



**UNIVERSITÀ
DI TRENTO**

DIPARTIMENTO

FACOLTÀ DI GIURISPRUDENZA



**Università di Trento
Facoltà di Giurisprudenza
Diritto civile A-J
2020-2021
Prof. Roberto Caso**

Lezione 12 – Il diritto alla protezione dei dati personali

Questa lezione ha tre scopi:

1. Descrivere brevemente l'evoluzione che conduce dal diritto alla riservatezza alla protezione dei dati personali;
2. illustrare per sommi capi il Regolamento generale sulla protezione dei dati personali UE 2016/679, per concentrarsi sulla disciplina del trasferimento dei dati personali verso paesi terzi e organizzazioni internazionali;
3. presentare un caso che riguarda la didattica universitaria a distanza in tempi di pandemia.

Parte 1 – Dal diritto alla riservatezza alla protezione dei dati personali

Con l'avvento delle tecnologie digitali il diritto alla riservatezza (o diritto alla protezione della vita privata e familiare) non è più idoneo a cogliere tutti gli aspetti giuridici della nuova realtà.

In proposito, così scrive Stefano Rodotà [Rodotà, 2000]:

“Nella società dell'informazione tendono a prevalere definizioni funzionali della privacy che, in diversi modi, fanno riferimento alla possibilità di un soggetto di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano. La privacy, quindi, può essere più precisamente definita, in una prima approssimazione, come il diritto di mantenere il controllo sulle proprie informazioni”.

Giovanni Pascuzzi riassume la vicenda del cambiamento del panorama giuridico in questi termini [Pascuzzi, 2020, 81-82]:

“L'introduzione delle tecnologie informatiche ha comportato un cambiamento importante del campo della tutela dei diritti della personalità. L'avvento dei calcolatori ha richiesto l'adozione di specifici meccanismi di tutela perché il problema non era più (solo) quello di salvaguardare la vita privata di persone famose dall'aggressione portata dai mass media, bensì quello di scongiurare i pericoli più o meno palesi e avvertibili (discriminazioni in testa) derivanti a ciascun cittadino dalla facilità con la quale possono essere trattate e incrociate le informazioni che lo riguardano. La rivoluzione digitale comporta addirittura il cambiamento della nozione e del contenuto del diritto alla riservatezza: non più diritto a essere lasciati soli, ma diritto al controllo sui propri dati”.

Non a caso, la Carta dei diritti fondamentali dell'Unione Europea distingue i due diritti.

“Articolo 7

Rispetto della vita privata e della vita familiare

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni”.

“Articolo 8

Protezione dei dati di carattere personale

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

Parte 2 – Il Regolamento generale sulla protezione dei dati personali UE 2016/679 e il trasferimento verso paesi terzi e organizzazioni internazionali

In Italia la regolamentazione della protezione dei dati personali è recente.

Scrive in proposito Giorgio Resta [Resta 2019, 356]:

“Il processo normativo per l’introduzione nel nostro Paese di una disciplina apposita è stato lungo e tortuoso, sicché l’Italia, in ambito comunitario, è stato uno degli ultimi Paesi a dotarsi di regole specifiche al riguardo; tuttavia, il modello che ne è risultato è considerato uno dei più moderni e garantisti del mondo.

Dapprima, è stata ratificata ed eseguita la Convenzione europea sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (l. 21 febbraio 1989, n. 98). Poi si è pensato di attuare senza molte modifiche la direttiva comunitaria in materia (n. 46 del 1995). Si è approvata la l. 31 dicembre 1996, n. 675. È stato poi redatto un vero e proprio «codice della privacy» (d.lg. 30 giugno 2003, n. 196), che è stato modificato con decreto legislativo approvato l’8 agosto 2018, onde adeguare la normativa italiana al Regolamento europeo in materia di tutela dei dati personali (n. 2016/679), con particolare riferimento al trattamento di dati delicati e complessi (ad es. dati sulla salute)”.

A differenza del diritto alla riservatezza che, sul piano civilistico, richiedeva un’azione della persona davanti al giudice ordinario, il diritto alla protezione dei dati personali opera innanzitutto sul piano preventivo e si traduce in una disciplina del trattamento.

Il trattamento deve rispondere ad alcuni principii e regole. Ai doveri che gravano in capo ad alcuni soggetti – in primo luogo, al titolare del trattamento dei dati – corrispondono i diritti dell’interessato.

Alcuni principii sono enunciati, lo si è visto nella prima parte della lezione, già a livello di art. 8 della Carta dei diritti fondamentali dell’Unione Europea.

Quei principii ed altri sono specificati all’art. del Reg. 2016/679:

- a) liceità, correttezza e trasparenza;
- b) limitazione della finalità;
- c) minimizzazione dei dati;
- d) esattezza;
- e) limitazione della conservazione;
- f) integrità e riservatezza;
- g) responsabilizzazione.

La liceità del trattamento si basa sul consenso dell’interessato o su altre condizioni elencate all’art. 6 RGDP.

Il RGDP disciplina i diritti dell’interessato al capo III (art. 15-22):

- a) diritto di accesso;
- b) diritto di cancellazione (diritto all’oblio) v. lezione n. 14;
- c) diritto di limitazione del trattamento;
- d) diritto alla portabilità dei dati;
- e) diritto di opposizione;

e) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (v. lezione n. 16).

Questa disciplina incentrata sul trattamento spiega perché sia prevista un'autorità indipendente di controllo, in Italia denominata Garante per la protezione dei dati personali.

In questa sede occorre evidenziare alcune nozioni fondamentali contenute nel Regolamento generale sulla protezione dei dati personali UE 2016/679 RGPD o, nell'acronimo inglese, GDPR.

Per "dato personale" si intende:

"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Per trattamento si intende:

"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Per titolare del trattamento si intende:

"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

Per responsabile del trattamento si intende:

"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento."

Nel diritto dell'Unione Europea l'elevato livello di protezione dei dati personali deve coordinarsi con il principio della libera circolazione degli stessi dati all'interno del territorio.

La disciplina del trattamento dei dati personali è articolata e assai complessa.

Tra i problemi di maggior rilievo possono evidenziarsi i seguenti.

a) Come opera il bilanciamento tra il diritto alla protezione dei dati personali e altri diritti fondamentali? Il diritto dell'Unione Europea sembra rispondere a un assetto di valori in parte

diverso da quello posto alla base della Costituzione italiana [cfr. Salvi 2015]. Secondo una corrente di pensiero, il bilanciamento deve comunque passare dal principio di dignità enunciato dall'art. 1 della Carta dei diritti fondamentali dell'Unione Europea [Resta 2019, 358 ss.].

b) Qual è il rapporto tra il generale diritto della personalità, composto di vari aspetti (nome, immagine, onore, reputazione, decoro, riservatezza, identità, oblio ecc.) e il diritto alla protezione dei dati personali?

c) Nella dimensione aterritoriale di Internet è possibile garantire l'elevato livello di protezione dei dati personali declamato nel diritto dell'Unione Europea?

Nel rinviare ad altri testi [Resta 2019; Pascuzzi 2020] l'illustrazione dei fondamenti della disciplina del trattamento, in questa lezione si vuole accennare a un caso riguardante il problema sub c). Il caso riguarda il trasferimento dei dati dall'Unione Europea verso paesi terzi e la sorveglianza di massa.

Si tratta del caso oggetto della recente sentenza della Corte di Giustizia dell'Unione Europea nota come Scherms II.

Il caso verte sull'interpretazione della disciplina del trasferimento dei dati verso paesi terzi e organizzazioni internazionali contenuta nel capo V del RGPD.

In estrema sintesi si possono evidenziare i seguenti punti.

I) Tutte le disposizioni normative gravitano sul principio generale che il livello di protezione delle persone fisiche garantito dal RGPD non deve essere pregiudicato (art. 44).

II) Decisione della Commissione Europea. Il trasferimento è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono "un livello di protezione adeguato". In tal caso il trasferimento non necessita di autorizzazioni specifiche (art. 45).

III) In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito "garanzie adeguate" e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (art. 46). Tra le "garanzie adeguate" non soggette ad autorizzazioni specifiche da parte di un'autorità di controllo figurano le "norme vincolanti d'impresa" disciplinate dall'art. 47 e le "clausole tipo" di protezione dei dati adottate dalla Commissione.

IV) Deroche in specifiche situazioni (art. 49). In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, l'art. 49 elenca una serie di deroghe specifiche che rendono ammissibile il trasferimento dei dati.

La disciplina del trasferimento dei dati verso paesi terzi e organizzazioni internazionali ricalca ampliandola quella della dir. 1995/46.

Uno dei problemi di maggior rilievo si pone con riferimento al trasferimento dei dati personali verso gli USA dove la sorveglianza digitale di massa è una pratica consolidata.

La Commissione Europea, sulla base della disciplina della dir. 1995/46, aveva emanato decisione 2000/520/CE che ammetteva il trasferimento dei dati personali verso gli USA sulla base di un accordo con questi ultimi denominato Safe Harbor (approdo sicuro).

Maximilian Schrems, un attivista austriaco che difende i diritti e le libertà su Internet, avviava un reclamo al Data Protection Commissioner (Commissario per la protezione dei dati) irlandese concernente il fatto che Facebook Ireland Ltd trasferiva negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in quel paese.

Nel frattempo, era scoppiato il c.d. “datagate” innescato dalle rivelazioni dell’ex agente dell’apparato di spionaggio statunitense Edward Snowden. Da quelle rivelazioni si veniva a sapere che i servizi di intelligence statunitensi avevano da tempo avviato programmi di sorveglianza di massa basati sul trattamento dei dati personali, anche dei cittadini europei.

Il 25 giugno 2013 il sig. Schrems investiva il Commissario per la protezione dei dati irlandese

“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»)” [CGUE sentenza 6 ottobre 2015 C-362/14 (Schrems I)].

Il Commissario si rifiutava di dar corso al reclamo. Schrems agiva allora presso il giudice ordinario (High Court) irlandese che sospendeva il giudizio proponendo le seguenti questioni pregiudiziali alla Corte di Giustizia UE sull’interpretazione della dir. 1995/46:

“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.”

La Corte di Giustizia nella sentenza 6 ottobre 2015 C-362/14 (Schrems I) così risolveva le questioni pregiudiziali:

“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”.

A seguito della dichiarazione di invalidità della decisione 2000/520 sul porto sicuro, la Commissione emanava una seconda decisione (UE) 2016/1250 in data 16 luglio che recepiva un nuovo accordo tra USA e UE denominato “privacy shield UE-USA” (scudo UE-USA per la privacy).

Ritenendo che anche questo nuovo quadro giuridico non garantisse la protezione dei dati personali degli europei, Schrems avviava una nuova fase della sua battaglia a difesa della privacy.

In una denuncia, presentata il 1° dicembre 2015, all'autorità irlandese di controllo della protezione dei dati personali:

“il sig. Schrems ha fatto valere, in particolare, che il diritto statunitense impone a Facebook Inc. di mettere a disposizione delle autorità statunitensi, quali la National Security Agency (NSA) e le Federal Bureau of Investigation (FBI), i dati personali che le sono trasferiti. Egli ha sostenuto che, poiché tali dati sono utilizzati nell'ambito di diversi programmi di sorveglianza in modo incompatibile con gli articoli 7, 8, e 47 della Carta, la decisione CPT non può giustificare il trasferimento dei suddetti dati verso gli Stati Uniti. Il sig. Schrems ha pertanto chiesto al Commissario di vietare o di sospendere il trasferimento dei suoi dati personali verso Facebook Inc. il 1° dicembre 2015, il sig. Schrems ha fatto valere, in particolare, che il diritto statunitense impone a Facebook Inc. di mettere a disposizione delle autorità statunitensi, quali la National Security Agency (NSA) e le Federal Bureau of Investigation (FBI), i dati personali che le sono trasferiti. Egli ha sostenuto che, poiché tali dati sono utilizzati nell'ambito di diversi programmi di sorveglianza in modo incompatibile con gli articoli 7, 8, e 47 della Carta, la decisione CPT non può giustificare il trasferimento dei suddetti dati verso gli Stati Uniti. Il sig. Schrems ha pertanto chiesto al Commissario di vietare o di sospendere il trasferimento dei suoi dati personali verso Facebook Inc.”

“Ritenendo che [...] la denuncia riformulata del sig. Schrems sollevasse la questione della validità della decisione CPT, il 31 maggio 2016 il Commissario ha adito la High Court (Alta Corte), fondandosi sulla giurisprudenza risultante dalla sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650, punto 65), affinché la High Court si rivolgesse alla Corte su tale questione. Con decisione del 4 maggio 2018 la High Court (Alta Corte) ha sottoposto alla Corte [UE] il [...] rinvio pregiudiziale”.

Le questioni pregiudiziali erano diverse. Qui interessa evidenziarne tre che la Corte di Giustizia UE con sentenza 16 luglio 2020 C-311/18 (Schrems II) così risolveva:

“L’articolo 46, paragrafo 1, e l’articolo 46, paragrafo 2, lettera c), del regolamento 2016/679 devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all’interno dell’Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell’Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell’Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest’ultimo, in particolare quelli enunciati all’articolo 45, paragrafo 2, di detto regolamento”.

“L’articolo 58, paragrafo 2, lettere f) e j), del regolamento 2016/679 deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, l’autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell’Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell’Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest’ultimo”.

“La decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull’adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, è invalida”.

A seguito della dichiarazione di invalidità della decisione di esecuzione (UE) 2016/1250 sullo scudo UE-USA per la privacy si stanno oggi moltiplicando i reclami alle autorità di controllo dei vari paesi membri dell’UE finalizzati a vietare il trasferimento dei dati personali verso gli USA.

Parte 3 – Didattica universitaria a distanza e trasferimento dei dati verso paesi terzi. Un caso

Ecco il caso:

“A causa della pandemia da COVID-19 l’Università dell’Isola che non c’è (in Italia) decide di garantire la prosecuzione dei propri corsi attraverso l’organizzazione di insegnamenti online (c.d. didattica a distanza o DAD). L’UniCNC si serve di diverse piattaforme per la didattica online, tra queste vi è anche la sempre più diffusa piattaforma statunitense Zoom.

Problema 1: Chi è il titolare del trattamento dei dati personali?

Problema 2: Le privacy policy di Zoom sono compatibili con il RGPD e l'interpretazione che ne è stata data dalla CGUE nel caso Schrems II?"

Bibliografia

G. Pascuzzi, *Il diritto dell'era digitale*, V ed., Bologna, Il Mulino, 2020

G. Resta, in G. Alpa e G. Resta, *Le persone e la famiglia 1. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile* diretto da R. Sacco, Utet, Torino, 2019, pp. 145-632

S. Rodotà, *Riservatezza*, in *Enciclopedia Treccani*, 2000

C. Salvi, *Capitalismo e diritto civile*, Bologna, Il Mulino, 2015

Roberto Caso

E-mail:

roberto.caso@unitn.it

Web:

<http://www5.unitn.it/People/it/Web/Persona/PER0000633#INFO>

<http://lawtech.jus.unitn.it/>

<https://www.robertocaso.it/>

Copyright by Roberto Caso

Licenza Creative Commons

Quest'opera è distribuita con [Licenza Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale](#)

La citazione di testi e la riproduzione di immagini costituisce esercizio dei diritti garantiti dagli art. 2, 21 e 33 Cost. e dall'art. 70 l. 1941/633