IAIC ITALIAN ACADEMY OF THE INTERNET CODE
MiBACT DGBIC DIREZIONE GENERALE BIBLIOTECHE E ISTITUTI CULTURALI
CREDA Centro Ricerca di Eccellenza per il Diritto di Autore

DIRITTO MERCATO TECNOLOGIA

ANNO 2016, NUMERO 3

ISSN (Online Edition): 2239 -7442

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

DIRITTO MERCATO TECNOLOGIA

INDICE DEL FASCICOLO N. 3
(settembre – dicembre 2016)

INTERNET OF THINGS: PRIVACY VS CONCORRENZA?

Davide De Filippis
Università Roma Tre

SOMMARIO: 1. Considerazioni introduttive. - 2. La nozione di *privacy*: dal "diritto ad essere lasciato solo" all'autodeterminazione informativa. - 3. Il "diritto all'oblio" nel Regolamento europeo generale sulla protezione dei dati. - 4. Obblighi informativi e il problema della legge applicabile al titolare del trattamento. - 5. La tutela dell'immagine del terzo nell'*Internet of Things*. - 6. Possibili accorgimenti a tutela della *privacy*: *privacy by design e privacy by default*. - 7. A mo' di (provvisorie) conclusioni: la concorrenza nel mercato dei dispositivi dell'IoT.

1. Considerazioni introduttive

L'uso della dizione "Internet delle Cose", focalizzando l'attenzione sull'oggetto, sembrerebbe pretermettere l'utente che tali dispositivi utilizza.

Probabilmente, questa impressione potrebbe, pure, trovare conferma nelle stime che indicano che il numero di oggetti connessi (esclusi PC, *smartphone* e *tablet*) passerà da 4,9 miliardi nel 2015 a 25 miliardi nel 2020[1]; nello stesso arco temporale, la popolazione mondiale si stima passerà dagli attuali 7,1 miliardi a 7,7 miliardi[2]. È evidente, allora, che, nel giro di pochi anni, potremo trovarci in un mondo dominato da "Cose" tra di loro interconnesse.

[1] Secondo quanto riportato sul sito *www.corrierecomunicazioni.it*, questa sarebbe la stima effettuata dalla società - nota nel campo della consulenza nell'*Information Technology* - Gartner.

[2] Fonte: U.S. Census Bureau. Lo studio è reperibile sul sito *www.census.gov/population/international*.

Tale riflessione viene, tuttavia, immediatamente smentita dalla constatazione che i *devices* dell'*Internet of Things* intanto esistono - o, comunque, vengono utilizzati - perché vi sono fruitori che hanno interesse ad un loro sfruttamento in termini di maggiori facilitazioni nella vita quotidiana[3].

Il problema che si cercherà di affrontare concerne il flusso di informazioni che tali dispositivi sono in grado di generare (*big data*) e la tutela delle persone i cui dati sono trattati, ponendo - nelle pagine successive - l'accento proprio sul possibile diverso atteggiarsi delle più recenti problematiche emerse in punto di trattamento di dati personali in considerazione delle peculiarità del fenomeno oggetto di esame.

In via di prima approssimazione, è possibile notare come, nonostante le nuove tecnologie garantiscano una semplificazione delle attività quotidiane, sia necessario, di contro, scongiurare il pericolo che un uso spregiudicato dei dati personali alimenti un "mercato" digitale, basato sullo sfruttamento commerciale delle informazioni individuali[4].

In questa prospettiva si registra l'attenzione che all'argomento è stata rivolta a diversi livelli. Innanzitutto, il Gruppo di lavoro per la tutela dei dati personali *ex* art. 29 della direttiva 95/46/CE ha elaborato un dettagliato parere[5] che mette in risalto, accanto al motivo di preoccupazione ora

[3] Più nel dettaglio, gli ambiti di utilizzo spaziano dal monitoraggio sui propri parametri vitali (si pensi ai dispositivi *quantified self*, vale a dire quelli che consentono una quantificazione del sé: dispositivi per misurare la pressione arteriosa, il battito cardiaco, i grassi presenti nel sangue …) al *lifelogging* o *life caching* (si tratta della tendenza a raccogliere attraverso dispositivi indossabili e memorizzare in *database* o in *cloud* tracce di tutti gli eventi considerati significativi della propria vita per poi eventualmente condividerli con altri) fino a giungere alle innovazioni offerte dalla domotica che permettono, tra le altre cose, risparmi di energia (attraverso, per esempio, le prese *wi-fi* che consentono l'accensione e lo spegnimento degli elettrodomestici a distanza) o un consumo di cibi più responsabile (il riferimento è al frigorifero che comunica la data di scadenza degli alimenti o elabora la lista della spesa).

[4] Così E. Germani, L. Ferola, *Il* wearable computing *e gli orizzonti futuri della privacy*, in *Dir. Informaz.*, 2014, pp. 75 ss., spec. p. 79.

[5] Si tratta dell'*Opinion 8/2014 on the Recent Developments on the Internet of Things*, adottata il 16 settembre 2014, disponibile al link: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion -recommendation/files/2014/wp223_en.pdf*

segnalato, alcuni aspetti - sui quali si tornerà nel corso dell'indagine - di spiccato interesse ai nostri fini. Non solo, la molteplicità di categorie di dati che un dispositivo dell'IoT è in grado di raccogliere, ma soprattutto il rischio di una sistematica sorveglianza delle abitudini degli individui (solo per citarne alcuni) appaiono ineludibili premesse nell'approccio alla presente tematica.

A distanza di poco tempo, nel corso della 36ma Conferenza internazionale delle Autorità di protezione dei dati personali, è stata adottata una Dichiarazione[6] nella quale si perviene ad una serie di conclusioni le quali, oltre ad ispirare i futuri orientamenti delle Autorità competenti sul tema, forniscono interessanti spunti di riflessione sul piano operativo. In particolare, colpisce come le stesse Autorità competenti in materia di *privacy* si sforzino di ricercare un (difficile) punto di equilibrio tra istanze di diverso segno alle quali si accennerà nel corso della trattazione.

In assenza di un quadro normativo che consenta di delineare chiaramente compiti e responsabilità dei produttori, i soggetti istituzionali coinvolti paiono, difatti, devolvere la tutela relativa ai profili informativi al buon senso delle imprese produttrici le quali, al contrario, sembrano maggiormente interessate ai "profitti" derivanti non solo dalla produzione dei dispositivi, ma, per l'appunto, ai dati generati da questi ultimi e ai servizi ad essi connessi.

A livello nazionale, appare, certamente, meno ambiziosa la consultazione pubblica su Internet delle Cose avviata dall'Autorità Garante per la Protezione dei dati personali[7] che consente a tutti i soggetti interessati di far pervenire osservazioni, commenti, informazioni e proposte ritenute utili. Il coinvolgimento finanche degli utenti - si può osservare - non potrà che giovare ad una regolazione, per dir così, *bottom-up*, ma esprimere un

[6] Cfr. *Mauritius Declaration on the Internet of Things*, disponibile al link: *http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf*.

[7] Il riferimento è alla decisione adottata dal Garante per la protezione dei dati personali il 26 marzo 2015 e pubblicata sulla Gazzetta ufficiale n. 101 del 4 maggio 2015. Va osservato che - anche con riferimento a quanto si dirà *infra* nel testo - è ormai spirato il termine di 180 giorni dalla predetta pubblicazione sulla GU.

giudizio complessivo sull'efficacia di simili iniziative[8] - essendo, a quanto consta, ancora ignoti i risultati di tale consultazione - potrebbe rivelarsi a dir poco prematuro.

Infine, va segnalata la posizione dell'Autorità per le Garanzie nelle Comunicazioni la quale nel *Rapporto finale dell'Indagine conoscitiva concernente i servizi di comunicazione Machine to Machine*[9] ha fornito un importante contributo in merito al problema oggetto di riflessione. Si tratta - nell'ottica di una auspicabile "connessione" tra le Autorità amministrative indipendenti[10] - di un importante documento nel quale vengono a delinearsi i profili regolatori relativi ai servizi *Machine to Machine* i quali, pur non

[8] Più di recente (11 aprile 2016), ha preso l'avvio, altresì, il "*Privacy Sweep 2016*", ovvero un'indagine a carattere internazionale volta a verificare, per l'appunto, il rispetto della *privacy* nell'Internet delle Cose. Segnatamente, il Garante italiano concentrerà la sua azione sulla domotica per verificare il grado di trasparenza nell'uso delle informazioni personali dei consumatori e il rispetto delle norme sulla protezione di dati da parte delle imprese, anche multinazionali, operanti nel settore. In generale, le ventinove Autorità garanti della *privacy* coinvolte valuteranno anche possibili interventi nei confronti delle imprese i cui dispositivi o servizi risulteranno in violazione delle norme sulla protezione dei dati.

[9] Agcom, *Indagine conoscitiva concernente i servizi di comunicazione Machine to machine (M2M)*, Rapporto finale all. A, Delibera n. 120/15/CONS del 11 marzo 2015, disponibile sul sito istituzionale dell'Autorità.

[10] Come sottolineato nell'introduzione del Garante *privacy* in Atti del Convegno "*Il pianeta connesso. La nuova dimensione della privacy*", Roma, 28 gennaio 2015, pp. 3 ss. Sulla necessità di un "dialogo" tra le Autorità amministrative indipendenti resta quanto mai attuale l'auspicio di M. Clarich, *Autorità indipendenti. Bilancio e prospettive di un modello*, Il Mulino, Bologna, 2005, il quale osserva (pp. 41 ss.) che «*un miglior coordinamento nell'esercizio dei poteri richiederebbe interventi legislativi volti ad allineare le competenze e a eliminare alcune incongruenze. Richiederebbe altresì un maggior impegno delle autorità a evitare invasioni di campo o duplicazioni di attività, per esempio attraverso accordi o protocolli d'intesa … Ma, se si crede nella bontà del modello delle autorità indipendenti, il coordinamento deve mantenere una dimensione orizzontale tendenzialmente paritaria, sia pure entro una cornice di regole che definiscano, distribuiscano e creino i raccordi (sotto forma di pareri, intese, proposte, ecc.) tra le varie competenze. Sarebbe invece incoerente imporre un "direttore d'orchestra", magari con una connotazione prettamente politica, dotato di poteri di indirizzo*».

coincidendo *in toto* con l'*Internet of Things*, possono essere ricondotti, ove utilizzino una connessione Internet, in quest'ultimo ambito[11].

Tale ultimo contributo, assieme a tematiche di indubbia rilevanza, solleva (ma non fornisce una risposta) un interrogativo di non poco momento che "aleggia", sovente, nella materia che occupa: a chi appartengono le informazioni desumibili dai dispositivi acquistati dagli utenti? Non è possibile indugiare su simili questioni che, per la portata, esulano dai limiti della presente ricerca. Allo stesso tempo, d'altro canto, potrebbe constatarsi - anche alla luce di quanto si dirà più innanzi - che mentre un controllo di tipo proprietario è possibile sui dati immessi "consapevolmente" dall'utente, difficilmente una simile conclusione potrà valere per la pluralità di altre informazioni (dati grezzi e aggregati) che un dispositivo dell'IoT è in grado di generare[12].

Dagli indirizzi - ora brevemente riassunti - dei soggetti istituzionali coinvolti emerge la complessità del fenomeno che ci si accinge ad esaminare; tale difficoltà di inquadramento riviene, probabilmente, dalla eterogeneità della sua fenomenologia (non solo dispositivi indossabili, ma anche città intelligenti, *smart grid*, ecc…) che oggi più che mai impone di ripensare alla stessa posizione dell'individuo il quale non pare più geloso del proprio isolamento, anzi aperto alla complessità, per l'appunto, del reale e pronto a cimentarsi con l'uso delle nuove tecnologie.

Al diritto nazionale (*i.e.*, d.lgs. 30 giugno 2003, n. 196 recante il *Codice in materia di protezione dei dati personali*) e sovranazionale[13],

[11] Sul punto, si rinvia all'approfondito studio di F. Graziadei, *L'Internet delle Cose: una prima ricognizione delle problematiche regolatorie*, in G. Olivieri e V. Falce (a cura di), *Smart cities e diritto dell'innovazione, Quaderni di Giurisprudenza Commerciale*, Milano, 2016, pp. 155 ss.

[12] In argomento cfr. R. Romano, Big Data, Smart Cities *e proprietà intellettuale: quale il giusto equilibrio?*, in G. Olivieri e V. Falce (a cura di), *Smart cities e diritto dell'innovazione, cit.*, pp. 263 ss., spec. pp. 266 ss.

[13] La presente indagine, infatti, non può prescindere dall'esame del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), che abroga la direttiva 95/46/CE. Si conclude così il lungo e tortuoso *iter* di riforma della materia della

nonché ai regolatori nazionali l'arduo compito di predisporre le opportune cautele.

2. La nozione di *privacy*: dal "diritto ad essere lasciato solo" all'autodeterminazione informativa

Utilizzando uno *smartwatch* oppure anche solo guardando una *Smart TV*, il fruitore genera, spesso ed anche inconsapevolmente, una enorme quantità di dati relativi alle sue prestazioni fisiche o abitudini televisive.

Si considerino, poi, i dispositivi *quantified self*: i dati prodotti, concernenti nella maggior parte dei casi le condizioni di salute, non sono soltanto quelli che vengono visualizzati sul dispositivo (si pensi, per esempio, ad un accelerometro in grado di misurare il livello di stress dell'interessato: il dato che viene visualizzato è solo quest'ultimo), ma anche quelli grezzi e quelli aggregati (per restare al nostro esempio il dato grezzo consiste nel misurare le mosse dell'addome mentre quelli aggregati sono il prodotto dell'estrazione delle informazioni sul ritmo respiratorio).

In sostanza, s'intende dire che potrebbe esservi, in primo luogo, il rischio che attraverso forme di profilazione degli individui s'imponga un forte condizionamento della libertà di scelta dei singoli attraverso

protezione dei dati personali avviato con la presentazione da parte della Commissione del "pacchetto protezione dati" nel gennaio 2012. Infatti, accanto a tale sopravvenienza normativa, sono state pubblicate sulla Gazzetta Ufficiale dell'Unione europea del 4 maggio 2016, altresì, la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI del Consiglio, e la Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Per una disamina degli elementi di continuità e di quelli innovativi del regolamento sulla protezione dei dati rispetto alla direttiva 95/46/CE cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016 e M. G. Stanzione, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, in *Europa e diritto privato,* 2016, pp. 1249 ss.

meccanismi che selezionano, all'insaputa degli interessati e sulla base di catalogazioni comportamentali predefinite da chi gestisce gli strumenti di comunicazione telematica, le offerte emergenti dal mondo non solo dei consumi, ma anche, più in generale, delle relazioni sociali[14]. A questo si aggiunga che, per effetto dell'eterogeneità dei dati raccolti, alcuni di essi potrebbero non essere adeguatamente rivedibili dalla persona interessata prima della pubblicazione, generando, per tale via, il rischio di una mancanza di controllo ed un'eccessiva auto-esposizione per l'utente.

Quest'ultimo, come già si rilevava, quando utilizza dispositivi tra di loro interconnessi, opta per l'ingresso nella Rete, la quale diviene vieppiù evanescente in quanto comincia ad essere incorporata in tutto ciò con cui noi

[14] Com'è noto, la profilazione consiste, secondo la definizione rinvenibile nel *considerando* 71 del Regolamento recentemente approvato (definizione analoga si ritrova nell'art. 4, n. 4, quanto alla disciplina del fenomeno cfr. l'art. 22), in una «*forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*». Si tratta - anche con riferimento alla profilazione come, del resto, si dirà per la materia che occupa - di garantire all'utente la formazione di un completo ed esatto convincimento circa il consenso da dare o negare alla richiesta di trattamento profilatorio. Ciò è possibile - oltre che per il tramite del rispetto di regole di trasparenza analoghe a quelle che osserveremo nel testo - attraverso la dichiarazione di illiceità di quei trattamenti che siano ottenuti mediante manifestazioni di consenso non pienamente libere da parte degli interessati perché condizionate rispetto al raggiungimento dei vantaggi o delle prestazioni offerte dal professionista al momento della raccolta (si pensi, p.e., ad un professionista che subordini i servizi da fornirsi al cliente rispetto al rilascio del consenso come se quest'ultimo possa essere una controprestazione necessaria alla conclusione del contratto). Infine, anche con riguardo a siffatta tecnica, è necessario che sussista un rapporto di proporzionalità tra informazioni raccolte e finalità perseguite con il trattamento. A simili conclusioni è pervenuta l'Autorità garante per la protezione dei dati personali in svariati provvedimenti: per una rassegna dei medesimi e per una complessiva analisi della problematica si rinvia a R. De Meo, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. Informaz.*, 2013, pp. 587 ss.

interagiamo[15], abbandonando così il suo stato di isolamento e il correlativo diritto di essere lasciato solo nell'intimità della propria vita privata.

Sarebbe, pertanto, auspicabile - ma del resto tracce di tale tendenza potrebbero riscontrarsi già nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea e, più recentemente, nell'art. 6 della Dichiarazione dei Diritti in Internet[16]- un definitivo superamento della nozione di *privacy* in termini di *right to be let alone*[17].

Per converso, occorrerebbe interpretare la tutela apprestata ai dati personali nell'ottica della disponibilità dei dati che riguardano il singolo e di conoscenza di chi e come li sta utilizzando[18]: volendo sintetizzare si dovrebbe discorrere di *autodeterminazione informativa*.

Nel moderno assetto socio-tecnologico, in altri termini, dovrebbe essere garantito all'utente il diritto-potere di «*mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata*»[19].

Alla luce di quanto fin qui detto, in considerazione dei rischi connessi all'utilizzo dei dispositivi dell'Internet delle Cose, occorrerebbe, dunque, ripensare alle modalità con le quali avviene l'espressione del consenso da parte dell'utente.

Si tratta di fornire a quest'ultimo tutte le informazioni relative alla tipologia dei dati raccolti, agli scopi che s'intendono perseguire e alla durata

---

[15] Così A. Spadaro, in Atti del Convegno "*Il pianeta connesso. La nuova dimensione della privacy*", cit., p. 22.

[16] Si tratta della Carta, elaborata anche all'esito di una consultazione pubblica, approvata dalla Commissione di studio sui diritti e doveri relativi ad Internet e pubblicata il 28 luglio 2015.

[17] Come formulata da Samuel D. Warren e Louis D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, p. 193.

[18] Cfr. S. Rodotà, *Il diritto di avere diritti*, Roma - Bari, 2012, p. 320.

[19] In questi termini S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 122. Osserva lo stesso S. Rodotà, *Il diritto di avere diritti*, *cit.*, p. 320, che «*l'originaria definizione della privacy come "diritto di essere lasciato solo" non è stata cancellata ma fa parte di un contesto via via arricchito da diversi punti di vista*» (virgolettato dell'A.) quali il «*controllare l'uso che gli altri fanno delle informazioni che mi riguardano*», la «*tutela delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale*».

di conservazione dei dati stessi in modo da ridurre sensibilmente le asimmetrie informative che esistono tra il produttore e l'utente.

In particolare, il fruitore del dispositivo deve essere edotto sin da subito sulla circostanza che - accanto alle informazioni che potremmo definire principali, ovvero quelle che, nell'esempio fatto in precedenza, sono visualizzabili sul dispositivo - vi sono quelle informazioni, apparentemente, secondarie (come detto: dati grezzi e aggregati) che potrebbero essere utilizzate per scopi totalmente diversi, necessitando, dunque, di un'informativa che renda nota al fruitore tale evenienza.

Inoltre, un'attenzione particolare deve essere riservata ai rischi relativi alla qualità dei dati che potrebbero derivare dalla loro natura sensibile, specie considerati gli usi in campo medico - sanitario.

Per consentire alle persone interessate un pervasivo controllo sulle informazioni ad esse relative deve essere, dunque, garantita la possibilità di revocare qualsiasi preventivo consenso ad un trattamento specifico e di opporsi al trattamento dei dati che le riguardano. Ferme le ulteriori considerazioni svolte più innanzi, è possibile, sin d'ora, rilevare la necessità che l'esercizio di tali diritti sia reso possibile senza vincoli o impedimenti tecnici o organizzativi e gli strumenti forniti per registrare il ritiro del consenso devono essere accessibili, visibili ed efficienti[20].

A tal proposito, non vanno sottovalutati, benché il punto in questa sede possa essere solo accennato, i rischi connessi alla rapida diffusione della propria immagine per effetto di un dispositivo dell'Internet delle Cose direttamente collegato ad un *social network* o ad un motore di ricerca (si pensi alle immagini scattate da un dispositivo indossabile e poi condivise nei *social networks*).

Infatti, se, da un lato, le persone interessate dall'Internet delle Cose sono ancora più propense a fare uso delle cose collegate quando possono condividere tali dati con altri utenti o con il pubblico (per esempio, gli utenti dei dispositivi *quantified self* tendono a condividere i dati con altri utenti sui *social network* per promuovere una sorta di concorrenza positiva all'interno

[20] Così *Opinion 8/2014 on the Recent Developments on the Internet of Things*, cit., p. 20.

del gruppo), dall'altro la diffusione della propria immagine potrebbe avere degli effetti pregiudizievoli della propria reputazione (o di quella dei propri cari), sulla attività professionale ovvero per le aziende o istituzioni presso le quali si è incardinati.

Si pensi al caso detto del "pirata ubriaco"[21] in cui una giovane aspirante insegnante aveva immesso la fotografia che la ritraeva con un cappello da pirata mentre beveva da un bicchiere di plastica, sulla sua pagina di *MySpace* (noto *social network*), inserendo anche la dicitura "il pirata ubriaco"; successivamente, la foto era stata notata dall'amministrazione della scuola in cui l'aspirante insegnante svolgeva il tirocinio. Nonostante la rimozione, la foto della donna si era, tuttavia, diffusa nella rete ed era stata indicizzata dai motori di ricerca, provocando, in definitiva, la mancata assunzione dell'insegnante da parte della scuola.

Dunque, a fronte della scarsezza di tutela rispetto alla riproduzione dei dati personali - tra i quali, come si specificherà meglio oltre, deve essere annoverata l'immagine - contenuti nei profili-utente, che possono essere reperiti tramite motori di ricerca, copiati su altri siti e riprodotti infinite volte nel tempo, con loro conseguente decontestualizzazione o permanenza presso i fornitori del servizio, occorrerebbe interrogarsi se, all'uopo, debba riconoscersi all'utente e del dispositivo e del *social network* il *diritto alla cancellazione ("diritto all'oblio")*[22].

3. Il "diritto all'oblio" nel Regolamento europeo generale sulla protezione dei dati

[21] Tratto da V. Mayer-Schonberger, *Delete: The virtue of forgetting in the Digital Age, Princeton University Press*, 2011, p. 1, tradotto in italiano per i tipi di Egea: *Delete. Il diritto all'oblio nell'era digitale*, Milano, 2010.

[22] Così è rubricato l'art. 17 del Regolamento (UE) 2016/679.

Nei più recenti approdi giurisprudenziali nazionali[23] ed europei[24] in materia, la richiesta di procedere alla cancellazione di un'informazione è

[23] Il riferimento è, tra le altre, a Cass., sez. III, sent., 5 aprile 2012, n. 5525, in *Dir. Informaz.*, 2012, pp. 910 ss. con nota di T.E. Frosini, *Il diritto all'oblio e la libertà informatica*; in *Guida al diritto*, n. 5 (Monografia), 2013, pp. 42 ss.; in *Foro it.*, c. 305, con nota di E. Tucci. La vicenda concerne la notizia, riportata da alcuni quotidiani dell'epoca (1993), di un personaggio politico imputato di corruzione e poi assolto; la notizia dell'imputazione e non dell'assoluzione rimane memorizzata nell'archivio storico di un quotidiano nella versione *on-line*, donde il ricorso per vedere riconosciuto il diritto all'oblio. La Corte di legittimità non ha ritenuto, in tal caso, fondata una simile pretesa, ma piuttosto salvaguarda il pur meritevole - come, del resto, si avrà modo di dire nel testo (ma cfr., anche, *infra* nota 28) - diritto del soggetto al riconoscimento e godimento della propria attuale identità personale o morale sulla base del convincimento che «*la notizia, originariamente* completa e vera *diviene* non aggiornata, *risultando quindi* parziale e non esatta, *e pertanto sostanzialmente* non vera» (corsivi nel testo).
La Suprema Corte, sez. I, ha, recentemente, avuto occasione di ritornare sul tema allorquando con l'ordinanza 17 luglio 2015, n. 15096, in *Diritto e Giustizia*, 2015, 29, p. 19, con nota di F. Valerio, *Esiste un tempo massimo di permanenza dei dati nel registro delle imprese? La parola alla Corte di Giustizia*, ha sollevato ben due questioni pregiudiziali dinanzi alla Corte di Giustizia dell'Unione europea, di cui una (probabilmente quella di maggior interesse) così recita: *«se il principio di conservazione dei dati personali in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati, previsto dall'articolo 6, lettera e), della direttiva 4 6/95/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995, attuata Decreto Legislativo 30 giugno 2003, n. 196, debba prevalere e, quindi, osti al sistema di pubblicità attuato con il registro delle imprese, previsto dalla Prima direttiva 68/151/CE del Consiglio del 9 marzo 1968 nonché dal diritto nazionale all'articolo 2188 c.c., e Legge 29 dicembre 1993, n. 580, articolo 8, laddove esso esige che chiunque, senza limiti di tempo, possa conoscere i dati relativi alle persone fisiche ivi risultanti»*. Pur essendo differenti le angolazioni (p.e., nella dottrina giuscommercialistica, G. Carraro, *Pubblicità commerciale e «diritto all'oblio» nella prospettiva dei diritti dell'uomo*, in *Relazione al VII Convegno Orizzonti del Diritto commerciale*, 2016, opta per l'analisi del sistema della pubblicità commerciale in rapporto agli effetti dell'art. 8 CEDU) dalle quali muovere per analizzare le possibili implicazioni non solo dell'ordinanza in commento ma soprattutto di una eventuale pronuncia di accoglimento dei giudici lussemburghesi, è possibile osservare - senza alcuna pretesa predittiva circa le conclusioni alle quali la Corte di Giustizia perverrà - quanto segue. Il portato (se non lo si è mal inteso) della recente pronuncia *Google Spain*, di cui si dirà alla nota successiva, impone, infatti, di considerare il diritto alla riservatezza come inidoneo a

prevalere su altri diritti di pari rango; quest'ultimo dovendosi, al contrario, contemperare con situazioni giuridiche soggettive paritetiche o, come nell'ipotesi del registro delle imprese, con l'interesse di una pluralità di soggetti di disporre con facilità di «*informazioni veritiere e non contestabili*» (così G.F. Campobasso, *Diritto commerciale, I, Diritto dell'impresa,* (a cura di) M. Campobasso, Torino, 2014, p. 114) su fatti e situazioni delle imprese con cui entrano in contatto.

Tra le pronunce di merito si segnala, quale prima applicazione della sentenza *Google Spain* (della quale tiene in considerazione, pure, le linee guida per l'implementazione dei principi genericamente affermati in quella sentenza, elaborate dal Gruppo di lavoro per la tutela dei dati personali *ex* art. 29 cit. e pubblicate in data 26 novembre 2014: per una breve disamina delle medesime si rinvia a L. Bugiolacchi, *Quale responsabilità per il motore di ricerca in caso di mancata deindicizzazione su legittima richiesta dell'interessato?,* in *Resp. civ. prev.*, 2016, pp. 571 ss., spec. pp. 575-577), Trib. Roma, sez. I, sent., 3 dicembre 2015, n. 23771, in *Danno e resp.*, 2016, pp. 299 ss. con nota di F. Russo, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei Tribunali italiani dopo il caso* Google Spain. Tra i commenti relativi a tale pronuncia cfr., anche, G. Citarella, *«Diritto all'oblio» e rilevanza del tempo*, in *Resp. civ. prev.*, 2016, pp. 583 ss., e M. Rizzuti, *Il diritto e l'oblio,* in *Corr. giur.*, 2016, pp. 1077 ss.

[24] Si tratta, in particolare, di Corte Giust. UE, grande sez., 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, ex multis* in *NGCC*, 2014, pp. 1054 ss. con nota di G. Giannone Codiglione, *Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa?*. Per un commento della pronuncia si rinvia, inoltre, al volume monotematico di G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015; cui *adde*: O. Pollicino, *Diritto all'oblio e conservazione dei dati. La Corte di giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014, pp. 2949 ss.; L. Bugiolacchi, *Mancata rimozione della indicizzazione di spazi web a richiesta dell'interessato: la nuova frontiera della r. c. dei motori di ricerca,* in *Resp. civ. prev.*, 2014, pp. 1530 ss., e R. Petti, *La protezione dei dati personali e il caso Google Spain,* in *questa Rivista*, 1/2015, pp. 77 ss. (ai quali si rinvia, altresì, per ampi riferimenti al tema della responsabilità del *provider*); F. Melis, *Il diritto all'oblio e i motori di ricerca nel diritto europeo,* in *Giornale di diritto amministrativo,* 2015, pp. 171 ss.; C. Flick, *Il diritto all'oblio nella sentenza «Google Spain» e la sua applicazione pratica*, in *www.astrid-online.it*; L. Pelliccioli, *La sentenza «Google Spain» e l'interpretazione del diritto: alcune considerazioni*, in *Ciberspazio e diritto*, 2015, pp. 87 ss.; A. Viglianisi Ferraro, *La sentenza* Google Spain *ed il diritto all'oblio nello* spazio giuridico europeo, in *Contratto e impresa/Europa*, 2015, pp. 159 ss.

In tale occasione - fermo quanto si dirà *infra* nel testo - i giudici lussemburghesi hanno avuto modo di ribadire, in alcuni (a parere di chi scrive) significativi passaggi (parr. 80-81), non solo la capacità del motore di ricerca di costruire, attraverso la sintesi di informazioni

stata, com'è noto, rivolta non tanto al sito *web* dal quale i dati erano stati inizialmente raccolti e, poi, conservati ma al gestore del motore di ricerca. La circostanza non è passata inosservata tanto è vero che la dottrina, che ha avuto occasione di analizzare i predetti arresti, ha obiettato che non di diritto all'oblio debba discorrersi ma di diritto alla cancellazione, al blocco, al congelamento delle informazioni relative all'individuo[25].

Sul punto, si è rilevato[26] che la notizia - pure ove venga "deindicizzata" a cura del gestore del motore di ricerca - comunque non sarà definitivamente

---

provenienti da diversi siti, il profilo, *rectius* l'identità, di un determinato soggetto con potenziale pregiudizio per la sua vita privata (volendo utilizzare le parole della Corte: «*un trattamento di dati personali … effettuato dal gestore di un motore di ricerca … consente a qualsiasi utente di Internet di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro, e consente dunque di stabilire un profilo più o meno dettagliato di tale persona*»), ma soprattutto, come già rilevato, l'opportunità di effettuare, a fronte della richiesta di cancellazione di determinate informazioni, un bilanciamento con altre posizioni giuridiche soggettive di pari rango (riprendendo sempre le parole della pronuncia in commento: «*poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta*»).

[25] Possono darsi, secondo G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto all'oblio su internet dopo la sentenza Google Spain*, cit., pp. 30 ss., almeno tre accezioni del "diritto all'oblio": una, tradizionale, che fa riferimento al diritto di un soggetto a non vedere pubblicate alcune notizie relative a vicende (in specie, fatti di cronaca), già legittimamente pubblicate, rispetto all'accadimento delle quali è trascorso un notevole lasso di tempo; una seconda che mette in risalto non tanto l'esigenza di cancellare, ma piuttosto quella, affermatasi con lo sviluppo di internet e delle Reti telematiche, di «*attribuire un peso all'informazione nell'ambito di uno scenario complessivo che vede l'identità come protagonista*» ed infine quella cui si accenna nel testo ove, evidentemente, l'oblio pare essere una «*finalità*» che «*si può raggiungere con la cancellazione, ma anche con il blocco*».

[26] Il punto è ben sottolineato, tra gli altri, da F. Pizzetti, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di*

espunta dalla rete, essendo, anzi, disponibile a chiunque acceda al sito fonte[27]; così facendo, secondo quanto affermato in via pretoria, potrebbe trovare tutela il paritetico diritto all'accesso al dato in ragione della trasparenza e del controllo democratico delle attività alle quali i dati si riferiscono. Segnatamente, l'esigenza di contemperare la conservazione della notizia nel patrimonio informativo dei giornali in rete con la pretesa della persona coinvolta alla salvaguardia dell'identità personale emerge in un recente arresto della Corte EDU[28]. In tale occasione, i giudici di Strasburgo, nel tentativo di individuare il predetto punto di equilibrio, hanno

far cadere il "Velo di Maya", in *Il diritto all'oblio su internet dopo la sentenza Google Spain, cit.*, pp. 255 ss., spec. pp. 268 ss.

[27] Anzi, come evidenziato da F. Di Ciommo, *Quello che il diritto non dice. Internet e oblio,* in *Danno e resp.*, 2014, pp. 1101 ss., spec. p. 1113, rischia di verificarsi, addirittura, un singolare e paradossale effetto *boomerang* a danno di coloro i quali siano riusciti ad ottenere da Google la deindicizzazione: a seguito della sentenza *Google Spain* cit. è nato, difatti, in Rete un servizio - denominato *Hidden from Google* - che cataloga i risultati deindicizzati, aggiornando la lista man mano che Google accoglie le richieste degli utenti di esercitare il proprio "diritto all'oblio".

[28] Si tratta della sentenza della CEDU, sez. IV, 16 luglio 2013, ricorso n. 33846/2007, *Węgrzynowski e Smolczewski c. Polonia*, in *Giornale di diritto amministrativo,* 2013, p. 1211. Per un commento della pronuncia cfr. L. Nannipieri, *La sopravvivenza* online *di articoli giornalistici dal contenuto diffamatorio: la pretesa alla conservazione dell'identità e la prigione della memoria nel cyberspazio,* in *www.forumcostituzionale.it*, pp. 1 ss., e C. Melzi d'Eril, *Con l'aggiunta di una postilla si può spiegare che il contenuto del pezzo è stato "condannato",* in *Guida al diritto*, n. 40, 2013, pp. 103 ss.; la stessa è oggetto di breve annotazione in: A. Viglianisi Ferraro, *La sentenza* Google Spain *ed il diritto all'oblio nello* spazio giuridico europeo, *cit.*, pp. 179-182, e A. L. Valvo, *Il diritto all'oblio nell'epoca dell'informazione "digitale",* in *Studi sull'integrazione europea*, 2015, 347 ss., spec. pp. 348-350. Di recente, tale arresto è stato ripreso, altresì, dai giudici nazionali: v., segnatamente, App. Milano, sez. II, sentenza 17 maggio 2016, n. 1890, *inedita*.
Più nel dettaglio, la vicenda trae origine da un articolo riguardante due avvocati polacchi - apparso su un quotidiano a stampa - ritenuto diffamatorio dal Tribunale e, tuttavia, rinvenibile sul sito del giornale. I due avvocati ne chiedevano la rimozione dagli archivi Internet sulla base del duplice presupposto che: a) l'articolo diffamatorio era presente nel motore di ricerca di *Google* e che in base ai meccanismi automatici di indicizzazione chiunque digitasse il loro nome veniva a conoscenza dei fatti di cui all'articolo in questione; b) la versione *online* del detto articolo amplificava il danno in ragione del potenziale maggior numero di lettori.

negato la rimozione (definitiva) dagli archivi internet di una notizia, nella specie, diffamatoria, imponendo, al contempo, la pubblicazione di un'aggiunta contenente la specificazione che l'articolo era stato qualificato come tale dall'Autorità giudiziaria[29].

Diversamente, nella maggior parte dei casi, i dati veicolati per il tramite dell'*Internet of things* non paiono concernere informazioni rispetto alle quali sia configurabile la necessità di operare un bilanciamento con siffatti diritti (segnatamente, quello di cronaca o all'informazione) che, eventualmente, possono venire in considerazione.

Ciò nondimeno, si tratta, in ogni caso, di prestare tutela al più generale interesse dell'individuo alla contestualizzazione o corretta ricostruzione della propria identità personale: il pregiudizio potrebbe venir arrecato proprio dal probabile "incrocio" tra le informazioni relative alle proprie abitudini di vita o finanche delle condizioni di salute generate da un dispositivo dell'IoT e quelle già presenti o immesse successivamente su un *social network*. Non è inverosimile, quindi, il rischio che ne derivi un'immagine di quell'utente, al quale i dati sono riferibili, travisata o, qualora quelle informazioni restino memorizzate per lungo tempo, non più attuale.

Un possibile rimedio a simili inconvenienti pare rinvenirsi nella recente sopravvenienza normativa[30] la quale pone, espressamente, a carico

[29] Va osservato (cfr., in tal senso, L. Nannipieri, *La sopravvivenza* online *di articoli giornalistici dal contenuto diffamatorio: la pretesa alla conservazione dell'identità e la prigione della memoria nel cyberspazio, cit.*, p. 15) che la sentenza in commento non "scomoda" propriamente il diritto all'oblio, andando ad incidere «*su un piano ancora più intimo di tutela delle prerogative individuali, quello della pretesa all'eliminazione dei tratti identitari falsi e potenzialmente pregiudizievoli, immessi illegittimamente nell'ambiente digitale ad opera di soggetti terzi rispetto all'interessato*». In ogni caso, la Corte EDU parrebbe palesare «*un certo* favor *nei confronti della libertà di stampa, il cui peso risulta sostanzialmente prevalente rispetto al diritto alla riservatezza anche in una delle sue massime espressioni, qual è la pretesa alla conservazione della propria identità di fronte ad un esercizio illegittimo del diritto di cronaca*».

[30] Il riferimento è, specialmente, all'art. 17 cit., paragrafo 2, Regolamento cit. (ma in senso analogo v., pure, il *considerando* 66) il quale, secondo G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità, cit.*, p. 34, non costituisce una novità atteso che una simile previsione era già contenuta all'interno della legge italiana.

del «*titolare del trattamento*», obbligato a cancellare i dati personali, l'adozione di «*misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali*»[31].

Pur rinviando alle pagine che seguono l'indagine in ordine alla corretta identificazione del titolare del trattamento, è ragionevole ritenere che gli utenti di un dispositivo dell'Internet delle Cose possano avvalersi del diritto all'oblio, *rectius* alla cancellazione, al fine di tutelarsi anche da dati e notizie da loro stessi immessi in rete e successivamente "indicizzati" dai motori di ricerca[32].

Non meno problematico appare, inoltre, il profilo relativo alla c.d. portabilità dei dati. I produttori di dispositivi dell'*Internet of Things* potrebbero essere fortemente indotti - in un settore ove gli interessi economici in gioco sono in costante aumento[33] - a consolidare la propria posizione monopolistica rendendo difficoltoso, come testimonia proprio l'esperienza delle piattaforme *social*[34], il trasferimento dei propri dati da un *device* ad un altro e precludendo, per tal via, l'ingresso nel mercato di nuovi *players.*

---

[31] Dovrebbe interpretarsi - essendo, diversamente, ridimensionata notevolmente la portata applicativa della previsione in commento (*contra* cfr. Miniussi D., *Il "diritto all'oblio": i paradossi del caso Google,* in *Rivista Italiana di Diritto Pubblico Comunitario*, 2015, pp. 209 ss., il quale pare ritenere che il gestore del motore di ricerca «*almeno in prima battuta, non sembra acquisire la qualifica di responsabile del trattamento per il solo fatto di catalogare, indicizzare e rendere disponibili ai terzi i dati*»; appare critico, pure, L. Bugiolacchi, *Mancata rimozione della indicizzazione di spazi web a richiesta dell'interessato: la nuova frontiera della r. c. dei motori di ricerca, cit.*, pp. 1535 ss.) - come «*titolare del trattamento*» o «*responsabile del trattamento*» anche il gestore del motore di ricerca.

[32] A simili conclusioni perviene, altresì, L. Ferola, *Dal diritto all'oblio al diritto alla memoria sul web. L'esperienza applicativa italiana,* in *Dir. Informaz.*, 2012, pp. 1001 ss.

[33] Secondo le stime dell'Osservatorio *Internet of Things* della *School of Management* del Politecnico di Milano solo nel 2014 il giro d'affari complessivo in Italia è stato di 1,55 miliardi di euro.

[34] Cfr. G. Giannone Codiglione, S. Sica, *Social network sites e il "labirinto" delle responsabilità,* in *Giur. mer.*, 2012, pp. 2714B ss.

É necessario, dunque, adottare misure che consentano, in modo efficace, agli utenti di scegliere un altro servizio che potrebbe non essere proposto dal produttore del dispositivo. In tal caso, all'utente deve essere riconosciuto il diritto, ormai consacrato nell'art. 20 del Regolamento (UE) 2016/679, «*di trasmettere i dati personali che lo riguardano forniti a un titolare del trattamento a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti*»[35].

4. Obblighi informativi e il problema della legge applicabile al titolare del trattamento

Il costante monitoraggio sulle abitudini dell'utente, l'indicazione della posizione in cui lo stesso si trova in uno qualsiasi dei momenti della sua giornata nonché la diffusione, spesso distorta, della sua immagine potrebbe, dunque, dar vita ad una sorta di *panoptycon* sociale generalizzato in cui ognuno controlla gli altri e tutti sono controllati costantemente.

A fronte di un siffatto rischio - inquietante, eppure non così lontano dal vero - occorre, a questo punto, interrogarsi se, alla luce del d. lgs. 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*", le istanze di tutela in punto di trattamento dei dati personali, che sono state sopra segnalate, possano dirsi sufficientemente protette.

Innanzitutto, si rileva che nella *Opinion 8/2014 on the Recent Developments on the Internet of Things*, citata in precedenza, si fa menzione del c.d. principio di "minimizzazione dei dati": i dati raccolti devono essere

[35] La norma - da leggersi in combinato con il *considerando* 68 del medesimo Regolamento - circoscrive, in particolare, l'esercizio di tale diritto alle sole ipotesi in cui l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto e il «*trattamento sia effettuato con mezzi automatizzati*». Non solo, il paragrafo 2 introduce l'ulteriore condizione della «*fattibilità tecnica*» della trasmissione diretta dei dati personali da un titolare del trattamento all'altro. Ad una prima lettura, sembrerebbe che la versione definitiva della norma risulti meno tuzioristica della precedente formulazione, contenuta nell'art. 18 della Proposta di Regolamento presentata dalla Commissione al Parlamento, ove un simile diritto veniva configurato senza particolari riserve.

strettamente necessari per il fine specifico precedentemente prefissato dal titolare del trattamento[36].

Del pari, nell'art. 3 del *Codice* richiamato tale principio si esplica nel "principio di necessità nel trattamento dei dati" per cui i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da ridurre al minimo l'uso di informazioni relative ai soggetti identificabili, privilegiando l'utilizzo di dati anonimi. Inoltre, in virtù del principio di proporzionalità, i dati personali e le varie modalità del trattamento devono essere pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, co. 1, lett. *d)*, d. lgs. n. 196/2003).

Si accennava, in precedenza, alla necessità che il consenso al trattamento dei dati personali nell'ambito dell'Internet delle Cose sia particolarmente "informato".

Alla stregua del diritto nazionale, prima della raccolta dei dati e dell'attivazione del *device,* dovrebbe essere fornita al fruitore un'informativa chiara e completa, recante tutti gli elementi richiesti dall'art. 13 del d. lgs. n. 196/2003 al fine di consentirgli un'adesione consapevole alle iniziative proposte; occorrerebbe, altresì, acquisire il relativo consenso specifico, informato e distinto nell'ipotesi in cui sia prevista la profilazione (art. 23, d.lgs. n. 196/2003).

Il consenso dovrebbe essere quantomeno documentato per iscritto a cura del titolare del trattamento, ovvero reso necessariamente dall'interessato nel caso di dati sensibili (art. 26, d.lgs. n. 196/2003).

Ai fini dell'applicazione degli obblighi informativi ora evidenziati e degli ulteriori obblighi previsti dal d.lgs. n. 196/2003 (tra gli altri: quelli riguardanti l'esercizio dei diritti degli interessati e il relativo tempestivo riscontro *ex* artt. 7-10, l'adozione delle misure anche minime di sicurezza *ex* artt. 31-35, la notificazione al Garante in caso di eventuale profilazione *ex* artt. 37, co. 1, lett. *d)*, e 163) diviene necessaria l'individuazione del titolare del trattamento[37].

---

[36] Cfr., pure, l'art. 5, par. 1, lett. c), Reg. cit.

[37] V'è da segnalare che il Regolamento (UE) 2016/679 introduce una serie di novità, in primo luogo nominalistiche, quanto ai soggetti deputati al trattamento e alla protezione dei dati personali sui quali conviene brevemente soffermarsi. Innanzi tutto, compare (rispetto a

Ciò, con buona probabilità, non è agevole nell'Internet delle Cose stante la convergenza di molteplici attori: produttori dei dispositivi, piattaforme *social*, applicazioni di terze parti. A questo devono, giocoforza, aggiungersi le difficoltà legate all'applicazione della normativa sul trattamento dei dati personali quando il titolare o il responsabile sia stabilito in un altro Stato membro o in un paese terzo.

Se si ritiene, alla stregua di quanto si ricava da uno dei documenti prima citati[38], che debbano qualificarsi titolari del trattamento proprio i produttori dei dispositivi, avendo questi ultimi sviluppato o modificato il sistema operativo o il *software* della Cosa che rende possibile la raccolta dei dati, ne determina la frequenza e le finalità, non si può, d'altro canto, pretermettere il rischio che proprio l'intervento combinato di una pluralità di soggetti comporti, come è facile immaginare, l'effetto pregiudizievole di un discarico di responsabilità tra i medesimi.

---

quanto accadeva nella precedente direttiva 95/46/CE ma analogamente alla scelta operata dal legislatore nazionale nel vigente Codice della *privacy*) la figura del titolare del trattamento ovvero «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*», mentre il responsabile del trattamento diviene - allineandosi, anche in tal caso, alla definizione contenuta nella legislazione nazionale - «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*». Scompare, invece, dal Regolamento cit. (permanendo, fino al prossimo adeguamento, nella legislazione interna) l'"incaricato del trattamento". Assolutamente innovativa la figura del "responsabile per la protezione dei dati personali" (*Data protection officer*) il quale viene designato dal titolare del trattamento e dal responsabile del trattamento ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni; b) le attività consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali consistono nel trattamento, su larga scala, di categorie particolari di dati personali (art. 9) o di dati relativi a condanne penali e a reati (art. 10). Tra i compiti si possono annoverare quelli di informazione, formazione, consulenza e sorveglianza interne all'organizzazione del titolare/responsabile del trattamento sull'adempimento della disciplina in materia di dati personali, svolgendo, all'uopo, pure una funzione di interlocuzione con l'autorità di controllo.

[38] Cfr. *Opinion 8/2014 on the Recent Developments on the Internet of Things, cit.*, p. 11.

Questo dipende, tra l'altro, da un corretto inquadramento della portata della nozione di stabilimento e, correlativamente, della latitudine del campo di applicazione non solo della normativa domestica, ma soprattutto del recente Regolamento che, in merito, contiene, secondo quanto ora si dirà, interessanti profili di novità.

Com'è noto, la moderna organizzazione dell'attività d'impresa implica – in molti casi e, in special modo, nel settore che occupa – il ricorso ad un'aggregazione di imprese societarie *formalmente* autonome e indipendenti l'una dall'altra, ma assoggettate tutte ad una direzione unitaria esercitata da una capogruppo. Questa organizzazione di gruppo è ben visibile, soprattutto, nel caso dei motori di ricerca (p.e., Google): solitamente, viene riservata alla capogruppo, di norma con sede negli Stati Uniti, la specifica attività di funzionamento del motore di ricerca, demandando, invece, alle controllate (o, comunque, soggette all'attività di direzione e coordinamento), collocate nei singoli Paesi in cui il servizio è offerto o in alcuni di essi ritenuti strategici, l'organizzazione e il funzionamento di importanti servizi collaterali (quali la gestione mail, la raccolta pubblicità, il redirezionamento), nonché delle funzioni essenziali per garantire la personalizzazione dell'attività rispetto alla nazionalità e alle preferenze dell'utente (si pensi alla prestazione del servizio di posizionamento)[39].

Sotto il profilo del trattamento dei dati personali, i problemi che possono venire in considerazione - e che, non a caso, hanno interessato, di recente, la Corte di Giustizia dell'Unione europea - possono concernere, per esempio, come nel già citato caso *Google Spain* e *Google*, la possibilità di estendere l'applicazione della direttiva 95/46/CE anche ad una filiale che svolga attività di comunicazione pubblicitaria in uno Stato membro ma la

[39] In termini analoghi cfr. G. Meruzzi, *Internet service providers, impresa di gruppo e responsabilità delle controllate,* in *Annali italiani del diritto d'autore, della cultura e dello spettacolo,* 2014, pp. 349 ss. al quale si rinvia, altresì, per l'esame del profilo relativo all'estensione alla controllata della responsabilità per gli illeciti commessi dalla controllante.

cui società madre sia stabilita in uno Stato terzo[40]; oppure, come accaduto nel caso *Weltimmo*[41], la determinazione di quale tra due legislazioni di Stati membri sia applicabile in base allo Stato in cui il trattamento è avvenuto.

Pur non potendosi prescindere dagli elementi precipui caratterizzanti le singole fattispecie, è possibile, in ogni caso, enucleare un "nocciolo duro" nella posizione dei giudici lussemburghesi: si tende ad accogliere, infatti, un'interpretazione flessibile della nozione di stabilimento tale per cui per determinare se una società, responsabile del trattamento dei dati, disponga 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, considerando, a tal uopo, la natura specifica delle attività economiche e delle prestazioni di servizi in questione[42]. Occorrerà – al fine di individuare la legge applicabile – stabilire, poi, se il trattamento dei dati personali abbia avuto luogo nel «*contesto delle attività*» dello stabilimento[43].

Non è difficile intravedere nelle conclusioni alle quali è pervenuta la Corte un certo spirito anticipatore delle previsioni contenute nel

[40] Per l'analisi di questo specifico aspetto della sentenza *Google Spain* cfr. G. Caggiano, *L'interpretazione del "contesto delle attività di stabilimento" del responsabile del trattamento dei dati personali*, in *Dir. Informaz.*, 2014, pp. 605 ss.

[41] Si tratta della sentenza 1 ottobre 2015 della Corte di giustizia dell'Unione europea, *Weltimmo s.r.o. contro Nemzeti Adatvédelmi és Információszabadság Hatóság*, causa C-230/14, in *questa Rivista*; cfr. pure, per un commento al profilo che, partitamente, rileva in questa sede, G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. Informaz.*, 2015, pp. 779 ss.

[42] Così il punto 29 della sentenza *Weltimmo* cit.

[43] Si rileva, chiaramente, al punto 52 della sentenza *Google Spain* (replicato al punto 35 della sentenza *Weltimmo*) che «*l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato "dallo" stesso stabilimento interessato, bensì soltanto che venga effettuato "nel contesto delle attività" di quest'ultimo*» (virgolettato nella sentenza). In tal senso cfr. già Gruppo art. 29, Parere n. 8/2010 sul diritto applicabile, adottato il 16 dicembre 2010, 0836-02/10/IT, WP 179, ove si legge (p. 16) che «*la nozione di "contesto di attività" non implica che la legge applicabile sia quella dello Stato membro in cui è stabilito il* responsabile del trattamento, *ma quella del paese in cui uno* stabilimento *del responsabile del trattamento svolge* attività *correlate al trattamento di dati*» (virgolettato e corsivi nel parere).

Regolamento appena emanato. Infatti, dopo aver illustrato in tre *considerando* l'impostazione del nuovo strumento normativo[44], l'art. 3 prevede, per l'appunto, l'applicazione rispetto al trattamento dei dati personali «*effettuato nell'ambito delle attività di uno stabilimento*» indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

Viene, inoltre, estesa la possibilità di veder assoggettati alle medesime norme anche il titolare o il responsabile del trattamento che non è stabilito nell'Unione quando le attività di trattamento riguardano: «*a) l'offerta di beni o la prestazione di servizi agli interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*».

Insomma, una notevole eterogeneità di criteri di collegamento che certifica, si potrebbe dire, la potenziale sovrapposizione di soggetti - e quindi di regole applicabili - come innanzi si rilevava. A tal proposito, è possibile osservare che se, per un verso, con il prossimo allineamento (per il quale è previsto come termine il 25 maggio 2018 che non appare, poi, così vicino

[44] Il riferimento è, in particolare, al *considerando* 22 che recepisce l'orientamento della Corte nella sentenza *Google Spain* secondo cui qualsiasi trattamento effettuato nell'ambito delle «*attività di stabilimento*» deve essere conforme al Regolamento indipendentemente dal luogo ove si svolga il trattamento di dati personali (all'interno dell'Unione o al di fuori). Nel *considerando* 23 viene, invece, affermata l'applicabilità della recente sopravvenienza normativa al «*trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non stabilito nell'Unione quando le attività di trattamento sono legate all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato*». Viene, più nel dettaglio, precisato che l'offerta di beni o servizi e l'intenzione di concludere affari con residenti nell'Unione non sarà ricostruibile sulla base di semplici elementi indiziari (p.e., semplice accessibilità ad un sito Internet), mentre potrebbero assumere rilevanza fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri nel caso in cui venga offerta la «*possibilità di ordinare beni e servizi in tale altra lingua o la menzione di clienti o utenti che si trovano nell'Unione*». Infine, con il *considerando* 24 si estende, in maniera innovativa, l'applicabilità del Regolamento anche all'ipotesi del trattamento dei dati personali riferito al monitoraggio del comportamento degli interessati «*nella misura in cui tale comportamento ha luogo all'interno dell'Unione*».

soprattutto se si considerano le evoluzioni tecnologiche che, nel frattempo, potrebbero realizzarsi) delle normative nazionali con il Regolamento simili problemi potrebbero venir elisi o quantomeno attenuati notevolmente. Per altro verso, ad oggi non paiono inverosimili prospettive (negative) di un'interferenza di normative applicabili a tutto detrimento, evidentemente, dell'utente di un dispositivo dell'IoT[45].

5. La tutela dell'immagine del terzo nell'*Internet of Things*.

Un profilo particolarmente problematico si può cogliere nel possibile diverso atteggiarsi della tutela della riservatezza quando vengano in considerazione le istanze di protezione dei terzi.

S'intende dire, in altri termini, che l'utilizzo di dispositivi, per esempio, dotati di *facial recognition* (*i.e.*, tecniche biometriche che utilizzano strumenti informatici per identificare o verificare l'identità di una persona a partire da una o più immagini che la ritraggono) oltretutto spesso associabili a sistemi di *tagging* automatico, potrebbe provocare il riconoscimento di un individuo (terzo rispetto a colui che utilizza il dispositivo) mentre viene fotografato o ripreso in video e la sua immagine essere successivamente *taggata* e inserita nei *social networks*, a cui magari si aggiungono dati relativi alla sua geolocalizzazione.

[45] Basti pensare ad una fattispecie di questo tipo: il produttore del dispositivo, che, in virtù di quanto detto nel testo, dovrebbe configurarsi quale titolare o responsabile del trattamento dei dati raccolti per il tramite del dispositivo, ha la sede centrale al di fuori dell'Ue; a ciò si aggiunga che il dispositivo medesimo, essendo collegato alla Rete, usufruisce, altresì, del collegamento ad un *social network* e consenta di effettuare ricerche mediante un motore di ricerca che ne indicizzi i risultati. S'immagini che sia il *social network* sia il motore di ricerca abbiano, anch'essi, la propria sede al di fuori dell'Ue. Occorrerà, in una simile ipotesi (ma la realtà dei dispositivi dell'Internet delle Cose potrebbe esserne foriera di altre ben più complesse), verificare se sia applicabile la legge di uno Stato membro in forza di uno stabilimento nel territorio dello Stato stesso purché tale stabilimento svolga attività correlate al trattamento; analogamente, sarà necessario valutare - alla stregua dell'interpretazione fornita dalla Corte di giustizia - se, pure, il *social network* e il motore di ricerca constino di una succursale in uno Stato membro. Evidentemente, una siffatta situazione, seppur alquanto remota, potrebbe rivelare un grave *deficit* di tutela dei dati dell'utente medesimo.

Tali operazioni potrebbero essere effettuate dal dispositivo (si pensi, per esempio, a quelli indossabili) in modo del tutto automatico, cioè senza che il soggetto ripreso e spesso lo stesso fruitore del dispositivo medesimo ne siano consapevoli, se non eventualmente a posteriori, quando l'informazione è già diffusa in rete, quindi non è più controllabile[46].

Al riguardo, sebbene il tema sia suscettibile di ampio approfondimento che la presente sede non consente, si devono considerare due profili che, pur tra loro in continuità, meritano di essere analizzati partitamente.

Infatti, occorre chiarire se nella fattispecie ora descritta venga in considerazione la tutela della riservatezza nell'ampia accezione che nelle pagine che precedono è stata accolta o si tratti soltanto di consentire al terzo inconsapevolmente fotografato o ripreso di tutelare la propria immagine.

L'art. 96 della legge 22 aprile 1941, n. 633 recante disposizioni in materia di "*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*" consente, infatti, la riproduzione e l'eventuale pubblicazione dell'immagine[47], previo consenso della persona interessata.

Ora, se non ricorrono, come probabilmente accade sovente, le "esimenti" di cui all'art. 97 della legge in discorso (notorietà o ufficio pubblico coperto dall'effigiato, pubblicazione dell'immagine per necessità di giustizia o polizia oppure a scopi scientifici, didattici o culturali, riproduzione collegata a fatti, avvenimenti o cerimonie di interesse pubblico o svoltesi in pubblico), occorre che la persona, che pur abbia prestato il consenso alla riproduzione, sia richiesta anche del consenso a che la propria immagine sia pubblicata in un *social network* e in quanto tale potenzialmente idonea a consentire la visione della fotografia ad un pubblico indifferenziato di utenti[48].

---

[46] Un problema analogo, ma con riferimento ai soli dispostivi indossabili, è posto da Germani E., Ferola L., *Il* wearable computing *e gli orizzonti futuri della privacy*, *cit.*, p. 86.

[47] Invero, la norma utilizza l'espressione «ritratto» ma, secondo S. Pagliantini, I. Gonnelli, *sub art. 10 c.c.*, in A. Barba, S. Pagliantini (a cura di), *Commentario del Codice civile - Delle persone*, vol. I, Padova, 2012, pp. 661 ss., spec. p. 663, il legislatore, che utilizza il termine "immagine" nell'art. 10 c.c., considera, in questo settore, i due termini come sinonimi.

[48] A conclusioni analoghe è pervenuto il Trib. Napoli, ord., 31 luglio 2014, *inedita*, che ha ordinato, in un giudizio di separazione, alla moglie di rimuovere le fotografie del marito dal

In termini maggiormente problematici si pone l'altro profilo, cui dianzi si accennava, relativo alla possibilità di configurare l'immagine quale "dato personale". Si tratta di un interrogativo al quale, soprattutto, la giurisprudenza[49] ha fornito, recentemente, risposte di diverso segno.

Secondo un primo orientamento[50], «*l'immagine come tale, pur possedendo capacità identificativa del soggetto, quando viene trattata non*

proprio profilo *Facebook* in quanto tale pubblicazione era avvenuta senza il consenso del coniuge; v'è da segnalare che, all'uopo, l'organo giudicante ha ritenuto «*facilmente aggirabili dai navigatori più esperti*» le misure previste dalla stessa piattaforma e adottate dalla donna per restringerne la visione solo "ad amici".

[49] In dottrina, cfr. S. Ruscica, *I diritti della personalità*, Padova, 2007, p. 556, per l'opinione che considera la definizione di "dato personale" - come contenuta nell'art. 4, co. 1, lett. *b)*, del d. lgs. n. 196/2003 - talmente ampia da riuscire ad includere senz'altro l'immagine. *Amplius* cfr. M. Proto, *Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale*, Milano, 2012, pp. 51 ss. il quale ritiene che «*recando informazioni relative all'individuo rappresentato, anche i segni evocativi dell'immagine personale sono soggetti alle norme*» del Codice in materia di protezione dei dati personali sicché «*tanto "la raccolta" e "la consultazione", quanto la "comunicazione" e la "diffusione" di ritratti e fotografie esigono, da parte del soggetto raffigurato, un consenso qualificato*». In particolare, l'A. da ultimo citato sofferma l'attenzione sulle differenze della disciplina prevista dal d. lgs. n. 196/2003 rispetto a quella disegnata dagli artt. 96 ss. della legge sul diritto d'autore. Effettivamente, se per un verso con la esposizione, la riproduzione e la messa in commercio del ritratto possono trovare attuazione la "comunicazione" e la "diffusione", il "blocco" e la "distruzione" dei dati personali sarebbero, invece, qualificate, al pari di quelle appena citate, quali "operazioni" di "trattamento". Inoltre, fermo quanto si dirà nel testo a proposito dell'art. 5, co. 3, Codice della *privacy*, si può osservare che l'uso dell'immagine senza il preventivo consenso dell'effigiato sarebbe "scriminato" in ipotesi ulteriori rispetto a quelle contemplate dal citato art. 97 l. dir. aut.: basti porre mente al trattamento di dati «*necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato*» (art. 24, co. 1, lett. b, Cod. *privacy*) o al trattamento di dati effettuato da un soggetto pubblico *ex* art. 19, co. 2 e 3, Cod. *privacy*.

[50] Il riferimento è, segnatamente, a Cass., sez. III, sent., 5 giugno 2009, n. 12997 in *Giustizia Civile, Massimario*, 2009, p. 871. Nel caso di specie, una donna, affetta da alcune patologie, si recava presso un mago che le era stato riferito possedere poteri curativi; la stessa, però, veniva ripresa, senza il suo consenso e senza che la sua immagine fosse oscurata, mentre tentava di deambulare da un'emittente televisiva che successivamente trasmetteva la sequenza durante un programma televisivo.

è automaticamente dato personale, ma lo è soltanto se chi esegue il trattamento la correli espressamente ad una persona o fornisca altra informazione atta a consentire di risalire alla persona». A tale conclusione si perviene facendo leva sull'argomento letterale di cui all'art. 4, co. 1, lett. b), del *Codice* citato: la nozione di dato personale sarebbe incentrata sul concetto di informazione la quale sottenderebbe «*un riferimento alla idoneità identificativa diretta della informazione o alla idoneità identificativa indiretta, cioè per il tramite di altra informazione, del dato*».

In altri termini, volendo esemplificare l'itinerario argomentativo seguito dalla Corte di legittimità, l'immagine ben potrebbe costituire un'informazione, cioè una notizia relativa alla persona effigiata. Tuttavia, affinché quest'ultima costituisca un "dato personale", occorrerebbe una didascalia o altra modalità che permettano di identificare la persona[51].

Tale posizione parrebbe, per certi versi, superata da un filone giurisprudenziale[52] più recente che, nel diverso ambito della

[51] Prosegue, con riferimento al caso concreto di cui alla nota precedente, la Corte: «*se viene trasmessa l'immagine di una persona per televisione senza che si dica nei modi indicati chi è, senza cioè che la si identifichi direttamente, l'informazione così offerta, rappresentata dalla stessa immagine, non identifica di per sé quella persona. L'identificazione potrà farsi da parte di chi percepisce l'immagine e conosce la persona, nel senso che è capace di ricollegare l'immagine trasmessa ad essa. Questa identificazione, però, non è nel dominio di chi esegue il trattamento dell'immagine, cioè di chi la trasmette, mentre l'articolo 4, lettera b) esige che essa o sia fatta direttamente dal titolare attraverso una indicazione che raccordi l'informazione ad un soggetto, o sia fatta indirettamente, cioè attraverso altra informazione, sempre fornita dal titolare, che permetta di risalire al soggetto*».

[52] Tale orientamento è stato inaugurato da Cass., sez. I, sent., 9 agosto 2012, n. 14346, in *Guida al diritto*, n. 38, 2012, p. 38; successivamente si veda, pure, Cass., sez. II, sent., 2 settembre 2015, n. 17440, in *Diritto e Giustizia*, 2015, 31, p. 36, con nota di M. Alovisio, *Videosorveglianza, cartelli e informativa privacy in azienda.* In passato, benché in un contesto normativo (legge n. 675/1996) e fattuale (trattasi di pubblicazione su un quotidiano di una fotografia che ritraeva l'effigiato mentre si sottoponeva all'esame etilometrico sotto il controllo della polizia), cfr. Trib. Biella, sent., 29 marzo 2003, in *Dir. Informaz.*, 2003, pp. 538 ss., nella quale si legge che «*è del tutto irrilevante che il quotidiano non abbia riportato altre informazioni relative all'attore (nome, indirizzo, ecc…) in quanto la foto rappresenta un "dato personale" a sé stante mentre le altre informazioni, se sussistenti, avrebbero semmai potuto integrare ulteriori "dati personali" rispetto alla fotografia*».

videosorveglianza, ha avuto occasione di affermare – invero in maniera alquanto apodittica - che «*non può dubitarsi, nonostante in dottrina sia stato sollevato qualche dubbio al riguardo, che anche l'immagine di una persona, in sé considerata, quando in qualche modo venga visualizzata o impressa, possa costituire "dato personale" ai sensi dell'art. 4, lett. b), del d.lgs. n. 196 del 2003*».

Si tratta, come ognuno vede, di una questione la cui portata valica i confini del presente contributo per cui, in questa sede, è possibile limitarsi a sommarie considerazioni. Principiando dalla stessa nozione di "dato personale", questa pare destinata a subire un ampliamento o, comunque, una specificazione per effetto del citato Regolamento appena emanato. Ivi (art. 4, n. 1), infatti, si considera «*identificabile*» la persona fisica che può essere «*identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

Il riferimento ad «*elementi caratteristici*» della «*identità fisica*» sembrerebbe idoneo a ricomprendere proprio la rappresentazione delle sembianze visive della persona, cioè la riproduzione grafica delle sue fattezze, in sostanza l'immagine senza necessità che la medesima rechi con sé ulteriori "contrassegni".

Ciò, del resto, non costituisce un'assoluta novità dacché una dottrina[53] ormai risalente già interpretava l'immagine quale una manifestazione

[53] Cfr. G. Bavetta, voce *Immagine (diritto alla)*, in Enc. dir., vol. XX, Milano, 1970, pp. 144 ss. (spec. par. 3), ma *amplius* cfr. già A. De Cupis, *I diritti della personalità*, vol. IV, t. I, in A. Cicu, F. Messineo (diretto da), *Trattato di diritto civile e commerciale*, Milano, 1959, pp. 256 ss., il quale, nel precisare la dimensione entro cui è tutelata l'immagine, rileva (p. 266) come «*la violazione del diritto all'immagine non si verifica soltanto quando si pone in evidenza, mediante l'aggiunta di indicazioni identificatrici, il nesso tra l'immagine e l'individuo. Certo, allora si* allarga *la conoscenza del determinato individuo, considerato nel suo aspetto fisico, al di là della cerchia di coloro che tale conoscenza già posseggono; mentre, quando quella precisazione non si compie, agli ignari l'immagine riprodotta appare semplicemente come un individuato emblema. Si verifica, comunque, pur in questa seconda ipotesi, se non un* allargamento *della conoscenza, un* rinnovamento *di certo, un*

positiva del diritto alla riservatezza; tale affermazione va, oggi, riletta alla luce del mutato contesto tecnologico nel quale è necessario, come detto, ripensare alla riservatezza ed interpretarla come autodeterminazione informativa specie ove si considerino le peculiarità dell'ipotesi qui esaminata, ovvero i rischi che potrebbero occorrere al terzo nel caso ignori di essere stato immortalato. In tal caso, appare innegabile la continuità tra immagine e riservatezza che divengono così singoli aspetti della persona che, considerata nella sua unitarietà, trova tutela e rilevanza a livello costituzionale[54].

Sulla scorta di queste brevi premesse è possibile ora tornare alla fattispecie prima ipotizzata, constatando che, in tal caso, l'immagine non solo sarebbe oggetto di pubblicazione, ma vi sarebbe l'aggiunta di un *tag*[55], oltre che della geolocalizzazione[56].

---

perfezionamento *di essa*» (corsivi dell'A.). Del resto, F. Ligi, *La tutela dell'immagine nel diritto comparato. I. Stati Uniti d'America,* in *Riv. dir. comm.*, 1954, pp. 67 ss., ricorda come già Warren e Brandeis, nel contributo citato *sub* nota 17, ritenevano la forma più semplice del «*right of privacy*» la tutela, per l'appunto, della propria immagine.

[54] Nel testo si aderisce alla posizione pressoché dominante della giurisprudenza (cfr. Cass., sez. III, sent., 10 maggio 2001, n. 6507, in *Nuova giur. civ. comm.*, 2002, pp. 529 ss., con nota di A. Zaccaria, *La lesione della reputazione personale e il problema dell'onere della prova,* ed ivi si rinvia per ulteriori riferimenti giurisprudenziali) la quale accede ad una concezione "monistica" dei diritti della personalità, ancorando il correlativo fondamento giuridico all'art. 2 Cost. «*inteso quale precetto nella sua più ampia dimensione di clausola generale, "aperta" all'evoluzione dell'ordinamento e suscettibile, per ciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità, in correlazione anche all'obiettivo primario di tutela "del pieno sviluppo della persona umana", di cui al successivo art. 3 cpv.*».

[55] Nel vademecum *Social privacy. Come tutelarsi nella società dei social media,* pubblicato dal Garante *privacy* nel maggio 2014, si specifica che «*sei stato taggato quando qualcuno ha attribuito il tuo nome/cognome a un volto presente in una foto messa on-line; di conseguenza, se qualcuno cerca il tuo nome, appare la foto indicata*».

[56] In argomento, di particolare interesse risulta la recente Cass., sez. II, sent., 26 gennaio 2016, n. 1422, in *Giustizia civile*, *Massimario*, 2016, relativa all'omessa comunicazione da parte del gestore di un impianto sciistico della presenza di etichette RFID (nel caso di specie rivelatrici, per l'appunto, della posizione geografica) e della possibilità di raccogliere dati personali ogniqualvolta lo sciatore si avvicinasse al tornello, munito di tesserino, per ottenerne l'apertura. La Corte, più nel dettaglio, ha escluso che «*la mancata formale*

Orbene, a fronte dell'inequivoca capacità identificativa della etichetta con la quale viene riconosciuta la persona "immortalata", si è portati a concludere che colui che indossa il dispositivo debba necessariamente richiedere il consenso espresso di quest'ultima. In definitiva, quando si tratti dell'immagine/dato personale non è più dato di desumere la prova e la sfera di autorizzazione dal comportamento (cioè dall'atto di disposizione implicito) del titolare del diritto, come può accadere, invece, per il consenso richiesto ai fini della normativa sul diritto d'autore[57].

Certamente, come pure è stato evidenziato[58], la soluzione ora prospettata non sarebbe immune da rilievi critici: basti soltanto pensare ai tempi necessari all'informativa *ex* art. 13 d. lgs. n. 196/2003 che rischierebbe di pregiudicare quell'immediatezza caratteristica del momento in cui avviene la "cattura" del ritratto. Tale obiezione, d'altro canto, considerati i rischi che sono stati poc'anzi evidenziati e, quindi, la necessità che il terzo si autodetermini nella scelta se permanere o allontanarsi dal luogo oggetto di ripresa non appare del tutto persuasiva.

La regola ora enunciata, tuttavia, conoscerebbe un'eccezione. Infatti, ai sensi dell'art. 5, co. 3, d. lgs. n. 196/2003 «*il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione*». Donde è agevole desumere che se l'invio occasionale di un'immagine ad amici o familiari soddisfa esigenze di carattere strettamente personale (per esempio, culturali o di

informativa in materia di dati personali» sia sanzionabile «*quando l'utente fruisce di un meccanismo, azionabile a sua iniziativa, che consente determinate prestazioni programmate, dovendosi escludere, a motivo di tale automatismo e del consenso dell'interessato, una preventiva informazione che è in se stessa*».

[57] Cfr. Cass., sez. I, sent., 16 maggio 2006, n. 11491, in *Giustizia civile, Massimario*, 2006, la quale ha, infatti, statuito che il consenso alla pubblicazione della propria immagine può essere prestato senza necessità di forme particolari e conferito anche implicitamente.

[58] Cfr. le posizioni sostanzialmente conformi, ma riferentisi esclusivamente alla immagine non dotata di *tag* o altro elemento che consenta la riconoscibilità, di B. Tassone, *Diritto all'immagine: fra uso non autorizzato del ritratto e lesione della* privacy, in *Danno e resp.*, 2005, pp. 881 ss., spec. p. 885, e G. Grasselli, *La fotografia tra tutela dell'immagine e* privacy, in *Resp. civ. prev.*, 2007, pp. 977 ss., spec. p. 984.

svago) e la relativa comunicazione resta confinata in una sfera circoscritta di conoscibilità non sarebbe necessario il consenso ai sensi della disciplina sulla riservatezza. A conferma di tale conclusione, è possibile richiamare una decisione del Garante *privacy*[59] nella quale è stata negata la cancellazione dell'etichetta (*tag*) che collegava il proprio profilo *Facebook* ad una foto pubblicata sul profilo di un'altra persona, relativa ad una campagna di sensibilizzazione sull'Aids e omosessualità (dati personali, per giunta, idonei a rivelare "*la vita sessuale*") perché la pagina *web* nella quale era stata "*taggata*" la ricorrente non risultava essere oggetto di diffusione, essendo stata inserita in un profilo "chiuso".

Sul piano dei possibili accorgimenti a tutela della *privacy*, infine, si deve segnalare l'adozione da parte del *social media* citato di un'opzione ("controllo dei tag") che consente di approvare o rifiutare i *tag* che gli utenti aggiungono ai *post* e solo in caso di approvazione il *tag* sarà visibile; la facoltatività nell'attivazione dell'opzione sembrerebbe confermare proprio la congruità della soluzione che è stata accolta perché, tra l'altro, in mancanza di tale accorgimento l'utente rimarrebbe, comunque, sprovvisto di un'adeguata tutela della propria riservatezza.

6. Possibili accorgimenti a tutela della *privacy*: *privacy by design e privacy by default*

Le violazioni della *privacy* in senso orizzontale, tra gli utenti, sembrano palesare uno dei profili maggiormente problematici posti dall'Internet delle Cose e che la disciplina nazionale, ma probabilmente anche quella europea, sulla riservatezza appare scarsamente idonea a tutelare.

Tale incertezza viene indubbiamente alimentata dalla non sempre chiara ripartizione nell'ambito specifico, per esempio, dei *social networks* delle responsabilità in caso di violazione dei diritti dei terzi a causa degli

[59] *Decisione su ricorso, Richiesta di cancellazione online della c.d. etichetta* (*tag*) *in un profilo Facebook,* 18 febbraio 2010, in *www.garanteprivacy.it, doc. web n. 1712776.*

user generated contents[60]. Tralasciando in questa sede tale ultimo profilo solo parzialmente inerente al tema oggetto della presente trattazione, non si può, ai nostri fini, sottacere l'importanza dell'adozione di un approccio *user - experience design*.

In generale, se già nel *web* 2.0 risultava, in molti casi, sempre meno indistinta la posizione di chi crea contenuti e di chi ne usufruisce e, soprattutto, la posizione di chi acquisisce e gestisce i dati e di chi ne è titolare (l'utente, detto altrimenti, viene a rivestire accanto a quello di mero utilizzatore dei dispositivi sovente anche un ruolo attivo), appare indispensabile nel *web* 3.0, per intenderci quello dell'Internet delle Cose, una corretta e sostanziale informazione che renda l'utente, quando utilizza un dispositivo, consapevole non solo dei rischi relativi alla propria riservatezza, ma anche abile nell'uso dello stesso.

Ciò è possibile se si comincia ad occuparsi del modo in cui gli utenti interagiscono con i sistemi informatici, per l'appunto, già nella fase dello sviluppo dei dispositivi.

L'inserimento di strumenti di protezione della *privacy* nel *design* dei prodotti informatici costituisce, difatti, un approccio regolatorio particolarmente utile riuscendo nel conciliare la promozione dell'innovazione tecnologica e dello sviluppo di nuovi beni e servizi informatici con la tutela dei dati e delle informazioni personali che a questa innovazione danno slancio e che da questi prodotti o servizi spesso sono utilizzati[61].

La tutela della *privacy* attraverso il *design* dei sistemi informatici implica, dunque, che chi sviluppa il sistema deve, sin dall'inizio, valutare quali possibili rischi alla riservatezza dei dati e all'autodeterminazione

[60] Per una ricostruzione complessiva del fenomeno si veda S. Scalzini, *I servizi* online social network *tra* privacy, *regole di utilizzo e violazione dei diritti dei terzi*, in *Giur. merito*, 2012, 2569 ss.; in tema una generale rassegna dei recenti orientamenti giurisprudenziali è proposta da E. Falletti (a cura di), *I* social network*: primi orientamenti giurisprudenziali*, in *Corr. giur.*, 2015, pp. 992 ss.

[61] Article 29 Working Party, *The Future of Privacy: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, consultabile al sito *ec.europa.eu*, p. 12.

informativa del soggetto derivino da ciò che si sta realizzando e quali siano i possibili rimedi. Si tratta, in altri termini, di intervenire a protezione della *privacy* dell'utente non più o non solo in una logica *ex post* quando all'utente, sia che l'aggressione provenga in modo verticale, dal produttore, sia in modo orizzontale, da un altro utente, non resta che attivare i tradizionali rimedi (risarcitori), ma è necessario agire quando vi è un maggior numero di soluzioni possibili, cioè proprio nella fase della progettazione.

La necessità di privilegiare da parte dei produttori dei dispositivi dell'Internet delle Cose e, più in generale, degli strumenti informatici un siffatto approccio proattivo rappresenta oramai parte integrante anche della regolamentazione europea appena adottata[62].

L'art. 25 del Regolamento fa, infatti, menzione della «*protezione dei dati fin dalla progettazione*» la quale impone - ma sulla portata precettiva di tale norma sia consentito esprimere qualche perplessità[63] - che «*al momento di determinare i mezzi del trattamento*» il titolare del trattamento medesimo ponga «*in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di*

[62] Per la verità, già nella direttiva 95/46/CE cit. si richiedeva che i responsabili del trattamento di dati prendessero misure idonee a livello tecnico e organizzativo già al tempo del *design* e poi al momento del trattamento allo scopo di impedire trattamenti non autorizzati.

[63] L'inciso («*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*») con cui si apre la norma pare, infatti, rivelare tutta la tensione (già evidenziata) tra i contrapposti interessi in gioco: da un lato, gli oneri finanziari che l'adozione di un simile approccio reca con sé soprattutto in ragione della dotazione patrimoniale, talora esigua, che caratterizza le imprese (sovente *start up*) operanti in questo settore, dall'altro l'ormai nota rilevanza dei *diritti* e delle *libertà* degli interessati. Sulle possibili problematiche applicative della disposizione in esame cfr., seppur con riferimento all'art. 23 della Proposta di Regolamento cit., Koops B.J. e Leenes R., *Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law*, in *International Review of Law, Computers & Technology*, 2014, pp. 159 ss.

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».

Analoghe considerazioni è possibile svolgere per un approccio, parallelo a quello della *privacy by design*, che segnala come, sempre nella fase di progettazione di sistemi informatici funzionale alla tutela della *privacy*, determinate informazioni o determinati principi debbano essere protetti in maniera rafforzata: la *privacy by default settings.* Essa implica l'utilizzo di determinate impostazioni in automatico, con una scelta predisposta da parte di chi costruisce il sistema informatico, salva la possibilità di cambiamento da parte dell'utente dell'opzione prescelta[64].

Infatti, accade, non di rado, che l'utente, ove un'impostazione sia già preselezionata, tenda, a causa di un'inerzia riconducibile a svariati fattori (mancata conoscenza di altre opzioni, preferenza per lo *status quo* esistente, l'essere impostata di *default* legittimerebbe l'opzione agli occhi dell'utente), a restare sugli stessi *default settings*, pur avendo la possibilità di cambiarli.

Occorre, dunque, scongiurare tale rischio attraverso un approccio che tenga conto di *default* di una soluzione favorevole alla parte debole. Non a caso, al paragrafo 2 del citato art. 25 il Regolamento prevede, in omaggio al sopra richiamato principio di minimizzazione dei dati, che, per impostazione predefinita, vengano raccolti «*solo i dati personali necessari per ogni specifica finalità del trattamento*»[65] e che sempre di *default* detti meccanismi debbano garantire che i dati personali «*non siano resi accessibili a un numero indefinito di persone*».

Accanto a tali obblighi, che rappresentano, comunque, un importante approdo nella riflessione in punto di protezione dei dati personali, si potrebbero citare alcuni accorgimenti, nell'esame dei quali, per ovvi motivi, non ci si addentrerà.

---

[64] Sul tema cfr. A. Principato, *Verso nuovi approcci alla tutela della* privacy*:* privacy by design *e* privacy by default settings, in *Contratto e impresa/Europa*, 2015, pp. 197 ss., spec. p. 202.

[65] Un siffatto obbligo - viene, opportunamente, precisato - opera «*per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità*».

Per esempio, le impostazioni predefinite delle applicazioni *social* dei dispositivi dell'Internet delle Cose dovrebbero chiedere agli utenti di rivedere, modificare e decidere le informazioni generate dal loro dispositivo prima della pubblicazione su piattaforme sociali; i produttori dei dispositivi potrebbero, *by default*, consentire di disabilitare le interfacce *wireless* quando non sono impiegate o utilizzare identificatori casuali per evitare che un identificare permanente sia adoperato per il rilevamento della posizione oppure, ancora, i dispositivi dell'Internet delle Cose, segnatamente quelli indossabili e *quantified self*, potrebbero offrire - analogamente a quanto accade per gli *smartphone* - un'opzione di "non raccogliere" per disabilitare rapidamente i sensori di raccolta dei dati. Si tratta, evidentemente, di proposte che si rivolgono agli *stakeholders* e che, attualmente, non sono vincolanti per i medesimi[66].

7. A mo' di (provvisorie) conclusioni: la concorrenza nel mercato dei dispositivi dell'IoT

Riprendendo le considerazioni svolte in sede di premessa, è possibile confermare - grazie al quadro delle tutele che si è cercato sin qui di tracciare - l'impressione che la disciplina sulla riservatezza rincorra un inarrestabile processo tecnologico e che la tutela della medesima rimanga, in molti casi, affidata all'iniziativa dei produttori dei dispositivi. Questi ultimi, d'altro canto, ricavano ingenti benefici economici dal trattamento dei dati cui non è facile rinuncino spontaneamente ove a ciò non corrispondano adeguati vantaggi in termini competitivi.

L'Internet delle Cose e, più in generale, tutti i fenomeni collegati alla (e per mezzo della) Rete (*smart cities*, *smart grid* e così via) paiono, d'altro canto, lanciare una sfida senza precedenti alle stesse imprese operanti nel neonato mercato: la "ricchezza" di queste ultime non è più (o non solo) rappresentata, in senso atecnico, dal valore della produzione, ma dalla messe di dati che dai dispositivi da esse prodotti è possibile estrarre ed elaborare.

[66] Molte delle proposte si trovano, infatti, elaborate nell' *Opinion 8/2014 on the Recent Developments on the Internet of Things*, cit.

In apertura del presente scritto, del resto, si segnalava pure come, nonostante l'apparente e preoccupante "invasione" dei dispositivi finora esaminati, in realtà l'esistenza, *rectius* il destino, di questi ultimi appaia strettamente legato all'utente che tali dispositivi utilizza in quanto sono i dati personali a costituire la linfa delle più recenti tecnologie. Allo stesso tempo, però, non è ben chiaro - né ciò emerge dai documenti elaborati dai soggetti istituzionali che, più da vicino, si sono occupati della tematica - quanto lo stesso fruitore sia consapevole che i suoi dati[67] costituiscano, per dir così, un *thesaurus* per le imprese operanti nel mercato dell'*Internet of Things*.

Da tale consapevolezza discenderebbe, volendo enucleare una possibile conseguenza, che l'utente possa - nel momento in cui acquista un dispositivo e opta per quello che consente, *by design* e *by default*, di tutelarlo più adeguatamente - determinare l'insuccesso, e la conseguente fuoriuscita dal mercato, di quelle imprese che offrano, a livello di trattamento dei dati personali, inferiori garanzie di sicurezza.

Tale affermazione necessita, immediatamente, di essere precisata: il protagonismo dell'utente non comporta, certamente, una rivoluzione copernicana della nozione di concorrenza come elaborata da autorevole dottrina[68]; al contrario, pure nel mercato dei dispositivi dell'IoT, occorrerebbe che i pubblici poteri intervengano promuovendo e tutelando il

[67] Sulla titolarità dei dati da parte dell'interessato v. *supra*, par. 1.

[68] Il riferimento è, com'è noto, a M. Libertini, voce *Concorrenza*, in *Enc. dir.*, Annali III, Milano, 2010, pp. 191 ss. (ma analoghe considerazioni sono svolte in Id., *Diritto della concorrenza dell'Unione europea*, Milano, 2014, pp. 2 ss.), il quale elabora una nozione di concorrenza - in passato ritenuta autoevidente - c.d. dei moderni. Secondo l'A., mentre nella concezione originaria "tutela della concorrenza" e "tutela della libertà (individuale) di iniziativa economica" coincidevano e la concorrenza, come bene meritevole di tutela giuridica, veniva concepita come una condizione di naturale equilibrio dei mercati; nell'ultimo mezzo secolo, sulla scorta dell'elaborazione dell'ordoliberalismo tedesco, si affermano almeno tre mutamenti paradigmatici: «*la concorrenza non è più vista come un ordine "naturale", bensì come un ordine "costruito" dal potere pubblico in base a propri giudizi di valore*»; «*la concorrenza da tutelare non è vista come uno stato di equilibrio ideale (come tale, in effetti, irraggiungibile, e perfino non auspicabile, perché corrisponderebbe ad una situazione di economia perfettamente statica), bensì come un processo dinamico*»; «*la concorrenza da tutelare non è più vista come un libero gioco di scelte e volontà individuali, bensì una libera competizione fra imprese*».

processo dinamico del "gioco della concorrenza" tra le imprese. Volendo essere maggiormente perspicui, la tutela della concorrenza, benché orientata al benessere collettivo[69], si riferisce, tuttavia, alla competizione fra imprese.

Pur nella consapevolezza di una più compiuta valorizzazione del ruolo attivo dell'utente[70], anche nel settore che occupa permane, dunque, la primaria funzione - soprattutto nella fase applicativa della recente sopravvenienza normativa - delle Autorità di regolazione. L'obiettivo pro concorrenziale si raggiunge, in particolare, non solo consentendo, come più volte ribadito, al fruitore di accedere, quantomeno, a tutte le informazioni utili e necessarie per effettuare l'acquisto di un dispositivo o avvalersi di un servizio, ma anche aprendo il mercato all'ingresso di nuovi *players*.

Sul punto, un possibile terreno di intervento regolatorio potrebbe riguardare, ad esempio, l'offerta di connettività su rete mobile per i già richiamati servizi *Machine to Machine* e l'accesso al mercato di fornitori di tali servizi di connettività atteso che questo mercato sembra «*allo stato*,

[69] Infatti, il consolidarsi del confronto competitivo tra le imprese dovrebbe essere funzionale alla realizzazione di obiettivi, *lato sensu*, solidaristici; ciò è imposto non solo dalle norme presenti già all'interno della nostra Costituzione (si pensi all'art. 2 e all'*utilità sociale* e ai *fini sociali* di cui, rispettivamente, al co. 2 e 3 dell'art. 41 Cost.), ma, più in generale, dall'affermarsi del modello, recepito dall'art. 2, paragrafo 2, TUE, di un'*economia sociale di mercato altamente competitiva*.

In argomento, cfr. M. Libertini, *A "highly competitive social market economy" as a founding element of the european economic constitution,* in *Concorrenza e mercato*, 2011, pp. 491 ss.; Id., *Diritto della concorrenza dell'Unione europea*, cit., p. 51 e P. De Pasquale, *L'economia sociale di mercato nell'Unione europea,* in *Studi sull'integrazione europea*, 2014, pp. 265 ss. In termini più generali, si veda il recente contributo di A. Toffoletto, *Note minime a margine di Laudato si',* in *Le Società*, 2015, pp. 1203 ss.

[70] A livello generale, occorre, in ogni caso, dare atto di una tendenza alla frantumazione della unità della qualificazione di consumatore di talché quest'ultima non pare essere più adeguatamente ricompresa nella tradizionale definizione di cui all'art. 3, co. 1, lett. a), Cod. cons.: basti pensare all'emersione nella *Sharing Economy* della figura del *prosumer* rispetto alla quale pare difficile individuare un *discrimen* tra produttore e consumatore. Su tale problematica cfr. M. Rabitti, *Smart cities e tutela dei consumatori*, in G. Olivieri e V. Falce (a cura di), *Smart cities e diritto dell'innovazione*, cit., pp. 321 ss. e M. Maugeri, *Elementi di criticità nell'equiparazione, da parte dell'AEEGSI, dei «prosumer» ai «consumatori» e ai «clienti finali»*, in *Nuova giur. civ. comm.*, 2015, pp. 406 ss.

sviluppato da pochi grandi operatori che, aggregando le diverse infrastrutture nazionali attraverso gli accordi di roaming (talvolta specializzati per il M2M), offrono servizi di connettività globale. Si manifestano, pertanto, rischi di market preemption, technology lock-in, nonché di restrizioni della concorrenza attraverso l'applicazione di sconti esclusivi e/o la commercializzazione di prodotti/servizi specializzati tra gli operatori aderenti all'alleanza. Tale circostanza pone diverse difficoltà di entrata nel mercato per gli operatori nazionali (più piccoli nella competizione globale)»[71].

L'opera del regolatore potrebbe, in definitiva, venire agevolata dalla natura degli interessi coinvolti i quali, a ben guardare, non paiono, poi, così distanti tra loro.

La concorrenza tra gli operatori del mercato dei dispositivi dell'*Internet of Things* potrebbe, infatti, facilmente esplicarsi anche sul piano della capacità di innovare, offrendo così dispositivi più efficienti con l'acquisizione di un minor numero di informazioni o predisponendo sistemi di tutela più efficaci o comprensibili agli utenti[72]. A questi ultimi, investiti di un nuovo protagonismo, resterebbe, invece, affidato il compito non solo e non tanto di utilizzare (informandosi) consapevolmente simili dispositivi ma, soprattutto, divenire parte attiva nella selezione dei produttori che si riveleranno più sensibili a siffatte istanze.

[71] Cfr. Agcom, *Indagine conoscitiva concernente i servizi di comunicazione Machine to machine (M2M)*, *cit.*, p. 64.

[72] Ciò potrebbe essere corredato dall'adozione di strumenti di certificazione anche, eventualmente, a livello sovranazionale ovvero meccanismi di mutuo riconoscimento: così GPDP, *Avvio della consultazione pubblica su Internet delle Cose*, cit.