

Anna Papa

La complessa individuazione di un “equo” bilanciamento tra tutela della privacy e profilazione nella *big data society*

SOMMARIO: 1. Introduzione: circolazione dei dati, dignità della persona e diritto alla “autodeterminazione informativa”. – 2. Il profilo “passivo” del diritto all’autodeterminazione informativa. – 3. Il profilo “attivo” dell’autodeterminazione informativa. – 4. Tutela della autodeterminazione informativa e profilazione degli utenti. – 5. Quali prospettive della garanzia di autodeterminazione informativa degli utenti del web.

1. Introduzione: circolazione dei dati, dignità della persona e diritto alla “autodeterminazione informativa”

L’affermarsi delle tecnologie digitali ha, come è noto, intensificato in modo esponenziale la produzione di dati e informazioni. È stato calcolato, infatti, che nel decennio appena trascorso ne è generato un numero dieci volte superiore a quello dei precedenti 5000 anni¹ e, aspetto particolarmente interessante, la stragrande maggioranza di essi è stata prodotta dall’interazione tra gli utenti del *web*, dando la misura di quanto sia incessante la creazione e lo scambio dei dati e delle informazioni nella *Internet society* e di come, accanto ad una realtà fisica, si sia ormai formata una realtà digitale, in costante evoluzione e diversificazione.

I dati stessi presentano peraltro una origine composita. Una parte, infatti, sono generati in vario modo e destinati ad alimentare una banca dati o a diventare *big data*, locuzione ormai nota e anch’essa in continua evoluzione. Un’altra parte della realtà digitale costituisce, invece, il risultato dei da-

¹ Come viene sottolineato, mentre dai primi graffiti ad oggi l’umanità ha prodotto un numero di dati pari a 4,4 ZB (potenza 7 di mille), in pochi anni, dal 2013 al 2020, se ne produrranno complessivamente 44 ZB.

ti condivisi in Rete dagli utenti e destinati quindi ad alimentare lo spazio informativo di *Internet*, definito nel decennio scorso una immensa biblioteca. In comune, invece, tutti i dati hanno la caratteristica di essere unità elementari che presentano non solo un valore informativo bensì si pongono come fattore cruciale di produzione di ricchezza e ciò ne rende inevitabile un loro utilizzo ed uno scambio sempre più dinamico e finalizzato.

Il ruolo centrale degli utenti nelle dinamiche della Rete è ormai da tempo analizzato dagli studiosi del diritto, per la parte che qui rileva, costituzionale, essendo ormai condivisa l'attenzione e l'esigenza di ricondurre tali processi nell'alveo dei principi costituzionali ed in particolare del rispetto di quanto previsto in materia di diritto di informazione e comunicazione e di dignità della persona. Come è noto, infatti, le costituzioni democratiche contemporanee pongono la persona al centro della propria costruzione, alla quale riconoscono un catalogo ampio e dinamico di diritti. In particolare, per la parte che qui rileva, il riconoscimento del principio della dignità umana (art. 3, comma 1 ma anche art. 41, comma 2) comporta l'individuazione di nuove situazioni giuridiche soggettive, non espressamente previste dalla Costituzione italiana, ma definite in ambito giurisprudenziale o nelle Carte internazionali e sovranazionali che compongono la base condivisa dei diritti nello spazio europeo. In questo ambito rientrano, per quanto qui rileva, anche la tutela della privacy e della riservatezza dei dati che, insieme al diritto ad essere informati, ricavabile dall'art. 21 Cost., costituiscono la dimensione positiva e negativa di quello che può essere definito il "diritto alla autodeterminazione informativa"².

²Come è noto, il tema del diritto alla autodeterminazione si presenta alquanto complesso e per molti aspetti "divisivo", sia in dottrina che in giurisprudenza, atteso l'indubbio legame che, in qualsiasi regime politico, unisce l'individuo alla società nel quale egli realizza la propria personalità. In questa sede, essendo necessario delimitare il tema, il riferimento è esclusivamente al concetto di autodeterminazione che la Corte costituzionale ha elaborato proprio in materia di privacy, nello specifico con riferimento al consenso informato laddove ha affermato che "la circostanza che il consenso informato trova il suo fondamento negli artt. 2, 13 e 32 della Costituzione pone in risalto la sua funzione di sintesi di due diritti fondamentali della persona: quello all'autodeterminazione e quello alla salute, in quanto, se è vero che ogni individuo ha il diritto di essere curato, egli ha, altresì, il diritto di ricevere le opportune informazioni in ordine alla natura e ai possibili sviluppi del percorso terapeutico cui può essere sottoposto, nonché delle eventuali terapie alternative; informazioni che devono essere le più esaurienti possibili, proprio al fine di garantire la libera e consapevole scelta da parte del paziente e, quindi, la sua stessa libertà personale, conformemente all'art. 32, secondo comma, della Costituzione". Cfr. Corte costituzionale, sent. n. 438/2008. Con la sent. n. 253/2009 la Corte ha poi ribadito il proprio orientamento. Per una ricostruzione delle problematiche che attengono al tema dell'autodeterminazione in senso ampio, cfr., tra gli altri, L. ANTONINI, *L'autodeterminazione nel sistema dei diritti costituzionali*, in AA.VV., *Autodeterminazione. Un diritto di spessore costituzionale?*, Torino, 2012.

2. Il profilo “passivo” del diritto all’autodeterminazione informativa

Tra i diritti che rilevano nella *digital economy* un ruolo centrale è rivestito, come è noto, dalla tutela della privacy e della riservatezza dei dati personali³. Benché distinte, queste due situazioni giuridiche soggettive sono fortemente correlate; anzi può dirsi che la tutela della riservatezza dei dati rappresenti un aspetto del più generale diritto alla privacy⁴, inteso come

³Come è noto, la prima ricostruzione dottrinale della nozione di *privacy* si deve all’intuizione di due giuristi americani, Louis Brandeis e Samuel Warren, che nel 1890 definiscono la *privacy* come “*right to be let alone*”, traducibile come “diritto ad essere lasciati in pace”, individuando l’intimità della vita domestica dell’individuo quale bene giuridico necessitante di tutela ordinamentale. In tale accezione il termine *privacy* coincide in sostanza con la pretesa di ciascun soggetto a vedere impedita l’altrui curiosità, vietando le indiscrezioni e le pubblicità non volute, nonché la conoscenza e la divulgazione di vicende personali non autorizzate. Questa impostazione resta sostanzialmente immutata sino all’affermarsi di un nuovo modello di società che, sulla spinta di un forte cambiamento dovuto alle innovazioni tecnologiche, assiste a un incremento e ad una diffusione esponenziale dei mezzi di informazione e di comunicazione. Ciò impone una rimeditazione della tradizionale definizione di *privacy*, costringendo a un ampliamento delle ipotesi in cui essa è garantita attraverso la previsione di margini di protezione sempre più estesi, trasformandola da mero *ius excludendi alios* ad un vero e proprio diritto di controllo dei propri dati personali. Non si ritiene più, in sostanza, che il diritto al riserbo sia circoscritto al solo potere di vietare qualsiasi circolazione di informazioni sul proprio conto, ma lo si estende anche al potere di vigilare su queste, avendo la possibilità, all’occorrenza, di verificare, rettificare e cancellarne i contenuti. Ne deriva che, all’interno degli ordinamenti di *common law* in cui per prima si sviluppa, la *privacy* si trasforma così rapidamente in un diritto complesso, da comprendere contenuti estremamente eterogenei: da un lato, il potere di regolare l’accesso alla propria sfera di intimità, consentendo o meno l’intromissione da parte di terzi in tale spazio personalissimo; dall’altro, il controllo sulle informazioni che riguardano la propria persona in tutte le sue espressioni e manifestazioni, siano esse fisiche, ideologiche, affettive, morali o patrimoniali. La nozione di *privacy* che si afferma descrive, quindi, una posizione multiforme e sfaccettata, una varietà di situazioni accomunate dal riconoscimento, in capo alla persona, del diritto di autodeterminarsi nella propria sfera personale, senza subire intromissioni dall’esterno, ma anche esercitando un controllo sulle informazioni che la riguardano. Per un *excursus* su questi aspetti si consenta il rinvio a A. PAPA, *Il diritto dell’informazione e della comunicazione nell’era digitale*, Torino, 2018.

⁴La nozione di riservatezza nell’esperienza italiana si è sviluppata a seconda delle precipe esigenze che di volta in volta richiedevano soddisfacimento e ha comportato una scomposizione della tradizionale nozione di *privacy* in diversi frammenti: il diritto alla riservatezza, il diritto alla protezione dei dati personali, il diritto all’identità personale, il diritto all’anonimato e il diritto all’oblio. Emblematico, al riguardo, si presenta l’art. 2, d.lgs. 30 giugno 2003, n. 196 (cosiddetto “Codice della Privacy”), nella sua formulazione originaria il quale si poneva come garanzia “che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato”, distinguendo tuttavia poi tra “riservatezza”, “identità personale” e “diritto alla protezione dei dati personali”. In questa prospettiva protezionistica della dimensione personale dell’individuo, impermeabile all’altrui curiosità e all’altrui

diritto di ciascun individuo ad autodeterminare la propria proiezione sociale, filtrando l'esteriorizzazione delle informazioni che lo riguardano.

Entrambe queste situazioni giuridiche soggettive non sono espressamente previste e tutelate dalla Costituzione italiana. Per quanto riguarda la tutela dei dati ciò è inevitabilmente conseguenza del periodo storico in cui la Carta fu scritta, ancora lontano dall'avvento della digitalizzazione. Per quanto riguarda, invece, la tutela della privacy, la mancata previsione può presumibilmente ascrivarsi a motivazioni diverse, come ad esempio il non manifestato interesse sociale per la sua tutela o la volontà dei Costituenti di non dare rilievo costituzionale a diritti, allora di incerta definizione, suscettibili di porsi come limiti costituzionali alla libertà di manifestazione del pensiero, definita pochi anni dopo la "pietra angolare dell'ordine democratico"⁵.

L'assenza di un esplicito riconoscimento costituzionale non ha tuttavia impedito che nel tempo a queste due situazioni giuridiche soggettive venisse riconosciuto valore costituzionale ed oggi è sostanzialmente incontroversa l'individuazione della loro fonte negli artt. 2-3, comma 1, Cost. Ciò è tuttavia avvenuto seguendo un percorso distinto, di natura giurisprudenziale per quanto riguarda la privacy⁶ e di normazione europea,

interesse a conoscere, può dirsi che la prima rielaborazione italiana della nozione di *riservatezza* abbia coinciso sostanzialmente con la tradizionale espressione del *right to be let alone*, aiutando il soggetto a preservare uno spazio di tranquillità inattaccabile da parte di chiunque, in soddisfacimento di quel bisogno di isolamento spirituale che comprende la facoltà di non comunicare ad altri gli accadimenti che attengono alla propria persona. Invero, la funzione principale accordata a tale diritto è, più propriamente, quella di salvaguardare l'interesse del soggetto a che i fatti della sua esistenza non siano *arbitrariamente* esposti all'attenzione della collettività, ipotizzando il riconoscimento di una posizione giuridica generale, da riconoscersi in capo a ciascun individuo e tutelabile dall'ordinamento, che si sostanzia in un potere di impedimento all'intromissione non autorizzata nella propria sfera intima da parte di qualsivoglia soggetto. L'elaborazione del diritto alla riservatezza nasce, quindi, dalla necessità di dotare il cittadino di uno strumento di reazione a fronte dell'invasione di terzi nello spazio privato dell'individuo, così da garantire a chiunque una dimensione assolutamente personale e sottratta ad ingerenze esterne. In tale accezione, come è evidente, il diritto al riserbo viene a collocarsi in posizione sostanzialmente antinomica rispetto al diritto di cronaca e, più in generale, alla libertà di manifestazione del pensiero garantita dall'art. 21 Cost., andando a limitarlo nella sua assolutezza e nelle sue molteplici modalità di espressione.

⁵ Il riferimento è alla nota sentenza della Corte cost. n. 84/1969. Su questi aspetti si consente il rinvio a A. PAPA, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, 2009.

⁶ La mancanza di un'esatta trasposizione in termini giuridici nell'ordinamento nazionale del concetto di privacy spiega la ragione per cui approcciarsi a questo tema abbia rappresentato per il legislatore, e per il giurista italiano, un'operazione tutt'altro che agevole. Sebbene, infatti, tale termine sia stato assorbito nel linguaggio comune oramai da tempo e nonostante sia intuitivamente chiaro il concetto che con questa espressione si intende evocare, essa tende a sollevare nell'interprete una serie di dubbi e difficoltà ermeneutiche nel momento in cui tale parola viene

con riferimento alla tutela della riservatezza dei dati.

Non è possibile in questa sede soffermarsi sul cammino giurisprudenziale che ha portato al riconoscimento del diritto costituzionale alla *privacy*⁷. Ap-

calata all'interno del sistema, per essere letta nella sua dimensione prettamente giuridica. Diverse le ragioni di tali problematicità. Innanzitutto, il *right to privacy* è un concetto che viene elaborato al di fuori dell'ordinamento italiano, affondando le sue radici nel contesto storico americano di fine ottocento e maturando sotto la pressione delle istanze di una collettività che si sentiva lesa dalle sempre più invadenti intromissioni nella propria sfera privata, prima da parte della stampa, poi dagli altri *mass media*, infine dai nuovi strumenti di comunicazione. In aggiunta al differente contesto socio-culturale di riferimento, assai distante dal suo omologo contemporaneo italiano, un ulteriore dato da prendere in considerazione è che tale diritto nasce e si sviluppa in un sistema giuridicamente assai diverso, qual è quello di *common law*. Il fatto, dunque, che la nozione di *privacy* abbia tardato ad essere assorbita dalla cultura giuridica italiana – e che, allo stato, non conosca in verità ancora un perfetto equipollente – non deve perciò stupire, ma è la naturale conseguenza della resistenza del sistema al tentativo di importare concetti afferenti a una tradizione giuridica differente. Resistenza che, per di più, si scontra con la liquida mutevolezza della nozione stessa di tale termine, il quale, col passare del tempo, ha mostrato ed è destinato a mostrare significati sempre nuovi, in parallelo con gli sviluppi della società e, soprattutto, delle continue acquisizioni della tecnologia, fonte di interessi sempre diversi che abbisognano costantemente di nuovi profili di tutela. Questa lentezza di adattamento ordinamentale risulta, peraltro, acuita dal fatto che l'innesto dell'istituto opera su un terreno giuridico strutturalmente assai più rigido, il quale, molto ossequioso della lettera della legge, non conosce quella dinamicità che caratterizza il meccanismo del precedente giurisprudenziale, affidando invece la tutela giurisdizionale di qualsiasi posizione alla necessaria individuazione di un suo fondamento normativo. Appare allora evidente che la ragione principe di tutte le difficoltà incontrate dal giurista italiano nell'approcciare alla tematica della tutela della *privacy* risiede essenzialmente nel fatto che il riconoscimento legislativo di tale situazione giuridica, quand'anche già avvertita sul piano sociale, ha tardato a farsi spazio nel mondo del diritto ed è stata quasi interamente demandata all'elaborazione di una coraggiosa giurisprudenza, senza mai poter godere di un'espressa e generale copertura normativa, né di una compiuta disciplina legislativa, se non in tempi recenti e limitatamente a determinati aspetti. D'altro canto, proprio alla luce di questo silenzio a lungo serbato dal legislatore, è possibile comprendere come mai dottrina e giurisprudenza maggioritarie si siano sempre dimostrate assai prudenti nel richiamarsi all'istituto della *privacy*, concetto a noi sostanzialmente alieno e spesso inafferrabile in ragione della sua perenne evoluzione, preferendo piuttosto frammentarlo e rimodularlo a seconda delle opportune esigenze, adattandolo di volta in volta all'esperienza giuridica nostrana attraverso l'impiego di termini dal contenuto parzialmente coincidente.

⁷ Il riconoscimento di valore costituzionale alla tutela della *privacy* è, come è noto, il frutto di una lunga evoluzione giurisprudenziale che ha visto protagonista soprattutto la Corte di cassazione. Già in una sentenza del 1963 (sent. n. 990/1963) la Suprema Corte aveva ritenuto meritevole di tutela il "diritto al riserbo" qualora fosse ravvisabile una violazione della libertà di autodeterminazione del singolo, realizzabile qualora "si divulgano notizie della vita privata, le quali, per tale loro natura, debbono ritenersi riservate, a meno che non sussista un consenso, anche implicito, della persona, desunto dall'attività in concreto svolta o, data la natura dell'attività medesima e del fatto divulgato, non sussista un prevalente interesse pubblico di conoscenza che va considerato con riguardo ai doveri di solidarietà politica, economica e sociale inerente alla posizione del soggetto". Solo nel 1975, però, come è noto, con la celebre pronuncia n. 2129 del 27 maggio 1975, si registra un'esplicita ammissione dell'esistenza di tale posizione da parte della Suprema Corte che definì in quella sede il diritto alla riservatezza come la "tutela di quelle situa-

pare invece importante soffermarsi sull'evoluzione del diritto alla riservatezza dei dati personali.

Con l'introduzione, lo sviluppo e la diffusione su larga scala delle nuove tecnologie (telefonia, *personal computers*, *internet*), è apparso evidente che per l'individuo si ponga come primaria l'esigenza non solo di vietare a chiunque l'accesso alla propria sfera privata o di impedire la diffusione di determinate informazioni, ma anche quello di mantenere un potere di controllo sull'ingente quantità di dati che lo riguardano e che vengono quotidianamente acquisite e gestite da altri, anche in ragione delle infinite modalità di applicazione della tecnologia nei diversi settori della vita quotidiana (*e-commerce*, motori di ricerca, *social networks*, *social media*, *smartphones*, *wearable computing*) e la conseguente produzione di un numero rilevante di informazioni personali, che vengono solitamente raccolte in "banche dati" al fine di essere elaborate, spesso in via automatizzata, tramite sofisticati strumenti elettronici, per poi essere ulteriormente cedute o vendute a terzi.

Si realizza quindi l'esigenza di un cambio di prospettiva, di passaggio "dal segreto al controllo", dal riserbo al *data protection*, da una concezione

zioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano tuttavia giustificate da interessi pubblici preminenti". Traslato nel sistema nazionale, dunque, il diritto alla riservatezza non coincide con la nozione estesa di *privacy* accolta dall'elaborazione statunitense; secondo la Corte, quest'ultima condurrebbe a un ambito di tutela troppo vasto e indeterminato della sfera della persona, né si presta a una lettura eccessivamente restrittiva, quale mera protezione dell'intimità domestica, valore già garantito dall'art. 14 Cost. e che rischierebbe di conferire una portata troppo limitata alla nozione di riserbo. La Suprema Corte ha optato, invece, per una soluzione mediana, facendo riferimento a una peculiare porzione di sfera della vita individuale e familiare, attinente a tutte quelle vicende "il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza)". La successiva giurisprudenza non ha mai mutato indirizzo, confermando a più riprese l'esistenza di un vero e proprio diritto alla riservatezza anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria. Una volta però accolta la possibilità di configurare un diritto alla riservatezza e verificata l'assenza di una disposizione idonea a consentirne la tutela nella normativa primaria, si è reso necessario individuarne il fondamento giuridico direttamente nella Costituzione e precisamente nell'art. 2 che, nella sua più ampia dimensione di clausola generale, consente infatti di colmare vuoti di tutela tramite un'interpretazione evolutiva e teleologica della Carta, in modo da adeguare il sistema ordinamentale a valori non esistenti al momento dell'approvazione, ma che via via necessitano di protezione. Esso rappresenta, quindi, un ottimo strumento di recezione costante e graduale di diritti e interessi emergenti nella società, in grado di conferire garanzia d'invulnerabilità a quelle libertà espresse dalla coscienza sociale nella sua progressiva evoluzione storica. Tale disposizione appare, dunque, il fondamento normativo più convincente per il diritto alla riservatezza, essendo peraltro idoneo ad apprestare copertura costituzionale ai nuovi valori emergenti della personalità alla luce dell'obiettivo primario di tutela "del pieno sviluppo della persona umana" sancito dall'art. 3 Cost.

individualistica di tutela dell'individuo ad una dimensione sociale, ove la diffusione di dati privati nello spazio fisico e virtuale deve avvenire sempre con il consenso e sotto il controllo del titolare di dette informazioni. Da qui la configurazione del "diritto alla protezione dei dati personali", il cui riconoscimento si è sviluppato essenzialmente per via normativa. Seppure in modo implicito, un primo riferimento si rinviene nell'art. 8 CEDU che, pur nominalmente posto a tutela del solo interesse al rispetto della vita privata e familiare, ha visto man mano implementare il suo contenuto grazie ad un'attualizzante giurisprudenza della Corte europea dei diritti dell'uomo, che ha attratto nell'ambito di applicazione di questa disposizione, oltre al diritto al riserbo, anche quello relativo al *data protection*, con conseguente potere del soggetto di controllare la circolazione delle informazioni che lo riguardano. Una esplicita disciplina si rinviene, invece, nella Convenzione di Strasburgo del 1981⁸, atto idealmente finalizzato a dettare a livello europeo alcuni principi generali in materia di *riservatezza*, nell'ottica di un'armonizzazione delle legislazioni degli Stati contraenti e allo scopo di fornire strumenti comuni per proteggere efficacemente i diritti inviolabili minacciati dalla invasività delle nuove tecnologie.

Sulla scia di quanto previsto dai due atti appena citati anche l'Unione europea, a partire dagli anni '90, ha adottato una serie di provvedimenti che giustificano oggi la qualificazione del diritto alla riservatezza dei dati come di un diritto di matrice sostanzialmente euro-unitaria. Tra le fonti vanno, infatti, ricordate le direttive 95/46/CE del Parlamento europeo e del Consiglio, (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), 97/66/CE (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni) e 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche), che sanciscono appunto definitivamente l'esistenza di un "diritto alla protezione dei dati di carattere personale" distinto e autonomo dal "diritto alla riservatezza". Questa distinzione è stata inoltre cristallizzata nella Carta dei diritti fondamentali dell'Unione europea del 2000 che reca nel Capo secondo, dedicato ai diritti di libertà, l'esplicito riconoscimento del diritto alla protezione dei dati di carattere personale (art. 8, comma 1), distinguendolo sia dal diritto di ogni individuo al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (sancito all'art. 7), sia dal chiarimento posto dall'art. 11, a mente del quale la libertà di espressione e d'informazione include la libertà

⁸ Convenzione n. 108 del 28 gennaio 1981, ratificata con legge 21 febbraio 1989, n. 98.

di opinione e la libertà di ricevere e di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera⁹.

Nell'ordinamento italiano il diritto alla protezione dei dati personali ha fatto definitivamente il suo ingresso, proprio sulla spinta di questi atti sovranazionali, attraverso l'adozione nel 1996 di una prima organica regolamentazione legislativa¹⁰, poi assorbita e implementata dal "Codice in materia di protezione dei dati personali" del 2003¹¹. Tale disciplina è andata ad integrarsi con la tutela giurisprudenziale del più generale diritto al riserbo e ne ha quindi assorbito, ferma restando la sua origine euro-unitaria, il fondamento costituzionale di cui all'art. 2 Cost., con relativi precipitati in punto di rango del diritto, caratteristiche, limiti e tecniche rimediali. Tale conclusione si impone non solo sulla base di una lettura evolutiva delle disposizioni costituzionali e di un'interpretazione adeguatrice delle stesse alla luce della disciplina internazionale e sovranazionale prima richiamata (artt. 7 CDFUE e 8 CEDU), ma anche, più in generale, in virtù di una pacifica visione antropocentrica del diritto, non esistendo plurimi diritti della personalità, ma diversi aspetti di un unico diritto della persona, dal contenuto indefinito e vario, cui l'ordinamento deve sempre assicurare una tutela piena ed effettiva.

Il Codice per la protezione dei dati personali e l'Autorità garante, che ne ha dato esemplificazione e attuazione, hanno svolto un ruolo fondamentale nell'affermazione di questo diritto non solo nel sistema normativo ma anche nella società italiana, che ha fatto propria la *ratio* della tutela, acquisendo dimestichezza con le nozioni di dato personale, con le sue specificazioni¹², di trattamento, di consenso.

⁹Proclamata dal Parlamento, dal Consiglio e dalla Commissione europea a Nizza il 7 dicembre 2000, la Carta, a seguito di modifiche e adattamenti, è stata sottoposta ad una nuova proclamazione il 12 dicembre 2007 a Strasburgo. Ai sensi dell'art. 6, par. 1, comma 1, del trattato sull'Unione europea, la Carta proclamata nel 2007 ha lo stesso valore giuridico dei trattati.

¹⁰Legge 31 dicembre 1996, n. 675 (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*).

¹¹D.lgs. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*).

¹²I dati personali erano divisi nella formulazione originaria del Codice in diverse categorie. I "dati sensibili" (art. 4, comma 1, lett. d) qualificavano quei dati idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, dell'interessato, cioè della persona fisica cui tali informazioni si riferiscono. Tra i dati sensibili assumevano peculiare rilievo quelli riguardanti lo stato di salute e la vita sessuale dell'individuo, ossia i cosiddetti "dati supersensibili", che, diversamente dalle altre tipologie, non ammettevano mai un trattamento in assenza del consenso del titolare. Esistevano poi i "dati giu-

Pur essendo comune e non controversa la comune matrice europea di questo diritto, ogni Stato dell'Unione ha comunque, nello scorso decennio, dato attuazione alle direttive in materia in modo fortemente condizionato dal nazionale contesto sociale di riferimento. Ne è risultato un quadro alquanto diversificato a fronte invece di un fenomeno sempre più globale. Per questo, il legislatore europeo nel 2012 – dinanzi alla complessità del contesto, in cui la spinta all'innovazione si intreccia inevitabilmente con la necessità di tutelare la sfera di identità dei singoli individui, la crescita democratica delle società digitali – ha intrapreso un lungo cammino finalizzato all'individuazione di nuove regole comuni a tutti gli Stati membri in materia di tutela dei dati personali¹³.

Alla base di tale decisione vi è stata, come appena ricordato, la convinzione che il sistema di norme vigenti, operanti sotto l'egida della direttiva "madre" 95/46/CE, non fosse più in grado di far fronte in maniera adeguata alle complesse sfide provenienti dall'utilizzo sempre più intenso di tecniche di profilazione e tecnologie di connessione. Tale intrinseca debolezza è stata certamente acuita dall'eccessiva frammentazione normativa, che ha esposto i cittadini europei ad elevate disparità di protezione e di azione, non più ammissibili in una fase così avanzata del processo di integrazione e addirittura controproducenti dinanzi alle nuove esigenze di tutela di carattere transfrontaliero, derivanti dallo straordinario incremento dell'utilizzo dei *social network* e dei siti *web* di origine extraeuropea. Le molteplici criticità del quadro normativo, a loro volta, si sono tradotte sovente in una forte instabilità del mercato europeo, caratterizzato da opera-

diziari", in grado di rivelare la qualità di indagato o imputato del soggetto, nonché le sue informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti (art. 4, comma 1, lett. e). Al di fuori delle categorie riportate, espressamente richiamate dal legislatore, si ponevano invece, in via residuale, i "dati comuni", ossia quelli che consentono in vario modo l'identificazione e il tracciamento della persona (nome e cognome, codice fiscale, indirizzo del domicilio, posta elettronica, numero di telefono) e i "dati semisensibili", categoria dai contorni indefiniti e alla quale si riconducono tutte quelle informazioni il cui trattamento espone comunque il soggetto al pericolo di un pregiudizio giuridicamente rilevante. Nel regolamento europeo la classificazione dei dati si presenta ora diversa e ad essa gli operatori e la stessa società dovranno parametrare i propri comportamenti e la relativa tutela.

¹³ È datata 25 gennaio 2012 la presentazione da parte della Commissione Europea del pacchetto completo sulla protezione dei dati personali in cui venivano presentate per la prima volta sia la proposta di regolamento oggetto del presente saggio, sia la proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati, intesa a sostituire la decisione quadro del 2008 sulla protezione dei dati.

tori economici costretti a misurarsi con regole diverse e spesso contraddittorie, a seconda dell'ambito territoriale e settoriale di riferimento, nell'erogazione dei propri prodotti e servizi. Le difficoltà derivanti dall'assenza di un omogeneo approccio regolativo a livello europeo, connesse ad un'iniziale inevitabile ritrosia verso l'impiego sempre più invasivo di dati personali, hanno inoltre favorito in alcuni settori un clima di diffuso scetticismo nei confronti proprio dell'impiego di tali tecnologie, impedendo un pieno sfruttamento delle relative potenzialità.

Al fine di consentire il superamento di tali criticità e di orientare i vantaggi connessi a quella che è stata definita la “quarta rivoluzione industriale”, senza nel contempo provocare una inaccettabile compressione della sfera dei diritti fondamentali dei cittadini, l'Unione ha dato vita ad una serie di iniziative finalizzate all'individuazione di regole condivise che fossero in grado di “traghetare” gli Stati membri verso la nuova era digitale¹⁴. Tale variegato percorso è culminato, almeno con riferimento alla fase di più stretta normazione, nell'adozione di un peculiare “pacchetto di protezione dei dati personali” costituito dal regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo alla circolazione delle informazioni personali¹⁵ e dalla direttiva (UE) 2016/680 concernente i settori di

¹⁴ La Commissione Europea nell'ambito della più ampia strategia dedicata alla creazione del Mercato unico digitale (*Digital Single Market*) ha lanciato nel 2016 l'iniziativa nota come “*Digitalising European Industry initiative*” (Digitalizzazione dell'industria europea) finalizzata a garantire che ogni impresa in Europa, indipendentemente dalle dimensioni, dall'ubicazione e dal settore, possa usufruire dei vantaggi derivanti dall'innovazione digitale. L'iniziativa si fonda sui seguenti quattro pilastri fondamentali: 1) Creazione di una piattaforma europea per le iniziative nazionali in materia di digitalizzazione industriale; 2) Innovazioni digitali per tutti: *digital innovation hubs*; 3) Rafforzare la leadership attraverso partenariati e piattaforme industriali, 4) La determinazione di un quadro normativo adatto all'era digitale; 5) Preparare i cittadini al futuro digitale. Nell'ambito di tale iniziativa è stata adottata la direttiva NIS e sono stati siglati documenti di rilievo per l'implementazione delle nuove tecnologie in diversi settori di rilievo per la società europea. Si ricordi, tra gli altri, l’“*EU eGovernment Action Plan 2016-2020 – Accelerating the digital transformation of government*” dedicato alla digitalizzazione della pubblica amministrazione e alla creazione di servizi digitali a favore degli utenti. COM(2016) 179 final; L’“*European Cloud Initiative – Building a competitive data and knowledge economy in Europe*” – finalizzata alla creazione di una economia europea basata sullo scambio dei dati e delle informazioni attraverso l'utilizzo di tecnologie come il *cloud computing*. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. COM(2016) 178 final.

¹⁵ 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto Privato*, fasc. 4, 2016.

prevenzione, contrasto e repressione dei crimini¹⁶. Dalla loro lettura, emerge immediatamente la duplice finalità che anima l’intero impianto normativo: da un lato, la volontà di non perdere lo straordinario volano rappresentato dalle nuove tecnologie digitali, assunte ormai a fattore strategico di crescita a livello mondiale delle moderne società avanzate; dall’altro la necessità che tale evoluzione non comprometta il nucleo dei diritti fondamentali riconosciuti al singolo che sono espressione e legittimazione delle tradizioni costituzionali europee.

3. Il profilo “attivo” dell’autodeterminazione informativa

Il diritto di ricevere informazioni corrette e plurali può essere ascritto in modo diretto al riconoscimento, prodottosi nel tempo da parte della giurisprudenza costituzionale, dell’esistenza di una terza situazione giuridica soggettiva, ricavabile dall’art. 21 Cost., che si sostanzia nel “diritto ad essere informati”. Come appare evidente, fonte di questo diritto non è la disposizione costituzionale di tutela della manifestazione del pensiero, *lato sensu* intesa, dal momento che quest’ultima non appare suscettibile di produrre alcuna pretesa in chi legge o ascolta tale esternazione, stante la sua natura squisitamente individuale. A dare fondamento a questo diritto è l’altra situazione giuridica soggettiva tutelata dall’art. 21 Cost., ossia il diritto di informare; infatti, pur non essendo configurabile un obbligo di informare, è altrettanto vero – come più volte ricordato dalla Corte costituzionale – che qualora un individuo, in particolar modo un giornalista, decida di farlo in modo professionale debba impegnarsi a produrre una informazione corretta ed imparziale, mentre è compito dell’ordinamento giuridico garantire che la stessa sia anche “plurale”. Seguendo tale impostazione la libertà di informazione svela un duplice angolo visuale a seconda del punto da cui muove la tutela costituzionale, articolandosi in un diritto ad informare ed in un corrispettivo diritto ad essere informati. Il riconoscimento di questa

¹⁶Direttiva (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 e che abroga la decisione quadro 2008/977/GAI del Consiglio con l’obiettivo di sostituire la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia. La direttiva, pubblicata nella Gazzetta Ufficiale dell’Unione europea insieme al regolamento e vigente dal 5 maggio 2016, è stato oggetto di recepimento nel biennio 2016-2018 da parte di tutti gli Stati membri.

duplicità assume un rilievo fondamentale ai fini dell'identificazione dell'essenza stessa dell'art. 21 Cost. e del valore del disposto costituzionale in relazione all'evoluzione in senso democratico della società. In altri termini, tale diritto, nella sua poliedricità, diviene coesistente alla forma democratica fissata dalla Carta Costituzionale sulla base della convinzione che “[...] i principi fondanti del nostro Stato esigono che la nostra democrazia sia basata su una libera opinione pubblica e sia in grado di svilupparsi attraverso la pari concorrenza di tutti alla formazione della volontà generale”¹⁷. Le due situazioni giuridiche soggettive (informare, essere informati) non costituiscono tuttavia situazioni giuridiche perfettamente speculari. In altri termini, il diritto di informare rappresenta una situazione giuridica autonoma e distinta dal diritto ad essere informati e la sua singola realizzazione non è direttamente correlata e soprattutto non vincolata alle esigenze della seconda. Tuttavia, una volta attivata, la libertà di informazione trova nelle garanzie del diritto ad essere informati il proprio limite.

Con riferimento all'evoluzione giurisprudenziale del diritto ad essere informati, in una prima fase la Corte costituzionale si era limitata a stabilire l'indubbia sussistenza di una tutela implicita e soprattutto indiretta, *ex art. 21 Cost.*, destinata non ad un diritto bensì ad un “interesse generale della collettività all'informazione”¹⁸, che richiedeva pluralità di fonti di informazioni, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei, alla circolazione delle notizie e delle idee e l'esclusione di interventi dei pubblici poteri suscettibili di tradursi, anche indirettamente, e contro le intenzioni, in forme di pressione per indirizzare la stampa verso obiettivi predeterminati a preferenza di altri”¹⁹. In un momento succes-

¹⁷ Nella sent. n. 112/1993, la Corte costituzionale ha sottolineato come “il ‘diritto all'informazione’ va determinato e qualificato in riferimento ai principi fondanti della forma di Stato delineata dalla Costituzione, i quali esigono che la nostra democrazia sia basata su una libera opinione pubblica e sia in grado di svilupparsi attraverso la pari concorrenza di tutti alla formazione della volontà generale”.

¹⁸ Corte costituzionale, sent. n. 94/1977, Al riguardo si è altresì specificato come “non è dubitabile che sussista, e sia implicitamente tutelato dall'art. 21 Cost., un interesse generale della collettività all'informazione di tal che i grandi mezzi di diffusione del pensiero (nella più lata accezione, comprensiva delle notizie) sono a buon diritto suscettibili di essere considerati nel nostro ordinamento, come in genere nelle democrazie contemporanee, quali servizi oggettivamente pubblici o comunque di pubblico interesse”.

¹⁹ Corte costituzionale, sent. n. 105/1972. Nello specifico, la Corte Costituzionale ha dichiarato l'illegittimità costituzionale di alcune disposizioni che, nel loro insieme, impedivano la libera diffusione e circolazione delle notizie e delle opinioni sia a mezzo della stampa periodica sia attraverso altri mezzi equipollenti, in quanto lesive non solo della libertà di manifestare il proprio pensiero ma anche e soprattutto “dell'interesse generale, anch'esso indirettamente protetto

sivo la Corte, inaugurando una giurisprudenza ormai consolidata che collega in modo stringente *democrazia, informazione e formazione dell'opinione pubblica*, ha riconosciuto il diritto ad essere informati quale situazione giuridica soggettiva costituzionale inviolabile e ricavabile dagli artt. 2-21 Cost. e ne ha definito le garanzie democraticamente necessarie che, come ricordato *supra*, si sostanziano nella completezza, oggettività e pluralità dell'informazione ricevuta.

Quanto appena ricostruito potrebbe, a prima lettura, presentare rilevanza solo nell'ambito, seppure fondamentale, della formazione dell'opinione pubblica e quindi dei rapporti tra governanti e governati. In realtà, ad una più attenta analisi, emerge chiaramente come la tutela del diritto ad una informazione corretta e plurale permei non solo i rapporti socio-politici ma anche quelli economici²⁰, assumendo quindi particolare rilevanza nell'ecosistema digitale dove l'informazione e la comunicazione tendono ad assumere una connotazione sempre più intersettoriale e lo scambio dei dati e delle informazioni si presenta suscettibile di assolvere a diverse finalità e a soddisfare plurimi interessi.

4. Tutela della autodeterminazione informativa e profilazione degli utenti

Un aspetto di particolare rilevanza nell'economia e società digitale è rappresentato dalla raccolta ed elaborazione dei dati degli utenti al fine di poterne profilare le abitudini e gli orientamenti, anche di spesa e di consumo²¹.

Prima di analizzare le problematiche della profilazione in Rete, appare opportuno soffermarsi brevemente sul termine profilazione e sulle sue finalità.

dall'articolo 21, alla informazione, il quale, in un regime di libera democrazia, implica pluralità di fonti di informazione, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei, alla circolazione delle notizie e delle idee”.

²⁰ Si pensi, ad esempio, alla normativa in materia di obbligo di informazione del consumatore.

²¹ La profilazione costituisce una risorsa strategica essenziale anche per lo svolgimento delle attività del settore Fintech. Per un verso le tecniche di Big Data Analytics possono facilitare una maggiore personalizzazione dei prodotti e dei servizi, favorendo una stima più accurata dei profili di rischio e delle esigenze dei consumatori. Dall'altro lato, tuttavia, le medesime tecniche possono avere effetti negativi sulla disponibilità e la convenienza economica degli stessi prodotti e servizi, in particolare, per alcuni consumatori con profili di rischio più elevati o per i quali sono disponibili solo poche informazioni a causa della loro limitata attività online.

Il termine profilazione, nel suo significato generale, trae la sua fonte dal verbo di riferimento, *profilare*, il cui significato è, come è noto, quello di disegnare qualcuno o qualcosa tracciandone la linea di contorno. Tracciandone quindi il profilo, ossia quella parte che appare esteriormente. In passato la profilazione si presentava molto rispondente al significato etimologico del verbo di riferimento: infatti, in quelle che possono oggi essere definite profilazioni “analogiche” erano di regola i diretti interessati che fornivano i dati e le informazioni e potevano quindi decidere quanto il profilo tracciato dovesse corrispondere alla propria identità, intesa come insieme di interessi, di preferenze, di orientamenti. Un metodo di profilazione attento a questo aspetto, ancora oggi molto utilizzato, è rappresentato dal sondaggio, anche definito come “profilazione progressiva diretta”, che consente di intercettare dati e informazioni molto puntuali esplicitati dal diretto interessato.

L’obiettivo della rappresentazione di una identità – intesa come insieme di interessi, di preferenze e di orientamenti – può essere perseguito sia attingendo a dati volontariamente forniti, come appena sottolineato, sia in modo indiretto, ossia senza la collaborazione del soggetto che viene profilato. Ed è questa la modalità oggi sempre più utilizzata, che si realizza attingendo da quell’enorme bacino di dati che vengono forniti dalla navigazione in Internet degli utenti.

Al riguardo giova rilevare che azioni di profilazione dei consumatori sono sempre esistite e sono proprie delle attività di marketing. Tuttavia, il fluire incessante di dati personali che caratterizza le società e le economie digitali, con l’affermarsi dei big data²², ha favorito negli ultimi anni il sorgere di tecniche di profilazione sempre più raffinate che, attraverso l’aggregazione, l’incrocio e la riorganizzazione dei dati raccolti, consentono di suddividere gli utenti in categorie distinte in base a caratteristiche omogenee, al fine di fornire prodotti “su misura” attraverso la previsione delle decisioni di consumo e dei relativi comportamenti²³.

²² Sul punto cfr. V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws, Rivista di diritto dei media*, 2/2018.

²³ Cfr. S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, p. 6; S. STABILE, *Le nuove frontiere della pubblicità e del marketing su internet*, in *Dir. Industriale*, 2009, p. 5; D. DE PASQUALE, *La linea sottile tra manipolazione della rete e pubblicità*, in *Dir. industriale*, 2012, p. 6; A. MANTELERO, *Si rafforza la tutela dei dati personali: “data breach notification” e limiti alla profilazione mediante i cookies*, in *Dir. informazione e informatica*, (II), 2012, pp. 4-5; R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. informazione e informatica*, (II), 2013, p. 3; M. MAGGIOLINO, *Big Data e prezzi personalizzati*, in *Concorrenza e mercato*, 2016, p. 1.

Questo processo, fondato su un uso intensivo dei dati, una velocità inarrestabile nella circolazione delle informazioni insieme alla straordinaria capacità di ricerca, elaborazione e stoccaggio delle stesse è stata a lungo sottostimato, soprattutto in relazione al suo impatto sulla società e sulla tutela degli individui, dai diversi decisori politici nazionali e sovranazionali e affidato all'esclusiva valutazione commerciale ed etica degli OTT e in particolare dei gestori delle piattaforme digitali. È però oggi considerazione condivisa che le attività di profilazione svolte esclusivamente mediante procedure automatizzate – come tali negativamente asettiche – rischiano non solo di esacerbare situazioni di discriminazione e di stereo-tipizzazione già esistenti, ma anche, e forse soprattutto, di condurre a fenomeni di "penalizzazione delle propensioni"²⁴, limitando le effettive possibilità di scelta del singolo, sino a condurre all'estrema conseguenza di inibire l'esercizio delle relative libertà fondamentali o di limitare l'erogazione di servizi essenziali²⁵.

Il regolamento europeo sulla tutela dei dati personali, nel tentativo di dare uniformità alla tutela della autodeterminazione informativa dei singoli, si occupa in modo diretto o indiretto di profilazione in diversi articoli e considerando. In primo luogo, l'art. 4 del GDPR fornisce una definizione della profilazione oggetto di disciplina, strutturandola su tre elementi caratterizzanti: il trattamento automatizzato, l'utilizzo di dati personali, la finalità della valutazione di aspetti personali²⁶. L'art. 22, invece, sancisce il

²⁴ Così V. MAYER-SCHÖNBERGER, K.N. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013. Su questi aspetti cfr., anche, C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, Speciale/2019; G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016; S. WACHTER, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in *Computer law & security Review*, n. 34/2018; O. POLLICINO, G. D'ACQUISTO, M. NALDI, M. BASSANI, F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dati personali e regolazione*, Milano, 2018; G. FINOCCHIARO, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in *Medialaws.eu, Rivista di diritto dei media*, 2/2019.

²⁵ Come sottolineato nel testo, partendo dalla convinzione "che ogni individuo non costituisca un'isola", ma che la relativa piena evoluzione della propria personalità si nutra necessariamente di una molteplicità di momenti di interazione e di condivisione nelle formazioni sociali di cui fa parte, la protezione delle informazioni personali diviene una questione di tutela della stessa evoluzione democratica della società. Il corretto trattamento dei dati personali, soprattutto di carattere sensibile, costituisce premessa, infatti, irrinunciabile al pieno e consapevole esercizio degli altri diritti fondamentali allontanando fenomeni di compressione dei momenti di interazione tra i soggetti, non accettabili all'interno delle società democratiche". Così D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 24 ottobre 2018.

²⁶ L'art. 4 definisce la profilazione "qualsiasi forma di trattamento automatizzato di dati per-

diritto del singolo a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, e comunque – anche quando tale trattamento sia possibile – richiede che il titolare del trattamento attui tutte le misure necessarie per tutelare diritti, libertà e interessi legittimi dell’interessato²⁷. Ciò comporta l’assunzione di una specifica responsabilità da parte del titolare del trattamento chiamato a dover informare e richiedere il consenso per l’utilizzo dei dati, soprattutto se questi sono destinati ad essere usati per la profilazione, dovendo in quest’ultimo caso informare gli interessati della logica sottostante il processo decisionale che ha portato a sviluppare il loro profilo e le conseguenze che ne derivano²⁸.

Il combinato disposto della tutela costituzionale e di quella europea mira dunque a garantire all’individuo il diritto ad autodeterminare la propria identità digitale, quale emerge dal flusso di dati che lo riguardano e dalla profilazione che da questi ultimi viene elaborata. È tuttavia necessario auspicare che tale tutela si presenti oggi, e sempre più in futuro, fortemente dinamica e basata essenzialmente su principi, al fine di non rivelarsi sempre arretrata rispetto alla tecnologia con la quale è chiamata a relazionarsi.

sonali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

²⁷ L’art. 22, par. 1 stabilisce che: *“l’interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona”*.

²⁸ La stessa preoccupazione del legislatore è evidente quando al considerando 71 specifica che *“al fine di garantire un trattamento corretto e trasparente nel rispetto dell’interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell’interessato e che impedisca tra l’altro effetti discriminatori”*. Anche l’art. 13, par. 2, lett. f) e l’art. 15, par. 1, lett. h) stabiliscono il diritto dell’interessato di conoscere l’esistenza del processo decisionale automatizzato e, in particolare, di ottenere informazioni significative sulla logica utilizzata (i criteri assunti per raggiungere la decisione, senza che con ciò si debba necessariamente fornire una spiegazione complessa degli algoritmi utilizzati) e sulle conseguenze previste di tale trattamento.

5. Quali prospettive della garanzia di autodeterminazione informativa degli utenti del web

L'attenzione, che si registra negli ultimi anni in diversi ambiti di ricerca, al tema della profilazione trova il proprio fondamento, come sottolineato nel corso del lavoro, anche dall'acquisita consapevolezza che la profilazione influenzi la libera determinazione dell'individuo, interagendo e in parte interferendo da un lato con la complessa architettura cognitiva e dall'altro con la funzione narrativa della mente umana. L'individuo, infatti, rappresenta il precipitato di ciò che percepisce dall'ambiente circostante, in associazione a tanti ulteriori elementi di contesto (situazione personale e familiare, fede, appartenenza politica, ecc.) ed anche per questo in sistemi democratici la libera circolazione delle informazioni rappresenta un elemento fondamentale non solo quale declinazione della libertà di esprimersi e di informare ma anche nella sua declinazione di diritto a ricevere informazioni corrette, plurali, imparziali. Questo vale non solo con riferimento alle opinioni, in considerazione della loro rilevanza per la formazione dell'opinione pubblica, ma anche in relazione alla circolazione delle informazioni in ambito socio-economico, nelle quali la pluralità e la correttezza di queste ultime restano basilari per il buon funzionamento del sistema.

Da qui il dubbio di poter considerare plurale una serie di informazioni tutte uguali che l'individuo riceve essendo stato profilato. È infatti indubbio che le persone hanno molteplici strumenti, oltre al web, per ricevere le informazioni. Ma in Rete il problema resta nella misura in cui la personalizzazione dei contenuti "offerti" all'individuo e che egli riceve via mail, sui social o nelle prime pagine delle ricerche effettuate utilizzando i motori di ricerca tendono ad "assomigliargli", nel senso che corrispondono agli interessi, alle inclinazioni che egli ha manifestato e manifesta prevalentemente nelle sue ricerche di quel momento. Una sorta di bozzolo dal quale l'individuo si fa avvolgere e confortare. In società che vanno sempre più di corsa avere delle informazioni di questo tipo viene spesso considerata positivamente perché percepita come strumento di ottimizzazione del tempo. L'utilizzo dei big data nell'attività di profilazione consente, infatti, di far pervenire all'utente, attraverso le piattaforme social, solo le notizie che si ritiene egli voglia ricevere, confermandolo quindi sempre più nelle sue convinzioni. In questo modo viene però drasticamente ridotta la possibilità che egli possa formarsi una opinione sulla base di contenuti plurali. Tale situazione vale in ambito politico e sociale, ma anche nel settore commerciale. Anzi può dirsi che la profilazione può influire su ogni aspetto della vita di

una persona. Ciò rappresenta un rischio per il pluralismo che è il fondamento di una società democratica, nella quale è fondamentale che l'individuo venga messo in condizione di poter scegliere e pertanto deve conoscere, anzi essere circondato – e forse anche sommerso – dalla circolazione di idee, opinioni, conoscenze, ma anche oggetti, servizi diversi da quelli per i quali ha manifestato interesse in passato.

Il pluralismo informativo va quindi garantito ed appare evidente che tale compito non possa essere svolto dal soggetto privato che utilizza i dati e li scambia per finalità di profilazione bensì debba essere assunto da chi è chiamato a bilanciare tra diritti e interessi diversi, il legislatore e i soggetti chiamati a vigilare (in primo luogo le Autorità garanti) sulla tutela dei dati e del pluralismo informativo nell'ecosistema digitale.