 000 euro).
11. La Weltimmo ha allora adito il Fővárosi Közigazgatási és Munkaügyi Bíróság (tribunale amministrativo e del lavoro di Budapest), il quale ha considerato che non poteva ammettersi, a favore della ricorrente, l'assenza della sede o dello stabilimento in Ungheria, dal momento che la fornitura dei dati relativi agli immobili ungheresi interessati e il trattamento di tali dati avevano avuto luogo in Ungheria. Detto tribunale ha tuttavia annullato la decisione

dell'autorità ungherese di controllo per altri motivi, attinenti alla scarsa chiarezza di alcuni fatti.
12. Nel ricorso in cassazione la Weltimmo ha chiesto al giudice del rinvio che sia dichiarata l'inutilità di procedere a un ulteriore chiarimento dei fatti giacché, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, l'autorità ungherese di controllo non era competente e non poteva applicare il diritto ungherese nei confronti di un fornitore di servizi stabilito in un altro Stato membro. La Weltimmo ha sostenuto che, conformemente all'articolo 28, paragrafo 6, della direttiva 95/46, detta autorità avrebbe dovuto invitare la sua omologa slovacca ad agire al posto suo.
13. L'autorità ungherese di controllo ha sostenuto che la Weltimmo aveva, in Ungheria, un rappresentante cittadino ungherese, ossia uno dei titolari di tale società, che l'aveva rappresentata sia nel procedimento amministrativo sia in quello giudiziario in tale Stato membro. Tale autorità ha aggiunto che i server Internet della Weltimmo pare fossero ubicati in Germania o in Austria, ma che i titolari della medesima società abitavano in Ungheria. Infine, secondo detta autorità, si evince dall'articolo 28, paragrafo 6, della direttiva 95/46 che essa era in ogni caso competente ad agire a prescindere dal diritto applicabile.
14. Nutrendo dubbi sull'individuazione del diritto applicabile e sulle competenze dell'autorità ungherese di controllo alla luce degli articoli 4, paragrafo 1, e 28 della direttiva 95/46, la Kúria (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:
«1) Se l'articolo 28, paragrafo 1, della direttiva 95/46 debba essere interpretato nel senso che la normativa nazionale di uno Stato membro può applicarsi nel suo territorio a un responsabile del trattamento dei dati, stabilito esclusivamente in un altro Stato membro, che gestisce una pagina Internet di intermediazione immobiliare e che pubblicizza, tra l'altro, immobili situati nel territorio del primo Stato membro, i proprietari dei quali trasmettono dati personali a un dispositivo (server) per la memorizzazione e l'elaborazione di dati appartenente al gestore della pagina Internet e situato in un altro Stato membro.
2) Se, alla luce dei considerando da 18 a 20 e degli articoli 1, paragrafo 2, e 28, paragrafo 1, l'articolo 4, paragrafo 1, lettera a), della

direttiva 95/46 debba essere interpretato nel senso che l'autorità ungherese di controllo non può applicare la legge ungherese sulla protezione dei dati, quale diritto nazionale, al gestore di una pagina Internet di intermediazione immobiliare stabilito esclusivamente in un altro Stato membro neppure qualora detto gestore pubblicizzi, tra l'altro, immobili ungheresi i cui proprietari hanno trasmesso, probabilmente dal territorio ungherese, i dati relativi ai propri immobili a un dispositivo (server) per la memorizzazione e l'elaborazione di dati appartenente al gestore della pagina Internet e situato in un altro Stato membro.
3) Se, a fini interpretativi, rilevi che il servizio fornito dal responsabile del trattamento di dati che gestisce la pagina Internet sia rivolto al territorio dell'altro Stato membro.
4) Se, a fini interpretativi, rilevi che i dati concernenti gli immobili situati nel territorio dell'altro Stato membro e i dati personali dei proprietari siano stati effettivamente caricati dal territorio di detto altro Stato membro.
5) Se, a fini interpretativi, rilevi che i dati personali trasmessi in relazione ai citati immobili riguardino cittadini dell'altro Stato membro.
6) Se, a fini interpretativi, rilevi che i titolari della società stabilita in Slovacchia abitino in Ungheria.
7) Qualora dalle risposte alle questioni precedenti emerga che l'autorità ungherese di controllo possa svolgere un procedimento ma non possa applicare il diritto nazionale, dovendo attenersi a quello dello Stato membro di stabilimento, se l'articolo 28, paragrafo 6, della direttiva sulla protezione dei dati debba essere interpretato nel senso che l'Autorità ungherese per la protezione dei dati possa esercitare i poteri di cui all'articolo 28, paragrafo 3, della citata direttiva solo conformemente alla normativa dello Stato membro di stabilimento e che, pertanto, non possa imporre un'ammenda.
8) Se si possa ritenere che la nozione di "adatfeldolgozás" (elaborazione dei dati), utilizzata sia nell'articolo 4, paragrafo 1, lettera a), sia nell'articolo 28, paragrafo 6, della direttiva 95/46 sia identica alla nozione di "adatkezelés" (trattamento dei dati) impiegata nella terminologia di detta direttiva».

Sulle questioni pregiudiziali

Osservazioni preliminari

15. Per quanto attiene, anzitutto, all'ambito fattuale della controversia nel procedimento principale, occorre menzionare alcuni elementi informativi integrativi, presentati dall'autorità ungherese di controllo nelle sue osservazioni scritte e all'udienza dinanzi alla Corte.
16. Si evince da tali elementi, in primo luogo, che tale autorità avrebbe appreso, informalmente, dalla sua omologa slovacca che la Weltimmo non svolgeva nessuna attività nel luogo della sua sede, in Slovacchia. Inoltre, la Weltimmo avrebbe più volte spostato la sede da uno Stato a un altro. In secondo luogo, la Weltimmo avrebbe creato due siti di annunci immobiliari, scritti solamente in lingua ungherese, avrebbe aperto un conto bancario in Ungheria, destinato al recupero crediti, e avrebbe avuto una casella postale in tale Stato membro, per gli affari correnti. La posta sarebbe stata regolarmente prelevata e trasmessa alla Weltimmo per via elettronica. In terzo luogo, gli inserzionisti non soltanto devono essi stessi iscrivere i dati relativi ai loro immobili nel sito della Weltimmo, ma anche cancellare tali dati dal sito se non vogliono che continuino a figurarvi oltre il periodo di un mese sopra menzionato. La Weltimmo avrebbe avanzato un problema di gestione informatica per spiegare perché non aveva potuto cancellare i dati. In quarto luogo, la Weltimmo sarebbe una società composta di una o due persone soltanto. Il suo rappresentante in Ungheria avrebbe cercato di negoziare con gli inserzionisti il pagamento dei crediti insoluti.
17. Per quanto attiene, poi, alla formulazione delle questioni sottoposte, nonostante il giudice del rinvio utilizzi i termini «stabilito esclusivamente» nella prima e nella seconda questione, si evince dalla decisione di rinvio e dalle osservazioni scritte e orali presentate dall'autorità ungherese di controllo che, sebbene la Weltimmo sia registrata in Slovacchia e sia, di conseguenza, stabilita in tale Stato membro, ai sensi del diritto societario, sussistono dubbi sul fatto se sia «stabilita» unicamente in tale Stato membro, a norma dell'articolo 4, paragrafo 1, lettera a), de della direttiva 95/46. Chiedendo alla Corte di interpretare tale disposizione, il giudice del rinvio intende, infatti,

sapere cosa rientri nella nozione di «stabilimento» utilizzata in detta disposizione.
18. Occorre, infine, rilevare che nella prima e nella seconda questione, il giudice del rinvio afferma che il server usato dalla Weltimmo è istallato in Slovacchia, mentre, in un altro passo della decisione di rinvio, accenna che è possibile che i server di tale società si trovino in Germania o in Austria. Ciò detto, sembra opportuno considerare che non sia appurato in quale Stato membro si trova il server o si trovano i server usati da detta società.

Sulle questioni dalla prima alla sesta

19. Con le questioni dalla prima alla sesta, che occorre esaminare congiuntamente, il giudice del rinvio chiede in sostanza se gli articoli 4, paragrafo 1, lettera a), e 28, paragrafo 1, della direttiva 95/46 devono essere interpretati nel senso che, in circostanze quali quelle del procedimento principale, essi consentono all'autorità di controllo di uno Stato membro di applicare la sua normativa nazionale in materia di protezione dei dati nei confronti di un responsabile del trattamento, la cui società è registrata in un altro Stato membro e che gestisce un sito Internet di annunci immobiliari riguardanti beni immobili situati nel territorio del primo di tali due Stati. Detto giudice chiede in particolare se sia rilevante che tale Stato membro sia quello:
– verso il quale si rivolge l'attività del responsabile del trattamento dei dati personali,
– in cui sono situati i beni immobili interessati,
– a partire dal quale sono comunicati dati relativi ai proprietari di tali beni,
– del quale sono cittadini questi ultimi, e
– nel quale siano domiciliati i titolari di tale società.
20. Per quanto riguarda il diritto applicabile, il giudice del rinvio cita in particolare gli ordinamenti slovacco e ungherese; nel primo è il diritto dello Stato membro in cui è registrato il responsabile del trattamento dei dati personali di cui trattasi, mentre nel secondo è quello dello Stato membro cui si rivolgono i siti Internet di cui è causa nel procedimento principale, nel territorio del quale sono situati i beni immobili oggetto degli annunci pubblicati.

21. A questo proposito, occorre rilevare che l'articolo 4 della direttiva 95/46, rubricato «Diritto nazionale applicabile», di cui al capo I di tale direttiva, rubricato «Disposizioni generali», disciplina proprio la questione sollevata.
22. L'articolo 28 della direttiva 95/46, rubricato «Autorità di controllo», è, invece, dedicato al ruolo e ai poteri di tale autorità. In forza di tale articolo 28, paragrafo 1, essa è incaricata di sorvegliare, nel territorio del suo Stato membro, l'applicazione delle disposizioni di attuazione della direttiva adottate dagli Stati membri. Ai sensi dell'articolo 28, paragrafo 6, di detta direttiva, l'autorità di controllo esercita i poteri attribuitile, indipendentemente dalla legge nazionale applicabile al trattamento dei dati personali.
23. Occorre dunque determinare il diritto nazionale applicabile al responsabile di tale trattamento alla luce non dell'articolo 28 della direttiva 95/46, ma dell'articolo 4 della medesima.
24. Ai termini dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro.
25. Alla luce dell'obiettivo perseguito dalla direttiva 95/46, consistente nel garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, l'espressione «nel contesto delle attività di uno stabilimento» non può ricevere un'interpretazione restrittiva (v., in tal senso, sentenza Google Spain e Google, C‑131/12, EU:C:2014:317, punto 53).
26. Per conseguire tale obiettivo ed evitare che una persona venga privata della tutela cui ha diritto in forza della direttiva in parola, il considerando 18 della medesima direttiva enuncia che è necessario che qualsiasi trattamento di dati personali effettuato nell'Unione europea rispetti la legislazione di uno degli Stati membri e che è opportuno assoggettare i trattamenti effettuati da chiunque operi sotto l'autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato.

27. Il legislatore dell'Unione ha quindi previsto un ambito di applicazione territoriale della direttiva 95/46 particolarmente esteso, che ha inserito all'articolo 4 della stessa (v., in tal senso, sentenza Google Spain e Google, C‑131/12, EU:C:2014:317, punto 54).
28. Per quanto attiene, in primo luogo, alla nozione di «stabilimento», va ricordato che il considerando 19 della direttiva 95/46 enuncia che lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile e che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo (sentenza Google Spain e Google, C‑131/12, EU:C:2014:317, punto 48). Detto considerando precisa, inoltre, che, quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi.
29. Ne consegue, come ha sostanzialmente rilevato l'avvocato generale ai paragrafi 28 e da 32 a 34 delle sue conclusioni, una concezione flessibile della nozione di stabilimento, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva, 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.
30. A questo proposito, occorre segnatamente considerare, alla luce dell'obiettivo perseguito da tale direttiva, consistente nel garantire una tutela efficace e completa del diritto alla vita privata e nell'evitare che le disposizioni vengano eluse, che la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a

costituire un'organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l'ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui trattasi nello Stato membro in questione.
31. Inoltre, per realizzare detto obiettivo, occorre considerare che la nozione di «stabilimento», ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile.
32. Nel caso di specie, l'attività esercitata dalla Weltimmo consiste, quantomeno, nella gestione di uno dei vari siti Internet di annunci immobiliari riguardanti beni situati in Ungheria, scritti in lingua ungherese e i cui annunci diventano a pagamento dopo un mese. Occorre dunque affermare che tale società svolge un'attività concreta ed effettiva in Ungheria.
33. Inoltre, si evince in particolare dalle precisazioni fornite dall'autorità ungherese di controllo che la Weltimmo ha un rappresentante in Ungheria, il quale figura nel registro slovacco delle società a un indirizzo situato in Ungheria e il quale ha cercato di negoziare con gli inserzionisti il pagamento dei crediti insoluti. Tale rappresentante è stata la persona di contatto tra la società e coloro che avevano introdotto reclami e l'ha rappresentata nel corso dei procedimenti amministrativo e giudiziario. Inoltre, detta società ha aperto in Ungheria un conto bancario, destinato al recupero dei crediti, e si serve di una casella postale nel territorio di tale stato membro per la gestione dei suoi affari correnti. Questi elementi, che spetta verificare al giudice del rinvio, possono configurare, in una situazione come quella controversa, l'esistenza di uno «stabilimento», ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46.
34. Occorre, in secondo luogo, sapere se il trattamento dei dati personali di cui trattasi è fatto «nel contesto delle attività» di tale stabilimento.
35. La Corte ha già considerato che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato «dallo» stesso stabilimento interessato, bensì soltanto che venga effettuato «nel contesto delle attività» di

quest'ultimo (sentenza Google Spain e Google, C‑131/12, EU:C:2014:317, punto 52).

36. Nel caso di specie, il trattamento controverso nel procedimento principale consiste, in particolare, nel pubblicare, sui siti Internet di annunci immobiliari della Weltimmo, dati personali relativi ai titolari di tali beni e, eventualmente, nell'utilizzare tali dati per esigenze di fatturazione degli annunci allo scadere del termine di un mese.

37. A tal proposito, occorre ricordare che, per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l'operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v. sentenze Lindqvist, C‑101/01, EU:C:2003:596, punto 25, nonché Google Spain e Google, C‑131/12, EU:C:2014:317, punto 26).

38. Orbene, è indubbio che tale trattamento è avvenuto nel contesto delle attività, descritte al punto 32 della presente sentenza, che la Weltimmo svolge in Ungheria.

39. Pertanto, fatte salve le verifiche rammentate al punto 33 della presente sentenza, che spetta compiere al giudice del rinvio al fine di accertare, se del caso, che sussiste lo stabilimento del responsabile del trattamento in Ungheria, occorre considerare che tale trattamento si svolge nel contesto delle attività di tale stabilimento e che l'articolo 4, paragrafo 1, lettera a), della direttiva 96/46 consente, in una situazione quale quella controversa nel procedimento principale, l'applicazione del diritto ungherese in materia di protezione dei dati personali.

40. Il fatto che i titolari dei beni oggetto degli annunci immobiliari siano cittadini ungheresi, invece, non è assolutamente rilevante al fine di determinare il diritto nazionale applicabile al trattamento dei dati di cui è causa nel procedimento principale.

41. Tenuto conto di tutte le considerazioni che precedono, occorre rispondere alle questioni dalla prima alla sesta nei seguenti termini:

– l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione

stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento;
– per determinare se ciò si verifichi, in circostanze quali quelle controverse nel procedimento principale, il giudice del rinvio può tener conto, in particolare, del fatto, da un lato, che l'attività del responsabile di detto trattamento, nell'ambito della quale il medesimo ha luogo, consiste nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro e redatti nella lingua di quest'ultimo e che essa, di conseguenza, è principalmente, ovvero interamente, rivolta verso detto Stato membro e, dall'altro, che tale responsabile ha un rappresentante in detto Stato membro, il quale è incaricato di recuperare i crediti risultanti da tale attività nonché di rappresentarlo nei procedimenti amministrativo e giudiziario relativi al trattamento dei dati interessati;
– è, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento.

Sulla settima questione

42. La settima questione viene sottoposta soltanto nell'ipotesi in cui l'autorità ungherese di controllo consideri che la Weltimmo abbia, non in Ungheria, ma in un altro Stato membro, uno stabilimento, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, che svolge attività nel contesto delle quali è effettuato il trattamento dei dati personali interessati.
43. Con tale questione, il giudice del rinvio chiede, in sostanza, se, nel caso in cui l'autorità ungherese di controllo giungesse alla conclusione che il diritto applicabile al trattamento dei dati personali non è il diritto ungherese, ma il diritto di un altro Stato membro, l'articolo 28, paragrafi 1, 3 e 6, della direttiva 95/46 debba essere interpretato nel senso che detta autorità può esercitare soltanto i poteri previsti all'articolo 28, paragrafo 3, di tale direttiva, conformemente al diritto tale altro Stato membro, e non può imporre sanzioni.
44. Per quanto attiene, in primo luogo, alla competenza di un'autorità di controllo ad agire in un simile caso, occorre rilevare che, in forza dell'articolo 28, paragrafo 4, della direttiva 95/46, qualsiasi persona può presentare a ciascuna autorità di controllo, una domanda relativa

alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali.
45. Di conseguenza, in una situazione quale quella controversa nel procedimento principale, l'autorità ungherese di controllo può essere adita da persone, quali gli inserzionisti di beni immobili di cui trattasi nel procedimento principale, che si ritengono vittime di un trattamento illecito dei dati personali che le riguardano nello Stato membro nel quale possiedono tali beni.
46. Occorre esaminare, in secondo luogo, quali siano i poteri di tale autorità di controllo alla luce dell'articolo 28, paragrafi 1, 3 e 6, della direttiva 95/46.
47. Si evince dall'articolo 28, paragrafo 1, di tale direttiva che ciascuna autorità di controllo creata da uno Stato membro sorveglia, nel territorio di tale Stato membro, l'osservanza delle disposizioni di attuazione della direttiva 95/46, adottate dagli Stati membri.
48. In forza dell'articolo 28, paragrafo 3, della direttiva 95/46, tali autorità di controllo dispongono in particolare di poteri investigativi, come il diritto di raccolta di qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, e di poteri effettivi d'intervento come quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento.
49. Tenuto conto della non tassatività dei poteri appena elencati e del tipo di poteri di intervento menzionati in tale disposizione, nonché del margine di manovra di cui dispongono gli Stati membri per il recepimento della direttiva 95/46, occorre considerare che tali poteri di intervento possono comprendere quello di sanzionare il responsabile del trattamento di dati, eventualmente imponendogli un'ammenda.
50. I poteri conferiti alle autorità di controllo devono essere esercitati nel rispetto del diritto procedurale dello Stato membro cui esse appartengono.
51. Si evince dall'articolo 28, paragrafi 1 e 3, della direttiva 95/46 che ciascuna autorità di controllo esercita tutti i poteri che le sono stati conferiti nel territorio dello Stato membro cui appartiene, per

assicurare in tale territorio il rispetto delle norme in materia di protezione dei dati.
52. Tale applicazione territoriale dei poteri di ciascuna autorità di controllo è conforme all'articolo 28, paragrafo 6, di tale direttiva, ai sensi del quale ciascuna autorità di controllo è competente a esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma dell'articolo 28, paragrafo 3, di detta direttiva e ciò indipendentemente dalla legge nazionale applicabile. Tale articolo 28, paragrafo 6 precisa anche che ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro e che le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.
53. Tale disposizione è necessaria per garantire la libera circolazione dei dati personali in tutta l'Unione, continuando a sorvegliare il rispetto delle norme dirette a tutelare la vita privata delle persone fisiche di cui alla direttiva 95/46. Infatti, in mancanza di detta disposizione, nel caso in cui il responsabile del trattamento dei dati personali fosse soggetto alla legge di uno Stato membro, ma violasse il diritto alla tutela della vita privata delle persone fisiche in un altro Stato membro, in particolare rivolgendo la sua attività verso tale altro Stato membro senza però esservi stabilito, ai sensi di tale direttiva, sarebbe difficile, se non impossibile, per tali persone far rispettare il loro diritto a detta tutela.
54. Si evince quindi dall'articolo 28, paragrafo 6, della direttiva 95/46 che l'autorità di controllo di uno Stato membro alla quale persone fisiche presentano un reclamo relativo al trattamento di dati personali che le riguardano, in base all'articolo 28, paragrafo 4, di tale direttiva, può esaminare tale reclamo indipendentemente dalla legge applicabile e, di conseguenza, anche se il diritto applicabile al trattamento dei dati interessati è quello di un altro Stato membro.
55. Tuttavia, in tale ipotesi, i poteri di tale autorità non comprendono necessariamente tutti quelli di cui è investita secondo il diritto dello suo Stato membro.
56. Infatti, come rilevato dall'avvocato generale al paragrafo 50 delle sue conclusioni, dalle esigenze derivanti dalla sovranità territoriale dello Stato membro, dal principio di legalità e dalla nozione di Stato

di diritto discende che il potere sanzionatorio non può avere luogo, in linea di principio, al di fuori dei limiti legali entro cui un'autorità amministrativa è autorizzata ad agire secondo il diritto nazionale del suo Stato membro.

57. Così, quando ad un'autorità di controllo viene presentato un reclamo, secondo l'articolo 28, paragrafo 4, della direttiva 95/46, essa può esercitare i suoi poteri investigativi indipendentemente dal diritto applicabile e ancor prima di sapere quale sia il diritto nazionale che si applica al trattamento controverso. Tuttavia, essa, qualora giunga alla conclusione che si applica il diritto di un altro Stato membro, non può imporre sanzioni al di fuori del territorio del suo Stato membro. In una situazione del genere, essa è tenuta, in virtù dell'obbligo di collaborazione di cui all'articolo 28, paragrafo 6, di tale direttiva, a chiedere all'autorità di controllo di tale altro Stato membro di accertare un'eventuale violazione di tale diritto e di imporre sanzioni se questo lo consente, appoggiandosi, se del caso, sulle informazioni che essa le avrà comunicato.

58. L'autorità di controllo cui è proposto un reclamo, nell'ambito di tale collaborazione può essere indotta a svolgere altre indagini, su istruzione dell'autorità di controllo dell'altro Stato membro.

59. Ne consegue che, in una situazione quale quella controversa nel procedimento principale, nell'ipotesi in cui il diritto applicabile sia quello di uno Stato membro diverso dall'Ungheria, l'autorità ungherese di controllo non potrebbe esercitare i poteri sanzionatori attribuitile dalla legge ungherese.

60. Risulta dalle considerazioni sopra esposte che occorre rispondere alla settima questione dichiarando che, nell'ipotesi in cui l'autorità di controllo di uno Stato membro cui sia proposto un reclamo, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46, giunga alla conclusione che il diritto applicabile al trattamento dei dati personali interessati non è il diritto di tale Stato membro, ma quello di un altro Stato membro, l'articolo 28, paragrafi 1, 3 e 6, di tale direttiva deve essere interpretato nel senso che tale autorità di controllo potrebbe esercitare i poteri effettivi d'intervento attribuitile in base all'articolo 28, paragrafo 3, di detta direttiva solamente nel territorio del suo Stato membro. Pertanto, essa non può imporre sanzioni sulla base del diritto di tale Stato membro nei confronti del responsabile del trattamento di

tali dati che non è stabilito in tale territorio, ma, secondo l'articolo 28, paragrafo 6, della medesima direttiva, dovrebbe chiedere all'autorità di controllo dello Stato membro del quale si applica legge d'intervenire.

Sull'ottava questione

61. Con l'ottava questione, il giudice del rinvio chiede alla Corte quale sia la portata della nozione di «adatfeldolgozás» (elaborazione dei dati), utilizzata in particolare all'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, relativo alla determinazione del diritto applicabile, e all'articolo 28, paragrafo 6, di tale direttiva, relativo alla competenza dell'autorità di controllo.
62. Si evince dalla direttiva 95/46, nella versione in lingua ungherese, che essa utilizza sistematicamente il termine «adatfeldolgozás».
63. Il giudice del rinvio fa presente che la legge sull'informazione utilizza, segnatamente nelle disposizioni dirette ad attuare le disposizioni della direttiva 95/46 relative alla competenza delle autorità di controllo, il termine «adatkezelés» (trattamento dei dati). Orbene, come si evince dall'articolo 3, punto 10, di tale legge, tale termine ha un significato più ampio di quello del termine «adatfeldolgozás», definito all'articolo 3, punto 17, di detta legge e ingloba quest'ultimo termine.
64. Sebbene la nozione di «adatfeldolgozás», secondo la comune accezione e così come si evince dalla legge sull'informazione, abbia un significato più stretto rispetto alla nozione di «adatkezelés», occorre tuttavia notare che la versione della direttiva 95/46 in lingua ungherese definisce il termine «adatfeldolgozás» all'articolo 2, lettera b), in un modo ampio, che corrisponde al termine «adatkezelés».
65. Di conseguenza occorre rispondere all'ottava questione dichiarando che la direttiva 95/46 deve essere interpretata nel senso che la nozione di «adatfeldolgozás» (elaborazione dei dati), utilizzata nella versione di tale direttiva in lingua ungherese, in particolare agli articoli 4, paragrafo 1, lettera a), e 28, paragrafo 6, della medesima, deve essere intesa in un significato identico a quello del termine «adatkezelés» (trattamento dei dati).

Sulle spese

66. Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi,
La Corte (Terza Sezione) dichiara

1) L'articolo 4, paragrafo 1, lettera a), della 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, deve essere interpretato nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento.
Per determinare se ciò si verifichi, in circostanze quali quelle controverse nel procedimento principale, il giudice del rinvio può tener conto, in particolare, del fatto, da un lato, che l'attività del responsabile di detto trattamento, nell'ambito della quale il medesimo ha luogo, consiste nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro e redatti nella lingua di quest'ultimo e che essa, di conseguenza, è principalmente, ovvero interamente, rivolta verso detto Stato membro e, dall'altro, che tale responsabile ha un rappresentante in detto Stato membro, il quale è incaricato di recuperare i crediti risultanti da tale attività nonché di rappresentarlo nei procedimenti amministrativo e giudiziario relativi al trattamento dei dati interessati.
È, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento.
2) Nell'ipotesi in cui l'autorità di controllo di uno Stato membro cui sia proposto un reclamo, ai sensi dell'articolo 28, paragrafo 4, della

direttiva 95/46, giunga alla conclusione che il diritto applicabile al trattamento dei dati personali interessati non è il diritto di tale Stato membro, ma quello di un altro Stato membro, l'articolo 28, paragrafi 1, 3 e 6, di tale direttiva deve essere interpretato nel senso che tale autorità di controllo potrebbe esercitare i poteri effettivi d'intervento attribuitile in base all'articolo 28, paragrafo 3, di detta direttiva solamente nel territorio del suo Stato membro. Pertanto, essa non può imporre sanzioni sulla base del diritto di tale Stato membro nei confronti del responsabile del trattamento di tali dati che non è stabilito in tale territorio, ma, secondo l'articolo 28, paragrafo 6, della medesima direttiva, dovrebbe chiedere all'autorità di controllo dello Stato membro del quale si applica legge d'intervenire.
3) La direttiva 95/46 deve essere interpretata nel senso che la nozione di «adatfeldolgozás» (elaborazione dei dati), utilizzata nella versione di tale direttiva in lingua ungherese, in particolare agli articoli 4, paragrafo 1, lettera a), e 28, paragrafo 6, della medesima, deve essere intesa in un significato identico a quello del termine «adatkezelés» (trattamento dei dati).

CORTE DI GIUSTIZIA UE, Grande Sezione, sentenza 6 ottobre 2015, causa C-362/14

Rinvio pregiudiziale – Dati personali – Protezione delle persone fisiche con riguardo al trattamento di tali dati – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 47 – Direttiva 95/46/CE – Articoli 25 e 28 – Trasferimento di dati personali verso paesi terzi – Decisione 2000/520/CE – Trasferimento di dati personali verso gli Stati Uniti – Livello di protezione inadeguato – Validità – Denuncia di una persona fisica i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti – Poteri delle autorità nazionali di controllo

Sentenza

1. La domanda di pronuncia pregiudiziale verte sull'interpretazione, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), degli articoli 25, paragrafo 6, e 28 della 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 (GU L 281, pag. 31), come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003 (GU L 284, pag. 1; in prosieguo: la «direttiva 95/46»), nonché, in sostanza, sulla validità della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 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, pag. 7).

2. Tale domanda è stata presentata nell'ambito di una controversia fra il sig. Schrems e il Data Protection Commissioner (commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal

sig. Schrems per il fatto che Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») trasferisce negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in tale paese.

Contesto normativo

La direttiva 95/46

3. I considerando 2, 10, 56, 57, 60, 62 e 63 della direttiva 95/46 così recitano:
«(2) (...) i sistemi di trattamento dei dati sono al servizio dell'uomo; (…) essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire (…) al benessere degli individui;
(...)
(10) (...) le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950,] e dai principi generali del diritto comunitario; (…) pertanto il ravvicinamento di dette legislazioni 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;
(...)
(56) (...) lo sviluppo degli scambi internazionali comporta necessariamente il trasferimento oltre frontiera di dati personali; (…) la tutela delle persone garantita nella Comunità dalla presente direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato; (…) l'adeguatezza della tutela offerta da un paese terzo deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti;

(57) (...) per contro, (...) deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato;
(...)
(60) (...) comunque i trasferimenti di dati verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione della presente direttiva, in particolare dell'articolo 8;
(...)
(62) (...) la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali;

(63) (...) tali autorità devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali; (...)».

4. Gli articoli 1, 2, 25, 26, 28 e 31 della direttiva 95/46 dispongono quanto segue:

«Articolo 1
Oggetto della direttiva
1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
(…)

Articolo 2
Definizioni
Ai fini della presente direttiva si intende per:
a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) “trattamento di dati personali” (“trattamento”): qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali, 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;
(...)
d) “responsabile del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;
(...)

Articolo 25
Principi
1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.
2. L’adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d’origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.
3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.

4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.
5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.
6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

Articolo 26
Deroghe
1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:
a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per

co[n]statare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.
2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.
3. Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.
In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo 31, paragrafo 2.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
(...)

Articolo 28
Autorità di controllo
1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri.
Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.

2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
3. Ogni autorità di controllo dispone in particolare:
– di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
– di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
– del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.
4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.
Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.
(...)
6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.
(…)

Articolo 31
(...)
2. Nei casi in cui è fatto riferimento al presente articolo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE [del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, pag. 23)], tenendo conto delle disposizioni dell'articolo 8 della stessa.
(...)».

La decisione 2000/520

5. La decisione 2000/520 è stata adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.

6. I considerando 2, 5 e 8 di tale decisione così recitano:
«(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.
(...)
(5) Per il trasferimento di dati dalla Comunità agli Stati Uniti, il livello adeguato di protezione di cui alla presente decisione sarebbe raggiunto ove le organizzazioni si conformino ai "principi dell'approdo sicuro in materia di riservatezza" ("The Safe Harbor Privacy Principles"), in prosieguo "i principi", nonché alle "domande più frequenti" ("Frequently Asked Questions"), in prosieguo "FAQ", pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che forniscono indicazioni per l'attuazione dei principi stessi. Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio [Federal Trade Commission (FTC)] ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.
(...)

(8) Nell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione».

7. Ai sensi degli articoli da 1 a 4 della decisione 2000/520:

«Articolo 1
1. Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo di applicazione di detta direttiva, si considera che i "Principi di approdo sicuro in materia di riservatezza", in prosieguo i "principi", di cui all'allegato I della presente decisione, applicati in conformità agli orientamenti forniti dalle "Domande più frequenti" (FAQ) di cui all'allegato II della presente decisione, pubblicate dal Dipartimento del commercio degli Stati Uniti in data 21 luglio 2000, garantiscano un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti sulla base della seguente documentazione pubblicata dal Dipartimento del commercio degli Stati Uniti:
a) riepilogo delle modalità di esecuzione dei principi di approdo sicuro, di cui all'allegato III;
b) memorandum sui danni per violazioni della riservatezza ed autorizzazioni esplicite previste dalle leggi degli Stati Uniti, di cui all'allegato IV;
c) lettera della Commissione federale per il commercio (FTC), di cui all'allegato V;
d) lettera del Dipartimento dei trasporti degli Stati Uniti, di cui all'allegato VI.

2. Le seguenti condizioni devono sussistere in relazione a ogni singolo trasferimento di dati:
a) l'organizzazione che riceve i dati si è chiaramente e pubblicamente impegnata a conformarsi ai principi applicati in conformità alle FAQ, e

b) detta organizzazione è sottoposta all'autorità prevista per legge di un ente governativo degli Stati Uniti, compreso nell'elenco di cui all'allegato VII, competente ad esaminare denunce e a imporre la cessazione di prassi sleali e fraudolente nonché a disporre il risarcimento di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei principi applicati in conformità alle FAQ.
3. Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b).
Articolo 2
La presente decisione dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva 95/46/CE. Essa nulla dispone relativamente all'applicazione di altre disposizioni della stessa direttiva, relative al trattamento di dati personali all'interno degli Stati membri e in particolare dell'articolo 4 della stessa.

Articolo 3
1. Fatto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:
a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera a) del "principio di esecuzione" di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ, oppure

b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.
La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE.
2. Gli Stati membri comunicano immediatamente alla Commissione l'adozione di misure a norma del paragrafo 1.
3. Gli Stati membri e la Commissione s'informano altresì a vicenda in merito ai casi in cui l'azione degli organismi responsabili non garantisca la conformità ai principi applicati in conformità alle FAQ negli Stati Uniti.
4. Ove le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione.

Articolo 4
1. La presente decisione può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/CE, fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai

sensi dell'articolo 25 della direttiva 95/46/CE, nonché di eventuali applicazioni discriminatorie della decisione stessa.
2. La Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46/CE».

8. L'allegato I della decisione 2000/520 così recita:
«Principi di approdo sicuro (safe harbor) del dipartimento del commercio degli Stati Uniti, 21 luglio 2000
(...)
(...) il Dipartimento del commercio sta provvedendo a pubblicare sotto la propria autorità statutaria questo documento e le Frequently Asked Questions ("i principi") al fine di incoraggiare, promuovere e sviluppare il commercio internazionale. I principi sono stati messi a punto in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta. Giacché questi principi sono stati concepiti esclusivamente a tal fine una loro estensione ad altri fini può non risultare opportuna. (...)

La decisione di un'organizzazione di qualificarsi per l'approdo sicuro è puramente volontaria, e la qualifica può essere ottenuta in vari modi. (...)

L'adesione a tali principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si

applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.
(...)».

9. L'allegato II della decisione 2000/520 è redatto come segue:
«Domande più frequenti (FAQ)
(...)

FAQ 6 – Autocertificazione
D: Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?
R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate.

Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni:
1) denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;
2) descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE;
3) descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: a) dove il pubblico può prenderne conoscenza; b) la data della loro effettiva applicazione; c) l'ufficio cui rivolgersi per eventuali reclami, richieste di accesso e qualsiasi altra questione riguardante l'approdo sicuro; d) lo specifico organo statutario competente ad esaminare i ricorsi contro

l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); e) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; f) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) (…) e g) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.

Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato "Principi di approdo sicuro". (...)

Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. (...)
(...)

FAQ 11 – Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement)
D: Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?
R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso. Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: 1) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i

principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2) uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrispondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati. Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo. Il settore privato può indicare altri meccanismi di applicazione, purché rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge.

Meccanismi di ricorso:

I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. (...)
(...)

Attività della Commissione federale per il commercio (Federal Trade Commission, FTC):
La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. (...)
(...)».

10. Ai sensi dell'allegato IV della decisione 2000/520:
«Tutela della riservatezza e risarcimento danni, autorizzazioni legali, fusioni e acquisizioni secondo la legge degli Stati Uniti

Il presente documento risponde alla richiesta della Commissione europea di chiarimenti sulla legge statunitense per quanto riguarda a) risarcimento dei danni per violazione della sfera privata (privacy), b) le "autorizzazioni esplicite" previste dalla legge degli Stati Uniti per l'uso di dati personali in modo contrastante con i principi "approdo sicuro" (safe harbor), c) l'effetto delle fusioni e acquisizioni sugli obblighi assunti in base a tali principi.
(...)

B. Autorizzazioni legali esplicite

I principi "approdo sicuro" contengono un'eccezione qualora atti legislativi, regolamenti o la giurisprudenza "comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". È ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge. Per quanto riguarda le autorizzazioni esplicite, sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti. La limitata eccezione al rigoroso rispetto dei principi "approdo sicuro" cerca di stabilire un equilibrio in grado di conciliare i legittimi interessi delle parti.
L'eccezione è limitata ai casi in cui esiste un'autorizzazione esplicita. Tuttavia, come caso limite, la legge, il regolamento o la decisione del tribunale pertinenti devono esplicitamente autorizzare una particolare condotta delle organizzazioni aderenti ai principi "approdo sicuro". In altre parole, l'eccezione non verrà applicata se la legge non prescrive nulla. Inoltre, l'eccezione verrà applicata soltanto se l'esplicita autorizzazione è in conflitto con il rispetto dei principi "approdo sicuro". Anche in questo caso, l'eccezione "si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". Ad esempio, se la legge si limita ad autorizzare un'azienda a fornire dati personali alle pubbliche

autorità, l'eccezione non verrà applicata. Al contrario, se la legge autorizza espressamente l'azienda a fornire dati personali ad organizzazioni governativ[e] senza il consenso dei singoli, ciò costituisce una "autorizzazione esplicita" ad agire in contrasto con i principi "approdo sicuro". In alternativa, le specifiche eccezioni alle disposizioni relative alla notifica al consenso rientrerebbero nell'ambito dell'eccezione (dato che ciò equivarrebbe ad una specifica autorizzazione a rivelare informazioni senza notifica e consenso). Ad esempio, una legge che autorizzi i medici a fornire le cartelle cliniche dei loro pazienti agli ufficiali sanitari senza il previo consenso dei pazienti stessi potrebbe consentire un'eccezione ai principi di notifica e di scelta. Tale autorizzazione non permetterebbe ad un medico di fornire le stesse cartelle cliniche alle casse mutue malattie o ai laboratori di ricerca farmaceutica perché ciò esulerebbe dall'ambito degli usi consentiti dalla legge e dunque dall'ambito dell'eccezione (...). L'autorizzazione in questione può essere un'autorizzazione "autonoma" a fare determinate cose con i dati personali ma, come illustrato negli esempi di cui sopra, è probabile che si tratti di un'eccezione a una legge generale che proscrive la raccolta, l'uso o la divulgazione dei dati personali.
(...)».

La comunicazione COM(2013) 846 final

11. Il 27 novembre 2013 la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio, intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» [COM(2013) 846 final; in prosieguo: la «comunicazione COM(2013) 846 final»]. Tale comunicazione era corredata di una relazione, parimenti datata 27 novembre 2013, contenente le «conclusioni dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA sulla protezione dei dati personali» («Report on the Findings by the EU Co‑chairs of the ad hoc EU-US Working Group on Data Protection»). Tale relazione era stata elaborata, come indicato dal suo punto 1, in cooperazione con gli Stati Uniti d'America in seguito alle rivelazioni dell'esistenza, in tale paese, di diversi programmi di

controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. Detta relazione conteneva, segnatamente, un'analisi dettagliata dell'ordinamento giuridico statunitense per quanto attiene, in particolare, alle basi giuridiche che autorizzano l'esistenza di programmi di controllo, nonché la raccolta e il trattamento di dati personali da parte delle autorità americane.

12. Al punto 1 della comunicazione COM(2013) 846 final, la Commissione ha precisato che «[g]li scambi commerciali sono oggetto della decisione [2000/520]», aggiungendo che tale decisione «fornisce una base giuridica per il trasferimento dei dati personali dall'UE a società stabilite negli Stati Uniti che hanno aderito ai principi d'Approdo sicuro». Inoltre, sempre al punto 1, la Commissione ha messo in evidenza l'importanza sempre maggiore dei flussi di dati personali, legata segnatamente allo sviluppo dell'economia digitale, il quale ha effettivamente «portato a una crescita esponenziale nella quantità, qualità, diversità e natura delle attività di trattamento dei dati».

13. Al punto 2 di tale comunicazione, la Commissione ha osservato che «le preoccupazioni sul livello di protezione dei dati personali dei cittadini dell'[Unione] trasferiti agli Stati Uniti nell'ambito del principio dell'Approdo sicuro sono aumentate», e che «[l]a natura volontaria e dichiarativa del regime ha difatti attirato grande attenzione sulla sua trasparenza e sulla sua applicazione».

14. Inoltre, essa ha indicato, in questo stesso punto 2, che «[i] dati personali dei cittadini dell'[Unione] inviati negli USA nell'ambito [del] regime [dell'approdo sicuro] possono essere consultati e ulteriormente trattati dalle autorità americane in maniera incompatibile con i motivi per cui erano stati originariamente raccolti nell'[Unione] e con le finalità del loro trasferimento agli Stati Uniti», e che «[l]a maggior parte delle imprese Internet americane che risultano più direttamente interessate [dai] programmi [di controllo], sono certificate nell'ambito del regime Approdo sicuro».

15. Al punto 3.2 della comunicazione COM(2013) 846 final, la Commissione ha rilevato l'esistenza di un certo numero di carenze quanto all'attuazione della decisione 2000/520. Da un lato, essa ha ivi

menzionato il fatto che talune imprese americane certificate non rispettavano i principi di cui all'articolo 1, paragrafo 1, della decisione 2000/520 (in prosieguo: i «principi di approdo sicuro») e che dovevano essere apportati miglioramenti a tale decisione concernenti «i punti deboli strutturali relativi alla trasparenza e all'applicazione, i principi sostanziali dell'Approdo sicuro e il funzionamento dell'eccezione per motivi di sicurezza nazionale». Dall'altro, essa ha osservato che l'«Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'[Unione] europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi».

16. La Commissione ha concluso, a questo stesso punto 3.2, che, se, «[t]enuto conto dei punti deboli individuati, il regime Approdo sicuro non può continuare ad essere applicato secondo le attuali modalità, (…) abrogarlo nuocerebbe [tuttavia] agli interessi delle imprese che ne sono membri, nell'[Unione] e negli USA». Infine, sempre a detto punto 3.2, la Commissione ha aggiunto che essa intendeva cominciare «col discutere con le autorità americane i punti deboli individuati».

La comunicazione COM(2013) 847 final

17. Sempre il 27 novembre 2013, la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite [COM(2013) 847 final; in prosieguo: la «comunicazione COM(2013) 847 final»]. Come risulta dal suo punto 1, tale comunicazione si basava, segnatamente, sulle informazioni ricevute nell'ambito del Gruppo di lavoro ad hoc Unione europea‑Stati Uniti e faceva seguito a due relazioni di valutazione della Commissione, pubblicate, rispettivamente, nel 2002 e nel 2004.

18. Il punto 1 di tale comunicazione precisa che il funzionamento della decisione 2000/520 «si basa sugli impegni assunti dalle imprese che vi aderiscono e sulla loro auto‑certificazione» e aggiunge che

«[l]'adesione è volontaria, ma [che] una volta sottoscritta le norme sono vincolanti».

19. Inoltre, emerge dal punto 2.2 della comunicazione COM(2013) 847 final che, al 26 settembre 2013, 3 246 imprese, facenti parte di numerosi settori dell'economia e dei servizi, erano certificate. Tali imprese fornivano, principalmente, servizi sul mercato interno dell'Unione, in particolare nel settore di Internet, e una parte di esse erano imprese dell'Unione con controllate negli Stati Uniti. Alcune di queste imprese trattavano i dati relativi ai loro dipendenti in Europa e li inviavano in tale paese a fini di gestione delle risorse umane.

20. Sempre al punto 2.2, la Commissione ha sottolineato che «[o]gni insufficienza a livello di trasparenza o di applicazione da parte americana [aveva] l'effetto di far ricadere la responsabilità sulle autorità per la protezione dei dati europee e sulle imprese che si avvalgono del regime in oggetto».

21. Si evince, segnatamente, dai punti da 3 a 5 e 8 della comunicazione COM(2013) 847 final che, nella prassi, un numero considerevole di imprese certificate non rispettava, o rispettava solo in parte, i principi dell'approdo sicuro.

22. Inoltre, al punto 7 di tale comunicazione, la Commissione ha affermato che «tutte le imprese partecipanti al programma PRISM [programma di raccolta di informazioni su larga scala], e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro», e che tale sistema «è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'[Unione]». A tal riguardo, la Commissione ha constatato, al punto 7.1 di detta comunicazione, che «un certo numero di basi giuridiche previste dalla legislazione americana consente la raccolta e il trattamento su larga scala di dati personali conservati o altrimenti trattati da società ubicate negli Stati Uniti» e che «[a] causa dell'ampia entità dei programmi, può accadere che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto è

necessario e proporzionato alla protezione della sicurezza nazionale come previsto dall'eccezione di cui alla decisione [2000/520]».

23. Al punto 7.2 della comunicazione COM(2013) 847 final, intitolata «Limitazioni e rimedi», la Commissione ha sottolineato che «i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA» e che «[n]on vi è inoltre alcuna possibilità, né per gli interessati [dell'Unione] che per quelli americani, di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo statunitensi».

24. Secondo il punto 8 della comunicazione COM(2013) 847 final, fra le imprese certificate figuravano «[l]e imprese del web come Google, Facebook, Microsoft, Apple, Yahoo», le quali contano «[centinaia di] milioni di clienti in Europa» e trasferiscono dati personali negli Stati Uniti a fini del loro trattamento.

25. La Commissione ha concluso, a questo stesso punto 8, che «l'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito di Approdo sicuro solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti».

Procedimento principale e questioni pregiudiziali

26. Il sig. Schrems, cittadino austriaco residente in Austria, è iscritto alla rete sociale Facebook (in prosieguo: «Facebook») dal 2008.

27. Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento.

28. Il 25 giugno 2013 il sig. Schrems ha investito il commissario di una denuncia, con la quale lo invitava, in sostanza, ad esercitare le proprie competenze statutarie, vietando a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti. In tale denuncia egli faceva valere che il diritto e la prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo contro le attività di controllo ivi praticate dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quelle della National Security Agency (in prosieguo: la «NSA»).

29. Considerando di non essere obbligato a procedere ad un'indagine sui fatti denunciati dal sig. Schrems, il commissario ha respinto la denuncia in quanto priva di fondamento. Egli ha ritenuto, infatti, che non esistessero prove del fatto che la NSA avesse avuto accesso ai dati personali dell'interessato. Il commissario ha aggiunto che le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato.

30. Il sig. Schrems ha proposto un ricorso dinanzi alla High Court (Corte d'appello) avverso la decisione di cui al procedimento principale. Dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, tale giudice ha dichiarato che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico. Tuttavia, detto giudice ha aggiunto che le rivelazioni del sig. Snowden avevano dimostrato che la NSA ed altri organi federali avevano commesso «eccessi considerevoli».

31. Orbene, secondo questo stesso giudice, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti. La supervisione sull'operato dei servizi di intelligence verrebbe effettuata nell'ambito di un procedimento segreto e non contraddittorio. Una volta che i dati

personali sono stati trasferiti verso gli Stati Uniti, la NSA e altri organi federali, come il Federal Bureau of Investigation (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala.

32. La High Court (Corte d'appello) ha constatato che il diritto irlandese vieta il trasferimento dei dati personali al di fuori del territorio nazionale, fatti salvi i casi in cui il paese terzo in questione assicura un livello di protezione adeguato della vita privata, nonché dei diritti e delle libertà fondamentali. L'importanza dei diritti al rispetto della vita privata e all'inviolabilità del domicilio, garantiti dalla Costituzione irlandese, implicherebbe che qualsiasi ingerenza in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge.

33. Orbene, l'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale o della repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la High Court (Corte d'appello), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest'ultima.

34. Tuttavia, la High Court (Corte d'appello) considera che tale causa verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell'Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli articoli 7 e 8 della Carta sia dai principi enunciati dalla Corte nella sentenza Digital Rights Ireland e a.

(C‑293/12 e C‑594/12, EU:C:2014:238). Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.

35. La High Court (Corte d'appello) osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale. Pertanto, anche se il sig. Schrems non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all'articolo 25, paragrafo 6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d'America garantiscono un livello di protezione adeguato, oppure se l'articolo 8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.

36. È in tale contesto che la High Court (Corte d'appello) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:
«1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi

verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».

Sulle questioni pregiudiziali

37. Con le sue questioni pregiudiziali, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se e in che misura l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520, con la quale la Commissione constata che un paese terzo assicura un livello di protezione adeguato, osti a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, allorché tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non assicurano un livello di protezione adeguato.

Sui poteri delle autorità nazionali di controllo ai sensi dell'articolo 28 della direttiva 95/46, in presenza di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva

38. Occorre rammentare, in via preliminare, che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta (v. sentenze Österreichischer Rundfunk e a., C‑465/00, C‑138/01 e C‑139/01, EU:C:2003:294, punto 68; Google Spain e Google, C‑131/12, EU:C:2014:317, punto 68, nonché Ryneš, C‑212/13, EU:C:2014:2428, punto 29).

39. Risulta dall'articolo 1, nonché dai considerando 2 e 10 della direttiva 95/46, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle

persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali. L'importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto fondamentale alla tutela dei dati personali, garantito dall'articolo 8 della stessa, è inoltre sottolineata nella giurisprudenza della Corte (v. sentenze Rijkeboer, C‑553/07, EU:C:2009:293, punto 47; Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punto 53, nonché Google Spain e Google, C‑131/12, EU:C:2014:317, punti 53, 66 e 74 e la giurisprudenza ivi citata).

40. Per quanto attiene ai poteri di cui dispongono le autorità di controllo nazionali quanto al trasferimento di dati personali verso paesi terzi, si deve rilevare che l'articolo 28, paragrafo 1, della direttiva 95/46 obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento di tali dati. Detto obbligo risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE (v., in tal senso, sentenze Commissione/Austria, C‑614/10, EU:C:2012:631, punto 36, e Commissione/Ungheria, C‑288/12, EU:C:2014:237, punto 47).

41. La garanzia d'indipendenza delle autorità nazionali di controllo è diretta ad assicurare che il controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali sia efficace e affidabile e deve essere interpretata alla luce di tale finalità. Essa è stata disposta al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità. L'istituzione, negli Stati membri, di autorità di controllo indipendenti, costituisce quindi, come rilevato dal considerando 62 della direttiva 95/46, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali (v. sentenze Commissione/Germania, C‑518/07, EU:C:2010:125, punto 25, nonché Commissione/Ungheria C‑288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata).

42. Al fine di garantire tale protezione, le autorità nazionali di controllo devono, segnatamente, assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali (v., in tal senso, sentenze Commissione/Germania, C‑518/07, EU:C:2010:125, punto 24, e Commissione/Ungheria C‑288/12, EU:C:2014:237, punto 51).

43. A tal fine, dette autorità dispongono di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'articolo 28, paragrafo 3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti, come sottolineato dal considerando 63 di tale direttiva. In tal senso, dette autorità godono, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie.

44. È vero che si evince dall'articolo 28, paragrafi 1 e 6, della direttiva 95/46 che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale articolo 28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo.

45. Tuttavia, l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v., in tal senso, sentenza Parlamento/Consiglio e Commissione, C‑317/04 e C‑318/04, EU:C:2006:346, punto 56) effettuato nel territorio di uno Stato membro. Infatti, tale disposizione definisce il «trattamento di dati personali» alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

46. Il considerando 60 della direttiva 95/46 precisa che i trasferimenti di dati personali verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione di tale direttiva. A tal riguardo, il capo IV di detta direttiva, nel quale figurano gli articoli 25 e 26 della medesima, ha predisposto un regime che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi. Tale regime è complementare al regime generale attuato dal capo II di questa stessa direttiva, riguardante le condizioni generali di liceità dei trattamenti di dati personali (v., in tal senso, sentenza Lindqvist, C‑101/01, EU:C:2003:596, punto 63).

47. Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46.

48. Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.

49. Inoltre, il considerando 57 di detta direttiva precisa che i trasferimenti di dati personali verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati.

50. Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione del livello di protezione ad essi accordato in ciascuno di tali paesi, l'articolo 25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata, come rilevato

dall'avvocato generale al paragrafo 86 delle sue conclusioni, vuoi dagli Stati membri vuoi dalla Commissione.

51. La Commissione può adottare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato. Conformemente al secondo comma di tale disposizione, una siffatta decisione ha come destinatari gli Stati membri, i quali devono adottare le misure necessarie per conformarvisi. Ai sensi dell'articolo 288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (v., in tal senso, sentenze Albako Margarinefabrik, 249/85, EU:C:1987:245, punto 17, e Mediaset, C‑69/13, EU:C:2014:71, punto 23), nella parte in cui produce l'effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo da essa interessato.

52. Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell'Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità (sentenza Commissione/Grecia, C‑475/01, EU:C:2004:585, punto 18 e la giurisprudenza ivi citata).

53. Tuttavia, una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale natura non può, come rilevato dall'avvocato generale, segnatamente, ai paragrafi 61, 93 e 116 delle

sue conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta, nonché dall'articolo 28 di detta direttiva.

54. Né l'articolo 8, paragrafo 3, della Carta né l'articolo 28 della direttiva 95/46 escludono dall'ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

55. In particolare, l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, il quale dispone che «[q]ualsiasi persona (…) può presentare [alle autorità nazionali di controllo] una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede alcuna eccezione a tal riguardo nel caso in cui la Commissione abbia adottato una decisione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

56. Inoltre, sarebbe contrario al sistema predisposto dalla direttiva 95/46, nonché alla finalità degli articoli 25 e 28 della stessa se una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, di detta direttiva avesse come effetto di impedire ad un'autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese terzo interessato da tale decisione.

57. Al contrario, l'articolo 28 della direttiva 95/46 si applica, per la sua stessa natura, a ogni trattamento di dati personali. Pertanto, anche in presenza di una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati da detta direttiva.

58. Se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all'articolo 8, paragrafi 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali (v., per analogia, sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punto 68).

59. Una domanda, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46, con la quale una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo fa valere, come nel procedimento principale, che il diritto e la prassi di tale paese non assicurano, nonostante quanto constatato dalla Commissione in una decisione adottata in base all'articolo 25, paragrafo 6, di tale direttiva, un livello di protezione adeguato, deve essere intesa nel senso che essa verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

60. A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (v., in tal senso, sentenze Commissione e a./Kadi, C‑584/10 P, C‑593/10 P e C‑595/10 P, EU:C:2013:518, punto 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C‑583/11 P, EU:C:2013:625, punto 91, nonché Telefónica/Commissione, C‑274/12 P, EU:C:2013:852, punto 56). Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo.

61. Ciò premesso, la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (v. sentenze Melki e Abdeli,

C‑188/10 e C‑189/10, EU:C:2010:363, punto 54, nonché CIVAD, C‑533/10, EU:C:2012:347, punto 40).

62. Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione, come una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto (v., in tal senso, sentenze Foto‑Frost, 314/85, EU:C:1987:452, punti da 15 a 20, nonché IATA e ELFAA, C‑344/04, EU:C:2006:10, punto 27). A fortiori, in sede di esame di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, avente ad oggetto la compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di detta direttiva con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione.

63. Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda, come nel procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

64. Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall'articolo 28, paragrafo 3, secondo comma, della direttiva 95/46, in combinato con l'articolo 47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai punti 61 e 62 della presente sentenza, tali

giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati (v., in tal senso, sentenza T & L Sugars e Sidul Açúcares/Commissione, C‑456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata).

65. Nell'ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione.

66. In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

Sulla validità della decisione 2000/520

67. Come si evince dalle spiegazioni del giudice del rinvio relative alle questioni sollevate, il sig. Schrems fa valere, nel procedimento principale, che il diritto e la prassi degli Stati Uniti non assicurano un livello di protezione adeguato ai sensi dell'articolo 25 della direttiva 95/46. Come rilevato dall'avvocato generale ai paragrafi 123 e 124 delle sue conclusioni, il sig. Schrems esprime dubbi, che tale giudice sembra peraltro condividere nella sostanza, concernenti la validità della decisione 2000/520. In tali circostanze, in virtù delle constatazioni effettuate ai punti da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta direttiva, letta alla luce della Carta.

Sui requisiti risultanti dall'articolo 25, paragrafo 6, della direttiva 95/46

68. Come è già stato rilevato ai punti 48 e 49 della presente sentenza, l'articolo 25, paragrafo 1, della direttiva 95/46 vieta i trasferimenti di dati personali verso un paese terzo che non garantisce un livello di protezione adeguato.

69. Tuttavia, ai fini del controllo di tali trasferimenti, l'articolo 25, paragrafo 6, primo comma, di tale direttiva, dispone che la Commissione «può constatare (…) che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 [di tale articolo], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (…), ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

70. È vero che né l'articolo 25, paragrafo 2, della direttiva 95/46 né nessun'altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato. In particolare, l'articolo 25, paragrafo 2, di detta direttiva si limita ad enunciare che l'adeguatezza del livello di protezione garantito da un paese terzo «è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati» ed elenca, in maniera non esaustiva, le circostanze che devono essere prese in considerazione in occasione di una siffatta valutazione.

71. Tuttavia, da un lato, come si evince dalla lettera stessa dell'articolo 25, paragrafo 6, della direttiva 95/46, tale disposizione esige che un paese terzo «garantisc[a]» un livello di protezione adeguato in considerazione della sua legislazione nazionale o dei suoi impegni internazionali. Dall'altro, sempre secondo tale disposizione, l'adeguatezza della protezione assicurata dal paese terzo viene valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

72. In tal modo, l'articolo 25, paragrafo 6, della direttiva 95/46 attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta e mira ad assicurare, come rilevato dall'avvocato generale al paragrafo 139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

73. È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi.

74. Si evince dalla formulazione espressa dell'articolo 25, paragrafo 6, della direttiva 95/46 che è l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire un livello di protezione adeguato. Anche se gli strumenti dei quali tale

paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.

75. In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo.

76. Analogamente, alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo.

77. Inoltre, come rilevato dall'avvocato generale ai paragrafi 134 e 135 delle sue conclusioni, in sede di esame della validità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, occorre anche tenere conto delle circostanze intervenute successivamente all'adozione di tale decisione.

78. A tal riguardo, occorre constatare che, alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non assicura un livello di protezione adeguato, il

potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da un paese terzo risulta ridotto, cosicché è necessario procedere ad un controllo stretto dei requisiti risultanti dall'articolo 25 della direttiva 95/46, letto alla luce della Carta (v., per analogia, sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punti 47 e 48).

Sull'articolo 1 della decisione 2000/520

79. La Commissione ha considerato, all'articolo 1, paragrafo 1, della decisione 2000/520, che i principi di cui all'allegato I della medesima, applicati in conformità agli orientamenti forniti dalle FAQ di cui all'allegato II di detta decisione, garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti. Risulta da tale disposizione che sia tali principi sia tali FAQ sono stati pubblicati dal Dipartimento del commercio degli Stati Uniti.

80. L'adesione di un'organizzazione ai principi dell'approdo sicuro avviene sulla base di un sistema di autocertificazione, come si evince dall'articolo 1, paragrafi 2 e 3, di tale decisione, in combinato disposto con la FAQ 6 figurante all'allegato II a detta decisione.

81. Sebbene il ricorso, da parte di un paese terzo, ad un sistema di autocertificazione non sia di per sé contrario al requisito previsto dall'articolo 25, paragrafo 6, della direttiva 95/46, secondo il quale il paese terzo di cui trattasi deve garantire un livello di protezione adeguato «in considerazione della (…) legislazione nazionale o [degli] impegni internazionali» di tale paese, l'affidabilità di un siffatto sistema, con riferimento a tale requisito, poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali.

82. Nella specie, in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati

unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.

83. Inoltre, ai sensi dell'articolo 2 della decisione 2000/520, quest'ultima «dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi [dell'approdo sicuro] applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva [95/46]», senza tuttavia contenere le constatazioni sufficienti quanto alle misure tramite le quali gli Stati Uniti d'America assicurano un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

84. A ciò si aggiunge che, in conformità all'allegato I, quarto comma, della decisione 2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

85. A tal riguardo, al titolo B del suo allegato IV, la decisione 2000/520 sottolinea, per quanto attiene ai limiti ai quali è assoggettata l'applicabilità dei principi dell'approdo sicuro, che «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge».

86. In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

87. Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. A tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata).

88. Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

89. A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane,

dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale.

90. Inoltre, la suesposta analisi della decisione 2000/520 è corroborata dalla valutazione della stessa Commissione quanto alla situazione risultante dall'esecuzione di tale decisione. Infatti, in particolare ai punti 2 e 3.2 della comunicazione COM(2013) 846 final, nonché ai punti 7.1, 7.2 e 8 della comunicazione COM(2013) 847 final, il cui contenuto viene illustrato rispettivamente ai punti da 13 a 16, nonché ai punti 22, 23 e 25 della presente sentenza, tale istituzione ha constatato che le autorità americane potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione.

91. Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata).

92. Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punto 52 e la giurisprudenza ivi citata).

93. In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta [v. in tal senso, in relazione alla 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, pag. 54), sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punti da 57 a 61].

94. In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta (v., in tal senso, sentenza Digital Rights Ireland e a., C‑293/12 e C‑594/12, EU:C:2014:238, punto 39).

95. Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso

effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGT‑Rioja e a., da C‑428/06 a C‑434/06, EU:C:2008:488, punto 80).

96. Come è stato rilevato segnatamente ai punti 71, 73 e 74 della presente sentenza, l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione, come emerge segnatamente dai punti precedenti della presente sentenza.

97. Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

98. Di conseguenza, e senza che occorra esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto, si deve concludere che l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido.

Sull'articolo 3 della decisione 2000/520

99. Si evince dalle considerazioni svolte ai punti 53, 57 e 63 della presente sentenza che, considerato l'articolo 28 della direttiva 95/46, letto alla luce, segnatamente, dell'articolo 8 della Carta, le autorità

nazionali di controllo devono poter esaminare, in piena indipendenza, ogni domanda relativa alla protezione dei diritti e delle libertà di una persona con riguardo al trattamento di dati personali che la riguardano. Ciò vale in particolare allorché, in occasione di una siffatta domanda, tale persona sollevi questioni attinenti alla compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva, con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

100. Tuttavia, l'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 contiene una disciplina specifica quanto ai poteri di cui dispongono le autorità nazionali di controllo con riferimento ad una constatazione effettuata dalla Commissione in relazione al livello di protezione adeguato, ai sensi dell'articolo 25 della direttiva 95/46.

101. Così, ai sensi di tale disposizione, tali autorità possono, «[f]atto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva [95/46], (…) sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi [della decisione 2000/520]», a condizioni restrittive che fissano una soglia elevata di intervento. Per quanto tale disposizione non pregiudichi i poteri di dette autorità di adottare misure intese ad assicurare il rispetto delle disposizioni nazionali adottate in applicazione di questa direttiva, cionondimeno essa esclude che le medesime possano adottare misure intese a garantire il rispetto dell'articolo 25 della direttiva medesima.

102. L'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 deve pertanto essere inteso nel senso che esso priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46, nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato, sul fondamento dell'articolo 25, paragrafo 6, di tale direttiva, che un paese terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

103. Orbene, il potere di esecuzione che il legislatore dell'Unione ha attribuito alla Commissione con l'articolo 25, paragrafo 6, della direttiva 95/46 non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo previsti al punto precedente della presente sentenza.

104. Ciò premesso, occorre constatare che, adottando l'articolo 3 della decisione 2000/520, la Commissione ha ecceduto la competenza attribuitale all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che, per questo motivo, esso è invalido.

105. Poiché gli articoli 1 e 3 della decisione 2000/520 non possono essere separati dagli articoli 2 e 4, nonché dagli allegati alla medesima, la loro invalidità inficia la validità di tale decisione nel suo complesso.

106. Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida.

Sulle spese

107. Nei confronti delle parti nel procedimento principale, la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) L'articolo 25, paragrafo 6, della 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, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a

norma della direttiva 95/46 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, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

2) La decisione 2000/520 è invalida.

TRIBUNALE ROMA, Sezione I civile, sentenza 3 dicembre 2015, n. 23771

Nel bilanciamento di opposti interessi, spesso il diritto all'oblio soccombe al diritto all'informazione, specialmente laddove il soggetto interessato rivesta una funzione di natura pubblica, quale quella dell'avvocato.

Ragioni di fatto e di diritto della decisione

Con ricorso depositato il 17/12/2014 il ricorrente, avvocato, ha convenuto in giudizio la società resistente chiedendo, sul presupposto dell'esistenza di un diritto all'oblio, la deindicizzazione di quattordici links risultanti da una ricerca a proprio nome, effettuata tramite il motore di ricerca (...), meglio elencati nell'atto introduttivo, nei quali era contenuto il riferimento ad una risalente vicenda giudiziaria nella quale era rimasto coinvolto senza che fosse mai stata pronunciata alcuna condanna, con condanna della controparte al risarcimento del danno derivante dall'illegittimo trattamento dei suoi dati personali, da quantificarsi nella misura non inferiore ad Euro 1.000,00.

La società resistente si è costituita eccependo la nullità dell'avverso atto introduttivo ed evidenziando, preliminarmente, la cessazione della materia del contendere relativamente a quattro URL in contestazione (non comparendo gli stessi al momento della costituzione tra i risultati di ricerca e comunque corrispondendo a pagine web prive di contenuti); ha comunque sostenuto nel merito l'inesistenza del diritto all'oblio rivendicato da controparte in relazione alla notizia oggetto di doglianza, con particolare riferimento all'irrilevanza dell'asserita erroneità delle notizie, all'assenza del requisito del trascorrere del tempo, oltre che al ruolo dell'interessato nella vita pubblica. Ha quindi concluso chiedendo il rigetto dell'avversa domanda, anche sotto il profilo del risarcimento del danno, con vittoria di spese. Alla prima udienza del 9.6.2015 la causa, ritenuta matura per la decisione, è stata rinviata al 10.11.2015 per la discussione, con lettura del dispositivo all'esito della camera di consiglio. Deve premettersi l'infondatezza

dell'eccepita nullità dell'atto introduttivo per indeterminatezza della domanda, in considerazione della intelligibilità dei relativi petitum e causa petendi, tanto da consentire al giudice di pronunciarsi sulla richiesta di deindicizzazione ed alla resistente di difendersi adeguatamente, vista la consistente memoria di costituzione prodotta, unitamente alla pertinente produzione documentale effettuata. Occorre inoltre preliminarmente evidenziare che effettivamente dei quattordici url in contestazione solo dieci allo stato ancora rientrano tra i risultati della ricerca a nome dell'odierno ricorrente, per come correttamente indicato nella memoria di costituzione, con la conseguente esclusione dei predetti dall'effettuata richiesta di deindicizzazione. Quanto agli altri URL, nel merito, la domanda non è fondata e deve essere respinta per le ragioni che seguono. Tutti i links ancora rinvenibili sul motore di ricerca (...) a nome di contengono il riferimento a notizie di cronaca circa una vicenda giudiziaria in cui il medesimo sarebbe rimasto coinvolto nel 2012/2013 unitamente ad altri personaggi romani, alcuni esponenti del clero ed altri ricondotti alla criminalità della c.d. (...), relativamente a presunte truffe e guadagni illeciti realizzati dal sodalizio criminoso. Ebbene, l'odierna vicenda deve essere correttamente inquadrata nel trattamento dei dati personali e nel c.d. diritto all'oblio, configurabile quale peculiare espressione del diritto alla riservatezza (privacy) e del legittimo interesse di ciascuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona derivante dalla reiterata pubblicazione di una notizia (ovvero nella specie il permanere della sua indicizzazione sui motori di ricerca), con pregiudizio alla propria reputazione e riservatezza (attesa l'attenuazione dell'attualità della notizia e dell'interesse pubblico all'informazione con il trascorrere del tempo dall'accadimento del fatto). Quest'ultimo, ove ritenuto sussistente, impedisce il protrarsi del trattamento stesso (e quindi l'indicizzazione, con la conseguente fondatezza della domanda di deindicizzazione nei confronti del gestore del motore di ricerca), per come risultante anche dalla recente pronuncia in materia resa dalla Corte di Giustizia Europea (Grande Sezione del 13.5.2014 nella causa C-131/12, sentenza Co.), oltre che dalle, conformi, successive decisioni del Garante per la protezione dei dati personali.

Secondo la citata pronuncia, in sintesi, gli utenti - in caso di ricerca nominativa su (...) - non possono ottenere dal gestore del motore di ricerca la cancellazione dai risultati di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico: il diritto all'oblio, infatti, deve essere bilanciato, ad avviso della corte, con il diritto di cronaca e con l'interesse pubblico alla conoscenza dei fatti acquisibili per il tramite dei links forniti dal motore di ricerca.

Ad avviso della Corte "occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica".

In altri termini, "dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi". Ed ancora "i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe

qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi". Solo in alcuni casi pertanto, prosegue la pronuncia, la persona interessata può "esigere dal gestore di un motore di ricerca che questi sopprima dall'elenco di risultati, che appare a seguito di una ricerca effettuata a partire dal nome di questa persona, dei link verso pagine web legittimamente pubblicate da terzi e contenenti informazioni veritiere riguardanti quest'ultima, a motivo del fatto che tali informazioni possono arrecarle pregiudizio o che essa desidera l' "oblio" di queste informazioni dopo un certo tempo". E' dunque necessario, spiega la Corte, "verificare in particolare se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome". La pronuncia citata ha quindi previsto l'obbligo, per un motore di ricerca (nel caso di specie, (...)), di rimuovere dai propri risultati (c.d. "deindicizzazione") i link a quei siti che siano ritenuti dagli interessati lesivi del loro "diritto all'oblio" (o "right to be forgotten"), in relazione alla pretesa a ottenere la cancellazione dei contenuti delle pagine web che, secondo l'interessato, offrono una rappresentazione non più attuale della propria persona. Nel caso in cui il motore di ricerca non accolga la richiesta, l'interessato potrà rivolgersi all'autorità nazionale per la protezione dei dati personali o all'autorità giudiziaria. Il 26 novembre 2014 l'Article 29 Data Protection Working Party (organo consultivo indipendente istituito in conformità all'articolo 29 della Direttiva 95/46/CE sulla protezione dei dati personali) ha pubblicato delle linee guida per l'implementazione della menzionata pronuncia della Corte di Giustizia (causa C-131/12), le quali per quel che qui specificamente interessa contengono una serie di criteri per orientare l'attività delle autorità nazionali nella gestione dei reclami degli interessati a seguito del mancato accoglimento, da parte del motore di ricerca, delle richieste di deindicizzazione, chiarendo che nessun criterio è di per sé determinante. Tra di essi, figura in primo luogo quello della natura del richiedente (in particolare, la circostanza per cui il richiedente rivesta

un ruolo di rilievo pubblico, come nel caso di personaggi politici, dovrebbe tendenzialmente orientare verso il diniego della richiesta di deindicizzazione). I principi esposti dalla riportata pronuncia e contenuti nelle linee guida emanate dal WP29 nello scorso mese di novembre sono stati infine integralmente recepiti dal Garante Privacy nelle decisioni rese successivamente ad essa (cfr., ad esempio, decisione n. 618 del 18 dicembre 2014 e n. 153 del 12.3.2015, quest'ultima prodotta dalla stessa parte resistente agli atti del giudizio). Nella decisione n. 618/2014 ad esempio il Garante ha respinto il ricorso di una persona che contestava la decisione del motore di ricerca di non deindicizzare un articolo che riferiva di un'inchiesta giudiziaria in cui risultava implicata osservando che il trattamento dei dati personali del ricorrente era avvenuto in origine per finalità giornalistiche secondo quanto previsto dagli artt. 136 ss. del Codice, nonché dalle disposizioni contenute nel "Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (allegato A del Codice medesimo, pubblicato sulla Gazzetta Ufficiale del 3 agosto 1998) ed era stato effettuato lecitamente e nel rispetto del principio di essenzialità dell'informazione riguardo a fatti di interesse pubblico relativi ad una vicenda giudiziaria recente e di indubbio interesse pubblico, soprattutto nell'ambito locale in cui si sono verificati i fatti descritti, non sussistendo quindi i presupposti riconosciuti dalla Corte di Giustizia europea nella sentenza del 13 maggio 2014 per l'esercizio del diritto all'oblio, anche in considerazione del fatto che i medesimi risultavano essere assolutamente recenti, oltre che di pubblico interesse. Ancora, nella seconda, è stato evidenziato che il diritto all'oblio, "anche ove sussista il suo principale elemento costitutivo, ovvero il trascorrere del tempo, incontra un limite quando le informazioni in questione sono riferite al ruolo che l'interessato riveste nella vita pubblica con conseguente prevalenza dell'interesse della collettività ad accedere alle stesse rispetto al diritto dell'interessato alla protezione dei dati" e sono state inoltre richiamate le predette linee guida nella parte in cui è individuato tra i criteri per la disamina delle richieste di deindicizzazione da parte dei motori di ricerca quello del ruolo dell'interessato nella vita pubblica e quello della natura pubblica o privata delle informazioni allo stesso riferite (è

stata infatti rigettata, nella richiamata prospettiva, la richiesta essendo le notizie state pubblicate in un arco temporale compreso tra il 2010 ed il 2012, risultate ad avviso del Garante recenti ed ancora di pubblico interesse in quanto riguardanti un'importante indagine giudiziaria non ancora conclusa, nell'ambito della quale i profili attinenti a momenti passati assumevano rilievo alla luce dell'attività professionale esercitata dall'istante).

Alla luce dei principi emersi dalle menzionate pronunce, oltre che dalle riportate linee guida, deve ritenersi che le notizie individuate tramite il motore di ricerca risultano, nella specie, piuttosto recenti; invero, il trascorrere del tempo, ai fini della configurazione del diritto all'oblio, si configura quale elemento costitutivo, come risultante anche dalla condivisibile sentenza n. 5525/2012 della Suprema Corte, nella quale questo viene configurato quale diritto "a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino oramai dimenticate o ignote alla generalità dei consociati", presupposto nella specie assolutamente insussistente, risalendo i fatti al non lontano 2013 (o al più al luglio 2012, secondo due dei risultati della ricerca) ed essendo pertanto gli stessi ancora attuali.

Del resto, la medesima appare di sicuro interesse pubblico, riguardando un'importante indagine giudiziaria che ha visto coinvolte numerose persone, seppure in ambito locale - romano, verosimilmente non ancora conclusa, stante la mancata produzione da parte dell'istante di documentazione in tal senso (archiviazioni, sentenze favorevoli...).

I dati personali riportati risultano quindi trattati nel pieno rispetto del principio di essenzialità dell'informazione.

Né può in questa sede il ricorrente dolersi della falsità delle notizie riportate dai siti visualizzabili per effetto della ricerca a suo nome, non essendo configurabile alcuna responsabilità al riguardo da parte del gestore del motore di ricerca (nella specie (...)), il quale opera unicamente quale "caching provider" ex art. 15 D.Lgs. n. 70/2003: in tale prospettiva pertanto il medesimo avrebbe dovuto agire a tutela della propria reputazione e riservatezza direttamente nei confronti dei gestori dei siti terzi sui quali è avvenuta la pubblicazione del singolo

articolo di cronaca, qualora la predetta notizia non sia stata riportata fedelmente, ovvero non sia stata rettificata, integrata od aggiornata coi successivi risvolti dell'indagine, magari favorevoli all'odierno istante (il quale peraltro deduce di non aver riportato condanne e produce certificato negativo del casellario giudiziale).

Ancora, risulta che l'odierno ricorrente è avvocato in Svizzera, libero professionista, circostanza che consente di ritenere che questo eserciti un "ruolo pubblico" proprio per effetto della professione svolta e dell'albo professionale cui è iscritto, laddove tale ruolo pubblico non è attribuibile al solo politico (cfr. linee guida del 26.11.20014) ma anche agli alti funzionari pubblici ed agli uomini d'affari (oltre che agli iscritti in albi professionali).

In conclusione, nell'ottica del sopra menzionato bilanciamento, l'interesse pubblico a rinvenire sul web attraverso il motore di ricerca gestito dalla resistente notizie circa il ricorrente deve prevalere sul diritto all'oblio dal medesimo vantato.

La domanda deve pertanto essere integralmente respinta, con liquidazione delle spese di lite secondo il principio della soccombenza, nella misura di cui in dispositivo ed in difetto di nota.

P.Q.M.

1) rigetta il ricorso;

2) condanna il ricorrente alla rifusione delle spese di lite in favore della parte resistente, complessivamente liquidate in Euro 4.000,00 per compensi, oltre accessori come per legge.

Così deciso in Roma il 24 novembre 2015.

Depositata in Cancelleria il 3 dicembre 2015.

Editoriale

Contributi

Rassegna giuridica

ISTITUTO ITALIANO PRIVACY

ISSN 2239 -7671

Anno VI, numero 3, 2015 - Diritto, Economia e Tecnologie della Privacy

€ 25,00