Archivio selezionato: Dottrina

IL REGOLAMENTO EUROPEO SULLA PRIVACY: ORIGINI E AMBITO DI APPLICAZIONE

Europa e Diritto Privato, fasc.4, 2016, pag. 1249
Maria Gabriella Stanzione
Classificazioni: UNIONE EUROPEA - Ce - - riservatezza
Sommario: 1. Cenni introduttivi. - 2. L'ambito di applicazione territoriale: verso un'« applicazione universale » del diritto dell'Unione Europea? - 3. L'ambito di applicazione materiale - 4. Le nuove prospettive della tutela della privacy.

1. Il processo di evoluzione della tutela dei dati personali, fondato sul crescente coinvolgimento della persona nella gestione della propria sfera privata, prende l'avvio nel momento in cui l'integrazione europea inizia a guardare oltre il mercato unico (1), verso l'orizzonte assai più ampio dei diritti della persona (2). Alla persona è, così, riconosciuto un potere di controllo e di intervento sulla base di un diritto all'autodeterminazione informativa, che gradualmente inizia a configurarsi quale autonomo diritto alla protezione dei dati personali (3).

Con il Trattato di Lisbona si tocca il punto più alto di tale percorso, dopo la mancata occasione della c.d. Costituzione europea: il nuovo art. 6 TUE sancisce l'accoglimento del sistema di principi e diritti fondamentali contemplati dalla Carta di Nizza tra le fonti originarie dell'Unione, al medesimo livello dei trattati, nonché l'adesione alla CEDU, alle cui norme è attribuito valore di principi generali (4).

In linea con i principi stabiliti dalla Convenzione di Strasburgo del 1981 (5), la Carta dei diritti fondamentali dell'Unione sancisce, all'art. 8, il diritto alla protezione dei dati personali, riconoscendolo come diritto autonomo, separato da quello al rispetto della propria vita privata e familiare (art. 7). Ad esso deve aggiungersi l'art. 16 TFUE, così come modificato dal Trattato di Lisbona, che attribuisce ad ogni persona il diritto alla protezione dei propri dati personali. Si trascorre, per dirla con Stefano Rodotà, dalla tutela statica e negativa della riservatezza, che, costruita sul modello della proprietà privata, si esaurisce nell'esclusione delle interferenze altrui — in un *right to be let alone* — alla protezione dei dati personali, provvista altresì di una tutela dinamica, composta di regole rigorose che delineano le modalità del trattamento e conferiscono poteri di controllo e di intervento alla persona interessata (6).

Se non è possibile ridurre la persona ai suoi dati, sempre più questi sono indispensabili per il libero sviluppo della personalità e la loro manipolazione può incidere sulla percezione che essa ha di sé e sulla sua rappresentazione nella società (7). Si individua, così, il punto di congiunzione tra tutela dell'identità personale e protezione dei dati personali, per cui non v'è l'una senza il soddisfacimento dell'altra nella prospettiva della dignità della persona e della libera costruzione della personalità che discende dalle tradizioni costituzionali comuni (art. 2 cost. it., art. 2 I *GrundGesetz*, art. 9.2 *const. esp.* e così via) (8).

Quale diritto fondamentale, la protezione dei dati personali può confliggere con altri diritti di pari rango, come quello all'informazione, per cui la piena soddisfazione dell'uno spesso significa rendere inoperante l'altro (9). Siffatta evenienza deve essere ben distinta dai conflitti con altri interessi — che taluni tornano pericolosamente a definire superiori — quali la sicurezza pubblica e le ragioni di ordine pubblico. Dall'altro lato, premono le istanze del mercato e dei suoi protagonisti. La ricerca di un punto di equilibrio tra le opposte esigenze in gioco informa di sé la dir. 24-10-1995 n. 46, che per prima stabilisce i principi e gli standard della disciplina comunitaria in tema di protezione dei dati personali (10).

L'intervento armonizzatore europeo si inserisce in un contesto caratterizzato da una forte disomogeneità nella protezione dei dati personali. Se la gran parte degli ordinamenti europei si era dotata di normative in attuazione della citata Convenzione di Strasburgo del 1981 —

particolarmente interessante il *Data Protection Act* inglese del 1984 —, in altre esperienze, tra cui l'Italia, perdurava una situazione di totale vuoto normativo, che dottrina e giurisprudenza stentavano a colmare. La direttiva del 1995 diviene pertanto un significativo punto di riferimento nella materia tanto all'interno che al di fuori dell'ambito comunitario.

Essa ha il merito di introdurre principi e strumenti tesi a ridurre la posizione di asimmetria informativa tra titolare del trattamento e persona interessata, come il diritto di quest'ultima al controllo sui propri dati personali, la limitazione delle finalità del trattamento, la qualità dei dati.

Al centro della disciplina si pone il consenso della persona interessata, libero, informato e inequivocabilmente prestato, vale a dire accompagnato da un'informativa sufficientemente dettagliata, che indichi in modo rigoroso le finalità della raccolta, l'entità dei dati, le modalità di conservazione, nonché l'eventuale trasmissione a terzi sotto forma di comunicazione o diffusione dei medesimi. Da tale principio, discendono una serie di diritti dell'interessato — nonché di corrispondenti obblighi gravanti sul titolare del trattamento —, tra cui il diritto all'informazione in tutte le fasi del trattamento stesso, il diritto alla revoca del consenso, quello alla cancellazione dei dati ceduti e via enumerando.

E, tuttavia, dinanzi all'incessante avanzare del progresso scientifico e tecnologico, che introduce sempre nuove modalità di invasione nella sfera privata delle persone — si pensi alle tecniche di profilazione, al *data mining*, alla *dataveillance* — la logica del consenso rivela tutta la sua insufficienza. Tale problema è già affrontato *in nuce* nella dir. 95/46, con l'adozione, accanto al profilo del consenso, di una serie di principi volti a limitare l'attività di raccolta dei dati personali, che impongono al titolare l'obbligo di trattare i soli dati necessari ad adempiere alle finalità prestabilite, dati che devono essere adeguati, pertinenti e proporzionati alle medesime finalità. In tale prospettiva, una delle norme più lungimiranti della direttiva citata è forse quella dell'art. 15, che stabilisce che “gli Stati membri riconoscono ad ogni persona il diritto a non essere sottoposta ad una decisione che produca effetti giuridici o che abbia effetti significativi nei suoi confronti, fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento e così via”.

L'attuazione di siffatto principio si configura negli anni successivi quale obiettivo estremamente difficile da raggiungere, nonostante i tentativi dei legislatori nazionali e l'adozione di ulteriori normative in ambito sovranazionale, tra cui la dir. 15-12-1997 n. 66 sul « trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni » (11) e la dir. 12-7-2002 n. 58 relativa al « trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche » (12), che si mostrano probabilmente troppo prudenti nella ricerca di un contemperamento tra tutela dei diritti dei singoli e interessi del mercato, nonché tra i primi e le ragioni di matrice pubblicistica, in primo luogo quelle concernenti la sicurezza pubblica.

Ben più concreta considerazione — a prescindere dalla validità delle soluzioni fornite — per un'effettiva attuazione dei principi in materia di protezione dei dati personali dimostra, invece, la Corte di Giustizia, in modo costante nella sua giurisprudenza e in particolare nelle assai note e controverse decisioni *Digital Rights Ireland Ltd.* (13), *Google Spain SL* (conosciuta anche come sentenza *Costeja González*) (14) e *Schrems* (15). Non è questa la sede per approfondire le problematiche poste dalle pronunce citate, che hanno sollevato un dibattito dottrinale tuttora assai vivace. Basterà qui ricordare che, nella prima, la Corte di Giustizia dichiara invalida la direttiva 2006/24/CE sulla conservazione dei dati personali ai fini di renderli disponibili per il perseguimento di reati gravi, come quelli legati alla criminalità organizzata e al terrorismo, ritenendo che essa interferisse in modo eccessivo con i diritti fondamentali delle persone nonché violasse il principio di proporzionalità. Nella sentenza *Google Spain* i giudici europei affermano categoricamente che i diritti della personalità — in particolare si discorre del diritto alla c.d. de-indicizzazione — prevalgono sugli interessi economici degli operatori (16). Nell'ultima decisione, relativa ai flussi transfrontalieri di dati di cittadini europei verso gli Stati Uniti, la Corte

sancisce l'incompatibilità di un'aprioristica supremazia delle esigenze di carattere pubblicistico con il sistema di principi posto alla base della dir. 95/46 (17).

A ben vedere, la giurisprudenza della Corte di Giustizia ha in tali casi confermato una linea forte di protezione della *privacy*, anticipando, altresì, meccanismi di tutela che saranno recepiti nella nuova *General Data Protection Regulation* (18). Tra questi, il c.d. *target principle*, per cui si estende l'applicazione territoriale anche ai soggetti stabiliti al di fuori dell'Unione, laddove gli stessi offrano beni o servizi agli individui ivi residenti ovvero ne controllino il comportamento.

Occorre chiedersi, allora, se si vada verso un'applicazione universale del diritto dell'Unione europea (19), fondata sulla natura di diritto fondamentale della protezione dei propri dati personali, attribuito alle persone in quanto tali a prescindere dalla cittadinanza e dalla nazionalità (20). Ben al di là del più limitato obiettivo unificatore di fornire un "livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali nel territorio dell'Unione" (21); obiettivo che appare, altresì, più vicino grazie all'adozione di un regolamento (22).

Nei lavori preparatori della nuova normativa (23) è emerso più volte che, sebbene la *ratio* e i principi della dir. 95/46 rimangano validi e siano posti al centro del regolamento del 2016, essa non ha impedito la frammentazione della protezione dei dati personali nel territorio dell'Unione né ha eliminato l'incertezza giuridica e la convinzione — largamente diffusa — che in particolare le operazioni condotte in rete possano comportare dei rischi per la tutela delle persone.

Sotto questo profilo, se è fuor di dubbio che lo strumento del regolamento sia funzionale a conseguire un elevato livello di unificazione, d'altra parte la disciplina prevede in taluni casi un certo margine di manovra degli Stati membri, che — secondo il considerando n. 10 regolamento cit. — "dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento" né si esclude che "il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito". Tutto questo, ovviamente, sempre nel quadro dei principi generali e delle norme del regolamento medesimo.

2. Nel nuovo regolamento si stabilisce la regola generale in materia di applicazione territoriale, in virtù della quale la disciplina in parola si applica al trattamento dei dati personali "effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" (24), ovvero al trattamento effettuato da un titolare stabilito in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale, ai sensi dell'art. 3, par. 3, regolamento cit. (25).

L'applicabilità della normativa europea si fonda, pertanto, sulla nozione di stabilimento, definito dal considerando n. 22 « l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile » nel contesto delle quali sono trattati i dati personali. Si precisa, altresì, che non è determinante la forma giuridica assunta, si tratti di una succursale o di una filiale dotata di personalità giuridica.

Quello che rappresentava una delle questioni cruciali sotto il regime della dir. 95/46, vale a dire l'individuazione del diritto nazionale applicabile (26), viene meno con il passaggio alla fonte regolamentare. In passato, la soluzione di siffatto problema si fondava sul criterio dello stabilimento, il quale subisce un significativo mutamento di funzione con l'entrata in vigore del nuovo regolamento. Nel contesto di una disciplina uniformata, infatti, il nodo centrale diviene quello dell'applicabilità della normativa allorché il titolare del trattamento sia stabilito in un paese terzo.

A tal proposito, risulta utile analizzare l'evoluzione della nozione di stabilimento e della sua

funzione nell'ambito che qui ci occupa (27). In via generale, il diritto di stabilimento costituisce una delle modalità in cui si concretizzano le quattro libertà di circolazione delle persone, dei servizi, delle merci e dei capitali, poste a fondamento dell'integrazione socio-economica europea, rendendo possibile la mobilità dei professionisti e delle imprese nel territorio dell'Unione. Tale diritto è riconosciuto tanto ai cittadini che esercitano attività economiche quanto alle persone giuridiche che operano legalmente sul territorio di uno Stato membro (artt. 49 e 56 TFUE). Ne discende che essi possono svolgere un'attività economica a livello transfrontaliero, stabile e continuativa, pur conservando il proprio stabilimento nel paese d'origine (28).

Sotto il profilo della protezione dei dati personali, la nozione di stabilimento ha attraversato una serie di rielaborazioni ad opera della dottrina e della giurisprudenza, ancor prima che iniziasse il percorso di riforma della disciplina europea, soprattutto con riferimento all'utilizzo di servizi online, che al tempo della direttiva del 1995 non esistevano o non si configuravano nelle medesime modalità. I primi e più rilevanti problemi interpretativi, infatti, sono emersi con riguardo alle questioni — assurte al centro del dibattito nell'ultimo decennio — relative alla responsabilità degli Internet Service Provider (ISP) (29), nell'ipotesi in cui le imprese titolari del trattamento abbiano la propria sede al di fuori dello Spazio Economico Europeo.

Le prime risposte si rinvengono nella giurisprudenza della Corte di Giustizia e nei pareri del Gruppo di Lavoro *ex* Articolo 29 n. 1 del 2008 (30) e n. 8 del 2010 (31); questi ultimi a loro volta hanno influenzato la più recente elaborazione giurisprudenziale della Corte di Lussemburgo. Nel primo dei pareri citati si consolida la nozione di « esercizio effettivo e reale dell'attività mediante un'organizzazione stabile », che si realizza allorché al trattamento dei dati personali partecipino stabilimenti situati nel territorio di uno Stato membro, nonostante la sede dell'impresa titolare si trovi in un paese terzo, mentre nessun rilievo assume la forma giuridica di detto stabilimento (filiale dotata di personalità giuridica, agenzia o semplice ufficio locale). Al centro della questione si pone, dunque, la condizione che il trattamento sia svolto nel contesto delle attività di uno stabilimento situato in uno Stato membro, che si realizza ogniqualvolta il soggetto stabilito nel territorio di uno Stato membro svolga un ruolo centrale per il trattamento medesimo, ad esempio per il fatto che su di esso ricade la responsabilità dei rapporti con gli utenti del servizio in una data giurisdizione o l'obbligo di adempiere alle decisioni giudiziarie o delle autorità garanti ovvero che esso vende pubblicità mirata agli abitanti di quello Stato. Il criterio dell'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile è posto a fondamento del successivo Parere del 2010 sul diritto nazionale applicabile. Il Gruppo di Lavoro ha, infatti, affermato che l'ambito di applicazione territoriale della normativa nazionale di attuazione della dir. 95/46 dipende dal luogo di stabilimento del titolare del trattamento, per la cui individuazione non rilevano i criteri della cittadinanza dell'interessato, del suo luogo di residenza abituale, né dell'ubicazione fisica dei dati personali.

La Corte di Giustizia ha accolto tali impostazioni, elaborando una nozione « flessibile » di stabilimento. In particolare, nella citata sentenza *Google Spain SL*, i giudici europei osservano che per determinare se una società dispone di uno « stabilimento » 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 dei servizi in questione" (32). Nella successiva pronuncia *Weltimmo*, la Corte chiede al giudice del rinvio di tenere concretamente conto del fatto che "l'attività [..] 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 del fatto che la società possiede "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" (33).

La nuova disciplina adotta tale prospettiva nella misura in cui accoglie un « approccio orientato ai

destinatari del servizio » qualora il titolare del trattamento non sia stabilito nel territorio dell'Unione. Due sono, infatti, i criteri adottati dal secondo paragrafo dell'art. 3, nei quali è possibile rinvenire una delle novità più rilevanti del regolamento in parola: da un lato, l'offerta di beni o la prestazione di servizi a persone interessate nell'Unione e, dall'altro — andando al di là di quanto proposto dal Gruppo di Lavoro —, il monitoraggio del comportamento di tali soggetti, allorché esso avvenga all'interno dell'Unione.

Nel primo caso, infatti, si è nell'ambito dell'orientamento analizzato, per cui le nuove questioni interpretative si porranno con riferimento agli elementi probanti l'esistenza di un'offerta di beni o servizi, a prescindere dalla sussistenza di un'obbligazione di pagamento dell'interessato. Nella seconda ipotesi, si assiste ad una significativa innovazione dal momento che le risposte all'interrogativo sull'applicabilità della disciplina europea si legano all'interpretazione della nozione di « monitoraggio del comportamento degli utenti » (34) — e alla sua variabilità — e apre ancora di più le frontiere dell'applicazione del diritto dell'Unione in materia di protezione dei dati personali.

In tale prospettiva è possibile interpretare la norma del nuovo regolamento, che prevede — nelle ipotesi in cui trova applicazione l'art. 3, par. 2 — l'obbligo in capo al titolare o al responsabile del trattamento di designare un rappresentante nell'Unione (35). Tale previsione non si applica, tuttavia, alle autorità o agli organismi pubblici ovvero se il trattamento dei dati è occasionale, non riguarda dati sensibili o dati relativi a reati e condanne penali ed è improbabile che esso comporti un rischio per i diritti e le libertà delle persone, tenendo conto della natura, contesto, ambito di applicazione e finalità del trattamento.

3. È possibile riscontrare un sensibile ampliamento dell'ambito di applicazione materiale del nuovo regolamento europeo, sebbene apparentemente la norma del paragrafo 1 dell'art. 2 non si discosti dalla corrispondente previsione della dir. 95/46, discorrendo di “trattamento interamente o parzialmente automatizzato di dati personali” e di trattamento “non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi”. A ben vedere, dal confronto tra le definizioni di « dati personali » e di « trattamento » accolte nei due atti normativi emergono talune — non trascurabili — differenze. In primo luogo, viene estesa la nozione di dati personali, in relazione alle informazioni che identificano o rendono identificabile la persona: nuovi sono, infatti, gli esempi di identificativi quali nome, numero di identificazione, dati relativi all'ubicazione, identificativo online ovvero specifici elementi relativi all'identità genetica della persona.

Tra le definizioni ora si annoverano, altresì, i dati genetici, vale a dire relativi alle caratteristiche genetiche, ereditarie o acquisite di una persona, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute, risultanti in particolare da un campione biologico e i cc.dd. dati biometrici, definiti come le informazioni ottenute da un trattamento tecnico specifico relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona (ad. es immagine facciale o dati dattiloscopici).

La nuova disciplina non precisa ulteriormente la nozione di dati personali, che rimane piuttosto ambigua (36) se si fa riferimento soltanto al testo dispositivo, laddove indicazioni interpretative possono essere rinvenute nel preambolo, nonostante sia privo di valore giuridico vincolante (37): al considerando n. 26 si enuncia che per determinare se una persona sia identificabile è opportuno valutare “tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona direttamente o indirettamente”. Si specifica, inoltre, che gli individui potrebbero essere associati con identificativi online forniti dai loro dispositivi, come indirizzi IP, marcatori temporanei (i cc.dd. *cookies*) ovvero *tag* di identificazione a radiofrequenza (*RFID tags*) (38). Ne discende che i trattamenti — come la profilazione — possono anche concernere soggetti che non saranno mai identificati con il proprio nome (39).

In ogni caso, il regolamento amplia significativamente l'elenco di operazioni che — singolarmente

o nel loro insieme, nonché compiute o meno con l'ausilio di processi automatizzati — costituiscono un trattamento di dati personali. Alle tradizionali attività — di raccolta, registrazione, organizzazione, conservazione, elaborazione o modifica, estrazione, consultazione, impiego, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, nonché congelamento, cancellazione o distruzione — si aggiungono la strutturazione, l'uso e la limitazione.

Nuova è la definizione di « profilazione », che si riferisce a qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di essi per valutare determinati aspetti relativi ad una persona fisica, in particolare le cc.dd. analisi predittive riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti della persona interessata (art. 4.5).

Non muta, invece, la definizione di archivio di dati personali, che continua a riferirsi a qualsiasi insieme strutturato di dati personali accessibile secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Tra le nuove misure finalizzate alla protezione dei dati personali, il regolamento in parola introduce la « pseudonimizzazione », definita dall'art. 4, n. 5, regolamento cit., come il trattamento di dati personali in modo tale che questi non possano più essere attribuiti ad una persona specifica, senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e protette da misure tecniche volte a scongiurare l'identificazione delle persone fisiche. Nel preambolo si specifica che la pseudonimizzazione è finalizzata a ridurre i rischi per le persone interessate e aiutare i titolari e i responsabili del trattamento a rispettare gli obblighi di protezione dei dati (40). Tuttavia, la precisazione che l'introduzione di siffatto concetto nel regolamento “non è intesa a precludere altre misure di protezione dei dati” è diretta ad evitare che la sua applicazione comporti un aggiramento del sistema di tutela delineato dalla normativa europea (41).

Così come nella direttiva previgente, il regolamento passa poi a delimitare in negativo l'ambito di applicazione materiale della nuova disciplina. Come stabilito dal paragrafo 2 dell'art. 2, essa non si applica ai trattamenti di dati effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione né quelli svolti dalle persone fisiche nell'esercizio di attività a carattere esclusivamente personale o domestico (c.d. *household exclusion provision*). Quest'ultima riproduce testualmente la disposizione corrispondente della dir. 95/46, nonostante i non pochi dubbi interpretativi sollevatisi nella pratica applicativa sui criteri per stabilire il carattere personale o domestico di talune operazioni (42), come quelle legate all'uso dei social network (43).

Sono esclusi, altresì, i trattamenti effettuati dalle autorità pubbliche al fine di prevenire, accertare o perseguire reati, per dare esecuzione a sanzioni penali ovvero per contrastare o prevenire le minacce alla sicurezza pubblica (art. 2, par. 2 lett. d).

La nuova disciplina non si applica all'ulteriore profilo del trattamento di dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione europea, per i quali vigono le specifiche previsioni del reg. 18-12-2000 n. 45, che, tuttavia, dovranno essere adeguate ai principi e alla disciplina del 2016.

Infine, si stabilisce che il regolamento non pregiudica l'applicazione della dir. 8-6-2000 n. 31, relativa al commercio elettronico, in particolare per quel che concerne le norme sulla responsabilità dei prestatori di servizi (artt. 12-15 della direttiva citata) (44).

4. Dinanzi all'inadeguatezza mostrata da un approccio essenzialmente riparatorio, posto al centro della dir. 95/46, la nuova disciplina accoglie un'impostazione maturata nell'ultimo decennio, fondata su una tutela preventiva, che utilizza gli strumenti della valutazione di impatto sulla protezione dei dati personali e della c.d. protezione fin dalla progettazione e per impostazione

predefinita (nella terminologia inglese, *privacy by design* e *privacy by default*). La tutela, pertanto, è anticipata ad un momento anteriore al trattamento dei dati personali e prevede un impegno attivo dei titolari — in particolare quando si tratti di società di telecomunicazione — fin dalla progettazione dei prodotti e servizi il cui utilizzo incida sui dati degli utenti.

La valutazione di impatto sulla protezione dei dati personali è una tecnica utilizzata già da tempo da parte delle imprese e può avere ad oggetto tanto i trattamenti individualmente considerati, che l'aggregazione — e interazione — nella loro globalità di differenti trattamenti relativi alle medesime informazioni (45). Il vantaggio di tale strumento consiste nel fatto che esso segue la vita del prodotto o del servizio, agevolando l'adeguamento da parte delle imprese ai livelli di tutela previsti dalla legge.

Secondo l'art. 35 del reg. 2016/679, l'obbligo per il titolare di effettuare la valutazione d'impatto sussiste in via generale allorché il trattamento — soprattutto quando prevede l'uso di nuove tecnologie e avuto riguardo alla sua natura, oggetto, contesto e finalità — "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". La norma elenca le ipotesi particolari in cui è richiesta una valutazione d'impatto, che si riferiscono principalmente a operazioni di profilazione e monitoraggio del comportamento degli utenti, di sorveglianza sistematica di larga scala su una zona accessibile al pubblico ovvero che interessano categorie particolari di dati, come quelli tutelati dall'art. 9 del regolamento (art. 25, par. 3, regolamento cit.). Sebbene non si fornisca una definizione di « valutazione d'impatto », ne sono elencati i requisiti minimi, per cui essa deve necessariamente contenere una descrizione sistematica dei trattamenti previsti e delle finalità prestabilite, compreso l'interesse legittimo perseguito dal titolare; una valutazione della necessità e della proporzionalità dei trattamenti in relazione alle finalità; un'analisi dei rischi per i diritti e le libertà degli interessati, in virtù di quanto sancito dal paragrafo 1 dell'art. 35 e, infine, le misure previste per affrontare i rischi, includendo le garanzie e i meccanismi di sicurezza predisposti per la tutela dei dati personali e i diritti e libertà fondamentali, che dimostrino la conformità del trattamento stesso alla normativa europea.

Siffatta prospettiva si rinviene, altresì, nelle norme dell'art. 25 reg. cit., che introducono le nozioni di « protezione dei dati fin dalla progettazione » e di « protezione dei dati per impostazione predefinita », quali strumenti volti ad attuare i principi posti alla base della materia, enumerati dall'art. 4. Su tutti, il principio di minimizzazione dei dati personali, la cui nuova formulazione riflette l'intento del legislatore europeo di rendere assai più rigorosa la tutela: i dati dovranno essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati. Il principio di minimizzazione è richiamato espressamente nel paragrafo 1 della norma citata, che definisce la protezione fin dalla progettazione come quel complesso di misure che il titolare integra nel trattamento medesimo al fine di salvaguardare le persone interessate dalle violazioni di propri diritti e libertà fondamentali, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso.

Se tali tecniche erano già conosciute e adottate dalle imprese, con il regolamento del 2016 esse sono accolte nella disciplina europea, nella sezione relativa agli obblighi generali posti in capo al titolare e al responsabile del trattamento. I nuovi strumenti in esame sono tutti fondati su un'attenta valutazione dei rischi di violazione dei diritti e delle libertà fondamentali delle persone interessate, sulle cui basi sorge l'obbligo per il titolare di predisporre misure e soluzioni tecniche specificamente mirate alla tutela dei dati personali (i cc.dd. servizi e prodotti *privacy oriented*).

Ne discende un'impostazione al tempo stesso preventiva e promozionale della nuova normativa, volta ad attuare — seppure con qualche riserbo — i principi operanti nel diritto europeo. Tra questi, un ruolo sempre più importante sembra essere svolto dai principi di prevenzione e di precauzione (46), allorché la normativa, pur non richiamandoli, discorre dei rischi aventi « probabilità e gravità diverse » per i diritti e le libertà delle persone interessate (art. 25 reg. cit.) o prevede l'obbligo della valutazione d'impatto quando il trattamento « può presentare » un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 reg. cit.) (47).

Dalle considerazioni svolte deriva che il diritto dell'Unione si pone ancora una volta quale modello forte di tutela della *privacy*, dinanzi alle molteplici possibilità offerte dalle nuove tecnologie di svuotarlo di contenuto e renderlo inoperante. La nuova disciplina, infatti, appare tesa a garantire al cittadino europeo il medesimo livello di protezione a prescindere dal luogo in cui materialmente si svolge il trattamento dei propri dati personali — preservando il carattere universale dei diritti della persona — e anche di fronte all'incertezza di un pregiudizio, integrando meccanismi di tutela precauzionali e preventivi nel mezzo di comunicazione stesso.

Note:
Saggio sottoposto a referato.
(1) Il sistema attuale di principi forti che anima la materia della tutela della privacy si sviluppa precipuamente in ambito comunitario, sulla scia di un'elaborazione dottrinale prima ancora che giurisprudenziale e legislativa. Nella dottrina italiana, si segnalano, tra gli altri, i contributi di D. Messinetti, voce «Personalità (diritti della)», Enc. dir. (Milano 1983), XXXXIII, 355 s.; P. Rescigno, voce «Personalità (diritti della)», Enc. giur. Treccani (Roma 1990), XXIII, 2 s.; V. Zeno-Zencovich, voce «Personalità (diritti della)», Digesto civ. (Torino 1995), XIII, 430 s.; S. Rodotà, Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali, Riv. crit. dir. priv., 1997, 583 s.; nonché G. Alpa, Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto all'identità personale, Giur. merito, 1989, 464 s.
(2) Sul tema la letteratura è sconfinata. Per alcuni riferimenti bibliografici cfr. A. Gambino, La protezione «multilevel» dei diritti fondamentali (fra Costituzioni, trattati comunitari e giurisdizioni), Aa.Vv., Scritti in onore di Michele Scudiero (Napoli 2007), 1007 s.; nonché i contributi contenuti in Aa.Vv., Multilevel constitutionalism tra integrazione europea e riforme degli ordinamenti decentrati (Milano 2011). Per un'indagine sul ruolo delle corti europee e interne nell'ambito dei diritti della persona, cfr. G. Autorino, Diritti fondamentali e «cross fertilization»: il ruolo delle corti supreme, Dir. pubbl. comp. ed eur., 2014, IV, 2058 s.
(3) Così, S. Rodotà, Il diritto di avere diritti (Roma 2012), 397.
(4) L'art. 6 TUE prevede che: “L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni. 2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati. 3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali”.
(5) Convenzione del Consiglio d'Europa n. 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, ratificata in Italia con l. 21-1-1989, n. 98.
(6) Rodotà, Il diritto cit., 397.
(7) L'evoluzione della protezione della sfera privata della persona ha seguito una strada parallela a quella di un'altra nozione, ad essa intimamente legata, vale a dire l'identità personale, che da una freedom from consistente nel diritto a non veder travisata l'immagine che si ha di sé giunge a configurarsi come freedom to, allorché si afferma quale diritto di partecipare alla costruzione e alla tutela della propria identità non in astratto bensì nello specifico contesto delle relazioni sociali in cui si è calati. In siffatta prospettiva, si riconosce alla persona un diritto di svolgere un ruolo attivo in quelle situazioni – sempre più numerose – che incidono o possono incidere sulla propria identità. V. F.D. Busnelli, La persona alla ricerca dell'identità, Riv. crit. dir. priv., 2010, 1, 7 s. Sul dibattito riguardante i contenuti del diritto all'identità della persona e i suoi labili confini rispetto ad altri diritti della personalità, quali, in particolare, diritto all'immagine e diritto alla reputazione, si vedano in prospettiva generale, R. Tommasini, L'identità dei soggetti tra apparenza e realtà: aspetti di una ulteriore ipotesi di tutela della persona, Il diritto all'identità personale, a cura di G. Alpa, M. Bessone, L. Boneschi (Padova 1981), 84 s.; Aa.Vv., La lesione dell'identità personale e il

danno non patrimoniale (Milano 1985); V. Zeno-Zencovich, Onore e reputazione nel sistema del diritto civile (Napoli 1985), 363 s.; M. Costantino, Oggetto e tutela dell'esclusività dell'immagine di sé, Id., Rischi temuti, danni attesi, tutela privata (Milano 2002), 257 s.; G. Pino, Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale (Bologna 2003); di recente cfr. anche N. Irti, La persona, Manuale di diritto privato europeo, Vol. I, a cura di C. Castronovo - S. Mazzamuto, (Milano 2007), 212 s.
(8) Cfr. S. Rodotà, La vita e le regole. Tra diritto e non diritto (Milano 2006), 180 e G. Finocchiaro, Identità personale su internet: il diritto alla contestualizzazione dell'informazione, Diritto dell'Informazione e dell'Informatica, 2012, 380. L'Autrice si interroga sul rapporto tra dato personale e identità personale.
(9) È d'obbligo il riferimento a N. Bobbio, L'età dei diritti (Torino 1992), spec. 6 s.
(10) Pubblicata nella G.U.C.E. n. L 281 del 23 novembre 1995, in attuazione della quale il Parlamento italiano ha approvato la l. 31-12-1996, n. 675 (in S.O. alla G.U. 8 gennaio n. 5), recante «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali». Siffatta legge ha, altresì, istituito l'Autorità Garante per la protezione dei dati personali.
(11) Pubblicata nella G.U.C.E. n. L 24 del 30 gennaio 1998.
(12) Pubblicata nella G.U.C.E. n. L 201 del 31 luglio 2002.
(13) Corte eur. giust. 8-4- 2014 C-239/12, Digital Rights Ireland Ltd.
(14) Corte eur. giust. 13-5- 2014 C-131/12, Google Spain SL/Google Inc, Agencia Española de Protección de Datos, Mario Costeja Gonzàlez. Tra gli innumerevoli commenti della pronuncia in parola, v. i contributi di G.M. Riccio, Diritto all'oblio e responsabilità dei motori di ricerca, Dir. Inf., 2014, 4-5, 753; S. Sica-V. D'Antonio, La procedura di de-indicizzazione, ivi, 2014, 703 s.; G. Finocchiaro, Il diritto all'oblio nel quadro dei diritti della personalità, ivi, 591 s.; G. Giannone Codiglione, Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa, Nuova giur. civ. comm., 2014, 11, 1054.
(15) Corte eur. giust. 6-10-2015 C-362/14, Maximillian Schrems v. Data Protection Commissioner. Per tutti, S. Sica-V. D'Antonio, I Safe Harbour Privacy Principles: genesi, contenuti, criticità, Dir. Inf., 2015, 803 s.
(16) Cfr., per tutti, G. Resta, Anonimato, responsabilità, identificazione: prospettive di diritto comparato, Dir. Inf., 2014, 171.
(17) Sul punto, si veda l'analisi di Sica - D'Antonio I Safe Harbour Privacy Principles: genesi, contenuti, criticità cit., 820.
(18) In virtù di quanto disposto dall'art. 16 TFUE, che attribuisce al Parlamento e al Consiglio dell'Unione Europea il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e le norme relative alla libera circolazione di tali dati, Il regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, costituisce il nucleo centrale della nuova normativa, e abroga espressamente la direttiva 95/46/CE. Ad esso si aggiunge la Direttiva UE 2016/680, che disciplina i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.
(19) Riccio, Diritto all'oblio cit., 759. Significativa al riguardo è la parabola dei cc.dd. Safe Harbour Principles, linee guida in materia di trasferimenti di dati personali dall'Unione europea verso gli Stati Uniti, cristallizzati nella decisione 2000/520, adottata dalla Commissione sulla base dell'art. 25, par. 6, direttiva 95/46/CE. Sul punto, cfr. D'Antonio, Il trasferimento dei dati all'estero, comm. sub artt. 42-45, La nuova disciplina della privacy, a cura di P. Stanzione - S. Sica (Milano 2004), 155 s. Tali principi sono divenuti presto, nella pratica, uno strumento per attestare l'adeguamento agli standard europei di tutela da parte degli operatori statunitensi in modo presuntivo, vale a dire privo di un effettivo controllo sul rispetto dei diritti fondamentali dei soggetti coinvolti. La Corte di Giustizia dell'Unione ha pertanto annullato la citata decisione, nella sentenza Schrems, che ha segnato una svolta nella materia dei trattamenti transfrontalieri dei dati personali. Le maggiori criticità della decisione annullata riguardavano l'esistenza di una sorta di supremacy clause in favore del diritto statunitense, in virtù della quale i principi di tutela potevano subire pesanti limitazioni per soddisfare esigenze di carattere pubblicistico, riguardanti la sicurezza nazionale, l'interesse pubblico o l'amministrazione della giustizia degli Stati Uniti ovvero in caso di conflitto con “legittimi interessi di ordine superiore” riconosciuti dalla legislazione o dalla giurisprudenza. Ampiamente, sul tema, Sica - D'Antonio, I Safe Harbour

Privacy Principles cit.
(20) Come enunciato dal considerando n. 2 del regolamento 2016/679.
(21) Così il considerando n. 10 regolamento cit.
(22) L'art. 94 regolamento cit. stabilisce che la direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018.
(23) In seguito alla sua presentazione, il 25 gennaio 2012, la proposta di regolamento elaborata dalla Commissione europea è stata sottoposta all'analisi e agli emendamenti della Commissione parlamentare per le libertà civili, la giustizia e gli affari interni (commissione LIBE), che ha rappresentato l'interlocutore principale, sebbene non l'unico all'interno del Parlamento europeo. Tra le altre commissioni coinvolte nell'esame della proposta di regolamento si rinvengono: la Commissione per il Mercato Interno e la Protezione dei Consumatori (IMCO); Industria, Ricerca ed Energia (ITRE); Affari Economici e Monetari (ECON); Affari Giuridici (JURI) e Sviluppo e Affari Sociali (EMPL).
(24) Va rilevato che costituisce una novità la previsione dell'applicabilità ai responsabili del trattamento, la norma in parola, infatti, getta le basi delle disposizioni che prescrivono un regime di obblighi in capo al responsabile del trattamento indipendente da quello del titolare. Cfr. C. Cuijpers - N. Purtova - E. Kosta, Data Protection Reform and the Internet. The Draft of Data Protection Regulation, Research Handbook on EU Internet Law, a cura di A. Savin - J. Trzaskowski, Tilburg Law School, (Cheltenham - Northampton 2014), 543.
(25) Quest'ultima ipotesi si verifica assai raramente e riguarda il caso di consolati, ambasciate e così via.
(26) L'art. 4 della dir. 95/46, rubricato “Diritto nazionale applicabile”, prevede, al par. 1, che: «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;b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea».
(27) Sul diritto di stabilimento, in una prospettiva più generale, v. A. Guaccero, Libertà di stabilimento e diritto societario degli Stati membri: Europa vs. USA, in questa Rivista, 2007, 133 s.
(28) G. Caggiano, Attività di stabilimento e trattamento dei dati personali, Dir. inf. 2014, 607.
(29) In argomento, Caggiano, Attività di stabilimento e trattamento dei dati personali cit., 605 s. Sul tema generale, denso di problematiche, della responsabilità dell'Internet Service Provider v. G.M. Riccio, Alla ricerca della responsabilità dei motori di ricerca, Danno e resp., 2011, 7, 753 s.; Id., Social network e responsabilità civile, Dir. inf., 2011, 859 s.; A.G. Parisi, E-Contract e privacy (Torino 2015), 67 s. e ivi ampia bibliografia.
(30) Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca, consultabile all'URL http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.
(31) Parere 8/2010 sul diritto applicabile consultabile all'URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_it.pdf.
(32) La Corte fonda l'applicabilità della direttiva sul fatto che Google Spain costituisce una filiale di Google Inc. nel territorio spagnolo, volta alla comunicazione e alla vendita di comunicazione commerciale diretta ai residenti di quello Stato membro e pertanto integri uno «stabilimento» ai sensi dell'art. 4 e respinge l'argomento secondo cui il trattamento di dati personali oggetto della controversia non rientra nel contesto delle attività dello stabilimento in parola. Sul punto, G. Caggiano, Attività di stabilimento e trattamento dei dati personali cit., 612 s.
(33) Corte eur. giust. 1-10-2015, C-230/14, Weltimmo.
(34) La norma citata specifica che il monitoraggio del comportamento degli interessati deve avvenire all'interno dell'Unione. Il considerando n. 24 offre qualche spunto interpretativo, allorché

precisa che «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».
(35) L'art. 27, par. 4, regolamento cit., specifica che il rappresentante è incaricato dal titolare o dal responsabile a fungere da interlocutore, in aggiunta in sostituzione di questi, delle autorità di controllo e degli interessati sulle questioni relative al trattamento. Altresì, la designazione di un rappresentante fa salve le azioni legali che potrebbero essere promosse contro il titolare o il responsabile del trattamento (art. 27, par. 5).
(36) Come emerso nel parere del Gruppo di Lavoro ex Articolo 29 n. 4/2007 (consultabile all'URL ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), la nozione di dati personali accolta dalla direttiva 95/46/CE ha generato differenti interpretazioni negli ordinamenti europei. Una delle questioni, ad esempio, era quella della natura di dati personali degli indirizzi IP, sulla quale è atteso il pronunciamento della Corte di Giustizia (caso Patrick Breyer v. Bundesrepublik Deutschland C-582/14).
(37) La Corte di Giustizia ha stabilito chiaramente che il preambolo di un atto legislativo europeo è privo di valore giuridico vincolante e che non possa essere fatto valere per derogare alle disposizioni stesse dell'atto in questione (Corte eur. giust. 19-11-1998, C-162/97, Nilsson, Hagelgren and Arrborn, par. 54). Pur tuttavia, le enunciazioni introduttive ad un atto normativo dell'Unione sono state utilizzate dalle Corti europee per interpretare disposizioni ambigue dell'atto medesimo. Cfr. T. Klimas - J. Vaiciukaité, The Law of Recitals in European Community Legislation, ILSA Journal of International and Comparative Law, 2008, 1, 61 s.
(38) Il riferimento a tali dispositivi è particolarmente rilevante nella prospettiva del c.d. Internet of Things. V., sul punto, S.J. Eskens, Profiling the European Consumer in the Internet of Things. How will the General Data Protection Regulation apply to this form of personal data processing, and how should it?, Thesis Research Master Information Law (Amsterdam 2016).
(39) L. Costa - Y. Poullet, Privacy and the regulation of 2012, Computer Law and Security Review, 2012, 3, 254 e s. e spec. 255. Cfr., inoltre, il parere 4/2007 del Gruppo di Lavoro Ex Articolo 29.
(40) Così il considerando n. 28 regolamento cit.
(41) C. Burton - L. De Boel - C. Kuner - A. Pateraki - S. Cadiot - S. Hoffman, The Final European Union General Data Protection Regulation, BNA Privacy and Security Law Report, 25 january 2016. V., altresì, G. Resta, Anonimato, responsabilità, identificazione: prospettive di diritto comparato, Dir. inf.., 2014, 2, 171 s.
(42) Il discrimen sembra essere quello di cui discorre il considerando n. 18, vale a dire l'assenza di connessioni con un'attività commerciale o professionale.
(43) Il considerando n. 18 fa espresso riferimento all'uso dei social networks, ricomprendendolo tra le attività a carattere personale o domestico cui la nuova disciplina non si applica. Tuttavia, la medesima previsione precisa che la normativa si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere domestico.
(44) Sul tema, Parisi, E-contract cit., passim e spec. 67 s. e ivi ampia bibliografia.
(45) A. Mantelero, Competitive value of data protection: the impact of data protection regulation on online behaviour, International Data Privacy Law, 2013, 3, 229 s.
(46) La Corte di Giustizia ha più volte affermato la natura di principi generali del principio di prevenzione e di quello di precauzione. Sulla differenza tra le due nozioni, sia consentito il rinvio a M.G. Stanzione, L'incidenza del principio di precauzione sulla responsabilità civile negli ordinamenti francesi e italiano, in www.comparazionedirittocivile.it.
(47) Cfr. Rodotà, Il diritto di avere diritti cit., 403. L'A. sostiene che il ricorso all'algoritmo non può divenire una forma di deresponsabilizzazione e che «questa consapevolezza ormai diffusa dovrebbe indurre ad adottare almeno il “principio di precauzione” e a costruire un adeguato contesto istituzionale, oggi assai debole anche perché le norme ricordate sono aggirate o ignorate, evitando che il rapporto sempre più importante tra l'uomo e la macchina venga governato solo dalla logica economica».