EMANUELE LUCCHINI GUASTALLA

Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori

1. – Il reg. (UE) n. 679 del 2016 del Parlamento Europeo e del Consiglio è stato emanato il 27 aprile 2016 e pubblicato nella Gazzetta ufficiale dell'Unione Europea del 4 maggio 2016 (1).

(1) Tra i primi commenti alla nuova normativa si segnalano, in particolare, il volume collettaneo AA.VV., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, diretto da Giu. Finocchiaro, Bologna, 2017; il volume di BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento* Privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; il volume AA.VV., *La nuova disciplina europea della* privacy, a cura di Sica, D'Antonio e G.M. Riccio, Milano, 2016; i due tomi di PIZZETTI, Privacy *e il diritto europeo alla protezione dei dati personali*, I (*Dalla dir. 95/46 al nuovo regolamento europeo*) e II (*Il regolamento europeo 2016/679*), Torino, 2016, ove si ripercorre il cammino che, dalla nascita del diritto alla protezione dei dati personali, ha condotto alla "costruzione" del diritto dell'Unione in questa materia. Un ampio commento alla recente normativa è offerto *ivi*, I, p. 147 ss., e II, *passim*. V. inoltre i saggi di M.G. STANZIONE, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1249 ss.; SPINA, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679*, in *Riv. regolaz. merc.*, 2016, p. 143 ss.; TASCIOTTI, *La* privacy *esiste ancora?*, Canterano, 2017, p. 453 ss. e p. 663 ss.

Per un più ampio inquadramento, precedente l'emanazione del recente regolamento ma ancora attuale, sulla protezione dei dati nell'ambito dello spazio europeo di libertà, sicurezza e giustizia, v. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Heidelberg-Dordrecht-London-New York, 2012, *passim* ma spec. 19 ss., nonché AA.VV., *European Data Protection: Coming of Age*, a cura di Gutwirth, Leenes, de Hert e Poullet, Dordrecht-Heidelberg-New York-London, 2013, *passim* ma spec. 3 ss.

Da un punto di vista teorico, sulle istanze di tutela sollevate dal trattamento di dati personali e sull'opportunità di affrontare la materia a partire dalla *propertisation* di tali dati, v. l'ampio lavoro di PURTOVA, *Property Rights in Personal Data. A European Perspective*,

Il provvedimento (intitolato «alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati») abroga e sostituisce la dir. 95/46/CE (recante il «regolamento generale sulla protezione dei dati»), che per anni ha rappresentato la pietra angolare della normativa dell'Unione Europea in materia di protezione dei dati personali.

Il nuovo regolamento – destinato a trovare applicazione a partire dal 25 maggio 2018 – si articola in 11 capi per un totale di 99 articoli. La parte dispositiva è preceduta da ben 173 "*considerando*", i quali chiariscono il contesto e le ragioni della nuova normativa (2).

Particolarmente interessante è il *considerando* 9, dove il legislatore comunitario riconosce espressamente che la dir. 95/46/CE «non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione (...) che (...) le operazioni *online* comportino rischi per la protezione delle persone fisiche» (3). Le divergenze nell'attuazione e nell'applicazione della dir. 95/46/CE nei singoli Stati membri hanno così dato luogo alla «compresenza di diversi livelli di protezione (...) dei dati personali» (4) e ciò, secondo il legislatore comunitario, può ostacolare la libera circolazione di tali dati all'interno dell'Unione e «costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione» (5).

Non è però soltanto a questi inconvenienti che si è inteso ovviare con l'emanazione del nuovo regolamento. Infatti, l'esigenza di una riforma della materia è sorta anche (e forse soprattutto) dalla continua evoluzione degli stessi concetti di *privacy* e di *data protection*, dovuta principalmente all'incessante progresso dei servizi *on line*.

La precedente dir. 95/46/CE era stata adottata nel 1995 con due principali obbiettivi: 1) salvaguardare il diritto fondamentale dei soggetti

---

Alphen aan der Rijn, 2012, *passim* e spec. p. 193 ss. con riferimento all'ordinamento dell'Unione.

(2) Com'è noto, è *ius receptum* che i preamboli degli atti legislativi europei sono privi di forza vincolante, come ha affermato la stessa Corte di giustizia in diverse occasioni; nondimeno, le corti europee hanno fatto un largo uso dei preamboli a fini interpretativi. Cfr. sul punto KLIMAS,VAIČIUKAITÉ, *The law of recitals in European Community legislation*, in *ILSA Journ. Int. Compar. Law*, 2008, p. 61 ss. e spec. p. 72 ss.

(3) Così il *considerando* n. 9.

(4) *Ibidem*.

(5) *Ibidem*.

alla protezione dei dati; 2) garantire la libera circolazione dei dati personali fra gli Stati membri.

Negli anni immediatamente successivi, l'entità fenomenica della condivisione e della raccolta di dati è aumentata in modo letteralmente vertiginoso. Com'è noto, le tecnologie attuali consentono agli operatori economici di impiegare moli imponenti di dati personali come mai in precedenza era stato fatto e con finalità che un ventennio fa non erano neppure immaginabili.

Internet, infatti, è ormai a pieno titolo un *advertisement supported service* che si basa in larghissima parte sulla profilazione dell'utenza: in questo contesto, come ebbe ad affermare nel 2009 il Commissario europeo per la tutela dei consumatori Meglena Kuneva, «[*p*]*ersonal data is the new oil of the internet and the new currency of the digital world*» (6): i dati personali, insomma, sono divenuti un vero e proprio carburante per lo svolgimento dell'attività di numerosissimi operatori. Per altro verso, gli stessi utenti di servizi *online* rendono universalmente pubbliche innumerevoli informazioni personali: una pratica, questa, che è divenuta quasi un *modus vivendi* per gran parte della popolazione mondiale e che ha finito con il trasformare le stesse relazioni sociali, specialmente per i c.d. nativi digitali (7). Conseguenza di tutto ciò è l'esponenziale aumento del rischio che il potenziale "invasivo" del sistema informativo telematico nell'esistenza umana divenga strumento per nuove e sempre più sofisticate forme di controllo sociale (8).

Tutto ciò ha finito col mettere inesorabilmente in luce l'inidoneità del quadro normativo offerto dalla direttiva del 1995, pur rimanendone validi gli obbiettivi e i principi di fondo. È divenuto necessario, quindi, instau-

---

(6) Parole pronunciate il 31 marzo 2009 a Bruxelles, nell'ambito di una *Roundtable on Online Data Collection, Targeting and Profiling* (testo leggibile nel sito *www.istitutoitalianoprivacy.it*). In quell'occasione la Kuneva, parlando di internet, ha sottolineato che «*the development of marketing based on profiling and personal data is what makes it go round. (...) We accept this reality because it is one chosen by users. Internet users have massively opted for free services offered in exchange for acceptance of advertisement. Today, advertisement online is individually targeted and increasingly based on the user's profile and behaviour*».

(7) Cfr. NUNO GOMES DE ANDRADE, MONTELEONE, *Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regardind Privacy and Their Legal Implications*, in AA.VV., *European Data*, cit., p. 119 ss.

(8) Cfr. sul punto MANTELERO, VACIAGO, *The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, in *Computer Law Rev. Int.*, 2013, p. 161 ss.

rare un quadro giuridico più solido e coerente, adeguato allo sviluppo dell'economia digitale nel mercato interno.

2. – Il nuovo regolamento trova applicazione a qualsiasi forma di trattamento (interamente o parzialmente) automatizzato di dati personali, nonché al trattamento non automatizzato di dati personali contenuti in un archivio (art. 2^1). Sono fatte salve soltanto le tassative esclusioni di cui all'art. 2^2, fra cui figurano i trattamenti effettuati dagli Stati membri nell'esercizio di attività relative alla politica estera e alla sicurezza comune, o quelli effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, o ancora quelli «effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico» (c.d. *household exclusion provision*) (9).

L'art. 4, secondo lo stile definitorio tipico del legislatore comunitario, fornisce – tra le altre – le fondamentali definizioni di "dato personale" e di "trattamento".

Generalissima (10) è quella di "*dato personale*", che coincide con qualsiasi informazione riguardante una persona fisica identificata o identificabile (il c.d. interessato) (11). Peraltro, particolare attenzione è riservata ad alcune particolari categorie di dati personali: i "*dati genetici*", relativi alle caratteristiche genetiche – ereditarie o acquisite – di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute e che risultano in particolare dall'analisi di un campione biologico; i "*dati biometrici*", relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; i "*dati relativi alla salute*", fisica o mentale, di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria.

La particolare attenzione riservata a tali categorie si esprime nella disciplina loro riservata, la quale si ritrova negli artt. 9 e 10, e, in estrema sintesi, si risolve nel divieto di trattamento dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o

---

(9) V. sul punto BOLOGNINI, PELINO, in BISTOLFI, BOLOGNINI e PELINO, *Il Regolamento*, cit., p. 19 ss., nonché SPANGARO, in AA.VV., *Il nuovo Regolamento*, cit., p. 23 ss.

(10) Nonché fondamentalmente ambigua, come rilevato da M.G. STANZIONE, *Il regolamento*, cit., p. 1260.

(11) Su questo concetto v. l'ampia analisi di PIZZETTI, *Privacy*, cit., I, p. 183 ss., nonché PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 43 ss.

filosofiche, l'appartenenza sindacale, e nel trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Ciò, naturalmente, fatte salve le eccezioni analiticamente individuate dall'art. 9^2, fra cui figura il caso in cui il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso, nonché il caso in cui il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, e riguardi unicamente le persone collegate all'ente, e i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.

Il "*trattamento*", invece, è definito come qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o a insiemi di dati personali (12). Pertanto, costituiscono trattamento di dati personali la relativa 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.

3. – Entrando nel vivo della nuova disciplina, merita di soffermarsi subito sui principi fondamentali che la animano e che il legislatore comunitario enuncia nel capo II del regolamento (artt. 5-11). L'art. 5, in particolare, enumera i «Principi applicabili al trattamento» mediante un elenco di predicati, tutti riferiti ai dati personali. Come sancito dal par. 1 della disposizione, i dati personali: sono, anzitutto, trattati in modo *lecito*, *corretto* e *trasparente* nei confronti dell'interessato; sono raccolti per *finalità determinate*, *esplicite* e *legittime*, e trattati in un modo che non può essere incompatibile con tali finalità; inoltre sono conservati in una forma che consenta l'identificazione degli interessati per un tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento; sono *adeguati*, *pertinenti* e *limitati* a quanto *necessario* per le finalità del trattamento; sono *esatti* e, se necessario, *aggiornati*; sono trattati in maniera da garantirne un'*adeguata sicurezza* e, in particolare, la *protezione* da tratta-

(12) Cfr., ampiamente, PIZZETTI, *Privacy*, cit., I, p. 193 ss., e PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 86 ss.

menti non autorizzati o illeciti, nonché dalla perdita, dalla distruzione o dal danno accidentali (13).

Il par. 2 dello stesso art. 5 afferma a sua volta un ulteriore principio, affermando che «[i]l titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo»: si tratta di quello che, nella versione italiana del regolamento, è stato indicato come principio di "responsabilità", ma che nella versione inglese suona come "*accountability*" (sulla traduzione di questo termine si avrà modo di tornare nel prosieguo del presente scritto).

Volendo tentare di isolare le linee di maggiore novità della nuova disciplina, pare utile concentrare l'esame della medesima, in particolare, su alcuni principi fondamentali, ovvero: quello di *liceità* del trattamento; quello di *trasparenza* nel trattamento; il c.d. diritto all'*oblio*; l'*accountability* del titolare del trattamento; la c.d. *privacy by design* e *by default*.

Proprio questi principi appaiono di maggiore interesse sotto il profilo privatistico, che ha sede, in prevalenza, nel capo III (artt. 12-23), intitolato ai «Diritti dell'interessato».

4. – Il principio di liceità del trattamento trova specificazione nell'art. 6 del regolamento. Questa disposizione àncora la liceità del trattamento a due requisiti alternativi: la *necessità* del trattamento e il *consenso* dell'interessato.

Il trattamento, in altre parole, è lecito solo se fondato, alternativamente, sulla *necessità* dello stesso o sul *consenso* dell'interessato – da esprimersi in relazione ad «una o più *specifiche* finalità», e dunque non genericamente – (14).

I casi di *necessità* sono individuati dallo stesso art. 6: si tratta, per es., del trattamento «necessario all'esecuzione di un contratto di cui l'interessato è parte», o del trattamento «necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica» (come, ad esempio, le emergenze cliniche), o ancora del trattamento «necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento» (si pensi, ad esempio, al trattamento che il notaio deve fare dei dati personali dei suoi clienti, al fine di dar corso alla pubblicità immobiliare di un suo atto, cui egli è tenuto per legge a dar corso).

---

(13) V. ora, ampiamente, BOLOGNINI, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 92 ss.

(14) V. più ampiamente sul punto, da ultimo, BRAVO, in AA.VV., *Il nuovo Regolamento*, cit., p. 101 ss.

L'art. 4 definisce il requisito del *consenso*, che rappresenta il parametro di liceità del trattamento quante volte questo non sia connotato dal carattere della necessità. Costituisce "consenso dell'interessato" qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, a che i dati personali che lo riguardano siano oggetto di trattamento (15).

Il consenso riceve all'art. 7 una disciplina riferita sia alla fase ad esso immediatamente precedente (che potrebbe essere definita come fase preconsensuale) sia a quella, successiva, dell'eventuale revoca.

Quanto alla prima fase, il regolamento stabilisce che, «[s]e il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro».

È prevista anche una sanzione: infatti, con una formulazione non del tutto lineare, l'art. 7 dispone che «[n]essuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante». In altre parole, nel caso in cui la dichiarazione scritta di contenuto complesso integri una violazione del regolamento, essa è inefficace: il consenso prestato dall'interessato, dunque, è *tamquam non esset*.

È inoltre previsto sempre dall'art. 7 – ma questa volta senza alcuna sanzione espressa – che l'interessato debba essere informato, prima di esprimere il consenso, della facoltà di revocarlo in seguito, senza pregiudizio della liceità del trattamento effettuato prima della revoca (16).

L'interessato, infatti, – passando ora all'esame della disciplina della fase post-consensuale – ha diritto di revocare in qualsiasi momento il proprio consenso. La revoca vale, naturalmente, soltanto *pro futuro*, essendo espressamente previsto che essa «non pregiudica la liceità del trattamento basata sul consenso prima della revoca». Inoltre, con formulazione non ineccepibile da un punto di vista tecnico, l'art. 7 soggiunge che «[i]l consenso è revocato con la stessa facilità con cui è accordato»; parrebbe, dunque, che questa prescrizione debba essere interpretata nel senso

---

(15) Sul tema del consenso al trattamento dei dati si veda il recente e ampio saggio di THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, p. 513 ss., ove si ritrovano ampi riferimenti alla dottrina degli ultimi decenni in questa materia.

(16) Sul rapporto tra informativa e consenso v. ora PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 180 ss. e spec. p. 186.

che la revoca non può essere soggetta a oneri o formalità ulteriori rispetto a quelli cui è soggetto il consenso (17).

Infine, da un punto di vista probatorio, l'art. 7 stabilisce che «il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali»: ciò, evidentemente, anche in attuazione del principio di *accountability*.

4.1. – Ora, mentre la fase pre-consensuale e quella post-consensuale ricevono una dettagliata disciplina nel regolamento, il consenso in sé – quale libero atto di volontà – è soltanto definito dall'art. 4, ma non compiutamente disciplinato. Al riguardo vi è un'unica disposizione: la regola interpretativa di cui al par. 4 dell'art. 7, secondo cui, «[n]el valutare se il consenso sia stato liberamente prestato, si tiene *nella massima considerazione* l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio [ad es. di posta elettronica o di *social networking*], sia condizionata alla prestazione del consenso al trattamento di dati personali *non necessario* all'esecuzione di tale contratto».

La norma fa riferimento al caso in cui si verifichino entrambe le seguenti condizioni: l'utente è stato posto di fronte a un *aut aut*: o presta il consenso, o non potrà fruire del servizio; il consenso ha ad oggetto, tra l'altro, un trattamento di dati *non necessario* – in quanto non strettamente funzionale – alla prestazione del servizio.

Questa situazione non è infrequente: basti pensare a quante volte l'accesso a un servizio *online* è subordinato alla prestazione del consenso non soltanto al trattamento dei dati da parte del gestore, ma anche alla trasmissione dei dati a operatori terzi ai fini, ad es., dell'invio all'utente di comunicazioni commerciali.

Il legislatore europeo ha dunque previsto che, ove il consenso sia stato prestato in tali condizioni, *sia ragionevolmente plausibile* che esso non sia stato prestato liberamente. Non si tratta di una presunzione, ma – per così dire – di un invito di fonte legislativa a prestare attenzione, tra le altre circostanze del consenso, a questa peculiare forma di condizionamento, potenziale indice di una menomata libertà decisionale dell'utente.

Questo approccio sembra da condividere, in quanto respinge la presunzione che il consenso dell'interessato sia privo del requisito della libertà per il solo fatto che esso è considerato dal gestore di un servizio alla

---

(17) Sulle possibili ripercussioni della revoca del consenso su un contratto già concluso v. le osservazioni di THOBANI, *La libertà*, cit., p. 553 ss.

stregua di un requisito necessario per accedere al servizio stesso (18). La libertà del consenso potrà senz'altro escludersi soltanto laddove il servizio in questione sia indispensabile per l'utente o il gestore sia obbligato a contrarre (19).

La libertà del consenso sarà invece implicita nei casi in cui sussista un nesso di strumentalità fra trattamento dei dati e servizio offerto dal gestore: ove tale collegamento sia ravvisabile e si presenti solido, non potrà dubitarsi della legittimità della condotta negoziale del gestore, il quale condizioni l'erogazione del servizio al rilascio, da parte dell'utente, dei propri dati di registrazione e del consenso al relativo trattamento. Un simile collegamento certamente sussiste nel caso dei c.d. *social network*, la cui attività consiste anche nella profilazione dei dati e delle preferenze degli utenti, con conseguente organizzazione dei contenuti promozionali rivolti al singolo fruitore (20).

---

(18) La prestazione del consenso da parte dell'utente si atteggia, in questi casi, come una sorta di "prezzo da pagare" per l'accesso al servizio, una condotta sostanzialmente libera, ma necessitata in vista della realizzazione di un interesse dell'agente: secondo la tassonomia delle situazioni soggettive, potrebbe parlarsi di *onere* in senso tecnico.

(19) Cfr. S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, II, 455 ss., secondo cui «il problema pratico più rilevante (...) riguarda le ipotesi in cui alla prestazione del consenso venga subordinata dalla controparte la conclusione del contratto o la prosecuzione del rapporto. Da un lato, infatti, sarebbe agevole affermare che non può considerarsi libero il consenso prestato da chi non poteva fare a meno del bene o del servizio offerto dalla controparte. Dall'altro, non sembra ipotizzabile un obbligo a contrarre in capo a chi ritiene indispensabile per lo svolgimento della propria attività il trattamento dei dati dei *partner* contrattuali» (*ivi*, p. 461).

(20) Nondimeno, com'è noto, il Garante per la protezione dei dati personali ha recentemente stabilito un generale divieto di installazione di *cookies* di profilazione da parte dei gestori di siti internet, senza che sia fornita agli utenti una preventiva informazione e senza che sia prestato da costoro il relativo consenso (si parla, in proposito, di *behavioral privacy*). Detta informazione è resta mediante un sintetico *banner* informativo contenente «l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (...) comporta la prestazione del consenso all'uso dei *cookie*» (provv. 8 maggio 2014, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei* cookie, consultabile sul sito internet *garanteprivacy.it*, doc. *web* n. 3118884). Tale soluzione è certamente in linea con la normativa in tema di informazioni raccolte nei riguardi del contraente o utente di servizi di comunicazione elettronica, la quale prevede che l'archiviazione delle informazioni nell'apparecchio terminale del contraente/utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente/utente abbia espresso il proprio consenso dopo essere stato informato (cfr. art. 122 d. lgs. 30 giugno 2003, n. 196.). Tuttavia, si tratta di un espediente che non può andare esente dai rilievi che lo stesso Garante aveva sollevato, come già ricordato, nei confronti dei meccanismi di consenso "necessitato", in cui il consenso dell'utente rappresenta una *condicio sine qua non* dell'erogazione del servizio: in altre parole, si tratta pur sempre di un consenso richiesto secondo la logica del "prendere o lasciare".

L'impostazione fatta propria dal regolamento è analoga a quella adottata nel 2013 dal nostro Garante per la protezione dei dati personali (21), secondo cui «[i]l consenso (...) deve intendersi libero quando non è preimpostato e non risulta – anche solo implicitamente in via di fatto – obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento». Peraltro, già nel 2010, il Garante si era spinto ben oltre l'impostazione del recente regolamento, affermando che «non può definirsi "libero", e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato "debba" prestare quale condizione per conseguire una prestazione richiesta» (22).

Il problema del libero consenso si fa ancor più delicato in relazione a uno dei trattamenti più insidiosi: quello di *profilazione*. Si tratta – ai sensi dell'art. 4 – di qualsiasi forma di trattamento automatizzato di dati personali consistente nel relativo impiego al fine di *valutare* determinati aspetti personali relativi a una persona fisica e, in particolare, per *analizzare* o *prevedere* aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti (23).

Il regolamento prevede una forte restrizione con riguardo a questa prassi, divenuta diffusissima e assai rilevante da un punto di vista economico (24). In particolare, l'art. 22 dispone che «[l]'interessato ha il diritto

---

(21) Provv. 4 luglio 2013 del Garante, intitolato *Linee guida in materia di attività promozionale e contrasto allo* spam (consultabile sul sito internet *garanteprivacy.it*, doc. *web* n. 2542348), ove sono citati diversi precedenti in senso conforme.

(22) Provv. 15 luglio 2010 intitolato *Raccolta di dati via Internet per finalità promozionali: sempre necessario il consenso degli interessati* (anch'esso consultabile sul sito internet *garanteprivacy.it*, doc. *web* n. 1741998).

(23) In generale sul punto, nella nostra dottrina, v. MACCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitari* online *e tutela della* privacy, in *Dir. inf.*, 2001, p. 425 ss.; MANTELERO, *Si rafforza la tutela dei dati personali:* data breach notification *e limiti alla profilazione mediante i* cookies, *ivi*, 2012, p. 781 ss.; DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, *ivi*, 2013, p. 587 ss.; più di recente, PALLONE, *La profilazione degli individui connessi a Internet:* privacy online *e valore economico dei dati personali*, in *Cibersp. dir.*, 2015, p. 295 ss., nonché, da ultimo, PACILEO, *Profilazione e diritto di opposizione*, in AA.VV., *La nuova disciplina*, cit., p. 177 ss. Per un più generale approccio al tema v. AA.VV., *Profiling the European Citizen. Cross-Disciplinary Perspective*, a cura di Hildebrandt e Gutwirth, Dordrecht, 2010, *passim*.

(24) Secondo ROVEGNO, *Identità digitale: tra esigenze di condivisione e necessità di tutela*, in *Cibersp. dir.*, 2013, p. 403 ss., «[l]a rappresentazione dell'immagine di noi stessi che forniamo sulla rete è sempre più accurata, e più lo diventa, maggiore è il valore, anche economico, che essa acquista». Altra questione è, poi, questa identità coincida o meno con quella "reale" del soggetto: tema sul quale invita a riflettere, con la consueta sensibilità, ALPA, *L'identità digitale e la tutela della persona. spunti di riflessione*, in *questa rivista*, 2017, p. 723 ss.

di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Questa regola è temperata da una limitata serie di eccezioni: una è quella del «consenso esplicito dell'interessato»; un'altra quella in cui la decisione sia autorizzata dalla legge; una terza – decisamente la più controversa – è quella in cui la decisione «sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento» (25).

4.2. – Sempre in tema di consenso dell'interessato, merita segnalare che una particolare enfasi è posta dal legislatore sul consenso dei minori «in relazione ai servizi della società dell'informazione» (art. 8) (26).

Qualora il trattamento dei dati dei minori sia fondato sul loro consenso, il trattamento è lecito solo se il minore abbia almeno 16 anni. In caso di minore infrasedicenne, il trattamento è lecito soltanto se e nella misura in cui esso è *prestato o autorizzato* dal titolare della responsabilità genitoriale. A questo riguardo, peraltro, gli Stati membri possono stabilire per legge un'età diversa, purché non inferiore ai 13 anni (27).

Il regolamento precisa che la regola del consenso del minore non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore (art. 8^3). La precisazione è certamente opportuna al fine di tenere separati i due piani – che certo si intersecano, ma senza

---

(25) Sul tema della deducibilità in contratto del consenso v. almeno l'ampia analisi svolta da THOBANI, *La libertà*, cit., p. 526 ss., ove numerosi riferimenti in materia. Una critica radicale alla logica del consenso al trattamento dei dati in relazione ai servizi *on line* è stata svolta, di recente, da MATTIONI, *Profili civilistici dell'identità digitale tra tutela e accertamento*, in AA.VV., *Identità ed eredità digitali. Stato dell'arte e possibili soluzioni al servizio del cittadino*, a cura di Pollicino, Lubello e Bassini, Roma, 2016, p. 55 ss. e spec. p. 65 ss., ove l'a., sviluppando le suggestioni offerte – quasi mezzo secolo fa – da Stefano Rodotà, ritiene che la tutela dei privati a fronte del trattamento dei propri dati personali sarebbe assai più efficacemente realizzata attraverso un controllo amministrativo dell'impiego dei dati personali, rinunciando così, una volta per tutte, a fondare la tutela dell'utente su un consenso che la legge pretende libero e consapevole, ma che nei fatti è spesso meramente formale.

(26) Del tema si sono già occupati, in Italia, SACCHETTI, Privacy*: nodi e scioglimenti con particolare riferimento alla tutela dei minori*, in *Fam. e dir.*, 1998, p. 289 ss., e – più di recente – STEFANELLI, Privacy *e immagine dei minori in* Internet, in *Cibersp. dir.*, 2012, p. 233 ss.

(27) Per un ampio inquadramento di tale disciplina, con particolare riferimento al tema dell'autodeterminazione del minore, cfr. SPOTO, *Disciplina del consenso e tutela del minore*, in AA.VV., *La nuova disciplina*, cit., p. 111 ss.

interferenze di carattere sostanziale – del rapporto tra le parti contrattuali, che si instaura con l'accordo negoziale e si muove lungo le linee del relativo regolamento, e del rapporto tra interessato e titolare del trattamento, che si instaura con il consenso del primo e si muove lungo le linee di una disciplina di fonte prevalentemente legale e di carattere essenzialmente imperativo (28).

5. – Il principio di trasparenza è alla base degli artt. 12 ss., relativi al rapporto fra il titolare del trattamento e l'interessato con riferimento all'informazione e all'accesso ai dati (29).

L'attuazione del principio è affidata soprattutto alla prescrizione di particolari modalità informative e a una notevole procedimentalizzazione delle stesse. È previsto che le informazioni destinate al pubblico o all'interessato debbano essere facilmente accessibili e di facile comprensione, ed espresse con linguaggio semplice e chiaro. Ciò riguarda in particolare l'informazione degli interessati circa l'identità del titolare del trattamento e le finalità del trattamento, nonché le ulteriori informazioni relative al diritto degli interessati di ottenere conferma e comunicazione del trattamento di dati personali che li riguardano.

Queste prescrizioni rientrano nella più generale tendenza del legislatore comunitario a favorire l'informazione degli utenti attraverso l'imposizione agli operatori di obblighi di chiarezza nella comunicazione. Ciò, nello specifico settore in esame, al fine di assicurare che gli utenti, da un lato, siano sensibilizzati ai rischi e resi edotti delle garanzie relative al trattamento dei propri dati; dall'altro lato, che siano informati circa le finalità specifiche del trattamento, onde consentire loro di valutare se i dati richiesti e le modalità di raccolta e conservazione siano effettivamente in linea con tali finalità.

È interessante sottolineare che il principio di trasparenza rappresenta il fondamento normativo dell'impiego dei c.d. *formati multistrato*. Com'è noto, le c.d. *privacy policies* sono documenti complessi, contenenti una gran quantità di informazioni di natura tecnico-giuridica. Ebbene, le comunicazioni multistrato mirano a migliorare la qualità dell'informazione,

---

(28) Ciò non toglie che dalle norme in materia di invalidità contrattuale, e segnatamente da quelle che disciplinano i vizi del consenso, possano trarsi indicazioni rilevanti al fine di valutare – non solo con riferimento al minore – la libertà del consenso al trattamento dei dati, come condivisibilmente rileva THOBANI, *La libertà*, cit., p. 519.

(29) In generale sul tema v. DI GENIO, *Trasparenza e accesso ai dati personali*, in AA.VV., *La nuova disciplina*, cit., p. 161 ss.

condensando in "strati" informativi semplificati tutto ciò di cui l'interessato necessita per comprendere la propria posizione e prendere decisioni: in questo modo, grazie ad un semplice sguardo a un'icona, egli dovrebbe essere in grado di comprendere come i suoi dati vengano utilizzati. Tutto ciò è previsto dall'art. 12[7], ove si prevede che «[l]e informazioni da fornire agli interessati (...) possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico».

È appena il caso di accennare, infine, al tema – strettamente collegato a quello della trasparenza – dei meccanismi di certificazione, dei sigilli e dei marchi di protezione dei dati, volti a consentire agli interessati di valutare rapidamente il livello di protezione dei dati stessi: essi trovano la propria disciplina nel capo IV del regolamento e segnatamente all'art. 42 ([30]).

6. – Il diritto all'oblio, nella specifica materia che ci occupa, è il diritto dell'interessato alla rettifica dei dati personali a lui riferiti e alla cancellazione degli stessi. Si tratta di un diritto assoluto, sacrificabile soltanto in presenza di interessi specificamente individuati dal legislatore.

Sul preciso contenuto del diritto all'oblio, da un punto di vista teorico, la dottrina ha avanzato diverse ipotesi ([31]). Alcuni vi hanno scorto una

---

([30]) Sul punto può rinviarsi alla puntuale analisi svolta da BISTOLFI, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 438 ss.

([31]) Il diritto all'oblio è venuto definendosi come autonomo diritto della personalità in relazione al diritto di cronaca: cfr. G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, p. 801 ss.; MORELLI, *Fondamento costituzionale e tecniche di tutela dei diritti della personalità di nuova emersione (a proposito del c.d. «diritto all'oblio»)*, in *Giust. civ.*, 1997, II, p. 515 ss.; MORELLI, *Oblio (diritto all')*, in *Enc. dir., Agg.*, VI, Milano, 2002, p. 848 ss.; MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della* privacy *storica*, Napoli, 2009, *passim*.

Fra i contributi che, con prospettive diverse, di sono occupati in particolar modo del diritto all'oblio nei contesti telematici, v. almeno M. MEZZANOTTE, *La memoria conservata in Internet ed il diritto all'oblio telematico: storia di uno scontro annunciato*, in *Dir. Internet*, 2007, p. 398 ss.; FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, 2010, p. 391 ss.; MESSINA, *Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione*, in *Inform. dir.*, 2009, p. 93 ss.; DI CIOMMO e PARDOLESI, *Trattamento dei dati personali e archivi storici in rete: dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la rete, bellezza!*, in *Danno resp.*, 2012, p. 701 ss.; SPOTO, *Note critiche sul diritto all'oblio e circolazione delle informazioni in rete*, in *questa rivista*, 2012, p. 1048 ss.; MANGANO, *Diritto all'oblio*, in *Giur. mer.*, 2012, p. 2621 ss.; FEROLA, *Dal diritto all'oblio al diritto alla memoria sul* web. *L'esperienza applicativa italiana*, in *Dir. inf.*, 2012, p. 1001 ss.; DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, in *Danno resp.*, 2014, p. 1101 ss.;

naturale conseguenza della corretta applicazione dei principi generali del diritto di cronaca: così come non va diffuso il fatto la cui divulgazione non risponda a un reale interesse pubblico, allo stesso modo non va riproposta la vecchia notizia non più rispondente a un'attuale esigenza informativa. Da parte di altri il diritto all'oblio è stato inquadrato come uno dei molteplici aspetti del più generale diritto alla riservatezza o come un profilo del diritto all'onore. Altri ancora hanno parlato, in chiave soggettivistica, di una difesa dell'individuo dal ritorno del rimosso, dal ripresentarsi di ricordi dolorosi. Parrebbe, dunque, che il tratto comune a tutte queste ricostruzioni sia il seguente: che il diritto all'oblio è la traduzione sul piano giuridico dell'esigenza di tutelare l'interesse del soggetto a che non venga conservata memoria collettiva di vicende a lui relative ormai superate dal tempo, o di vicende a lui falsamente attribuite.

Sembra anche, tuttavia, che dal regolamento emerga un concetto ben più ampio di questo diritto, visto come generico diritto a ottenere la cancellazione dei propri dati personali in presenza di circostanze di varia natura ([32]). L'art. 17 del regolamento, infatti, stabilisce che «[l]'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali». E fra le circostanze – analiticamente individuate dalla disposizione – che costituiscono il presupposto del diritto all'oblio si ritrovano situazioni di natura obbiettiva e altre di natura soggettiva: fra le prime, possono ricordarsi: quella in cui i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti; quella in cui i dati personali sono stati trattati illecitamente e quella in cui i dati personali devono essere cancellati per adempiere un obbligo legale; fra le seconde, quella in cui l'interessato revoca il consenso su cui si basa il trattamento e

---

VIGLIANISI FERRARO, *La sentenza Google Spain ed il diritto all'oblio nello spazio giuridico europeo*, in *Contr. impr./Eur.*, 2015, p. 159 ss.; MINIUSSI, *Il «diritto all'oblio»: i paradossi del «caso Google»*, in *Riv. it. dir. pubbl. com.*, 2015, p. 209 ss.; VALVO, *Il diritto all'oblio nell'epoca dell'informazione «digitale»*, in *St. integr. eur.*, 2015, p. 347 ss.; COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, in *Dir. fam. pers.*, 2015, p. 740 ss.

Da ultimo, con particolare riferimento alla disciplina contenuta nel regolamento in esame, v. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, in AA.VV., *La nuova disciplina*, cit., p. 197 ss., nonché, sul fondamento del diritto all'oblio, con prospettiva di carattere generale, BONAVITA, *Le ragioni dell'oblio*, in *Cibersp. dir.*, 2017, p. 85 ss.

([32]) Cfr. da ultimo SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leggi civ. comm.*, 2017, p. 1023 ss.

non sussiste altro fondamento giuridico per il trattamento (vale a dire la necessità dello stesso), nonché quella in cui l'interessato si oppone al trattamento (33).

Il diritto all'oblio, tuttavia, non può essere esercitato laddove, pur sussistendo uno dei presupposti appena elencati, il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale (si pensi ancora al notaio, obbligato a dare pubblicità a un suo atto), per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, a fini di ricerca o statistici, o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

È molto difficile ricondurre ad unità di *ratio* i presupposti del diritto all'oblio individuati dal regolamento e, di conseguenza, ricostruire unitariamente tale diritto: se, certamente, esso è in parte riconducibile ai profili tradizionalmente evocati dalla dottrina, esso è anche concepito dal legislatore comunitario come difesa dell'interessato di fronte all'illegittimità del trattamento o alla mera inutilità dello stesso.

7. – L'attuazione del principio di *accountability* si ritrova nel capo IV del regolamento, intitolato al «Titolare del trattamento» e al «responsabile del trattamento» (quest'ultimo definito dall'art. 4 come il soggetto «che tratta dati personali per conto del titolare del trattamento») (34). L'art. 24, rubricato «Responsabilità del titolare del trattamento», stabilisce che il titolare «deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al (...) regolamento. Dette misure sono riesaminate e aggiornate qualora necessario» (35).

Quello di *accountability* è un concetto difficilmente traducibile in una parola della nostra lingua e reso, nella versione italiana del regolamento, con il termine "responsabilità". In realtà, esso si colloca a metà tra la responsabilità e la *compliance*, perché il titolare deve essere *compliant* rispetto alla normativa in esame. Bisognerà trovare un termine diverso o composto per evitare l'utilizzo del termine "responsabilità": problemi di

---

(33) Sul punto, in generale, v. PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 259 ss.

(34) Su tali figure v. G.M. RICCIO, Data Protection Officer *e altre figure*, in AA.VV., *La nuova disciplina*, cit., p. 33 ss.

(35) Puntuale, sul punto, l'analisi di BISTOLFI, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 323 ss.

traduzione esistono, ogni lingua ha dei termini difficilmente traducibili e quello dell'*accountability* appare proprio uno di questi casi.

In materia di tutela dei diritti della personalità, questo principio potrebbe apparire come un corollario del principio di trasparenza. Tuttavia, l'*accountability* dev'essere intesa non già come completa accessibilità, da parte dell'interessato, alle informazioni circa l'attività di un dato operatore, bensì come garanzia della conformità di tale attività alla disciplina di settore: conformità che l'operatore – il titolare del trattamento – dev'essere in grado di dimostrare in qualsiasi momento (36).

Da questo punto di vista, una sorta di facilitazione deriva dall'adesione del titolare del trattamento a un codice di condotta: così dispone l'art. 24[3], il quale afferma che «[l]'adesione ai codici di condotta (...) o a un meccanismo di certificazione (...) può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento». Al di là del piano probatorio, sembra comunque che il principio di *accountability* imponga ai titolari del trattamento, ai fini della sua attuazione, l'adozione di «un sistema di controllo della protezione dei dati, strutturato in base a *standard* di buona amministrazione riconosciuti universalmente e che sia verificabile (*auditable*) all'esterno, in quanto il rispetto delle regole in materia di dati personali da parte dei titolari del trattamento dei dati richiede non il mero adempimento delle disposizioni di legge ma la predisposizione di una vera e propria *governance* interna» (37).

Sui codici di condotta – tema che non è possibile affrontare compiutamente in questa sede – pare utile ricordare che essi sono disciplinati all'interno della sezione 5 del capo IV del regolamento (artt. 40-43), dedicata anche all'istituto della certificazione dei titolari del trattamento. In particolare, è prescritto agli Stati membri, da un lato, di incoraggiare

---

(36) È utile ricordare che l'idea di un sistema di *accountability* nel settore della *personal data protection* risale al 2010, allorché il gruppo di lavoro previsto dall'art. 29 della dir. 95/46/CE adottò un documento in cui veniva chiarito che il principio in questione era necessario al fine di rendere maggiormente effettive le misure adottate dai titolari del trattamento per garantire la protezione dei dati. Osserva SPINA, *Alla ricerca*, cit., p. 148, che l'*accountability* «poggia su una costruzione giuridica a due livelli: il primo diretto a implementare processi, misure e regole interne vincolanti; il secondo, quello di stimolare un processo virtuoso e volontario che vada oltre i requisiti minimi previsti dalla legge».

(37) Così SPINA, *Alla ricerca*, cit., p. 148, il quale, commentando la scelta del legislatore europeo, parla di «un modello di regolazione per la protezione dei dati personali basato su una forma ibrida di *enforced self-regulation* o piuttosto di vera e proprio *meta-regulation*» (*ibidem*): un modello in cui «[i]l regolatore (...) riveste (...) un ruolo di *auditor*, con responsabilità di monitoraggio e incentivazione dei sistemi di regolazione adottate dalle imprese e dagli organismi regolati» (*ivi*, p. 149).

l'elaborazione di tali codici – o l'adesione a codici già esistenti – da parte di associazioni e altri organismi rappresentativi delle categorie di titolari del trattamento (art. 40); dall'altro lato, di incoraggiare l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari e dai responsabili del trattamento (art. 41); a quest'ultimo fine, sono altresì regolati gli appositi organismi di certificazione (art. 43) (38).

8. – Il principio della *privacy by design* implica che la protezione dei dati sia *integrata* nell'intero ciclo di vita di una data tecnologia o servizio o processo, sin dalla relativa progettazione: in altre parole, che qualsiasi progetto debba essere realizzato avendo presente, sin dal principio – *by design*, appunto – la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto (informatiche e non). Si tratta di un approccio sempre più utilizzato al problema della protezione dei dati, volto a garantire la migliore operatività possibile della protezione (39).

Diverso principio – ma complementare a quello appena analizzato, in un'ottica di massima protezione efficiente dei dati – è quello della *privacy by default*, il quale implica che i dati vengano raccolti nella minore misura possibile e che le finalità del trattamento siano quanto più possibile limitate. Si tratta, in altre parole, della *summa* dei principi di "minimizzazione dei dati" e di "limitazione della finalità" (da cui discende a sua volta il principio della "limitazione della conservazione", il quale impone di limitare nel tempo quanto più possibile il trattamento e l'archiviazione dei dati raccolti).

Entrambi i principi appena ricordati – *privacy by design* e *by default* – sono stati accolti nel regolamento ed enunciati in via generale già nei "considerando", laddove si afferma che «il titolare del trattamento do-

---

(38) V. comunque, ampiamente, BOLOGNINI, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 421 ss., nonché POPOLI, in AA.VV., *Il nuovo Regolamento*, cit., p. 367 ss.

(39) Una più compiuta illustrazione del concetto, anche con riferimento alle rispettive origini concettuali, ne è offerta da PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy*:* privacy by design *e* privacy by default settings, in *Contr. impr./Eur.*, 2015, p. 197 ss., ove si trovano ulteriori riferimenti sul punto. V. inoltre D'ORAZIO, *Protezione dei dati* by default *e* by design, in AA.VV., *La nuova disciplina*, cit., p. 79 ss. Nella letteratura straniera, v. in particolare CAVOUKIAN, Privacy by Design*: Leadership, Methods, and Results*, in AA.VV., *European Data*, cit., p. 175 ss., nonché – con particolare riferimento alla *privacy by design* nel settore dei *social media* –DE WOLF, HEYMAN e PIERSON, *Privacy by Design Through a Social Requirements Analysis of Social Network Sites from a User Perspective*, *ivi*, p. 241 ss.

vrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di *default*. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare [40] i dati personali il più presto possibile, (...) consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati (...), i produttori (...) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni» [41].

L'auspicio è attuato attraverso l'art. 25 del regolamento, che rappresenta il fulcro normativo dei predetti principi. Secondo tale disposizione, «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del (...) regolamento e tutelare i diritti degli interessati».

È inoltre previsto che il titolare adotti «misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento» (*ivi*): obbligo questo che «vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità» (*ivi*).

Anche in questo caso, il titolare potrà servirsi di un meccanismo di certificazione *ex* art. 42 come elemento per dimostrare la conformità del trattamento ai predetti principi.

---

[40] La "pseudonimizzazione", ai sensi dell'art. 4, è un trattamento effettuato in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'ausilio di informazioni aggiuntive: ciò, naturalmente, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecnico-organizzative intese a garantire che i dati non siano attribuiti a una persona fisica identificata o identificabile. La pseudonimizzazione è altresì funzionale alla sicurezza dei dati personali. L'art. 32, infatti, elenca una serie di misure che il titolare del trattamento è tenuto a porre in essere al fine di garantire un livello di sicurezza adeguato al rischio (da determinarsi con riguardo alle potenziali conseguente della distruzione, della perdita, della modifica, della divulgazione non autorizzata dei dati, o dell'accesso, accidentale o illegale, ai medesimi) e tra queste misure – la cui adozione è rimessa alla discrezionalità dell'operatore – vi sono la cifratura dei dati personali e, appunto, la pseudonimizzazione degli stessi. Sulle modalità di pseudonimizzazione v., da ultimo, D'ACQUISTO e NALDI, Big Data *e* Privacy by Design. *Anonimizzazione. Pseudonimizzazione. Sicurezza*, Torino, 2017, p. 117 ss.

[41] Così il *considerando* n. 78 del regolamento.

9. – Il capo VIII del regolamento (artt. 77-84) è intitolato a «Mezzi di ricorso, responsabilità e sanzioni» (42). Al suo interno ritroviamo l'art. 82, rubricato «Diritto al risarcimento e responsabilità», il quale afferma la regola generale per cui «[c]hiunque subisca un danno materiale o immateriale causato da una violazione del (...) regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento». Naturalmente, il responsabile del trattamento, stante la sua peculiare posizione nei confronti del titolare, «risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi (...) specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento».

Occorre anche segnalare che il regolamento prevede espressamente, in caso di concorso di responsabilità, un regime di solidarietà passiva. È infatti stabilito che, «[q]ualora più titolari del trattamento o responsabili del trattamento (...) siano coinvolti nello stesso trattamento e siano (...) responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno»: ciò, come pure è previsto dalla disposizione, «al fine di garantire il risarcimento effettivo dell'interessato». Ne consegue che, «[q]ualora un titolare (...) o un responsabile (...) abbia pagato (...) l'intero risarcimento del danno, tale titolare (...) o responsabile (...) ha il diritto di reclamare dagli altri titolari (...) o responsabili (...) coinvolti (...) la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno»: parte che dovrà determinarsi alla stregua della regola generale di cui all'art. 2055 c.c. (43).

Il regolamento sembra contemplare anche la possibilità di una prova liberatoria, in quanto prevede che tanto il titolare quanto il responsabile sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non è loro imputabile. L'affermazione secondo cui la prova liberatoria *sembra* essere prevista, deriva dalla circostanza che la formulazione dell'art. 82 si presta ad essere letta in almeno due modi, al fine di coordinare la disposizione con le categorie del nostro sistema della responsabilità civile:

---

(42) In generale, sull'attuazione del c.d. principio di responsabilità nel regolamento, v. PARISI, *Responsabilità e sanzioni*, in AA.VV., *La nuova disciplina*, cit., p. 289 ss.

(43) In generale, sulla responsabilità da illecito trattamento dei dati personali, v. RATTI, in AA.VV., *Il nuovo Regolamento*, cit., p. 615 ss. Sul danno risarcibile in particolare, v. ampiamente PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento*, cit., p. 597 ss.

una prima lettura potrebbe essere nel senso che il legislatore comunitario, nel parlare di *imputabilità*, faccia riferimento proprio al criterio di cui all'art. 2046 c.c., oppure al nesso di causalità tra la condotta del titolare o del responsabile e il danno: una lettura, questa, che finirebbe con lo svuotare di contenuto la disposizione del regolamento, la quale si risolverebbe in un pleonasmo (cioè nel dire che non vi è responsabilità allorché non vi sia imputabilità o nesso causale);

una seconda lettura, invece, potrebbe essere quella di ritenere che l'esonero dipenda da una condotta attiva dell'agente, come quella consistente nell'aver fatto tutto il possibile per evitare il danno, alla stregua di quanto previsto in diverse ipotesi di responsabilità oggettiva contemplate dal nostro ordinamento (es. artt. 2047[1] e 2048[3] c.c.).

10. – Il regolamento oggetto della presente analisi costituisce un punto di partenza e, al contempo, una sfida. L'obbiettivo primario è quello di rendere effettivo, in tutti gli Stati membri dell'Unione, un livello uniforme ed elevato di protezione dei dati personali dei cittadini europei, dei quali occorre rafforzare la fiducia – sotto questo profilo – nel rapporto con le p.a. e con gli operatori economici privati.

A questi ultimi il regolamento richiede di andare oltre gli aspetti meramente formali dell'applicazione della disciplina e propone un profondo cambiamento culturale, affinché le prassi si adeguino costantemente ai cambiamenti determinati dall'incessante evoluzione delle tecnologie (*cloud computing*, *social media*, interconnessione delle banche dati, ecc.) (44).

Tutto ciò presenta senza dubbio un forte impatto organizzativo: basti pensare all'applicazione del principio della *privacy by design*, che aspira a rimodulare gli schemi di progettazione dei servizi, dei *software*, dei processi aziendali. Il risultato perseguito, tuttavia, è ambizioso quanto prezioso: si tratta, in ultima analisi, di agevolare sia gli utenti di servizi, sia gli stessi operatori economici – finalmente dotati di un'unica normativa in tema di *privacy* –, a tutto vantaggio di quel mercato che ancora oggi appare costituire il perno intorno al quale ruota gran parte del sistema normativo e delle politiche comunitarie.

---

(44) Secondo SPINA, *Alla ricerca*, cit., p. 152, «[s]arebbe ingenuo credere che il regolamento (...) completi un'opera di armonizzazione a livello europeo delle norme sulla protezione dei dati personali», anche in ragione della «probabile inerzia che condizionerà i primi anni di vita» di esso. Maggiormente fiduciosa appare M.G. STANZIONE, *Il regolamento*, cit., p. 1264.