Convegno annuale Associazione Gruppo di Pisa – Genova 18/19 giugno 2021
Il diritto costituzionale e le sfide dell'innovazione tecnologica

IDENTITÀ DIGITALE E TUTELA DELLA PRIVACY

SIMONE SCAGLIARINI

SOMMARIO: 1. Premessa: due diritti a contenuto "tecnologicamente condizionato". – 2. Privacy, identità ed innovazione tecnologica: una rassegna diacronica. – 2.1. Dal *right to be let alone* all'autodeterminazione informativa (passando per la protezione dei dati). – 2.2. Dall'identità personale al diritto all'oblio (passando per l'identità digitale). – 3. Il contesto ordinamentale vigente: alcune premesse. – 3.1. Privacy e identità digitale nell'attuale quadro normativo europeo e nazionale. – 3.2. La (parziale) insufficienza della tutela a livello "micro"… – 3.3. … e la sua strutturale inefficacia a livello "macro". – 4. Una (apparente) digressione: un problema culturale in tema di riservatezza. – 5. Tra presente e futuro: quale tutela nel mondo digitale? – 5.1. Un percorso *de jure condito*. – 5.2. Una proposta *de jure condendo*. – 5.3. Volgendo lo sguardo all'orizzonte. – 6. Nota conclusiva.

1. Premessa: due diritti a contenuto "tecnologicamente condizionato"

L'incidenza delle innovazioni tecnologiche, al pari di altri elementi "di contesto", sull'evoluzione dei diritti di libertà, i quali, per tale via, acquisiscono nuovi e ulteriori significati a fronte del mutamento delle forme e delle modalità con cui il bisogno sottostante si manifesta, è un dato ormai acquisito[1].

Quando, tuttavia, volgiamo il discorso dal generale allo specifico delle due situazioni soggettive di cui andrò a trattare – ovvero l'identità digitale e la privacy[2] – l'intensità della correlazione con lo sviluppo tecnologico, che rappresenta peraltro uno dei non pochi punti di contatto tra di esse[3], assume un valore tutt'affatto particolare. I diritti in questione, infatti, presentano uno stretto legame con tale contesto, per cui è la stessa sfida dell'evoluzione tecnologica ad averne non solo gradualmente determinato l'emersione di nuovi profili ma anche,

[1] Sia sufficiente, per tutti, richiamare le parole di A. D'ALOIA, *Introduzione. I diritti come* immagini in movimento*: tra* norma *e* cultura *costituzionale*, in ID. (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, XXVI, secondo cui «ad arricchire il quadro dei diritti, o meglio dei significati e delle modalità di tutela dei medesimi, concorrono […] una pluralità di condizioni causali (esigenze della convivenza sociale, *nuove cognizioni e possibilità tecnologiche*, confronto di modelli culturali eterogenei) […] che in qualche caso si alimentano e si intersecano vicendevolmente» (corsivo mio).

[2] Uso per ora, per semplicità espositiva, questo lemma come comprensivo tanto della riservatezza quanto della protezione dei dati personali e dell'autodeterminazione informativa, pur nella consapevolezza che i concetti non sono esattamente sovrapponibili; ritornerò sul punto *infra*, in particolare nota 34.

[3] Giacché, come scrive G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Digesto Discipline Privatistiche – sezione civile*, *Aggiornamento V*, Torino, 2010, 723 «indubbiamente riservatezza, protezione dei dati personali, identità personale […] costituiscono le facce di un unico prisma».

successivamente, condizionato lo sviluppo[4]. Di modo che, in buona sostanza, trattare di come l'innovazione ha inciso e tuttora incide su identità e privacy equivale a parlare della storia stessa di questi diritti ed a disegnarne gli attuali (ma quanto mai mobili) confini, individuandone i tratti caratterizzanti che essi assumono oggigiorno. Nella prima parte di questa indagine ritengo, perciò, necessario soffermarmi, seppure giocoforza brevemente, almeno sui passaggi più rilevanti (e in più di un caso davvero epocali) che segnano il percorso evolutivo seguito dalle situazioni soggettive *de quibus*, soprattutto per sottolineare la molteplicità di quei nuovi profili che, mercé le nuove tecnologie, esse hanno assunto, arricchendosi di facoltà prima sconosciute, ma pur sempre ad esse ascrivibili.

Ciò premesso, nell'incredibile ampiezza e nella pressoché sterminata varietà di impostazioni che un discorso su questi temi potrebbe assumere e delle prospettive che si potrebbero abbracciare, ritengo opportuno, dopo questa rassegna diacronica, soffermare l'attenzione su quella che mi pare una delle maggiori sfide che oggi si gioca sul tema dei dati personali.

Mi riferisco, in particolare, alla circostanza per cui, in questa era dell'economia digitale, ci troviamo di fronte ad un mercato dominato da soggetti privati, il cui potere, derivante dal possesso di enormi raccolte di informazioni note come *Big data*[5] ed ancor più dalle operazioni di analisi che, attraverso algoritmi, su di esse si possono compiere, insidia l'esercizio stesso di prerogative statali[6], ponendo a rischio, al contempo, la garanzia per molte, se non tutte, le libertà che il costituzionalismo ha consentito di affermare[7]. Di modo che la protezione dei dati e dell'identità digitale finisce, in questo contesto, per travalicare la tradizionale garanzia individuale ed assumere piuttosto una valenza universale.

La risposta che il legislatore, a partire da quello sovranazionale, ha fornito nell'attuale contesto per (tentare almeno di) offrire una tutela efficace alle situazioni soggettive in esame, che cercherò di analizzare – di nuovo, necessariamente, per cenni esemplificativi – in seguito, presenta indubbiamente pregi, ma anche non poche e non trascurabili criticità, derivanti da una inadeguatezza strutturale del quadro regolatorio vigente al cospetto della problematica segnalata. Ed è alla luce di questo contesto che intendo provare a suggerire una prospettiva di lettura, a mio avviso non ancora così diffusa, che evidenzi come, più che i rischi provenienti dallo Stato per i

---

[4] Stante la «"naturale" tendenza ad entrare in conflitto con la sfera di autonomia privata individuale» di cui parla L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004, 234, con particolare riferimento alle tecnologie della comunicazione e dell'informazione.

[5] La definizione di questo concetto può essere data facendo riferimento allo standard ISO/IEC 20546:2019 *Information technology – Big data – Overview and vocabulary*, reperibile sul sito istituzionale dell'*International Organisation of Standardization*, come set di dati estesi, le cui caratteristiche sono le famose "4 v" (volume, varietà, velocità e/o variabilità) che richiedono una tecnologia scalabile (e cioè capace di incrementare le proprie prestazioni qualora vengano fornite nuove risorse) per poter essere archiviati, manipolati, gestiti e analizzati in modo efficiente. In realtà, come ricorda T. MAURO, *I* big data *tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, 651 ss., nella misura in cui sussistano le "4 v" se ne aggiunge una quinta, non certo meno importante, data dal valore economico che gli stessi acquisiscono.

[6] Ne cercherò di offrire più di un esempio *infra*, specialmente al paragrafo 3.3.

[7] Del resto, che vi sia uno stretto legame di strumentalità tra la tutela della privacy e quella degli altri diritti è considerazione nota da tempo: cfr., *ex plurimis*, F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 9 ss.

diritti di cui andrò trattando, vada riguardata la possibilità di ottenere da esso una maggiore tutela, specialmente nei confronti di poteri privati, di modo che un cambiamento della cultura (non solo) giuridica sul punto possa poi indurre verso interventi regolatori maggiormente adeguati di fronte a questa sfida che occorre affrontare. Interventi che, conclusivamente, mi prometto di ricostruire, sia in ottica *de jure condito*, che in prospettiva *de jure condendo*, ivi incluse le proposte normative di recente presentazione in sede europea.

2. Identità, privacy ed innovazione tecnologica: una rassegna diacronica

Volendo, dunque, prendere le mosse da una, seppur sintetica, rassegna diacronica dei passaggi fondamentali che segnano l'origine, dapprima, e le tappe evolutive successive dei diritti qui esaminati in raffronto allo sviluppo tecnologico, mi sembra necessario prenderli in esame distintamente.

2.1. Dal right to be let alone *all'autodeterminazione informativa (passando per la protezione dei dati)*

Per quanto riguarda il diritto alla riservatezza[8], si può facilmente osservare come esso presenti fin dal suo apparire un qualche legame con il progresso tecnologico. Mi riferisco all'arcinota vicenda che ha rappresentato il *casus belli* da cui nasce il primo e conosciutissimo scritto dal titolo *The Right to Privacy*[9]. Vicenda che trae origine dalle indiscrezioni apparse sulla stampa circa le feste che si svolgevano nell'abitazione di uno dei due autori, noto avvocato bostoniano, laddove è l'implementazione di alcune innovazioni tecnologiche – e segnatamente la diffusione della stampa, grazie alla (allora) piuttosto recente introduzione delle rotative e della fotografia istantanea[10] – a far sì che la lesione alla privacy, appunto, dell'interessato, da semplice pettegolezzo conoscibile ad una fascia ristretta di popolazione venisse ad assumere dimensioni assai più ampie e preoccupanti[11].

---

[8] La bibliografia sul tema è davvero sterminata. Per limitarmi a qualche citazione generale sull'origine e la storia di questa nozione, e rinviando alle successive note per ulteriori riferimenti, sia qui sufficiente richiamare P. PATRONO, *Privacy e vita privata (dir. pen.)*, in *Enc. Dir*., vol. XXXV, Milano, 1986; A. CERRI, *Riservatezza (diritto alla) III) Diritto costituzionale*, in *Enc. Giur.*, vol. XXVII, Roma, 1995; A. CLEMENTE (a cura di), *Privacy*, Padova, 1999; G. BUSIA, *Riservatezza (diritto alla)*, in *Digesto Discipline Pubblicistiche*, *Aggiornamento I*, Torino, 2000, 476 ss.; e R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e continuità*, in ID. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, vol. I, Milano, 2003, 3 ss.

[9] S. D. WARREN – L. D. BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, vol. 4, n. 5/1890, 193 ss.

[10] L'evoluzione di queste tecnologie è definita «il nocciolo della questione» da F. PIZZETTI, *Privacy*, cit., 47 ss., il quale sottolinea come «gran parte […] della materia che dobbiamo studiare è connesso alle evoluzioni tecnologiche».

[11] Gli stessi Autori, del resto, individuano esplicitamente i pericoli per la privacy in «instantaneous photographs and newspaper enterprise» ed in «numerous mechanical devices» (S. D. WARREN – L. D. BRANDEIS, *The Right*, cit., 195).

Ma anche l'ingresso in Italia, per via pretoria, dello stesso diritto non è scollegato da un rapporto con tecnologie che erano allora di recente introduzione o in corso di forte sviluppo e potenziamento. Basti dire del famoso "caso Caruso"[12], in cui la richiesta risarcitoria, per la prima volta accordata da un giudice di merito, per lesione della riservatezza, è imputabile ad un'opera cinematografica a carattere biografico, od al "caso Esfandiari", che registra il primo espresso riconoscimento del diritto alla riservatezza nell'ordinamento italiano da parte della giurisprudenza di legittimità[13], in cui la causa era stata instaurata a seguito della pubblicazione di riprese fotografiche, rese possibili solo dall'evoluzione delle prestazioni di tali apparecchi[14], od ancora alle pronunce degli anni '90 che inducono questa volta il giudice delle leggi a riconoscere, seppur ancora non in modo generale ed espresso, il diritto alla riservatezza, decisioni originate dalla normativa in tema di intercettazioni[15], strumento di indagine che già allora (e ancor più in seguito) diveniva sempre più penetrante grazie all'affinamento delle tecnologie a disposizione dell'Autorità giudiziaria.

È, in ogni caso, innegabile che, a partire dagli anni '70 del secolo scorso, siano soprattutto le tecnologie informatiche a far compiere un salto di qualità nell'evoluzione del diritto *de quo*[16], poiché con l'introduzione delle prime banche dati emerge un profilo fino ad allora sconosciuto, ovvero la protezione dei dati personali, intesa quale diritto da parte del diretto interessato al controllo dell'uso che viene fatto da parte di terzi delle proprie informazioni[17]. Infatti, seppur in misura irrisoria rispetto agli attuali *Big data* cui ho fatto cenno e sui quali tornerò ampiamente, già le semplici banche dati, gestite con l'ausilio dell'informatica delle origini, ben potevano (come tuttora a maggior ragione possono) rappresentare il modo di conoscere e raccogliere notizie sul conto altrui e di rielaborarle successivamente. E se, allora, dato l'elevato costo di queste tecnologie, ciò avveniva principalmente in capo alla Pubblica Amministrazione, con il rischio, ad esempio, di schedature per finalità politiche, con il progressivo diffondersi dell'informatica e la drastica

---

[12] Deciso con la sentenza Trib. Roma, 14 settembre 1953, in *Foro italiano*, 1954, I, 2, 115 ss., confermata in sede di gravame da App. Roma, 17 maggio 1955, in *Foro italiano*, 1956, I, 793 ss.

[13] Cass. civ. sez. I, 27 maggio 1975, n. 2129 in *Giurisprudenza italiana*, 1976, I, 1, 970 ss.

[14] L'incidenza del progresso tecnologico sul *revirement* della Suprema Corte è esplicitato *apertis verbis* nel punto 2 della motivazione in diritto, allorché il Collegio afferma che l'esigenza di tutela della personalità sta assumendo aspetti allarmanti «dato il *continuo sviluppo della moderna tecnologia*, la quale offre ai poteri pubblici o ai privati smisurate possibilità, mediante perfezionati strumenti di acquisizione conoscitiva, di penetrante controllo su ogni aspetto di vita e di rapida divulgazione generale dei dati acquisiti» (corsivo mio).

[15] Mi riferisco in particolare alle pronunce 23 luglio 1991, n. 366; 11 marzo 1993, n. 81; 24 febbraio 1994, n. 63; e 30 dicembre 1994 n. 463.

[16] Di una nozione di privacy riconfigurata dalle nuove tecnologie, che si distacca dalla risalente concezione del *righ to be let alone* ragiona P. COSTANZO, *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, in P. CARETTI (a cura di), *Studi in memoria di Paolo Barile*, Firenze, 2012, 9 ss.

[17] Non a caso, proprio in quegli anni, il sociologo americano A. WESTIN, nella sua notissima opera *Privacy and Freedom*, New York, 1967, 7 definisce la privacy come «the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others». Su questo passaggio dell'evoluzione del diritto al nostro esame, cfr. in particolare, per limitarci a qualche citazione esemplificativa all'interno di una vastissima letteratura, V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA – M. BESSONE (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1984, 32 ss.; S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, 1991, 521 ss.; nonché, di recente, A. MONTI – R. WACHS, *Protecting Personal Information. The Right to Privacy Reconsidered*, Oxford, 2019.

riduzione dei costi di immagazzinamento delle informazioni oggi si tratta di una prassi diffusa pure presso soggetti privati, anche e soprattutto per scopi di natura commerciale. Così che la libertà di autodeterminazione delle proprie scelte (negoziali, ma più in generale, di comportamento e, ancor più in generale, di vita), in quanto prevedibili, rischia di divenire solo un «simulacro di libertà»[18]; da qui, la necessità che il singolo debba potere controllare l'uso da parte di terzi delle informazioni sulla propria persona. È così compiuto il passaggio da una tutela di tipo proprietario su informazioni riguardanti fatti, vicende e dati personali, secondo la concezione fino ad allora dominante, ad una garanzia in termini di diritti della personalità, come conseguenza di quei mutamenti sociali e tecnologici che sul diritto al nostro esame, alla pari (ma forse anche più) di ogni altra situazione soggettiva, hanno inciso significativamente[19].

Se poi, con un enorme balzo temporale, proiettiamo queste considerazioni dalla tecnologia informatica degli albori, negli anni '70, allo sviluppo digitale dell'epoca attuale, caratterizzato dalla estrema diffusione della rete internet, dei *social network*, e vieppiù dell'intelligenza artificiale, le osservazioni appena svolte mostrano tutto il peso e la rilevanza che hanno acquisito quelle problematiche emerse, con incomparabilmente minore gravità, ormai cinque decadi orsono[20]. Il mondo della rete, in cui si stanno velocemente (specie nell'attuale contesto di emergenza pandemica) spostando tutte le attività della vita quotidiana (dal lavoro allo studio, dagli acquisti ai contatti sociali, ecc.)[21], si nutre voracemente di dati, che vengono acquisiti, raccolti, conservati e variamente trattati, per le finalità più disparate, da quelle di rilevanza privatistica (la profilazione commerciale, per esempio) alla programmazione di politiche pubbliche. Di ciò si è dimostrata ben consapevole anche la Corte costituzionale, che proprio recentemente, con la sentenza 23 gennaio 2019, n. 20[22], ha avuto l'occasione per affermare che il diritto alla

---

[18] L'espressione è di G. ARENA, *La tutela della riservatezza nella società dell'informazione*, in *Scritti in onore di Pietro Virga*, vol. I, Milano, 1994, 90.

[19] Lo stretto rapporto esistente tra diritto alla riservatezza e mutamenti sociali era evidenziato con particolare forza già da S. RODOTÀ, *Tecnologie dell'informazione e frontiere del sistema socio-politico*, in *Politica del diritto*, 1982, 28 ss.; nonché, più recentemente, *ex plurimis*, da C. SARTORETTI, *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese*, Torino, 2008, 1 ss. Anche il parallelo legame con l'evoluzione tecnologica è evidenziato con forza da molti Autori, tra cui L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati*, in L. CALIFANO – C. COLAPIETRO, *Innovazione tecnologica e valore della persona*, Napoli, 2017, 9, la quale ricorda come «il percorso di costruzione del diritto alla protezione dei dati personali si intreccia con il parallelo crescente sviluppo dell'innovazione tecnologica delle comunicazioni elettroniche».

[20] L'avvento di internet è indicato come un vero e proprio spartiacque in materia di privacy da T. E. FROSINI, *Il costituzionalismo nella società tecnologica*, in Liber amicorum *per Pasquale Costanzo*, vol. I, *Costituzionalismo, reti e intelligenza artificiale*, Genova, 2020, spec. 6 ss.

[21] Efficace l'espressione utilizzata al riguardo da M. CALISE – F. MUSELLA, *Il principe digitale*, Roma-Bari, 2019, 5: se nella realtà virtuale «sino a poco tempo fa ci sembrava di "andare"» oggi essa «ha inghiottito le nostre vite». Sulla progressiva confusione tra il mondo digitale e quello "analogico", cfr. le osservazioni di L. FLORIDI, *La quarta rivoluzione*, Milano, 2014, spec. 47 ss., ove l'A. introduce a tal fine il concetto di *onlife*, come vita in cui la distinzione tra ciò che è in rete e ciò che ne è fuori appare quanto mai sfumata e non sempre così netta e percettibile.

[22] La decisione è stata oggetto di numerosi commenti, soprattutto in relazione al profilo del rapporto tra diritto eurounitario e diritto interno, di cui segna un passaggio fondamentale. Per limitarmi a citare qualcuna tra le note che più si concentrano sugli elementi attinenti al discorso che stiamo svolgendo, v., almeno, O. POLLICINO, *Visibilità del potere, riservatezza individuale e tecnologia digitale. Il bilanciamento delineato dalla Corte*, ne *Il diritto dell'informazione e dell'informatica*, 2019, 110 ss.; I. NICOTRA, Privacy *vs trasparenza, il Parlamento tace e il punto*

riservatezza, il quale «trova riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.) […] e che incontra specifica protezione nelle varie norme europee e convenzionali», oggi «si caratterizza particolarmente quale diritto a controllare la circolazione delle informazioni riferite alla propria persona»[23].

Peraltro, della pronuncia testé citata sembra significativo anche il passaggio in cui la Consulta osserva che «sono le stesse peculiari modalità di pubblicazione imposte dal d.lgs. n. 33 del 2013 ad aggravare il carattere, già in sé sproporzionato, dell'obbligo di pubblicare i dati […] L'indicizzazione e la libera rintracciabilità sul web, con l'ausilio di comuni motori di ricerca, dei dati personali pubblicati, non è coerente al fine di favorire la corretta conoscenza della condotta della pubblica dirigenza e delle modalità di utilizzo delle risorse pubbliche. Tali forme di pubblicità rischiano piuttosto di consentire il reperimento "casuale" di dati personali»[24]. Ora, ciò che appare estremamente interessante nell'ottica della nostra ricognizione è che il giudice delle leggi imputa proprio alle modalità tecniche adottate (per la diffusione di alcuni dati a fini di trasparenza amministrativa) il maggiore *vulnus* arrecato al diritto alla riservatezza: una dimostrazione ulteriore di come le scelte tecnologiche incidano su questo diritto.

La situazione soggettiva di cui andiamo parlando, peraltro, ha conosciuto, sempre a partire dallo stesso periodo del secolo scorso, un ulteriore e parallelo arricchimento delle facoltà ad esso riferibili, con il profilarsi del c.d. diritto all'autodeterminazione informativa[25], consistente nella libertà di effettuare in autonomia le proprie scelte di vita, in senso ampio, e, conseguentemente, nel diritto a non subire pressioni da parte di terzi, potendo controllare e selezionare le informazioni che si intendono far entrare nella propria sfera privata[26]. Un elemento, a ben vedere, che, al pari

---

di equilibrio lo trova la Corte, in *Federalismi.it*, n. 7/2019; e B. PONTI, *Il luogo adatto dove bilanciare il "posizionamento" del diritto alla riservatezza e alla tutela dei dati personali* vs. *il diritto alla trasparenza nella sentenza n. 20/2019*, in *Istituzioni del federalismo*, 2019, 525 ss.

[23] *Considerato in diritto*, punto 2.2. Si osservi, per inciso, che dal tenore letterale della pronuncia sembra potersi dedurre che il giudice delle leggi non aderisca alla tesi da tempo affermatasi in dottrina (su cui, per tutti, C. M. BIANCA, *Note introduttive*, in C. M. BIANCA – F. D. BUSNELLI (a cura di), *La protezione dei dati personali*, tomo I, Padova, 2007, XX ss.; F. PIZZETTI, *Il prisma del diritto all'oblio,* in ID. (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 32 ss.; e G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, 2017, 1 ss.) del diritto alla protezione dei dati come autonoma figura soggettiva, sulla base, tra l'altro, della distinzione fatta dalla Carta dei diritti fondamentali dell'Unione europea tra diritto alla vita privata e, appunto, protezione dei dati, preferendo invece la diversa ricostruzione che individua in esso soltanto un nuovo profilo della riservatezza intesa in senso ampio (su cui mi sia consentito rinviare a S. SCAGLIARINI, *La riservatezza e i suoi limiti*, Roma, 2013, spec. 34 ss.).

[24] *Considerato in diritto*, punto 5.3.1.

[25] Per usare l'espressione coniata dal *Bundesvefassungsgericht* nella sentenza 15 dicembre 1983 (in *Rivista giuridica del lavoro*, 1985, I, 532 ss.) e che ha poi avuto fortuna anche nella dottrina italiana. Su questa ormai risalente vicenda, v. G. SARTOR, *Tutela della personalità e normativa per la «protezione dei dati»*, in *Informatica e diritto*, 1986, 95 ss.; R. LATTANZI, *La tutela dei dati personali dopo la ratifica della convenzione europea sulle banche-dati*, ne *Il diritto dell'informazione e dell'informatica*, 1990, 235; nonché S. SIMITIS, *Il contesto giuridico e politico della tutela della privacy*, in *Rivista critica di diritto privato*, 1997, 569, il quale ricorda come la Corte tedesca ebbe l'occasione di definire la normativa sulla privacy come un elemento imprescindibile delle società democratiche.

[26] Sulla riservatezza come libertà di autodeterminazione, nel contesto attuale, cfr., tra i tanti, M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della* privacy *storica*, Napoli, 2009, 51 ss.; C. DE GIACOMO, *Diritto, libertà e* privacy *nel mondo della comunicazione globale*, Milano, 1999, 25 ss.; e G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA – P. RIDOLA (a cura di), *I diritti costituzionali*, vol. II, Torino, 2006, 630 ss., i quali tutti rimarcano l'attuale impossibilità di pensare alla privacy solo in termini negativi e la

della protezione dei dati, è volto nella direzione di assicurare il potere di ciascuno di rivendicare il pieno controllo sui flussi informativi che lo riguardano, non solo "in uscita" ma anche "in entrata"[27], e che ulteriormente induce a superare la primigenia qualificazione della riservatezza in chiave di mera libertà negativa[28], per approdare ad una lettura anche in chiave positiva legata allo sviluppo della personalità umana[29].

L'emersione di questo nuovo aspetto della riservatezza, a differenza di quello precedente, non ha in effetti alle origini uno stretto legame con i profili tecnologici: basti pensare al *leading case* nella giurisprudenza costituzionale, ove il diritto in questione veniva richiamato in relazione alla raccolta delle questue effettuata (anche) senza alcun mezzo tecnico[30]. Le cose tuttavia cambiano significativamente con il procedere del tempo, allorché la sfera privata comincia a subire pressioni assai più pressanti, con finalità commerciale o propagandistica, attraverso nuovi e più efficaci mezzi, dal canale telefonico a quello televisivo. Ma anche a questo riguardo lo stacco più netto si ha con l'avvento della rete e forse ancor più dei *social network*, laddove il flusso di informazioni in entrata, per chiunque abbia (almeno) un profilo in essi, assume livelli niente affatto trascurabili[31], con effetti fortemente impattanti sulla libertà e autonomia di pensiero e sul diritto all'informazione. Tra gl'innumerevoli esempi che si potrebbero fare, mi limito a ricordare il ruolo ormai imprescindibile che i *social* esercitano nelle campagne elettorali[32], grazie alla possibilità offerta di individuare preferenze e sensibilità dei singoli elettori e su questa base porre in essere

---

polisemia che a tale espressione deve oggi essere riconosciuta. È peraltro in questa stessa direzione che F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, 20, descrive il "diritto di privacy" come una «costellazione di diritti».

[27] Come sottolinea S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 151 ss. e spec. 169, vi è un comune denominatore di tutti gli aspetti della privacy, da quello tradizionale di riservatezza in senso stretto a quello più recente di tutela dei propri dati, ed è il diritto di autodeterminarsi nella propria sfera privata senza intromissioni e di esercitare il controllo sulle proprie informazioni.

[28] Il passaggio dalla libertà negativa ad una visione più ampia è ricostruito, di recente, da G. M. SALERNO, *Le origini ed il contesto*, in L. CALIFANO – C. COLAPIETRO, *Innovazione*, cit., spec. 81 ss.

[29] In questo senso già C. CASONATO, *Riservatezza e trattamenti sanitari obbligatori in Italia e Stati Uniti: prime considerazioni*, in *Diritto e società*, 1993, 683 ss.

[30] Mi riferisco alla sentenza 2 febbraio 1972, n. 12, in *Giurisprudenza costituzionale*, 1972, 45 ss., con nota di A. CERRI, *Regime delle questue: violazione del principio di eguaglianza e tutela del diritto alla riservatezza*, il quale identificava, appunto, nel diritto all'autodeterminazione quel diritto alla riservatezza di cui la dottrina in quegli anni andava cercando il fondamento costituzionale. L'importanza della pronuncia rispetto all'evoluzione del concetto di riservatezza è sottolineata anche da F. MODUGNO, *I "nuovi diritti"*, cit., spec. 26, che vi legge il riconoscimento di un diritto che va oltre un mero profilo negativo della libertà di manifestazione del pensiero, in ragione di un concetto di riservatezza collegato alla «tutela dell'interiorità delle proprie convinzioni». La sostanziale marginalità dell'innovazione tecnologica nell'emersione del profilo dell'autodeterminazione informativa si evince anche dalla successiva sentenza 9 maggio 1985, n. 138, in *Giurisprudenza costituzionale*, 1985, 986 ss., commentata ancora una volta da A. CERRI, *Diritto di non ascoltare l'altrui propaganda*, nella quale la limitazione del diritto *de quo* passava, sì, attraverso un mezzo tecnico (i veicoli dotati di altoparlante), ma in realtà già ben conosciuto all'epoca e il cui ruolo, nella qualificazione in termini negativi della fattispecie, appare non rilevante.

[31] Scrive al riguardo C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, Napoli, 2018, 64, che «*la rivoluzione tecnologica ha inciso sulla stessa nozione di sfera privata*, che non concerne più, o non solo, i fenomeni di uscita delle informazioni dal proprio ambito di controllo, bensì coinvolge anche *i flussi dall'esterno verso l'interno*» (corsivi testuali).

[32] Almeno a partire dalle elezioni americane del 2012, secondo la ricostruzione di G. ZICCARDI, *Tecnologie per il potere*, Milano, 2019, 100 ss. Sul tema si veda anche la relazione a questo Convegno di Carlo Ferrajoli, *Rappresentanza e partecipazione politica*.

campagne mirate, specie per il consolidamento delle loro posizioni, tanto che oggi i canali *social* rappresentano fondamentali e potenti strumenti di formazione del consenso elettorale, giunti in noti casi ad influenzare in modo determinante l'esito di intere competizioni elettorali, attraverso l'operato di soggetti in grado di sfruttare con forza la grande capacità di penetrazione (e persuasione) di questa evoluzione tecnologica[33].

Peraltro, ho trattato distintamente i due profili della protezione dei dati e dell'autodeterminazione informativa non perché viaggino su binari paralleli, bensì al solo fine di sottolineare l'arricchimento progressivo degli elementi che compongono il diritto al nostro esame e porre in evidenza come l'intervento del legislatore abbia avuto l'ambizione di estendere gradualmente la tutela a tutti gli aspetti emergenti. Non si può però sottacere come, a buon diritto, da tempo la dottrina parli di autodeterminazione informativa, in generale, come diritto del singolo di decidere in quale modo configurare il rapporto della propria sfera privata con i terzi, sostanzialmente fondendo in questo concetto tanto la protezione dei dati quanto l'autodeterminazione informativa in senso stretto[34]. Posizione, questa, pienamente coerente non solo con il rilievo, già emerso, che si verte pur sempre nell'ambito di facoltà ascrivibili al diritto alla privacy in senso ampio, di cui costituiscono solo diverse declinazioni, ma anche con la stretta correlazione tra loro esistente, in quanto la tutela dell'una appare inestricabilmente legata alla garanzia per l'altra. È, infatti, attraverso il controllo sui dati che le società tecnologiche possono ricavare, grazie alla profilazione, informazioni su gusti, preferenze e comportamenti di massa, che poi vengono utilizzate per riproporre, più o meno insistentemente, al singolo individuo, in forma mirata sulla base del suo profilo, messaggi (commerciali, ma anche notizie di cronaca per esempio)

---

[33] Per portare un solo (ma celeberrimo) esempio, si pensi al caso di *Cambridge Analytica*, società nota per avere offerto consulenza a Donald Trump per la sua campagna elettorale, risultata poi vittoriosa, avendo a propria disposizione una enorme massa di dati di utenti di Facebook: tra la dottrina che ha preso in esame il caso, v., a titolo indicativo, D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda 'Cambridge Analytica'*, in *Federalismi.it*, n. 20/2018; nonché D. SUSSER – B. ROESSLER – H. F. NISSENBAUM, *Online Manipulation: Hidden Influences in a Digital World*, in *Georgetown Law Technology Review*, vol. 4, n. 1/2019, che inquadra la vicenda in ottica più generale. Sull'uso dei *social* e dei *big data* per finalità elettorali, tra i numerosi contributi, si vedano almeno quelli di M. CALISE – F. MUSELLA e di G. ZICCARDI, citati nelle note precedenti, che naturalmente dedicano spazio anche alla vicenda di cui sopra.

[34] Così, ad esempio, L. CALIFANO, *Il Regolamento*, cit., 12; o A. PAPA, *La problematica tutela del diritto all'autodeterminazione informativa nella* big data society, in Liber amicorum, cit., 477 ss. Maggiori perplessità suscitano, invece, quelle ricostruzioni ancora più ampie dell'autodeterminazione (come quella fatta propria da S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, spec. 319 ss.), in cui il concetto viene sostanzialmente a coincidere con la rivendicazione di un qualunque spazio di libertà, sulla scia del corrispondente della privacy americana. Sennonché, al riguardo, credo vada ribadito quanto su quest'ultima rilevava già A. BALDASSARRE, *Privacy e Costituzione*, Roma, 1974, 56, secondo cui «questo diritto tende inesorabilmente a sovrapporsi ad ogni situazione giuridica riconosciuta a protezione dell'integrità morale della persona», così che, come affermava G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Rivista diritto civile*, 1990, 867, la privacy negli Stati Uniti ha finito per svolgere la funzione del nostro art. 2 Cost. (nella sua lettura aperta). Né il decorso del tempo ha reso inattuale questa distinzione, giacché la vastità dell'accezione statunitense, che abbraccia, per esempio, le scelte di fine vita o in materia più generale di bioetica, resta estranea alla ben più puntuale definizione che la riservatezza, nei suoi pur variegati profili, ha nell'ordinamento italiano (ma, verrebbe da dire, più in generale nel costituzionalismo europeo).

che finiscono per cristallizzare preferenze ed opinioni e, in ultima istanza, ostacolare, appunto, la libertà di assumere in modo consapevole e pienamente informato le proprie determinazioni[35].

Insomma, dall'originaria tutela della riservatezza alla protezione dei dati personali fino all'autodeterminazione informativa, per limitarsi a citare i corsi principali di questa evoluzione senza perdersi nei tanti rivoli che questo flusso ha pure aperto in relazione ad aspetti più specifici, si evince come i singoli profili esaminati appaiono destinati ad integrarsi per «allargare e rafforzare le modalità di tutela della sfera privata, e la loro successione rivela il tentativo di un progressivo adeguamento ai mutamenti determinati dalle tecnologie dell'informazione e della comunicazione, per contrastarne gli effetti sul terreno del controllo, della classificazione e della selezione delle persone»[36].

2.2. Dall'identità personale al diritto all'oblio (passando per l'identità digitale)

Il diritto all'identità personale, inteso come «l'interesse del soggetto […] di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere riconosciuta con l'esplicazione dei criteri della normale diligenza e della buona fede oggettiva»[37] e quindi sulla base delle sue convinzioni culturali, ideologiche, religiose, ecc., e delle sue vicende umane e professionali[38], non ha un'origine strettamente legata all'uso delle tecnologie, dato che molte delle prime pronunce di merito, da cui è emerso questo diritto, traggono avvio da vicende giurisprudenziali relative al travisamento dell'immagine sociale di persone attraverso canali non innovativi, quali i manifesti elettorali piuttosto che la carta stampata e l'editoria tradizionale. Ciò nonostante, va dato altresì atto di come, dato il crescente numero di decisioni giudiziarie, specie negli anni '80, concernenti violazioni dell'identità attraverso il mezzo radiotelevisivo, già allora parte della dottrina ebbe a rilevare come il prorompere di questo diritto nelle aule giudiziarie potesse rappresentare «la contropartita negativa […] del progresso tecnologico dei mezzi di comunicazione»[39].

---

[35] Il circolo vizioso che si autoalimenta tra raccolta di dati a fini di profilazione e successiva utilizzazione ai fini di ridurre l'autodeterminazione informativa è ben evidenziato, *ex plurimis*, da L. CALIFANO, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, n. 16/2019, 3.

[36] Testualmente, S. RODOTÀ, *Tecnopolitica*, Roma-Bari, 2004, 168.

[37] Cfr., Cass. Civ., sez. I, 22 giugno 1985, n. 3769, in *Foro italiano*, 1985, I, 2211 ss.

[38] Anche sull'identità personale la bibliografia è ormai assai copiosa. Per la dottrina che per prima ha individuato il tema cfr. A. DE CUPIS, *Il diritto all'identità personale, Parte I. Il diritto al nome*, Milano, 1949, spec. 13, ove l'A. sottolinea come sia un bisogno connaturato all'uomo quello di «affermare la propria individualità distinguendosi dagli altri soggetti […] non soltanto come persona, ma anche come *una certa* persona» (corsivo mio). Più di recente v., *ex multis*, V. ZENO ZENCOVICH, *Identità personale*, in *Digesto Discipline Privatistiche – sezione civile*, vol. IX, Torino, 1993, 294 ss.; e L. TRUCCO, *Introduzione*, cit., in particolare 207 ss. per la ricostruzione dell'evoluzione del diritto.

[39] Sono queste le parole di F. MANTOVANI, *Il diritto all'identità personale e la tutela penale*, in *Il diritto all'identità personale*, Padova, 1981, 130, il quale leggeva pertanto nell'affermazione del diritto una rivendicazione proprio della protezione dai riflettori tecnologici. La questione è oggetto di approfondimento da parte di L. TRUCCO, *Introduzione*, cit., 217 ss., la quale dà conto anche delle coeve opinioni dottrinarie volte invece a sminuire questo aspetto per le ragioni citate nel testo.

Ad ogni modo, è certo che, quando, nel 1985, il diritto all'identità personale troverà espresso riconoscimento in sede di legittimità, allorché la Cassazione si pronuncerà in relazione al travisamento dell'identità personale del noto oncologo Umberto Veronesi[40], il mezzo attraverso cui il messaggio pubblicitario che aveva determinato la violazione del diritto era stato diffuso (ovvero la stampa periodica) non assumerà, in effetti, una sostanziale importanza nell'orientare la Suprema Corte[41].

Lo sviluppo tecnologico – e segnatamente delle tecnologie digitali e della rete internet – ha tuttavia inciso, in tempi successivi, in modo non meno significativo su questo diritto di quanto abbiamo visto essere avvenuto con riferimento alla riservatezza.

In primo luogo, infatti, la moltiplicazione dei frammenti della personalità individuale che vengono lasciati in rete[42], più ancora di quanto già non avvenga nella realtà materiale, ha indotto ormai a non parlare più (solo) di identità personale, ma anche di identità *digitale*[43], peraltro quale profilo da giustapporre a quello primigenio e non sostituivo (né mera proiezione) di esso. In sostanza, la rete, attraverso la frammentazione e successiva ricomposizione della personalità di un individuo, offre una rappresentazione (*rectius*, più rappresentazioni), che danno vita a proiezioni il più delle volte parziali e in ogni caso legate a contesti specifici[44], ma proprio per questo motivo facilmente non (del tutto) veritiere e pertanto meritevoli di formare oggetto di tutela[45].

In secondo luogo, l'incidenza delle tecnologie digitali sull'identità personale si manifesta in relazione a quel particolare (e di più recente emersione) profilo di essa, che è rappresentato dal diritto all'oblio, ovvero il diritto a che non siano oggetto di pubblicità eventi passati relativi alla vita di una persona, salvo sussista un perdurante interesse pubblico al mantenimento di essa. Una situazione soggettiva che si pone al crocevia, a ben vedere, tra riservatezza e identità, ma che a mio avviso merita di essere attratta nell'orbita di quest'ultima, per il fatto che essa è pur sempre finalizzata a garantire e proteggere l'immagine sociale del suo titolare, ancorché in relazione a fattispecie passate e non a comportamenti attuali[46]. Gli eventi trascorsi, in effetti, potrebbero

---

[40] Di cui era stata utilizzata una frase al di fuori del contesto specifico dell'intervista nella quale era stata pronunciata, travisandone il significato. La sentenza, già citata a nota 37, è stata commentata, tra gli altri, da F. MACIOCE, *L'identità personale in Cassazione: un punto di arrivo e un punto di partenza*, e M. DOGLIOTTI, *Il diritto all'identità personale approda in Cassazione*, entrambi in *Giustizia civile*, 1985, I, 3055 ss.

[41] Si noti, per inciso, che anche il *leading case* in materia della Consulta (la sentenza 3 febbraio 1994, n. 13), in cui si dibatteva del cognome come elemento distintivo della persona, verteva in ambito affatto estraneo al contesto tecnologico.

[42] Cfr. C. COLAPIETRO, *Il diritto*, cit., 35, ove l'A. afferma che «le nuove tecnologie tendono […] a *frantumare la personalità umana* che viene ridotta ad un'informazione parziale […] *resa acquisibile inconsapevolmente per mezzo di strumenti elettronici*» (corsivi testuali).

[43] In tema, tra i lavori ormai copiosi, v. G. RESTA, *Identità personale e identità digitale*, ne *Il diritto dell'informazione e dell'informatica*, 2007, 511 ss.; e G. ALPA, *L'identità digitale e la tutela della persona*, in *Contratto e impresa*, 2017, 723 ss.

[44] Il rischio che la profilazione degli individui e la frammentazione dei profili attinenti alla loro personalità in tante distinte immagini porti a travisare la reale personalità – e quindi a lederne l'identità – veniva denunciato già da G. RESTA, *Identità personale*, cit., 522.

[45] G. FINOCCHIARO, *Identità personale (diritto alla)*, cit., 737 ss.

[46] Non si tratta, tuttavia, di una ricostruzione pacifica in dottrina. Per la tesi che sostengo nel testo, cfr., tra gli altri, L. TRUCCO, *Introduzione*, cit., 266, che la ritiene una conclusione non implausibile; nonché L. FEROLA, *Riservatezza, oblio, contestualizzazione: come è mutata l'identità personale nell'era di Internet*, in F. PIZZETTI (a cura

descrivere in modo improprio ed inattuale l'identità di una persona, che tutto è fuorché statica ed immutabile[47], di modo che, in assenza del riconoscimento del diritto all'oblio, l'esistenza di un individuo rischierebbe di essere indelebilmente condizionata da fatti che non rispecchiano (più) il complesso di elementi che contribuiscono a definirne la personalità. Ora, questo particolare profilo di cui andiamo trattando, di per sé, ha indubbiamente una sua consistenza anche al di fuori del mondo digitale[48], sennonché appare innegabile come proprio in questo contesto i rischi per la sua garanzia appaiano di gran lunga maggiori. La rete, infatti, non dimentica[49], e la possibilità che un individuo possa liberarsi di ingombranti fardelli passati, che non rispecchiano la sua attuale personalità, è di assai difficile realizzazione, per due ordini di ragioni.

Anzitutto, la stessa conservazione delle notizie sostanzialmente *sine die*, che abbiamo visto caratterizzare l'internet, conduce verso un punto di convergenza tra il diritto all'oblio e l'identità digitale. Certo, le due nozioni non devono confondersi, giacché l'oblio si riferisce alla ripubblicazione di notizie a suo tempo legittimamente pubblicate, mentre l'identità in rete trascende dal singolo dato, che di essa è solo un frammento, per guardare all'immagine della persona per come esce dal web nel suo complesso[50]. Tuttavia, è pur vero che è la stessa facilità di

---

di), *Il caso*, cit., 177 ss., per la quale l'interesse all'oblio e quello all'identità personale «si fondono in un'unica dimensione». *Contra*, vi è chi, come M. MEZZANOTTE, *Il diritto*, cit., 81 ss., parla di un diritto, che costituisce il moderno sviluppo della privacy, ma autonomo e distinto tanto dal diritto alla riservatezza quanto da quello all'identità (analogamente, seppure con toni più sfumati, M. R. MORELLI, *Oblio (diritto all')*, in *Enc. Dir., Aggiornamento VI*, Milano, 2002, spec. 851 ss.); mentre altri (come C. COLAPIETRO – A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO – C. COLAPIETRO, *Innovazione*, cit., 128; o M. A. LIVI, *Quale diritto all'oblio?*, Napoli, 2020, 68 ss.) lo considerano parte del diritto alla protezione dei dati personali; laddove non manca neppure chi, come F. PIZZETTI, *Il prisma*, cit., 30 ss., preferisce ascriverlo al diritto alla riservatezza nel contesto della sfera più ampia di tutela della dignità della persona.

[47] Ciò che, peraltro, induce G. RESTA, *Identità personale*, cit., 524 a parlare della identità come processo e non come dato preesistente. L'A., peraltro, richiama al riguardo la pregressa giurisprudenza del Garante, volta proprio a garantire la corretta rappresentazione della persona in senso diacronico.

[48] E, in effetti, ivi trae i suoi primi riconoscimenti giurisprudenziali negli anni '90, in cui la materia del contendere riguardava violazioni del diritto all'oblio attraverso il mezzo televisivo o la tradizionale pubblicazione a stampa. Per una accurata ricostruzione in questo senso cfr., tra gli altri, A. MANTELERO *Il diritto all'oblio dalla carta stampata ad internet*, in F. PIZZETTI (a cura di), *Il caso*, cit., 145 ss.; nonché M. MEZZANOTTE, *Il diritto*, cit., spec. 112 ss., il quale ricorda comunque come esso condivida con il diritto alla riservatezza «uno sviluppo con il progresso ed il perfezionamento degli strumenti tecnologici che hanno permesso una maggiore invasività della sfera della persona».

[49] Come sottolinea G. FINOCCHIARO, *Identità personale (diritto alla)*, cit., 735, segnalando come il diritto all'oblio, che è gemmato dall'identità personale, al pari di essa è figlio della comunicazione e «vive una nuova vita» su internet. Sul tema della "memoria digitale", in una prospettiva più ampia, si vedano le interessanti riflessioni di V. MAYER-SCHÖNBERGER, *Delete. Il diritto all'oblio nell'era digitale* [2010], trad. it. di P. Conversano, Milano, 2013, spec. 104 ss., ove l'A. evidenzia vantaggi e limiti della capacità di memorizzazione incommensurabilmente ampia dell'ambiente digitale.

[50] Secondo quanto rileva G. FINOCCHIARO, *Identità personale su internet: il diritto alla contestualizzazione dell'informazione*, ne *Il diritto dell'informazione e dell'informatica*, 2012, spec. 386 ss. nel commentare la nota sentenza della Corte di Cassazione, sez. III, 5 aprile 2012, n. 5525, relativa, ancora una volta, ad un caso di reperibilità *on line* di una imputazione finale, finita poi in assoluzione, al contrario difficilmente rinvenibile nella rete. In tema, si veda anche l'efficace sintesi di L. FEROLA, *Conservazione, indicizzazione e rintracciabilità dei dati, tra diritto all'oblio e dovere di trasparenza*, in L. CALIFANO – C. COLAPIETRO, *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014, 245, per la quale il diritto all'oblio, in rete, non può essere confinato a «un mero diritto a dimenticare o cancellare informazioni risalenti nel tempo, alterando la realtà dei fatti» consistendo invece nella legittima pretesa ad «inquadrare il dato nel tempo per non essere segnati da una "lettera scarlatta" digitale e indelebile».

reperimento di informazioni non più attuali che, oltre a violare il primo, compromette la corretta realizzazione della seconda, così come, specularmente, la garanzia del primo è presupposto fondamentale perché non si abbia lesione nemmeno della seconda. Del resto, è la stessa dinamicità della personalità, come sottolineavo, ad esigere una tutela per il diritto all'oblio e la rete in questo genera problematicità non trascurabili, per il fatto che le informazioni in essa contenute sono, assai spesso, avulse dal loro contesto complessivo di riferimento. Da qui, dunque, emerge quell'ulteriore profilo dell'oblio meritevole di tutela, quale è il diritto alla contestualizzazione, ovvero la pretesa a che le notizie e le vicende pubblicate sul web siano integrate al fine di assicurare una rappresentazione completa del quadro in cui si inseriscono e quindi maggiormente rispondente alla personalità dell'interessato[51].

Non solo, ma, poiché ogni informazione in internet viene moltiplicata, attraverso la possibilità di dare vita a collegamenti, di archiviare notizie e ripubblicarle, nonché di indicizzarle in modo tale che sia possibile ritrovarle, anche in modo casuale e a distanza di molto tempo, l'oblio non può più passare solo attraverso il divieto di ripubblicazione di fatti relativi alla propria vita passata, ma acquista l'ulteriore profilo di diritto alla deindicizzazione, ovvero a rimuovere la possibilità, attraverso *link* e motori di ricerca, che quelle stesse notizie possano essere ritrovate in ulteriori spazi del web rispetto a quelli in cui originariamente erano apparse. Proprio questo è il caso affrontato in quello che forse è il più famoso precedente giurisprudenziale in materia, ovvero la sentenza *Google Spain*, con cui la Corte di Giustizia UE ha imposto, a tutela di questo diritto e valendosi della normativa allora vigente a protezione dei dati personali, ai motori di ricerca di impedire il collegamento alla persona interessata di una notizia risalente per la quale non ci sia alcun interesse che ne giustifichi la perdurante attualità, e questo anche laddove la notizia stessa sia legittimamente pubblicata *on line* (nel caso di specie, nell'archivio storico di una testata giornalistica)[52].

In questo senso, può dunque concludersi, con le parole della Suprema Corte[53], che «quando si parla di diritto all'oblio ci si riferisce, in realtà, ad almeno tre differenti situazioni: quella di chi desidera non vedere nuovamente pubblicate notizie relative a vicende, in passato legittimamente diffuse, quando è trascorso un certo tempo tra la prima e la seconda pubblicazione; quella, connessa all'uso di internet ed alla reperibilità delle notizie nella rete, consistente nell'esigenza di

---

[51] Cfr. G. FINOCCHIARO, *Identità personale su internet*, cit., 389 ss., che sottolinea come questo bisogno di tutela emerga in relazione alla circostanza che le informazioni reperibili sul web appaiono "appiattite". In tema, ampiamente, tra gli altri anche F. PIZZETTI, *Il prisma*, cit., 37 ss., che lega l'espansione di questa esigenza di tutela a «lo svilupparsi senza sosta delle tecnologie, il passaggio al *web 2.0* e l'esplosione dei *social networks* e degli strumenti mobili per connettervisi».

[52] Sulla sentenza, oggetto di un numero cospicuo di commenti, si vedano almeno quelli raccolti in G. RESTA – V. ZENO ZENCOVICH, *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015. Peraltro, la questione oggetto della pronuncia è analoga a numerosi precedenti, affrontati anche dal Garante per la protezione dei dati personali già diverso tempo addietro: maggiori notizie in P. COSTANZO, *Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutela dei diritti?*, in *Diritto dell'internet*, 2006, 548. Per gli sviluppi giurisprudenziali successivi a *Google Spain* ed in particolare le sentenze della Corte di Giustizia UE nelle cause C-136/17 e C-507/17, che hanno affrontato il tema della estensione territoriale del diritto all'oblio e conseguentemente della sua effettività nella rete globale, v. O. POLLICINO, *L'"autunno caldo" della Corte di Giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, n. 19/2019.

[53] Cass. Civ., sez. unite, sentenza 22 luglio 2019, n. 19681, in *Foro italiano*, 2019, I, 3071.

collocare la pubblicazione, avvenuta legittimamente molti anni prima, nel contesto attuale […]; e quella, infine, trattata nella citata sentenza *Google Spain* della Corte di giustizia dell'Unione Europea, nella quale l'interessato fa valere il diritto alla cancellazione dei dati»: ciò che dimostra come il riconoscimento di una nuova istanza quale effetto dell'innovazione tecnologica sia spesso al contempo anche la causa di ulteriori evoluzioni successive[54].

3. Il contesto ordinamentale vigente: alcune premesse

La, pur rapida, rassegna svolta, in chiave diacronica, sui due diritti oggetto della presente trattazione mi consente di partire, nell'analizzare il quadro normativo vigente, da due considerazioni di ordine generale.

La prima è che, nel contesto tecnologico e vieppiù nell'era del digitale, tanto la privacy quanto l'identità personale hanno abbandonato quel loro (supposto) originario sapore elitario e in qualche misura borghese, che per la riservatezza aveva rappresentato, insieme alla sua sostanziale novità rispetto alle precedenti esperienze costituzionali europee, un significativo ostacolo al suo riconoscimento esplicito nella Carta fondamentale[55], per rivelarsi quali bisogni comuni a tutti[56], perdendo, di conseguenza, anche la primigenia dimensione tipicamente privatistica, per assumere i connotati di un problema di rilevanza (anche) pubblicistica[57]. E così, parimenti, la loro tutela passa gradualmente dal piano strettamente individuale[58] a quello collettivo[59], da cui l'approvazione di leggi generali sulla protezione dei dati[60].

---

[54] In questo senso A. D'ALOIA, *Introduzione*, cit., XXVII.

[55] L'osservazione si deve ad A. BARBERA, *Art. 2*, in *Principi fondamentali. Art. 1-12*, in G. BRANCA (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 1975, spec. 55 ss., ove l'A. aggiunge, quale probabile ulteriore spiegazione, la generale arretratezza del Paese, la quale rendeva meno pressante che altrove la tutela di questo diritto.

[56] Il giudizio è alquanto ricorrente in dottrina; per la riservatezza, *ex plurimis*, cfr. M. G. LOSANO, *La privacy nelle legislazioni europee*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati. Aspetti giuridici e sociali*, Bologna, 1981, 51 ss.; nonché, più recentemente, A. BALDASSARRE, *Globalizzazione contro democrazia*, Roma-Bari, 2002, 257; per l'identità personale, v. V. ZENO ZENCOVICH, *Identità*, cit., 303.

[57] Con lungimiranza l'osservazione fu avanzata da S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 39 ss.

[58] Osserva al riguardo C. DE GIACOMO, *Diritto*, cit., 14, come la nozione di privacy (e i diritti che le ruotano intorno) non poteva attecchire che in ordinamenti liberali fondati su una visione individualistica di stampo lockiano. Il legame tra il pensiero liberale di Locke e la nascita della privacy è analizzato anche da M. MEZZANOTTE, *Il diritto*, cit., 40 ss.; e da A. ETZIONI, *The Limits of Privacy*, New York, 1999, 194 ss., il quale sottolinea come l'attuale prevalenza nella cultura dominante della dimensione individuale della privacy rispetto all'interesse generale si spieghi proprio per l'origine liberale del diritto in questione.

[59] Analogamente, G. BUSIA, *Riservatezza*, cit., 479, il quale afferma che la riservatezza «cessa di essere un diritto individuale […] per assumere una dimensione sociale».

[60] In Italia, in realtà, come noto, solo molto tempo dopo l'introduzione delle prime tecnologie informatiche, dato che la prima legge organica è la l. 31 dicembre 1996, n. 675, sulla quale, per tutti, G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997; E. GIANNANTONIO – M. LOSANO – V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali: commentario alla L. 675/1996*, Padova, 1999; A. LOIODICE – G. SANTANIELLO (a cura di), *La tutela della riservatezza*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, vol. XXVI, Padova, 2000; nonché M. G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001.

La seconda considerazione è che la questione dell'uso che viene fatto dei dati personali assume ormai una dimensione trasversale a tutti gli ambiti in cui si esplica la vita delle persone, di modo che il problema di fronteggiare questa pervasività con adeguate garanzie di controllo, da parte dell'individuo, sulle proprie informazioni coinvolge l'intero ordinamento ed impegna il legislatore su una molteplicità di fronti contemporaneamente[61], richiedendo una risposta di carattere, appunto, necessariamente sistematico. Pertanto, non solo tutele frammentarie come quelle che l'ordinamento italiano forniva prima del 1996[62] sarebbero assolutamente impensabili oggigiorno, ma, più in generale, le situazioni soggettive qui considerate esigono forme di garanzia che travalichino ambiti specifici settoriali e rispondano ad un'impostazione coerente ed universale.

In effetti, un fondamentale intervento normativo di questi anni, che ha rivoluzionato in larga parte una disciplina, sovranazionale e nazionale, risalente ad un passato (seppure prossimo) in cui lo sviluppo del digitale aveva dimensioni incomparabilmente inferiori a quelle attuali[63], è stato attuato dal legislatore eurounitario, proprio in una prospettiva di carattere generale. Mi riferisco al noto Regolamento (UE) 2016/679 del Parlamento e del Consiglio, che esplicita tale sua caratteristica fin dalla stessa intitolazione come *Regolamento* generale *sulla protezione dei dati*[64], e che è stato poi integrato dalle normative nazionali, sulla base delle previsioni della stessa disciplina sovranazionale, che rinvia esplicitamente alla legislazione interna per determinati profili e in relazione ad alcuni ambiti specifici[65].

---

[61] Tanto che P. PASSAGLIA, Privacy *e nuove tecnologie, un rapporto difficile. Il caso emblematico dei* social media*, tra regole generali e ricerca di una specificità*, in *Consulta OnLine*, 2016, 332 ss., indica questa «proliferazione di frontiere operative», insieme alla efficacia scemante degli strumenti giuridici di garanzia e alla incessante evoluzione tecnologica (e, più ampiamente, del contesto sociale), come una delle ragioni per le quali «trattare della *privacy* in rapporto alle nuove tecnologie è esercizio quanto mai arduo […] giacché la multiformità degli ambiti interessati sarebbe tale da richiedere un esame grandangolare della disciplina della *privacy*».

[62] Antecedentemente all'adozione della prima legge generale sulla privacy, infatti, non vi era un totale vuoto normativo, potendosi, al contrario, registrare una serie di sporadici interventi, pur sempre, però, di carattere episodico (o estemporaneo, come li qualifica G.M. SALERNO, *La protezione*, cit., 619), nell'ambito di discipline di settore, a tutela della riservatezza, i quali, a giudizio di P. COSTANZO, *La dimensione costituzionale della privacy*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Milano, 2008, 52, avrebbero rappresentato «figure sintomatiche» di un qualche riconoscimento del diritto in questione nella legislazione ordinaria. Per limitarci a qualche esempio, si può citare l'art. 4 della legge n. 300 del 1970, il c.d. Statuto dei diritti dei lavoratori, in tema di controlli a distanza, o all'art. 9 del d. lgs. 322 del 1989, che pone qualche garanzia di privacy nelle rilevazioni statistiche od ancora all'art. 24 della legge n. 241 del 1990, che annovera la riservatezza tra le possibili ragioni di limitazione del diritto di accesso. Mi sia consentito, per un'analisi di questi frammenti di tutela, rinviare a S. SCAGLIARINI, *La riservatezza*, cit., spec. 65 ss.

[63] Per un'analisi delle ragioni della sopravvenuta vetustà della disciplina precedente, v., *ex plurimis*, F. PIZZETTI, *Privacy*, cit., 36 ss., nonché 73 ss. per una sintesi del contenuto di quel *corpus* normativo.

[64] Nel seguito l'atto sarà citato anche con il suo acronimo inglese, invalso ormai nell'uso, di GDPR o, semplicemente, come Regolamento. Peraltro, questa connotazione in termini generali dell'atto non ne impedisce la specificazione in relazione a settori particolari, come previsto con la proposta di "Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE" (cd. Regolamento e-privacy) la quale, presentata nel 2017, ha ottenuto l'approvazione del Consiglio, avviando l'iter alla sua fase finale, nel febbraio del 2021. Per mera completezza, ricordo che l'Unione europea ha contribuito a definire il quadro complessivo del trattamento dei dati anche con l'adozione del *Regolamento del Parlamento europeo e del Consiglio 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*.

[65] Si legge infatti nel *Considerando* n. 10 che «Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme» e «non esclude che il diritto degli Stati membri stabilisca le condizioni

Non deve, peraltro, stupire che la regolazione in materia di protezione dei dati provenga (peraltro già da prima, con la direttiva 95/46/CE che il GDPR abroga) dalle Istituzioni dell'Unione, dato che, se è vero che trattiamo di situazioni soggettive fortemente condizionate dalla tecnologia (e normate proprio in vista dell'ulteriore, auspicato, sviluppo dell'economia digitale[66]), è evidente che sarebbe illusorio e fuorviante qualunque tentativo di intervento regolatorio nazionale[67], laddove non vi è fenomeno più "mobile" e atopico della tecnologia[68], tanto più di quella connessa al mondo digitale ed alla rete internet.

Ebbene, nel merito dell'atto normativo, che ovviamente non mi è possibile ricostruire se non con il mero richiamo di alcune previsioni paradigmatiche, credo non vi sia dubbio sul fatto che il Regolamento si ispiri, almeno nelle intenzioni, ad una forte tutela per i diritti qui presi in esame, in tutte le facoltà ad essi ascrivibili che ho in precedenza cercato di enucleare, ed introduca strumenti importanti a loro garanzia, che tuttavia scontano anche criticità per nulla trascurabili.

Cercherò di dare conto di quanto sopra, evidenziando dapprima, con l'aiuto di qualche esempio che credo possa essere utile, i pregi che il GDPR può vantare come strumento a difesa dei diritti *de quibus*, per poi fissare l'attenzione sugli aspetti problematici di questa regolazione.

3.1. Privacy e identità digitale nella normativa europea (ed integrativa nazionale)

Il quadro ordinamentale vigente, composto, come si è detto, dall'atto generale di origine sovranazionale e dalle normative interne di integrazione, offre forme di garanzia in relazione ad entrambe le situazioni soggettive di nostro interesse, proseguendo in quella tutela congiunta di

---

per specifiche situazioni di trattamento». Su tale (anomala per il tipo di fonte) caratteristica del Regolamento, si veda L. CALIFANO, *Il Regolamento*, cit., 17 ss.; nonché, volendo, S. SCAGLIARINI, *Dal "vecchio" al "nuovo" Codice della privacy*, in ID. (a cura di), *Il "nuovo" Codice in materia di protezione dei dati personali*, Torino, 2019, 1 ss., anche per ulteriori riferimenti normativi e dottrinari.

[66] Come dimostrato, a tacer d'altro, dal *Considerando* n. 7 del GDPR, ove di parla della «importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno» e dall'art. 1, paragrafo 3, che conferma la doppia anima dell'atto normativo, volta a garantire anche la *libera circolazione* dei dati. Questo aspetto di novità è posto in evidenza da C. COLAPIETRO, *Il diritto*, cit., 45, che sottolinea il conseguente passaggio da una tutela fondamentalmente statica e negativa ad una dinamica, coerente con la realtà dell'interconnessione globale.

[67] L'osservazione è unanimemente condivisa: per tutti, v. P. PASSAGLIA, Privacy, cit., 334. Ricordo, per inciso, che una regolazione a livello internazionale per la protezione dei dati è alquanto risalente. Già il 28 gennaio 1981, infatti, veniva adottata in seno al Consiglio d'Europa, la Convenzione n. 108 (su cui v., per esempio, G. BUQUICCHIO, *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in N. MATTEUCCI (a cura di), *Privacy*, cit., 67 ss.; e G. BUTTARELLI, *Banche dati*, cit., 8 ss.), la quale significativamente interveniva proprio, alla luce del mutato quadro tecnologico per la «protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale». La Convenzione in parola, peraltro, è stata oggetto di un Protocollo di emendamento approvato il 10 ottobre 2018 (ratificato dall'Italia con la l. 22 aprile 2021, n. 60), al fine di renderla più adeguata ad un contesto così diverso da quello per il quale era stata originariamente elaborata, peraltro seguendo la falsariga del Regolamento UE.

[68] Il rilievo circa la natura atopica della tecnologia emerge, come ovvio, da tempo; rinviamo, in ogni caso, per tutti, alle pagine di N. IRTI, *Norme e luoghi*, Roma-Bari, 2001, spec. 61 ss. Con specifico riferimento alla necessità di un intervento sovranazionale nell'ambito di nostro interesse, si vedano, di recente, le osservazioni di L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in L. CALIFANO – C. COLAPIETRO, *Innovazione*, cit., 205.

esse, che, almeno nel nostro Paese, si ritrova fin dalla prima legislazione in materia[69] e che trae fondamento nella contiguità delle stesse cui accennavo in apertura di queste note.

(A) Anzitutto, per quanto riguarda il profilo della protezione dei dati, appare evidente come la tutela di esso costituisca l'oggetto stesso dell'atto normativo e sia, pertanto, *in re ipsa*. Volendo citare solo qualche esempio delle garanzie che il Regolamento offre al riguardo, si possono richiamare, tra i principi fondamentali (e che assumono una valenza trasversale nel contesto complessivo dell'atto) enunciati dall'art. 5 del GDPR[70]: 1) il principio di liceità del trattamento, per cui si può procedere ad una qualunque operazione sui dati soltanto ove vi sia una base giuridica, tra quelle indicate negli articoli 6 (in generale), 9 (per i dati particolari) e 10 (per i dati giudiziari) del GDPR[71], che costituisca un titolo idoneo per procedervi[72]; 2) il principio di minimizzazione, in forza del quale andranno trattati i soli dati adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità indicate dal titolare, incorporando le esigenze di protezione in parola fin dalla progettazione di un qualunque processo che comporti un trattamento di dati, così da ridurre al minimo il ricorso ad essi (la c.d. privacy *by design* e *by default* di cui all'art. 25 del medesimo atto normativo[73]); 3) il principio di trasparenza, il quale non solo impone che l'interessato sia reso edotto del trattamento dei suoi dati, ma stabilisce altresì l'obbligo di informarlo adeguatamente circa le operazioni che su questi vengono svolte, la durata e le modalità delle stesse, nonché la possibilità di esercitare i diritti ad esso conferiti dal Regolamento (artt. 13 e 14 GDPR[74]); 4) il principio di responsabilizzazione (o *accountability*), che rappresenta la cifra caratteristica e il *fil rouge* che percorre, in filigrana, l'intero testo normativo, al fine di valorizzare il ruolo del titolare, chiamato a svolgere, prima di iniziare il trattamento e già nella fase di

---

[69] Già l'art. 1, comma 1, della legge n. 675 del 1996 (ripreso in realtà anche dall'art. 2 del d. lgs. n. 196 del 2003, nella sua versione originaria), infatti, affermava che «la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, *con particolare riferimento alla riservatezza e all'identità personale*» (corsivo mio). In dottrina, per un commento su questi aspetti, G. SANTANIELLO, *Il sistema delle garanzie della privacy (profili introduttivi)*, in A. LOIODICE – G. SANTANIELLO (a cura di), *La tutela*, cit., spec. 8, ove l'A. rileva come «la compresenza di queste due sfere di interessi […] fa del diritto sui dati personali un *novum*, in cui si saldano pretese di segno negativo (rivolte a impedire, a non far conoscere ad altri) e pretese di segno positivo (indirizzate a far fare, a far conoscere in un certo modo); e G. B. FERRI, *Privacy, libertà di stampa e dintorni*, in V. CUFFARO – V. RICCIUTO – V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, spec. 49 ss.

[70] Sui quali, in generale, si vedano, tra i tanti, i commenti puntuali di C. COLAPIETRO, *Il diritto*, cit., 75 ss.; e M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 179 ss.

[71] Eventualmente integrato dalla legislazione nazionale, ove la base giuridica si rinvenga in un obbligo legale o nell'esecuzione di un compito di pubblico interesse. Nel nostro ordinamento, sul punto, si vedano per esempio le previsioni di cui agli artt. 2/*ter*, 2/*sexies* e 2/*octies* del Codice privacy come novellato, da ultimo, dal d. lgs. n. 101 del 2018 per adeguarlo al mutato quadro europeo.

[72] Su tale principio, per tutti, v. F. BRAVO, *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 101 ss.

[73] Per un approfondimento sul punto, tra i tanti, v. F. SARTORE, Privacy-by-design*, l'introduzione del principio nel* corpus *del GDPR*, in R. PANETTA (a cura di), *Circolazione*, cit., 295 ss.

[74] Rispetto ai quali F. PIZZETTI, *Privacy*, cit., 270 ss., evidenzia come la distinzione che, con riferimento all'informativa, viene fatta tra interessati adulti e minori lascia percepire più di ogni altra previsione il concetto forte di trasparenza adottato dal GDPR. Per inciso, è d'uopo osservare che al medesimo principio può essere direttamente ricondotto (almeno) anche il diritto di accesso disciplinato dall'art. 15 del Regolamento.

progettazione di questo, un'attenta analisi, anche attraverso alcuni strumenti, come per esempio la valutazione di impatto, cui farò cenno più avanti, o la tenuta del registro od ancora la nomina di un Responsabile per la protezione dei dati[75], sui rischi per i diritti e le libertà degli interessati derivanti dal trattamento[76]. Su quest'ultimo punto, peraltro, merita di essere ricordato come, in alcuni casi (si pensi per esempio alle ipotesi in cui la base giuridica è data da un legittimo interesse[77]) il titolare sia chiamato a svolgere un vero e proprio bilanciamento tra l'interesse al trattamento e quelli contrapposti dei soggetti cui i dati si riferiscono[78], onde individuare quello prevalente. Fermo restando che, in ogni caso, dalla responsabilizzazione discendono tanto l'obbligo di predisporre misure di sicurezza proporzionali e adeguate al livello di rischio, quanto un (almeno per molte ipotesi ed in linea teorica[79]) severo apparato sanzionatorio, nel quale l'entità della "pena" fa da contraltare alla fiducia riposta nel corretto operare del titolare.

Ma anche l'autodeterminazione informativa è un profilo della cui tutela la normativa eurounitaria si fa carico, non solo in via indiretta, giacché attraverso il controllo sui propri dati evidentemente si impedisce anche che il flusso di informazioni in entrata avvenga senza regola alcuna, ma anche in via diretta, come oggetto principale di talune previsioni. Si pensi, ad esempio, all'art. 21 del GDPR, che disciplina il diritto di opposizione (con previsioni specifiche in tema di comunicazioni per finalità di marketing) od all'art. 130 del Codice della privacy, che appresta una tutela per il caso di comunicazioni indesiderate, quale fenomeno tipico di (sempre più facile) ingerenza tecnologica sulla riservatezza personale.

(B) Il Regolamento europeo, nonostante il titolo non vi faccia riferimento, contiene tuttavia, come dicevo, anche norme a garanzia dell'identità personale.

In questo contesto, per esempio, il divieto di profilazione, sancito dall'art. 22 del GDPR, è volto, tra l'altro, anche a proteggere l'identità in rete, evitando quella frammentazione che potrebbe

---

[75] La nomina del *Data Protection Officer* è considerata misura a garanzia dell'accountability, per esempio, da L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il Regolamento privacy europeo*, Milano, 2016, 330.

[76] Senza pretesa di completezza, al principio di *accountability*, oltre a quanto indicato nel testo, possono essere ricondotte almeno anche le previsioni del GDPR sugli obblighi in caso di contitolarità (art. 26), sulla nomina di un Responsabile (art. 28), sulle notifiche e comunicazioni in caso di *data breach* (artt. 33 e 34), sulle certificazioni e i codici di condotta (artt. 40-43), nonché, *last but not list*, sulla privacy *by design*, cui ho già fatto cenno, ma sulla quale tornerò brevemente più avanti nel testo.

[77] Per indicazioni su questo specifico *balancing test*, v., ad esempio, L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il Regolamento*, cit., 297 ss.

[78] Tanto che, al riguardo, F. BRAVO, *Il consenso*, cit., 176, legge nel GDPR l'emersione di un vero e proprio diritto a trattare i dati altrui laddove sussistano interessi meritevoli. In ottica analoga, C. COLAPIETRO – A. IANNUZZI, *I principi generali*, cit., 87, sottolineano come il GDPR non si ponga più nella prospettiva della mera protezione dell'interessato attraverso l'esclusione da interferenze altrui, bensì si indirizzi verso una tutela dinamica che segue il dato nella sua libera circolazione, quale obiettivo di non minore portata perseguito dal testo normativo.

[79] Giacché come si ricava dalla *Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP))*, forte sembra sia la difformità decisionale tra le singole Autorità nazionali (talora, come nel caso di quella irlandese, territorialmente competente sulla maggior parte delle multinazionali operanti in rete, propense più ad utilizzare poteri correttivi che sanzionatori) sia la difficoltà, lamentata unanimemente dagli stessi Garanti, a svolgere tutte le funzioni loro assegnate, per carenza di risorse umane e strumentali. Proprio rispetto a quest'ultima criticità, peraltro, la Risoluzione parlamentare suggerisce, al punto 16, l'introduzione di una tassa europea sul web, i cui introiti potrebbero concorrere a finanziare le funzioni di controllo.

ingenerare ricostruzioni parziali e, per ciò solo, inesatte della personalità individuale[80]. Ma, a ben vedere, anche il complesso di norme, tese a garantire che i dati siano integri, corretti ed aggiornati, è indirizzato a scongiurare il rischio che, da informazioni non (del tutto) esatte, possa essere travisata l'identità dell'interessato. Si vedano, in questo senso, le disposizioni sul diritto di rettifica (art. 16 del GDPR)[81] o su quello di limitazione del trattamento[82], specialmente allorché sia esercitato nelle more della verifica sull'esattezza dei dati (art. 18, par. 1, lett. a) del GDPR), od ancora l'obbligo di notifica ai destinatari che l'art. 19 del Regolamento pone a carico del titolare, qualora venga esercitata una delle due facoltà di cui sopra.

Nemmeno il diritto all'oblio, peraltro, è trascurato dal legislatore europeo, che anzi ad esso dedica una disposizione specifica, la quale reca la dizione "diritto all'oblio" già in rubrica, e cioè l'art. 17[83], ove si afferma, invero con una formulazione assai più *soft* di quanto la proposta inizialmente presentata lasciasse presagire[84], sia il diritto per l'interessato di chiedere ed ottenere la cancellazione dei propri dati sia l'obbligo per il titolare di procedere in tal senso "d'ufficio", vuoi in conseguenza dell'esercizio di altri diritti (come la revoca del consenso o l'opposizione a trattamenti basati sul legittimo interesse), vuoi in ulteriori circostanze specificate dal testo normativo, come il caso in cui i dati non siano più necessari per le finalità del trattamento. Peraltro, la stessa disposizione non trascura nemmeno l'aspetto della deindicizzazione, cui anzi è dedicato il secondo paragrafo, ove è stabilito l'obbligo per il titolare, che debba procedere alla cancellazione, di adottare misure ragionevoli, sulla base della tecnologia disponibile e dei costi di attuazione[85], ad «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».

---

[80] Lo evidenzia O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO – C. COLAPIETRO, *Innovazione*, cit., 573, cui rinvio anche per un'ampia disamina dei precedenti normativi sul punto e per la sottolineatura delle novità recate dal GDPR.

[81] Per un approfondimento del tema, v. F. CALISAI, *I diritti dell'interessato*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 344 ss., che ricollega appunto all'effettività di tutela per l'identità personale il diritto *de quo*.

[82] Osserva, in questa ottica, G. CRISTOFARI, *Il diritto alla limitazione del trattamento*, in R. PANETTA (a cura di), *Circolazione*, cit., 216, come il ricorso a questo diritto «dovrebbe aumentare contestualmente alla consapevolezza di ogni persona riguardo al controllo dei propri dati nel *processo di costruzione della propria identità digitale*» (corsivo mio).

[83] Sul quale, ampiamente, M. A. LIVI, *Quale diritto*, cit., spec. 80 ss., la quale tra l'altro sottolinea come la rubrica sembri in realtà confondere i due concetti di cancellazione e oblio, laddove invece la prima non realizza necessariamente solo il secondo né questo può essere soddisfatto solo dalla prima. La necessità della distinzione tra i due termini è argomentata anche da E. STRADELLA, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, in *Rivista AIC*, n. 4/2016, spec. 15 ss.

[84] La proposta originaria, infatti, prevedeva, tra l'altro, che il titolare informasse tutti i destinatari cui aveva comunicato i dati, della richiesta di cancellazione pervenute, affinché provvedessero di conseguenza. La portata dirompente che il testo originario avrebbe potuto avere è posta in luce da F. PIZZETTI, *Il prisma*, cit., 57 ss.; nonché da M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. PIZZETTI (a cura di), *Il caso*, cit., spec. 126 ss., cui rinvio per una dettagliata analisi del contenuto di quella formulazione normativa.

[85] Si osservi, per inciso, come il richiamo alla tecnologia disponibile, se può essere letto come limite volto ad evitare imposizioni troppo gravose a carico del titolare (così, aderendo alla lettura decisamente più diffusa, per esempio A. BERTI SUMAN, *Il diritto alla cancellazione*, in R. PANETTA (a cura di), *Circolazione*, cit., 212), può però rappresentare anche, al contrario, una clausola aperta, attraverso cui il GDPR, introducendo una sorta di "rinvio mobile" alle future evoluzioni tecniche, consente di mantenere un rapporto di proporzionalità, anche in senso più

Insomma, il Regolamento europeo, facendo sistema con le normative nazionali, ambisce oggi ad ergersi quale strumento di protezione generale e sistematica di situazioni soggettive così strettamente legate, che il livello di garanzia dell'una si riverbera inevitabilmente sulla concreta possibilità di adeguata tutela per l'altra.

Ma, pur con questo indubbio merito, il GDPR è davvero uno strumento pienamente efficace di difesa per le situazioni soggettive al nostro esame nel contesto dell'innovazione tecnologica, in special modo digitale?

Temo di no, per due ordini di ragioni, che cercherò di argomentare.

3.2. La (parziale) insufficienza della tutela a livello "micro"…

Un primo elemento di debolezza della normativa vigente in materia di protezione dei dati (e dintorni) attiene alla sua effettiva capacità di tutela a livello "micro", ovvero nei quotidiani e per così dire ordinari rapporti giuridici, perlopiù bilaterali, aventi ad oggetto un trattamento di dati, che si svolgono in un fisiologico contesto di mercato tra un titolare ed un interessato chiaramente identificati.

La tutela apprestata dal GDPR, infatti, nonostante l'atto normativo sia fondamentalmente improntato a criteri sostanziali[86] per garantire un'effettiva garanzia in concreto, come la valorizzazione del principio di *accountability* del titolare sembra dimostrare sopra ogni altro esempio[87], nei fatti presta però in alcuni casi il fianco a pratiche elusive, che possono essere poste in essere anche con stratagemmi (nemmeno troppo complessi) di carattere formale. Mi limito a due esempi, che mi paiono significativi di come la tutela offerta da due principi fondamentali, quali quello di legittimità e di minimizzazione, possa essere obliterata senza soverchi problemi.

Mi riferisco, anzitutto, all'istituto del consenso, che, se, nelle intenzioni del legislatore, rappresenta uno strumento, quando non il principale, di realizzazione dell'autodeterminazione informativa dell'interessato, si presta nella realtà ad essere utilizzato (anche) come la chiave di volta per eludere diverse tutele previste dal Regolamento. Si ponga, ad esempio, l'attenzione a quante garanzie possono essere facilmente rimosse semplicemente ove consti, appunto, il consenso dell'interessato, anche in relazione a profili che pure sono ritenuti particolarmente rischiosi nella valutazione del legislatore: è così per il divieto di trattamento delle categorie particolari di dati,

---

tutelante per l'interessato, tra gli obblighi del titolare e il progresso informatico, riducendo le conseguenze della propria inevitabilmente rapida obsolescenza (spunti in tal senso in L. DURST, *Oggetto e finalità*, *ivi*, 50).

[86] Rilevano al riguardo G. BUSIA – L. LIGUORI – O. POLLICINO, *Nota introduttiva*, in ID. (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2017, 12 come «la vera rivoluzione che il Regolamento comporta non è tanto nel dato normativo […] quanto nell'approccio che necessariamente dovranno adottare coloro che fondano la propria attività […] sul trattamento dei dati personali», il quale deve ispirarsi ad una attenzione per gli interessi sostanziali sottesi all'attività di trattamento ed in particolare all'effettivo livello di rischio per i diritti e le libertà degli interessati, per come nel caso specifico vengono in rilievo.

[87] Questo elemento di novità del Regolamento è valorizzato in particolare da L. CALIFANO, *Il Regolamento*, cit., 34 ss. Più in generale, sull'approccio sostanzialistico del GDPR, come precipitato dell'impostazione per principi dotati di elasticità interpretativa, v. C. COLAPIETRO, *Il diritto*, cit., spec. 88 ss.

oltre che per quello di profilazione[88] e finanche in relazione al trasferimento di dati al di fuori dell'Unione europea. Laddove, peraltro, in queste ultime due ipotesi il consenso in questione può anche essere ricompreso in quello più ampio contrattuale, nel caso in cui il trattamento in parola sia funzionale all'esecuzione di un accordo negoziale.

Certo, il GDPR circonda il consenso di diverse garanzie[89]. Così, anzitutto, l'art. 4 del Regolamento richiede, per la sua validità, una manifestazione di volontà "inequivocabile", e quindi non ricavabile da meri fatti concludenti, seppure esprimibile non soltanto mediante dichiarazioni, ma anche attraverso azioni positive. Il che, peraltro, a mio giudizio, rende priva di una effettiva capacità di assicurare una tutela più intensa la previsione di un consenso in forma "esplicita", introdotta con riferimento ai trattamenti maggiormente rischiosi di cui ho testé parlato, specialmente se si ammette, come mi pare corretto, che questo aggettivo non escluda forme diverse da quella della dichiarazione scritta[90]. Il consenso deve poi essere libero, non potendo essere condizionato dal rischio di subire pregiudizi nel caso in cui non venga prestato, ed informato, grazie in particolare alle indicazioni che il titolare deve fornire in occasione della sua acquisizione, senza contare che esso deve poter essere revocabile con la stessa facilità con cui è stato accordato. Se ne potrebbe, perciò, concludere che chi non abbia colpevolmente utilizzato gli strumenti conoscitivi posti a sua disposizione dalla normativa non potrebbe che imputare a se stesso eventuali limitazioni non previste della sua riservatezza.

Sennonché, uno sguardo alla pratica concreta dei rapporti quotidiani sembra dimostrare come, almeno in alcune – e nemmeno poche – situazioni, l'idea che realmente l'interessato possa autorizzare un trattamento solo con piena consapevolezza si scontra con una realtà che lo rende di fatto impossibile per le più svariate ragioni. Tra esse, si può pensare quanto meno alla tempistica dei rapporti non compatibile con un'adeguata istruttoria dei profili connessi alla protezione dei dati, alla difficoltà per l'interessato di comprendere realmente, sia sotto il profilo giuridico che soprattutto tecnico-informatico, il significato dell'informativa[91] fino alla sostanziale infungibilità

---

[88] Su cui si vedano i rilievi critici di L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il Regolamento*, cit., 274, ove gli AA. sottolineano come l'ammissione di deroghe fondate sul consenso non valorizza adeguatamente la posizione di parte debole dell'interessato.

[89] Sulla disciplina del consenso nel Regolamento 679/2016, anche in confronto alla previgente disciplina, v. L. CALIFANO, *Il Regolamento*, cit., 47 ss., ove l'A. esplicita anche alcune ragioni che rendono parziale la tutela offerta dall'istituto del consenso, pur leggendo (seppure a mio avviso con eccessivo ottimismo, per le ragioni che dirò a breve nel testo) nelle disposizioni sulla responsabilizzazione del titolare il meccanismo compensativo per completare questa (inevitabile) lacuna. Con riferimento ai limiti in concreto che il consenso sconta come mezzo di garanzia dell'autodeterminazione informativa, si vedano, tra gli altri, i rilievi di C. COLAPIETRO – A. IANNUZZI, *I principi generali*, cit., 115 ss.; e F. BRAVO, *Il consenso*, cit., spec. 157 ss.

[90] In questo senso L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il Regolamento*, cit., 224. In tema anche S. F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione*, cit., 117, la quale ricava dall'enunciato normativo l'ammissibilità della forma orale con esclusione dei fatti concludenti. Sennonché, questi ultimi sono già inammissibili, in radice, alla luce della definizione generale di consenso fornita dall'art. 4, di modo che la vera questione è se un'azione positiva espressamente rivolta al suo rilascio possa dirsi valida: il che, a mio avviso, non può essere negato.

[91] La necessità di una funzione informativa complementare da parte dei pubblici poteri per superare i limiti del consenso connessi alla difficoltà di questo istituto di realizzare, in concreto, una reale autodeterminazione informativa, è posta in evidenza da C. COLAPIETRO – A. IANNUZZI, *I principi generali*, cit., 120.

del servizio in relazione al quale il consenso al trattamento è richiesto[92]. In questa direzione, del resto, sembrano indirizzarsi anche i primi risultati di una interessante ricerca empirica, la quale «evidenzia come anche coloro che dichiarano di aver interesse per la protezione dei propri dati personali […] di regola non prestano attenzione o, in ogni caso, prescindono dall'informativa sulla *privacy*, anche in un ambiente non naturale (l'esperimento) ove i soggetti sono espressamente richiesti di eseguire il compito»[93]. Per conseguenza, questo strumento si dimostra in grado di approntare una protezione puramente formale[94], al pari della specifica sottoscrizione di alcune clausole contrattuali di civilistica memoria[95], che si risolve in una tutela destinata a rimanere sulla carta, quando addirittura non si ritorce a danno dello stesso interessato, ove questi sia convinto, attraverso il consenso, di avere eliminato ogni possibilità di lesione della propria sfera giuridica[96]. Né può ritenersi, a mio avviso, che l'esistenza di un'Autorità pubblica di controllo, con ampi poteri di intervento, o il fatto che il consenso non sia l'unica fonte di legittimità del trattamento spostino i termini del problema o compensino quanto detto finora, giacché non viene meno la considerazione che ci sono ipotesi in cui, senza violare in alcun modo la normativa, il consenso, essendo acquisito in circostanze fattuali che ne impediscono una reale efficacia protettiva per l'interessato, si rivela una garanzia facilmente eludibile[97]. Neppure i vari istituti riconducibili al

---

[92] Ancor più netta la posizione di G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, 2019, 92, la quale afferma che «l'antica tutela della privacy, *consent based*, assistita dalle garanzie dell'autonomia e della consapevolezza, non è più utilmente invocabile. Entrambi questi attributi si sono sbriciolati dinanzi ad assensi estorti con la coercizione psicologica di negare il servizio digitale a chi si fosse rifiutato di cedere i dati o li avesse ceduti senza cognizione di causa nell'ignoranza piena delle finalità del loro impiego».

[93] Testualmente, L. GATT – R. MONTANARI – I. A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, 374, ove gli AA. osservano anche come «il riscontrato atteggiamento verso la lettura o consultazione dell'informativa […] può indurre a considerare come il miglioramento delle modalità di redazione e della chiarezza dell'informativa, che pure rappresenta un costante obiettivo delle politiche comunitarie e nazionali anche attraverso le autorità di controllo, ragionevolmente non sia destinata a produrre significativi cambiamenti nel grado di consapevolezza degli utenti». Peraltro, per quanto gli AA. precisino, con rigore scientifico, che i risultati sono ancora parziali e provvisori, ci sono a mio avviso tutte le premesse per pensare che essi non si discosteranno da quelli definitivi.

[94] Analogamente, scrive G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in EAD. (a cura di), *Il nuovo Regolamento*, cit., 3, che «certamente non può soddisfare un sistema basato su un consenso che spesso è vuoto di effettivo significato» di modo che «si tratta di un modello sotto il profilo teorico centrato sull'autodeterminazione, che tuttavia spesso manca dei presupposti sui quali dovrebbe basarsi».

[95] Mi riferisco alla previsione di cui all'art. 1341 cod. civ., che per lungo tempo è stato l'unico argine di fronte a clausole vessatorie, ma che non ha mai offerto alcuna reale tutela, in quanto la seconda firma per accettazione specifica veniva (e viene) apposta senza una particolare consapevolezza e, in ogni caso, il più delle volte senza che in concreto vi sia comunque alcuna effettiva possibilità di rinegoziare le condizioni contrattuali imposte.

[96] Così L. GATT – R. MONTANARI – I. A. CAGGIANO, *Consenso*, cit., 376, secondo i quali vanno rilevati oggettivi «limiti del *consenso* preventivo sia perché reso inconsapevolmente sia perché – anche quando è reso consapevolmente – non si traduce in un effettivo impedimento alla dannosità del trattamento per la persona dell'utente, dannosità che continua a potersi verificare. Al contrario, la prestazione del consenso potrebbe avere un effetto distorsivo perché esso viene prestato senza che l'utente abbia cognizione degli strumenti di tutela *ex post* ed anzi sulla base della convinzione che la sola concessione del consenso elimini *a priori* la possibilità stessa di una lesione» (corsivi testuali).

[97] Analogamente F. BRAVO, *Il consenso*, cit., spec. 138 ss., il quale sottolinea come questa impostazione non sia casuale, ma risponda al preciso disegno, già evidenziato, di fare della protezione dei dati solo uno degli interessi in gioco, al pari, tuttavia, della libera circolazione degli stessi, di modo che si crea «un sistema di selezione degli interessi volto a garantire le nuove esigenze socio-economiche, *dettate dall'evoluzione tecnologica* […], nel quale

principio di *accountability*, visti in precedenza, possono dirsi tali da arginare le problematiche evidenziate, giacché, nella realtà dei fatti, la loro reale efficacia è piuttosto dubbia, in quanto essi presuppongono una buona dose di fiducia nella loro effettiva e conforme realizzazione da parte di un titolare consapevole (dei rischi e delle esigenze di tutela) e davvero intenzionato a porvi un qualche limite.

La critica, però, non può essere circoscritta al solo consenso.

Lo stesso principio di minimizzazione, pur di grande valore ideale, non rappresenta una seria barriera a protezione dei dati, almeno nel contesto dell'economia digitale. E questo perché, il più delle volte, al fornitore del servizio non interessa tanto acquisire una mole ingente di dati in sede di adesione alla proposta contrattuale (sicché egli può tranquillamente adeguarsi a tale principio), quanto piuttosto accumulare quelli che, derivando dall'utilizzo effettivo del servizio fornito, possono descrivere il comportamento dell'utente ed hanno perciò ben maggior valore economico[98]. Del resto, specialmente nel mercato digitale, l'utente avverte una necessità (seppure putativa, in molti casi) di determinati servizi, che lo spinge facilmente ad acconsentire a qualunque trattamento ed a fornire qualunque dato pur di ottenerli, specialmente laddove possa conseguire il risultato gratuitamente. Così che i dati, come ormai ben noto a chi abbia un minimo di sensibilità su questi temi, divengono in realtà il vero corrispettivo negoziale[99] e l'interessato, degradato da persona a oggetto da cui estrarre il maggior numero possibile di informazioni[100], diviene il prodotto stesso al centro dell'operazione negoziale.

---

l'esigenza di tutela del diritto fondamentale alla protezione dei dati personali finisce per perdere, nella sostanza (anche se non ancora nella forma), quella centralità che dovrebbe consegnargli l'applicazione del principio personalista».

[98] Dei *Big data* come «il nuovo asset delle imprese operanti in rete» parla G. DE MINICO, *Big Data*, cit., 90; nonché M. C. MENEGHETTI, *Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento*, cit., 427, la quale icasticamente afferma che «il dato è materia prima, moneta di scambio e prodotto finale al tempo stesso».

[99] Si tratta di una lettura diffusa in dottrina: v., ad esempio, P. COSTANZO, *Note minime in tema di tutela dei dati personali in internet e* privacy enhancing technologies, in *Studi in onore di Fausto Cuocolo*, Milano, 2005, 289 ss.; nonché, più di recente, A. DE FRANCESCHI, *Il "pagamento" mediante dati personali*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 1381 ss.; M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *Federalismi*.it, n.14/2020, 211; e G. DE MINICO, *Big Data*, cit., 102, la quale osserva sul punto come «il rapporto contrattuale continua a essere sinallagmatico solo che il corrispettivo contro il servizio digitale non è il denaro, ma la cessione in blocco dei dati alla controparte». Del resto, nella dottrina civilistica da tempo vi è chi ha portato l'attenzione su tale processo di mercificazione, in ragione dell'assimilazione del potere di controllo sui dati personali alle situazioni possessorie e proprietarie, e, per tale via, alla funzionalizzazione della «disciplina del trattamento alla tutela di poteri di disposizione dei dati piuttosto che alla tutela della persona umana» (F. G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008, 146). Parte della letteratura economica, tuttavia, contesta questa conclusione, sostenendo che non ci sia affatto scambio economico, essendo i dati (e le relative informazioni incorporate) connaturati all'uso della piattaforma stessa (cfr., tra molti, G. COLANGELO, Big data, *piattaforme digitali e antitrust*, in *Mercato Concorrenza Regole*, 2016, spec. 439; e I. GRAEF, *Market Definition and Market Power in Data: The Case of Online Platforms*, in *World Competition: Law and Economics Review*, vol. 38, 4/2015, 473 ss.). Il che, peraltro, in termini giuridici, non farebbe certo venir meno l'esigenza di protezione e quindi in sostanza nulla cambia rispetto al discorso che andiamo svolgendo.

[100] Secondo quanto scrive, in modo del tutto condivisibile, C. COLAPIETRO, *Il diritto*, cit., 35. Analogamente B. ROMANO, *Civiltà dei dati. Libertà giuridica e violenza*, Torino, 2020, 83, afferma che «la *merce della rete digitale è costituita dai dati*, in modo più specifico dalla loro estrazione e dal loro trattamento, che, considerata la enorme massa degli elementi da trattare, necessita della programmazione e dell'operatività di complessi algoritmi, capaci di filtrare i dati considerati utili e di trattarli con software ed hardware idonei a che se ne possa trarne un profitto, un

L'entusiasmo con cui è stata accolta dalla generalità dei consociati l'app Io[101], al di là del giudizio che possa darsi all'iniziativa del "*cashback* di Stato", pare dimostrare la facilità con cui, a fronte di benefici economici anche di modesta entità, vi sia una generalizzata pronta disponibilità a rinunciare ai propri dati senza porsi scrupoli eccessivi. La realtà ci dimostra, insomma, che l'interessato, spesso, rappresenta, sì, una vittima degli operatori del mercato digitale, ma che al contempo, manifestando una sorta di sindrome di Stoccolma, si lega con (più o meno deliberato) consenso al soggetto che pure pone a rischio di compromissione tanto la sua riservatezza quanto la sua identità digitale[102].

È ben vero che quanto siamo andati dicendo sinora si pone come un problema eminentemente culturale, che in quanto tale richiede misure che operano sullo stesso piano, da cui anche le numerose campagne informative meritoriamente portate avanti dalle Autorità di controllo, ivi incluso il Garante per la protezione dei dati personali italiano. Né va sottaciuto che il GDPR offre pur sempre una forma di tutela, che non può essere trascurata. Ma ciò non toglie che queste garanzie si rivelino non sempre e non del tutto adeguate, prestando così il fianco a qualche primo rilievo critico sulla loro effettiva e generalizzata efficacia.

3.3. … e la sua strutturale inefficacia a livello "macro"

Le criticità che abbiamo rilevato sinora attengono al funzionamento del GDPR come presidio a tutela di privacy e identità personale a livello "micro", ovvero quando si verte nell'ambito di rapporti, perlopiù bilaterali, tra soggetti determinati ed il titolare del trattamento è una realtà di dimensioni, più o meno ampie, ma comunque pur sempre giuridicamente "aggredibili".

Il discorso muta, però, e non certo in direzione meno problematica, quando, in ragione del pervasivo sviluppo delle tecnologie digitali e, specialmente, della rete e dei *social network*[103], diventa possibile disporre di ingenti masse di dati (i *Big data* cui ho fatto più volte riferimento),

---

accrescimento misurabile con il *quantum* del denaro» (corsivi testuali). In prospettiva economica, S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* [2019], trad. it. di P. Bassotti, Roma, 2019, 17 ss., chiarisce come «il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti. Alcuni di questi dati vengono usati per migliorare prodotti o servizi, ma il resto diviene il *surplus comportamentale* privato, sottoposto a un processo di lavorazione avanzato noto come "intelligenza artificiale" per essere trasformato in *prodotti predittivi*» (corsivi testuali). L'Autrice peraltro rileva come in questa nuova forma di sorveglianza (e di mercato) «lo sfruttamento dell'esperienza umana non basta»; invero, «le materie prime più predittive si ottengono» non più soltanto analizzando i dati prodotti ma «intervenendo sulle nostre esperienze per orientare il nostro comportamento a favore degli obiettivi economici» dei c.d. capitalisti della sorveglianza. Tanto che «i nuovi protocolli automatizzati sono progettati per influenzare e modificare il comportamento umano, per renderlo un mezzo di produzione subordinato a *mezzi di modifica del comportamento* sempre nuovi e più complessi» (corsivo testuale).

[101] Significativamente superiore a quello registrato per l'app Immuni: cfr., per questa notizia, F. BINI, *App: Io batte Immuni: così il cashback ha spinto i download molto più dell'emergenza sanitaria*, ne *La Repubblica*, 10 dicembre 2020.

[102] Sottolinea al riguardo G. DE MINICO, *Big Data*, cit., 90, come i Big data nascano per la noncuranza con cui «lasciamo cadere frammenti della nostra identità, che raccolti e riorganizzati da chi verrà dopo comporranno il patrimonio virtuale della sua attività d'impresa».

[103] Dei *social* come «la *miniera* dei *big data*» (corsivi testuali) discorre G. ZICCARDI, *Tecnologie*, cit., 221.

che conferiscono ai detentori straordinarie capacità conoscitive, grazie specialmente alla possibilità di elaborare queste informazioni facendo ricorso a più o meno complesse operazioni matematiche – i famigerati algoritmi – con i quali estrapolare previsioni sul comportamento di individui, previamente suddivisi in *cluster* sulla base dei criteri più variegati, per finalità vuoi di propaganda politica, vuoi di natura commerciale, bersagliandoli di proposte mirate su temi e prodotti di prevedibile (e previsto) interesse.

L'uso dei *Big Data*, in sé, può aprire, beninteso, grandi opportunità[104]. Basti pensare all'utilità che essi possono avere per l'Amministrazione Pubblica[105], che ne faccia uso per il perseguimento di finalità di pubblico interesse, come, per fare qualche esempio banale, allorché vengano analizzati dati sui flussi di traffico per la programmazione di infrastrutture e per la progettazione di politiche ambientali o quelli sulle abitudini di consumo alimentare per finalità di informazione, prevenzione e programmazione in ambito sanitario[106]. Ma queste masse di dati hanno anche una forza intrusiva senza precedenti rispetto alle situazioni soggettive di cui ci andiamo occupando.

In primo luogo, infatti, non è infrequente il rischio che le operazioni condotte sui dati portino a risultati inadeguati rispetto alle stesse finalità per le quali vi si è fatto ricorso[107], se solo si considera che la grande quantità di dati non implica necessariamente la loro qualità, ma semmai, all'opposto, proprio la vastità del patrimonio informativo e l'eterogeneità di esso potrebbero aumentare il pericolo di errori sia nella fase stessa di raccolta, che in quelle successive di classificazione ed elaborazione.

Ma soprattutto, ciò che desta allarme è il fatto che la raccolta ed elaborazione di questi dati su vastissima scala può dare facilmente luogo ad effetti potenzialmente devastanti per le conseguenze discriminatorie che dagli stessi risultati possono discendere. L'algoritmo, infatti, è un modello matematico che ammanta di scientificità (e, conseguentemente, di apparente oggettività) un meccanismo che riproduce in realtà le valutazioni e le priorità attribuite da chi lo ha creato: insomma, come è stato icasticamente affermato, «i modelli sono opinioni radicate nella matematica»[108]. Da ciò consegue che, in molti casi, anche malgrado la buona fede degli ideatori,

---

[104] In generale, su opportunità e rischi dei *Big data*, v., tra gli altri, l'ampia disamina di M. OREFICE, *I Big data. Regole e concorrenza*, in *Politica del diritto*, 2016, spec. 706 ss.

[105] Il tema dell'uso dei *Big Data* e degli algoritmi nell'Amministrazione Pubblica è un altro filone di indagine oggi già ben avviato e sviluppato. Al fine di non deviare eccessivamente dal discorso principale condotto nel testo – e rinviando comunque alla relazione a questo Convengo di Fabio Pagano dedicata al tema – mi limito qui a richiamare gli scritti di M. FALCONE, Big Data *e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista trimestrale di diritto pubblico*, 2017, 601 ss.; e F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra* Open e Big Data, in *Rivista di diritto amministrativo*, 2017, 799 ss.

[106] In generale, sull'utilità dei *big data* al fine di elaborare politiche pubbliche più efficaci, senza che questo si ponga (necessariamente) in contrasto con la privacy, M. MIDIRI, *Privacy*, cit., spec. 216; e S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto Discipline Pubblicistiche, Aggiornamento VII*, Milano, 2017, 601, il quale afferma che «l'insieme di questi dati rappresenta una miniera d'oro per lo sviluppo razionale di tutte le politiche pubbliche ipotizzabili, qualora debitamente analizzato».

[107] Lo sottolinea L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Roma, 2020, 28 ss.

[108] C. O'NEIL, *Armi di distruzione matematica* [2016], trad. it. a cura di D. Cavallini, Firenze-Milano, 2017, 33. Non diversamente, scrive A. SORO, *Persone in rete*, Roma, 2018, 117, che «numerose applicazioni hanno

il funzionamento dell'algoritmo coglie solo parzialmente la complessità di una situazione, finendo non solo per restituire risultati infondati, quando non addirittura palesemente discriminatori, ma anche, ove non costantemente aggiornato, per cristallizzare le situazioni individuali e sociali che prende in esame. È quanto accade, ad esempio, con molti modelli introdotti per la individuazione dei soggetti a maggior rischio di recidiva, laddove questi algoritmi, segnalando come più probabile la commissione di altri reati da parte di determinate categorie di persone (perlopiù di precise origini etniche ed inevitabilmente legate a specifici ambienti urbani più degradati ed in cui opportunità di istruzione e di lavoro appaiono maggiormente difficili a presentarsi), portino a concentrare controlli e indagini su quegli stessi soggetti, che a quel punto giocoforza con maggiore probabilità finiranno per risultare più propensi a delinquere. Cosicché il modello, apparentemente funzionante, in realtà esprime semplicemente una profezia che si autoavvera, determinata da un equivoco alla base che porta a confondere una correlazione con un rapporto di causalità[109].

Per non parlare, poi, dei casi in cui dell'algoritmo si faccia un uso fin dalla sua progettazione volutamente pensato al fine di cogliere situazioni di vulnerabilità (quali emergono, per esempio, da ricerche effettuate tramite un motore di ricerca…) per trarne un vantaggio economico, a tutto dispetto dell'eguaglianza sostanziale. Si pensi, tanto per citare un esempio, all'uso di algoritmi per individuare persone che dimostrino di soffrire di ipocondria, al fine di proporre loro messaggi promozionali di integratori e prodotti (pseudo)farmaceutici, sfruttando la particolare sensibilità al tema del destinatario.

Quanto abbiamo visto finora apre scenari certamente inquietanti.

Sennonché, quando i fenomeni descritti si producono nell'ambito del potere pubblico, se non una soluzione, almeno un argine verso le problematiche segnalate può ritrovarsi tanto nell'introduzione di un obbligo di trasparenza dell'algoritmo[110], che consenta la verifica del principio di imparzialità, quanto nella possibilità di far valere la responsabilità dell'organo politico o amministrativo chiamato a rispondere delle decisioni automatizzate, anche solo per la (ineliminabile, come dicevo) discrezionalità insita nella fase di impostazione dell'algoritmo stesso[111].

---

dimostrato che gli algoritmi non sono matematica pura – come tale, infallibile e neutra – ma piuttosto opinioni umane strutturate in forma matematica che riflettono spesso […] le precomprensioni di chi li progetta».

[109] Il caso, piuttosto noto, è diffusamente trattato, tra gli altri, C. O'NEIL, *Armi*, cit., 36 ss. La stessa A., peraltro, dopo aver fornito numerosi diversi esempi, nelle proprie conclusioni (spec. 294), sottolinea come, in generale, «i processi basati sui Big Data codificano il passato», di modo che, se si volesse utilizzare questi sistemi di analisi per indirizzare i comportamenti verso direzioni ritenute politicamente auspicabili, occorrerebbe inglobare in essi ulteriori parametri eticamente orientati. Su posizioni analoghe, *ex plurimis*, v. A. SORO, *Persone*, loc. cit.; e P. ZELLINI, *La dittatura del calcolo*, Milano, 2018, spec. 62 ss., il cui volume traccia anche una interessante storia del calcolo algoritmico.

[110] Su cui insiste particolarmente G. DE MINICO, *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal*, n. 1/2021, 398 ss.

[111] Al riguardo, per quanto concerne il nostro Paese, si vedano le preziose indicazioni fornite dalla giurisprudenza amministrativa e in particolare da Consiglio di Stato, sez. VI, sentenza 8 aprile 2019, n. 2270; e soprattutto 13 dicembre 2019, nn. 8472 e 8474, che argomentano sulla concorrente applicazione della normativa sul procedimento amministrativo con quella sulla protezione dei dati, e segnatamente l'art. 22 del GDPR. Di queste sentenze e di un primo seguito che hanno ricevuto trattano L. LIGUORI – M. V. LA ROSA, *Recent Italian administrative*

Toni ben più preoccupanti, a mio avviso, vengono invece raggiunti allorché ci si trovi dinnanzi a soggetti privati, non solo privi di un obbligo analogo di trasparenza, ma semmai ben attenti a proteggere, in quanto proprietà intellettuale, i loro algoritmi. Ciò vale specialmente quando i soggetti di cui si tratta rientrano nel novero delle c.d. *Big Tech*, cioè di quelle società, quali *Google*, *Amazon*, *Facebook*, *Apple*, *Microsoft*, ecc., di immani dimensioni (e fatturati), che operano in mercati legati alle nuove tecnologie, fornendo servizi ormai imprescindibili nell'attuale contesto e che rappresentano un canale formidabile per drenare moli consistenti di dati[112].

Peraltro, quello del possesso dei *Big data* (e, *a fortiori*, della loro elaborazione algoritmica a fini previsionali) da parte di queste multinazionali è un tema che travalica la sola possibile violazione dei diritti soggettivi al nostro esame[113], con i possibili effetti discriminatori di cui ho testé detto, giacché il valore dei dati è tale da offrire altresì la possibilità a questi poteri privati di giungere persino, come anticipavo, ad influenzare (se non determinare) le politiche pubbliche. Lo si è visto anche durante la pandemia, con l'imposizione agli Stati che intendessero utilizzare il sistema di Apple e Google, da un lato, di poterlo fare su una sola app per Paese, autorizzata dal relativo Governo (il che per l'Italia ha significato l'abbandono di alcuni applicativi sviluppati livello regionale, forse più funzionali alla gestione dell'emergenza da parte del servizio sanitario[114]), nonché, d'altro lato, della imposizione di un determinato standard tecnico, magari nel merito persino più rispettoso della privacy, ma pur sempre eteroimposto[115].

Anzi, il potere delle *Big Tech* giunge anche oltre, non mancando casi in cui esse sono arrivate ad opporre resistenza nei confronti di Stati che intendevano esercitare le loro prerogative sovrane[116]. Da questo punto di vista, per limitarmi a richiamare una vicenda in qualche misura

---

courts' decisions about algorithms and their relevance in administrative procedures: how to reconcile them with GDPR principles?, in *Medialaws*, 11 maggio 2021.

[112] Scrive al riguardo N. SRNICEK, *Capitalismo digitale* [2016], trad. it. a cura di C. Papaccio, Milano, 2017, 39, che l'economia odierna è «dominata da un nuovo ceto, che non ha il controllo dei mezzi di produzione, ma piuttosto dell'informazione», cosicché si è originata una nuova forma (*rectius*, una fase più evoluta) di capitalismo incentrato «sull'ottenimento dell'uso di un tipo particolare di materiale grezzo: i dati».

[113] Anzi, queste masse di dati ben potrebbero essere create al di fuori dell'ambito di applicazione della normativa a tutela della privacy, perché magari alimentate con dati anonimizzati, o essere formate utilizzando informazioni che gli interessati hanno lasciato liberamente disponibili in rete. Per una disamina delle plurime conseguenze della *datification*, v. le osservazioni di S. CALZOLAIO, *Protezione*, cit., 600 ss.

[114] Su questo aspetto v. M. PLUTINO, *"Immuni". Un'*exposure notification *app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *Dirittifondamentali*, n. 2/2020, 573, il quale peraltro ritiene che queste avrebbero avuto maggiori limiti nel rispetto dei diritti fondamentali.

[115] Laddove, peraltro, non manca chi ha sollevato dubbi sulla effettiva possibilità di controllare l'uso che dei dati faranno questi giganti del web, seppure in forma aggregata: così C. COLAPIETRO – A. IANNUZZI, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali*, n. 2/2020, 803; ed A. SANTOSUOSSO, *La regola, l'eccezione e la tecnologia*, in *BioLaw Journal*, 2020, 615, il quale rileva come, nel migliore dei casi, notevole sia il vantaggio economico che le due società hanno tratto dall'accumulazione di questi dati aggregati.

[116] Ciò che con la consueta lucidità e lungimiranza aveva intuito oltre dieci anni fa S. RODOTÀ, *Una Costituzione per internet*, in *Politica del diritto*, 2010, 341, quando scriveva, con un riferimento a Google che ben può essere esteso ad altre società con analoghe caratteristiche, che «non è soltanto una delle strapotenti società multinazionali. È un potere a sé, superiore a quello di un'infinità di Stati nazionali, con i quali negozia appunto da potenza a potenza […] Governa corpi, conoscenza, relazioni sociali».

legata proprio al tema della privacy[117], è emblematico il noto caso *Apple vs. FBI*, nel quale la *Big Tech* rifiutava di elaborare un software che avrebbe consentito l'accesso ai dati contenuti in un dispositivo, nel caso specifico fondamentali per un'indagine su un reato di estrema gravità, in quanto ciò avrebbe costituito una violazione della privacy, che proprio al Governo sarebbe spettato proteggere[118]. Ma, più di recente, si potrebbe citare il caso di *Facebook*, che, opponendosi all'approvazione da parte del Parlamento australiano di una riforma che avrebbe comportato per i giganti del web il pagamento di un equo compenso agli editori per l'utilizzo dei loro contenuti, ha bloccato tutte le *news* fornite attraverso le proprie pagine, comprese quelle relative alla salute ed ai servizi emergenziali, finché non ha raggiunto un accordo con lo Stato, che comporta, a determinate condizioni, la non applicazione nei confronti delle *Big Tech*, delle nuove previsioni normative[119]. Una vera e propria trattativa negoziale, insomma, con cui la società americana ha posto una sorta di veto nei confronti di uno Stato sovrano, minacciando di privarlo di informazioni essenziali (anche) per i suoi consociati.

Se poi aggiungiamo che l'elaborazione dei dati nelle disponibilità di tali "nuovi" attori viene effettuata soprattutto tramite algoritmi basati su modelli di apprendimento automatico (il c.d. *machine learning*), capaci di sfruttare la statistica per cercare di prevedere con precisione crescente, grazie alle similarità rilevate, finanche i (potenziali) comportamenti futuri degli individui, si ricava facilmente come essi dispongano di un potere, dal quale può derivare una forma ancora più penetrante di controllo. Infatti, come è già stato evidenziato in letteratura, «non dobbiamo più osservare il sistema per molti anni per costruire un modello empirico. Abbiamo invece un modello meccanicistico che usa una costruzione algoritmica, ovvero un insieme di istruzioni e calcoli matematici, per prevedere il futuro». Di modo che «gli algoritmi cominciano a produrre un fiume in piena di predizioni su tutto quello che riguarda la società, dalla diffusione delle epidemie alla gestione di catastrofi e alla politica […] Gli algoritmi sono in grado di sapere

---

[117] Anche perché la questione, in generale, cui sto facendo cenno nel testo è oggetto, in questo Convegno, della relazione di Marco Betzu, *Poteri pubblici e poteri privati nel mondo digitale*.

[118] La vicenda è piuttosto nota e sarebbe ultroneo intrattenersi su di essa in questa sede. Mi sia consentito rinviare, per tutti, a M. OROFINO, *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*; e G. E. VIGEVANI, *Apple v. FBI: i valori costituzionali in gioco*, entrambi in *DPCE Online*, vol. 26, n. 2/2016, rispettivamente 279 ss. e 299 ss. Aldilà del giudizio di merito sulle complesse questioni evocate, ai nostri fini si profila di interesse la lettera inviata ai propri clienti dall'amministratore di *Apple*, di cui l'ultimo A. citato riporta uno stralcio significativo. In essa, infatti, l'azienda annunciava il ricorso avverso l'ordine giudiziario di offrire collaborazione all'autorità inquirente, al dichiarato fine di garantire la privacy dei propri clienti, contestando al Governo federale statunitense quanto indicato nel testo. Sicché, uno dei profili di maggiore rilevanza del caso, sembra allora essere rappresentato proprio dal fatto che ad essere contrapposti erano «non lo Stato e i suoi cittadini ma il potere statuale e un altro potere non meno forte, ovvero una grande multinazionale che gestisce dati a livello globale. Ed è probabile che il comportamento di Apple nella vicenda non sia stato ispirato solo da aneliti libertari: la protezione degli iPhone dalle possibili intrusioni di un governo appare finalizzata principalmente a rafforzare il *brand* e il rapporto fiduciario con i clienti» (così G. E. VIGEVANI, *Apple*, cit., 307). Come risaputo, la vicenda si è poi chiusa con la rinuncia all'azione da parte del Governo, essendo riuscito il Dipartimento della Giustizia a decrittare il dispositivo grazie ad una società specializzata.

[119] Anche questa vicenda ha avuto una certa eco sulla stampa di tutto il mondo. V., per tutti, M. ROVELLI, *Facebook bloccato in Australia: raggiunto accordo col governo per il pagamento delle notizie*, ne *Il Corriere della Sera*, 23 febbraio 2021; A. MEADE – J. TAYLOR – D. HURST, *Facebook reverses Australia news ban after government makes media code amendments*, in *The Guardian*, 23 febbraio 2021; e J. MADDEN – D. SWAN, *Australian news content refriended on Facebook from Friday*, in *The Australian*, 25 febbraio 2021.

cosa ci piace, di cosa abbiamo bisogno, chi sono i nostri amici, le nostre inclinazioni politiche e religiose. E continuamente queste previsioni irrompono nella nostra vita attraverso offerte commerciali, pubblicità, medicine personalizzate. La nostra vita è scandita dalle predizioni»[120].

Certo, non mancano casi in cui il potere di cui dispongono queste società viene utilizzato per un interesse meritevole, come avvenuto ad esempio di recente allorché la *Premier League* inglese si è rivolta a *Facebook* e *Twitter* per chiedere loro di impedire la diffusione di messaggi a contenuto razzista o discriminatorio verso arbitri e calciatori[121]. Ciò, tuttavia, non fa che confermare che queste società hanno assunto potestà tipicamente statali ed il fatto che l'ordinamento sportivo si sia rivolto non (solo) alle Autorità Pubbliche ma direttamente (e pubblicamente) a soggetti privati per ottenere protezione nei confronti di violazioni giuridicamente rilevanti di diritti fondamentali appare assai significativo.

Di fronte all'uso degli algoritmi, che presuppone, per quanto visto finora, la raccolta e l'acquisizione di dati (anche) personali e quindi un trattamento potenzialmente soggetto alla normativa di protezione in precedenza richiamata, il Regolamento europeo predispone una tutela a dir poco inadeguata. L'unica norma, infatti, che viene in soccorso è l'art. 22, nel quale, come ricordavo in precedenza, è stabilito un generale divieto di decisione automatizzata, compresa la profilazione, quando questa incida in modo significativo sulla persona dell'interessato o produca effetti nella sua sfera giuridica, salvo che essa sia oggetto di specifico consenso (anche contrattuale) o sia prevista dalla legge, con la possibilità, nei primi due casi, di pretendere comunque l'intervento umano del titolare nonché di esprimere la propria opinione e contestare la decisione. Cosicché, pur nella nobiltà delle intenzioni[122], vengono riproposti meccanismi di tutela già deboli nei quotidiani rapporti bilaterali e quindi a maggior ragione totalmente inefficaci verso multinazionali di dimensioni colossali che offrono servizi tanto fondamentali quanto difficilmente sostituibili nella realtà contemporanea: non è certo difficile comprendere la facilità con cui queste società possono ottenere il consenso dell'interessato, che ben difficilmente verrà dato davvero liberamente (ammesso che la persona stessa se ne ponga il problema) se non al costo, raramente sopportabile, di rimanere esclusi da un servizio fondamentale[123]. Non solo, ma, più in generale, ciò che lascia insoddisfatti è la stessa inadeguatezza dell'approccio del testo normativo alla questione. Ragionare, infatti, in termini di tutela del singolo interessato, nel momento in cui ci troviamo di fronte a masse enormi di informazioni, magari raccolte anche in forma anonima e per

---

[120] In questi termini si esprime A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Milano, 2019, 22 ss.

[121] Il testo della missiva, data 11 febbraio 2021, si può leggere sul sito della *Premier League*.

[122] Giacché, come scrive efficacemente C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 714, «la fonte europea mostra di considerare la persona irriducibile alla particella elementare di una massa che sul web si risolve in un mistico insieme matematico trattabile esclusivamente con il calcolo».

[123] L'insufficienza dello schema consensuale eredità dell'approccio normativo preesistente è denunciata da A. MANTELERO, *La* privacy *all'epoca dei* Big Data, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 1181 ss. e spec. 1190, ove l'A. afferma espressamente che «il consenso è sempre meno, in concreto, strumento di reale autodeterminazione. Anzi, paradossalmente, quest'ultimo può divenire la soluzione più agevole per raccogliere dati per le finalità più disparate, stanti i limiti che affliggono sia lo strumento dell'informativa sia la reale libertà di scelta».

nulla trasparente, di cui l'individuo è chiamato a fare le spese a valle di un processo di classificazione, del quale tuttavia potrebbe ignorare persino l'esistenza ed in cui è impossibile possa far valere una qualche reazione a difesa della proprio intimità e personalità, appare una prospettiva del tutto inadeguata[124]. Insomma, di fronte al fenomeno dei *Big data* e del loro trattamento da parte di poteri privati di dimensioni colossali, sono le stesse esigenze di tutela ad essere sostanzialmente differenti[125] e, conseguentemente, a manifestare la strutturale inefficacia di quelle garanzie approntate con il Regolamento del 2016. Occorre, pertanto, individuare una diversa e ulteriore strada (*rectius*, come dirò, strade) per fare fronte al problema di assicurare, nel contesto dell'economia (e della società) digitale, il riconoscimento ed il rispetto di quei diritti fondamentali, rappresentati da privacy e identità personale, che nell'esperienza costituzionale, anche multilivello, si sono andati affermando ed hanno trovato esplicito riconoscimento.

Prima di procedere, tuttavia, ad una ricostruzione di quali potrebbero essere, *de jure condito* e *de jure condendo*, i possibili percorsi da seguire in questa direzione, mi pare necessario spendere qualche parola per evidenziare un problema culturale di fondo, che mi pare sia tuttora di ostacolo ad una reale presa di coscienza e reazione adeguata al fenomeno di cui sto parlando.

4. Una (apparente) digressione: un problema culturale in tema di riservatezza

Nel contesto che ho finora descritto, credo si registri nella cultura (invero non solo) giuridica prevalente una tendenza che appare paradossale. È infatti ancora piuttosto diffusa l'accentuazione dei rischi connessi all'acquisizione ed al trattamento di dati in ambito pubblico[126], soprattutto

---

[124] Analogamente, A. MANTELERO, Big Data: *i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, ne *Il diritto dell'informazione e dell'informatica*, 2012, 138, il quale sottolinea «la connotazione peculiare di tale potere, che differisce dalla semplice capacità di profilazione o di schedatura di massa, a cui hanno da sempre guardato le norme in materia di data protection. Nel caso dei *big data* emerge infatti una nuova ed ulteriore valenza assai rilevante ovvero la capacità predittiva che le analisi condotte con strumenti sofisticati su tali grandi aggregazioni possono conseguire, da qui una notevole valenza strategica, socio-politica e, non da ultimo, patrimoniale dei *big data*». Lo stesso A., *La* privacy, cit., 1196 ss., precisa come oggi vi sia una dimensione collettiva della privacy, diversa dalla semplice sommatoria delle singole dimensioni individuali, che si estende anche alle potenziali implicazioni pregiudizievoli per gli interessati.

[125] Osservano, in tal senso, V. COLOMBA – G. ZANETTI, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in A. LO GIUDICE (a cura di), *Privati del pubblico. Ovvero dell'indistinzione*, Sesto San Giovanni, 2017, 338 ss., che, se «una categoria normativa […] può infatti fisiologicamente modificarsi sotto la pressione di fatti e circostanze esterne […] questo è precisamente ciò che non accade con la nozione di privacy» giacché «quando sia in gioco lo studio di questa nozione, il mutamento è assai più radicale, e qualitativamente diverso. Nell'evoluzione normativa della nozione di privacy non si tratta solo di risposte (anche significativamente) diverse a una domanda persistente e fondamentale. Si tratta invece di riformulazioni radicali della domanda stessa ovvero di un riorientamento dell'orizzonte istituzionale e normativo». Così che – concludono gli Autori – «la mole di dati a disposizione, e la possibilità di elaborazione di essi comporta […] un più radicale cambio di scenario […]. È la domanda stessa che è cambiata, non semplicemente le risposte che a una domanda si possono offrire».

[126] Per citare qualche posizione dottrinale che mi sembra ascrivibile a questa prospettiva di maggiore diffidenza verso i soggetti pubblici, cfr. S. SIMITIS, *Il contesto*, cit., 581, per il quale «gli enti pubblici devono rinunciare alle informazioni che potrebbero ottenere. L'onniscienza, del resto, non è una caratteristica delle società democratiche. Tali società devono invece correre i rischi legati alla carenza di informazioni, anche laddove l'accesso ai dati sia tecnicamente possibile e la rinuncia ai dati appaia uno svantaggio»; T.E. FROSINI, Privacy*: diritto fondamentale*

laddove non si verta nell'ambito dell'erogazione di benefici, assai più di quanto avvenga a fronte dei grandi poteri privati, che pure dispongono, come ho cercato di rilevare, di ben maggiori possibilità di violare i diritti alla privacy ed all'identità, e non certo per la soddisfazione di un interesse generale[127]. Beninteso, nessuno nega che quella delineata sia una situazione preoccupante, epperò, allorché si dà luogo ad un trattamento di dati, mentre questo è guardato con una certa diffidenza in favore di un soggetto pubblico, assai minori riserve vengono sollevate verso soggetti (privati) che operano sul mercato, per scopi, sia pur legittimi, meramente lucrativi e commerciali. In questo senso, è sufficiente scorrere la *newsletter* periodica del Garante per la protezione dei dati personali, che pure svolge i propri compiti con un equilibrio che non merita le talora eccessive critiche pervenute, anche da voci autorevoli, proprio nella prospettiva di cui sto parlando[128], per notare come lo spazio dedicato ai provvedimenti adottati verso enti pubblici sia, con una certa sistematicità, maggiore di quello riservato a soggetti privati.

Certo, è evidente che il rischio per i diritti dei consociati da uno Stato che si atteggi a "Grande Fratello" non è frutto di fantasie e la storia ben lo dimostra; nello stesso contesto del nostro Paese, per lungo tempo, il pendolo ha oscillato sproporzionatamente dalla parte dello Stato e forse questa è una delle ragioni d'essere della tendenza di cui vado parlando[129]. Tuttavia, a me pare che ora lo stesso pendolo abbia subito un'oscillazione di senso opposto[130] e che questa atavica "paura del

---

oppure no, in *Federalismi.it*, n. 16/2008, 2, ove l'A. scrive che «nel bilanciamento dei diritti, prevale sempre e comunque il diritto fondamentale del cittadino, anche di fronte al diritto allo svolgimento dell'indagine penale» dato che «vivere in uno Stato costituzionale vuol dire godere pienamente dei diritti di libertà, senza se e senza ma»; o, più di recente, S. STAIANO, *Diritto alla riservatezza e potere pubblico*, in *Federalismi.it*, n. 17/2017, spec. 2 ss., ove l'A. afferma che «il potere pubblico è sempre stato, fin dalle origini, ed è ancora, quasi naturalmente, in tensione con il diritto alla riservatezza» e che anzi, nel contesto attuale, esso «diviene in prevalenza il maggiore attore che opera in tensione con esso».

[127] Una recente presa di posizione in senso analogo è quella di V. VISCO, *La strana idea di privacy che ci lascia in balia della pandemia*, in *Domani*, 25 ottobre 2020, ove l'A. afferma, condivisibilmente che «la tutela della privacy è un elemento fondamentale di ogni sistema politico basato sulle regole liberal democratiche, ma anche in questi sistemi occorre chiarire quali sono i limiti che l'interesse collettivo può porre a quelli individuali» mentre «i Garanti della privacy tendono a concentrarsi soprattutto sulla tutela dei cittadini nei confronti dello Stato e delle autorità pubbliche in generale».

[128] Tra cui l'articolo di V. VISCO, *La strana idea*, cit., ove la critica al Garante per essersi sistematicamente distinto in questo senso intervenendo nei confronti del Consiglio di Stato, dell'Istat, delle Università, dell'Inps e specialmente dell'Agenzia delle Entrate appare sproporzionata e per questo anche oggetto di replica da parte dell'Autorità con l'intervento del Presidente del giorno successivo (pubblicato sul sito istituzionale come doc. web 9472219), nel quale peraltro si ricorre però anche ad argomenti (come la successiva conferma in sede giurisdizionale di molti di questi provvedimenti) che non paiono in realtà del tutto validi a smentire la tendenza culturale che l'ex Ministro delle finanze intendeva evidenziare.

[129] Che il diritto alla riservatezza nei rapporti tra Stato ed individuo fosse decisamente sconosciuto nella tradizione giuridica italiana è affermato chiaramente da B. DENTE, *Le trasformazioni della politica italiana di protezione dei dati personali*, in B. DENTE – N. LUGARESI – M.S. RIGHETTINI (a cura di), *La politica della privacy tra tutela dei diritti e garanzia dei sistemi*, Firenze, 2009, 8 ss., per il quale le affermazioni alle origini della tradizione americana della tutela della riservatezza, sarebbero quasi agli antipodi di quanto avveniva nel nostro Paese.

[130] Così F. DE LEO, *Due o tre cose su dati di traffico e tutela della privacy*, in *Questione. giustizia*, 2004, 843. Ma, ancor prima, si veda quanto scriveva, con parole che suonano ancora attuali, M. G. LOSANO, *Dei diritti e dei doveri: anche nella tutela della privacy*, in ID. (a cura di), *La legge*, cit., spec. XIII ss., ove l'A., dopo aver ricordato che «il diritto alla privacy è stato collegato alle battaglie per liberare l'individuo delle ingerenze dello Stato», rileva come la pericolosità informatica si sia trasferita vieppiù nelle mani di grandi imprese multinazionali, di modo che «se

tiranno" conduca talora ad eccessi in una direzione speculare ed opposta rispetto a quella del passato[131].

La recente vicenda dell'app Immuni (e di analoghi sistemi adottati in contesti statali indubbiamente democratici) nel contesto di una pandemia e con la finalità di limitare i contagi, mi sembra paradigmatica al fine di dimostrare quanto nella società sia diffusa quella tendenza di cui vado parlando e che posizioni dottrinarie e prassi applicative, pur animate da ottime intenzioni, rischiano di fomentare. Infatti, nonostante i suoi difetti e i suoi limiti, anche prontamente e giustamente criticati[132], l'adozione di un sistema di questo tipo rappresenta un intervento chiaramente ispirato al perseguimento di un interesse di indubbia rilevanza costituzionale, nei confronti del quale, se certo la protezione dei dati non può soccombere *in toto* meritando di entrare in un giudizio di bilanciamento, tuttavia ben potrebbe essere chiamata a sopportare limitazioni[133]. Di modo che appare davvero paradossale, come è stato rilevato, che «da decenni ormai siamo disposti a rinunciare alla privacy relativa ai nostri dati per fruire di servizi apparentemente gratuiti, ma che, come noto a tutti, in realtà paghiamo in dati personali, mentre in questo momento di emergenza mondiale, in cui si tratta di arginare la pandemia, qualcuno solleva questioni relativamente a trattamenti di dati che sarebbero gestiti da strutture pubbliche e non da multinazionali private, che dall'analisi dei dati traggono profitto»[134].

Anzi, a parer mio, le garanzie introdotte in relazione all'uso di *Immuni* sono risultate forse ispirate ad un bilanciamento persino troppo attento alle esigenze di protezione dei dati. Mi riferisco, per esempio, alla opinione, peraltro largamente condivisa, per cui l'opzione per una triplice manifestazione di volontà in relazione all'attivazione delle notifiche fosse ineludibile, al fine di non coartare la libertà di scelta di avvalersi o meno dello strumento di tracciamento e,

---

in tempi di predominanza dello Stato era lecito sbilanciarsi a favore dell'individuo, di fronte all'odierno predominio dell'individuo è lecito chiedere un riequilibrio della situazione a favore della società».

[131] È una tesi che ho cercato di dimostrare già in altre sedi, cui mi permetto di rinviare per più ampie argomentazioni. V., almeno, S. SCAGLIARINI, *La riservatezza*, cit.; e ID., *In tema di privacy: virtù e vizi della cultura giuridica*, in *Ars Interpretandi*, 2017, 49 ss.

[132] Per esempio da G. DELLA MORTE, *Quanto* Immuni*? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Diritti umani* e *Diritto internazionale*, vol. 14, n. 2/2020, 303 ss.; o da M. OREFICE, *L'app Immuni: salute, privacy e trasparenza*, in G. DE MINICO – M. VILLONE (a cura di), *Stato di diritto. Emergenza. Tecnologia*, Genova, 2020, spec. 180 ss., la quale tuttavia, ad avviso di chi scrive, eccede talora nel pretendere una soluzione (tecnicamente) perfetta in una situazione in cui l'obiettivo primario dovrebbe essere la minimizzazione del danno derivante dalla circolazione del virus.

[133] Come scrive V. ZENO ZENCOVICH, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *Medialaws*, 26 maggio 2020, «occorre ristabilire alcune gerarchie di valori: la "*salus* [intesa in senso stretto e in senso figurato] *rei publicae"* deve prevalere su diritti individuali rilevantissimi ma obiettivamente secondari rispetto alla vita umana». Nel senso analogo a quanto sostenuto nel testo v. già N. MINISCALCO, *La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?*, in *Osservatorio costituzionale*, n. 3/2020, spec. 3.

[134] Testualmente C. COLAPIETRO – A. IANNUZZI, *App*, cit., 774. Non meno efficace V. ZENO ZENCOVICH, *I limiti*, cit., ove si legge che «quotidianamente centinaia di milioni di cittadini europei conferiscono a soggetti privati, consapevolmente o inconsapevolmente, dati analoghi a quelli che le "app" di tracciamento dovrebbero raccogliere […] i nostri spostamenti (e ovviamente anche le nostre preferenze) sono monitorati, aggregati e "venduti" attraverso le migliaia di cookies che con un semplice "click" abbiamo accettato» di modo che «chi dunque esprime forti dubbi sulle "app" di tracciamento dovrebbe in primo luogo prendere in mano il proprio telefono mobile e chiedersi se tali critiche siano coerenti con il proprio comportamento abituale e senza preoccupazioni».

conseguentemente, incidere sulla libertà del consenso, la quale sarebbe stata compromessa ove alla decisione di attivarla fosse stato collegato un determinato vantaggio in funzione incentivante[135]. È mia opinione, invece, che ciò sia frutto di una errata (seppure sostenuta anche dalle Istituzioni preposte all'applicazione della normativa[136]) lettura del canone di libertà del consenso, giacché, proprio al contrario, la possibilità di scegliere, da parte di ciascuno, se privilegiare la propria riservatezza o l'adesione a un programma in grado di contribuire a limitare la diffusione del contagio, avrebbe inverato maggiormente proprio il principio di autodeterminazione delle proprie scelte[137]. Di modo che, una qualche minore restrizione della libertà di circolazione (e non certo una differenziazione nell'accesso alle cure, sicuramente incostituzionale[138]) per coloro che avessero optato per l'utilizzo dell'applicativo, se ragioniamo in punto di diritto – e quindi prescindendo da eventuali difficoltà tecniche in concreto[139], che certo sarebbero state da risolvere preventivamente, così come da ragioni di opportunità di politica regolatoria[140] – credo sarebbe stata assolutamente ammissibile, non solo per la oggettiva minore rischiosità in termini di diffusione del contagio di chi avesse scelto di attivare Immuni, ma anche, più in generale, sulla base della funzione sociale che alla protezione dei dati viene attribuita esplicitamente dallo stesso GDPR e che consente di modulare il contenuto della pretesa individuale sulla base di interessi

---

[135] Tra gli altri, v. C. COLAPIETRO – A. IANNUZZI, *App*, cit., 796 ss., i quali tuttavia riterrebbero non inammissibile la (peraltro più invasiva) opzione della introduzione di un obbligo legale di utilizzo dello strumento. Le tre manifestazioni di consenso da parte dell'utilizzatore dell'app riguardano sia la scelta in sé di scaricarla, sia la sua effettiva attivazione che infine la procedura per la specifica attivazione delle notifiche in caso di contagio). In tema, ampiamente, anche C. BERGONZINI, *Non solo* privacy. *Pandemia*, contact tracing *e diritti fondamentali*, in *dirittifondamentali.it*, n. 2/2020, spec. 711 ss.

[136] In questo senso, infatti, si esprimono, in generale, le *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679* dell'*European Data Protection Board* del 4 maggio 2020, reperibili sul sito istituzionale, 8 ss.; con riferimento specifico alla necessaria volontarietà delle app di tracciamento, si veda il documento di poco precedente *Linee guida 4/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, adottate dallo stesso Comitato il 21 aprile 2020.

[137] Favorevole a misure incentivanti è, per esempio, M. PLUTINO, *"Immuni"*, cit., 569 ss.

[138] Concordo, in tal senso, con M. OREFICE, *L'app*, cit., 184.

[139] Segnalate, tra gli altri, da M. OREFICE, *L'app*, cit., 183, la quale lamenta che lo stesso Garante abbia trascurato le modalità concrete di funzionamento, come il fatto che *Immuni* risultasse compatibile solo con alcuni modelli, più recenti e costosi, di *smartphone*. Sennonché, è ovviamente doveroso pretendere che la scelta dello strumento cada su quello che consenta al maggior numero di persone di usufruire dei relativi benefici, per quanto tecnicamente possibile (e del resto diversi dei problemi che l'A. segnala sono poi stati risolti in tempi brevi), ma ciò non può portare ad escludere in radice una misura siffatta, qualora non riesca (come mai riuscirà) ad essere universale. Stante la situazione emergenziale, infatti, mi pare che compito dello Stato sia quello di contenere al massimo la diffusione del contagio, dotando la maggior parte possibile di popolazione degli strumenti utili, senza rinunciarvi *in toto*, in assenza di alternative, qualora una piccola parte (si pensi a chi uno *smartphone* non ce l'ha proprio, per esempio) ne restasse esclusa. Senza peraltro contare, come giustamente rilevano C. COLAPIETRO – A. IANNUZZI, *App*, cit., 791, che resta pur sempre il tracciamento manuale per le fasce non coperte dal *contact tracing*, di modo che i due strumenti risultano complementari, aumentando l'efficacia dell'intervento e dotando di strumenti più efficienti l'Autorità sanitaria.

[140] Come la decisione di evitare di introdurre «l'obbligo di un utilizzo di una applicazione tecnologica [che] sarebbe stato vissuto dai cittadini come un'imposizione, magari ingenerando comportamenti tendenti ad eludere l'obbligo» (così ancora C. COLAPIETRO – A. IANNUZZI, *App*, cit., 792, i quali invero considerano questo come un profilo giuridico, laddove invece a me pare sia una considerazione di opportunità in relazione alla maggiore efficacia dello strumento regolatorio).

collettivi (*i. e*. la tutela della salute, espressamente qualificata tale dall'art. 32 Cost.) concorrenti[141]. Con la posizione assunta in sede di regolazione, invece, si è posto al centro un problema – quello della privacy – che soluzioni tecniche consentivano (come hanno consentito) di minimizzare, limitando questo diritto in modo assolutamente proporzionale al vantaggio che sarebbe derivato in termini di tutela della salute[142], mentre sono rimasti nell'ombra i veri punti nevralgici della questione.

Mi riferisco, anzitutto, alla necessità, in ottica di eguaglianza sostanziale, laddove il ricorso alla tecnologia possa fornire strumenti più efficaci a tutela di un diritto (la salute, nella fattispecie) di porre in essere misure adeguate a prevenire ed evitare la situazione per cui «l'ignoranza informatica si traduce in un distanziamento tecnologico che a sua volta produce un effetto […] di distanziamento costituzionale»[143]. La vera questione, insomma, è quella di porre tutti nella condizione di fare ricorso all'app, rimuovendo gli ostacoli di fatto (si legga: *digital divide*), che ne avrebbero impedito la fruizione verosimilmente proprio a danno delle fasce più vulnerabili al contagio, anziani *in primis*. Infatti, «occorre […] sgomberare il campo dall'ambiguità di fondo che si cela nel dibattito pubblico sull'app: potere-non-averla non equivale a non-poterla-avere», di modo che si «pone un grande problema di tutela dell'uguaglianza sostanziale tra chi è effettivamente libero di non scaricare l'app (perché, pur potendolo fare, non lo fa) e chi non la scarica perché non ne ha la possibilità»[144].

Non meno rilevante, in secondo luogo, era il tema dell'opportunità di contrastare la diffusione del virus non (sol)tanto a livello nazionale ma europeo, anche tramite una applicazione unica e condivisa tra i vari Stati membri[145]: unitarietà di risposta che, tuttavia, non vi è stata (anche) per scelte di carattere tecnico in cui la protezione dei dati ha comunque avuto un proprio peso.

5. Tra presente e futuro: quale tutela nel mondo digitale?

---

[141] Sul tema v. A. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 586 ss.

[142] Anzi, come scrivono F. VARI – F. PIERGENTILI, *"*To no other end, but the... Safety, and publick good of the people*": le limitazioni alla protezione dei dati personali per contenere la pandemia di Covid-19*, in *Rivista AIC*, n. 1/2021, spec. 334 ss., la limitazione della privacy, anche conseguente all'introduzione di un uso obbligatorio dell'app in questione, sarebbe stata la misura meno invasiva per i diritti e le libertà costituzionali, considerate nel loro complesso, specialmente se posta a confronto con un *lockdown*, dagli effetti devastanti anche in termini economici.

[143] Il rilievo si deve ad A. RUGGERI, *Società tecnologicamente avanzata e Stato di diritto: un ossimoro costituzionale?*, in *Consulta OnLine*, 2020, 284 ss., che si pone nella prospettiva della (costituzionalmente dovuta) ricerca di efficaci strumenti in tale direzione, a fronte di uno (inevitabile ma non certo privo di vantaggi ed effetti positivi) spostamento crescente delle forme e dei mezzi di garanzia dei diritti verso il mondo digitale.

[144] Così E. CREMONA, *Contact tracing. Governance pubblico-privata e primi problemi di tutela dei diritti fondamentali*, in *Ianus - diritto e finanza*, 21 maggio 2020, 9 ss.

[145] Come condivisibilmente affermato da L. TRUCCO, *App Immuni: una storia stran(ier)a e incompiuta*, in *giustiziainsieme.it*, 18 maggio 2021, sarebbe stato invero opportuno approntare «una piattaforma comune ("paneuropea"), solida e capillarmente diffusa tra i vari Stati membri» di modo da contrastare non già a livello di singoli Stati membri ma sovranazionale la diffusione del virus.

Il progresso tecnologico, così come lo sviluppo prorompente e dilagante del mondo digitale e dell'informatica, non può realisticamente essere limitato: non può (e, sotto questo profilo, non deve) in quanto comporta inevitabili vantaggi e maggiori mezzi anche a garanzia dei diritti e degli interessi costituzionali[146], e non può in quanto al contempo vi è la materiale impossibilità di arrestare un processo di questo tipo, pure laddove lo si giudicasse negativamente.

Se questo è vero, allora, anche in relazione all'impatto su privacy e identità, il problema non è quello di scegliere tra l'opposizione o l'incentivazione del progresso tecnologico, quanto piuttosto quello di individuare gli strumenti ed i percorsi più idonei a beneficiare dei vantaggi che le tecnologie possono apportare, riducendone al contempo le esternalità negative[147]. In questo senso, diverse sono le direzioni verso cui ci si può indirizzare e, se recentemente mi pare che, già *de jure condito*, in diversi ordinamenti, come vedremo, sia emerso un interessante percorso, altri se ne potrebbero aggiungere. Infatti, a mio avviso, per un verso, qualche cosa si potrebbe ancora suggerire in termini di possibili spunti di revisione (*rectius* integrazione) del quadro normativo vigente, mentre, per altro verso, sempre *de jure condendo* ma a più lungo termine, si profilano all'orizzonte proposte normative promettenti – e di carattere più generale – sia per una rinnovata tutela, in via diretta, dei diritti oggetto qui di attenzione, sia, attraverso di essi, per la ricerca di una soluzione al ben più ampio complesso di questioni di fondamentale rilevanza per il diritto costituzionale, che ho cercato di enucleare in precedenza, implicate indirettamente della tutela della privacy e coinvolgenti, di fatto, l'intero sistema di governo della rete.

Provo ad approfondire, di seguito, le tre possibili soluzioni cui ho testé accennato.

5.1. Un percorso *de jure condito*

In primo luogo, *de jure condito*, se le garanzie approntate dal GDPR appaiono deficitarie per le ragioni già viste, mi sembra che vada valorizzato il tentativo di diverse *Authorities* di fare ricorso tanto alla legislazione a tutela della concorrenza quanto a quella consumeristica per offrire, seppure indirettamente, una maggiore e più efficace difesa anche alla privacy (e con essa, per il legame che ho ripetutamente sottolineato, all'identità).

In primo luogo, infatti, le *Big Tech*, cui ho fatto più volte riferimento, sono imprese che ricadono inevitabilmente nel raggio di azione della normativa concorrenziale, essendo palesemente in posizione dominante nei rispettivi mercati[148], dove rivestono un ruolo che la letteratura economica ha recentemente definito di "moligopolio"[149], onde sottolineare che esse si dovrebbero

---

[146] In questo senso, ad esempio, T. E. FROSINI, *Il costituzionalismo*, cit., 1 ss.; ed A. RUGGERI, *Società*, cit., 285, il quale rileva come «i diritti hanno avuto (ed hanno) non poco guadagno dallo sviluppo scientifico e tecnologico che ha messo a disposizione dell'uomo risorse ancora fino a poco tempo addietro inimmaginabili», seppure – precisa l'Autore – la diffusione dell'informatizzazione in ogni settore esponga gli stessi anche al rischio di danni irreparabili.

[147] Analogamente, scrive A. SANTOSUOSSO, *La regola*, cit., 612, che «il problema non è tecnologie sì o no, ma tecnologie come».

[148] Per un'analisi precisa con riferimento a *Google*, v. M. OREFICE, *I Big data*, cit., spec. 722 ss.

[149] V. in particolare, da ultimo, l'opera di N. PETIT, *Big Tech and the Digital Economy. The Moligopoly Scenario*, Oxford, 2020, ove l'A. riprende discorsi già sviluppati in lavori precedenti.

considerare contemporaneamente come monopoliste, rispetto agli specifici prodotti o servizi che ne rappresentano il *core business*, a causa di una sostanziale infungibilità degli stessi, e come oligopoliste, in relazione alla molteplicità di mercati (del mondo digitale) affini. Tra l'altro, la posizione dominante di queste imprese appare via via crescente e in corso di consolidamento, grazie a frequenti operazioni di incorporazione di nuove realtà imprenditoriali emergenti in forma di *start-up*, che ben rientrano nel novero delle concentrazioni, pure oggetto di disciplina antitrust[150].

Ebbene, ad aver attirato l'attenzione delle Autorità per la concorrenza è l'abuso che, in più occasioni, queste aziende fanno della loro posizione dominante, e ciò proprio grazie alle immense masse di dati personali di cui esse dispongono e che rappresentano il loro patrimonio più prezioso, non solo sotto il profilo della valutazione economica in sé, ma anche come arma a loro disposizione per sfruttare il mercato senza incontrare ostacoli particolari. Così che, in materia, si può realizzare, ritengo, un incrocio virtuoso tra disciplina *antitrust* e normativa a tutela della privacy[151], tanto che, a dispetto della presa di posizione originaria della Commissione europea, che rifiutava di vedere una connessione tra i due ambiti[152], oggi diverse Autorità preposte alla garanzia della concorrenzialità del mercato, in Europa come negli Stati Uniti, hanno avviato procedimenti nei confronti delle *Big Tech*[153].

---

[150] Lo rileva M. MIDIRI, *Privacy*, cit., 232.

[151] La cui opportunità, in dottrina, è oggetto di dibattito già da alcuni anni: cfr., per esempio, M. STUCKE – A. GRUNES, *Big Data and Competition Policy*, Oxford, 2016; F. COSTA-CABRAL – O. LYNSKEY, *Family Ties: The Intersection between Data Protection and Competition in EU Law*, in *Common Market Law Review*, vol. 54, n. 1/2017, 11 ss. Recentemente, nella dottrina italiana, v. le ampie considerazioni di T. MAURO, *I* big data, cit., 661 ss., il quale sottolinea come le due normative, pur operando su presupposti diversi, si applichino sullo stesso terreno, in cui è la protezione dei dati ad assumere un ruolo centrale, stante la sostanziale integrazione, nella società attuale, tra mondo digitale e reale.

[152] Mi riferisco a quanto stabilito dalla Commissione Europea, per esempio, nel caso *Google/DoubleClick* (Decisione 11 marzo 2008 nel caso COMP/M.4731, in particolare il par. 368) od ancora in quello *Facebook/WhatsApp*, (Decisione 3 ottobre 2014 nel caso COMP/M.7217, spec. par. 164, in cui l'Istituzione eurounitaria afferma espressamente che «any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules»).

[153] Tra i quali, oltre a quello di cu dirò a breve nel testo, si possono ricordare, senza pretesa di esaustività e per limitarci ai più recenti, almeno, negli Stati Uniti: 1) quello promosso dal Dipartimento di Giustizia e 11 Stati contro *Google* per l'abuso di posizione nel mercato dei motori di ricerca *on line* (v. il comunicato stampa del 20 ottobre 2020 disponibile sul sito del Dipartimento); 2) quelli promossi dalla *Federal Trade Commission* e da ben 46 Stati contro *Facebook*, in relazione all'acquisizione di *Instagram* e *WhatsApp* (si veda il comunicato pubblicato sul proprio sito web dall'Antitrust americana il 9 dicembre 2020; nonché, nell'UE, 3) quello avviato dalla Commissione Europea contro *Amazon* (AT 40462) per lo sfruttamento a proprio diretto vantaggio di dati non pubblici in possesso dei venditori che operano sulla sua piattaforma, avviato nel 2019 e formalizzato in una contestazione degli addebiti nel novembre 2020; 4) quello aperto dall'Autorità Garante della Concorrenza e del Mercato contro *Google* per l'abuso di posizione dominante nel mercato della raccolta pubblicitaria *on line* (che per l'azienda vale diversi miliardi di dollari, se si considera che il 92% dei suoi ricavi deriva dalla divisione "*Google Services*", in cui rientra la pubblicità, come si evince dal rapporto annuale *Form 10-K* del 2020 reperibile sul sito della *Securities and Exchange Commission* statunitense, Item 7) realizzato sfruttando le enormi capacità di raccolta di dati sui singoli consumatori attraverso cookies ed altri sistemi di tracciamento (si veda il comunicato relativo al procedimento A542 del 28 ottobre 2020 pubblicato sul sito istituzionale dell'Antitrust).

Il più significativo di questi, limitandoci all'area dell'Unione europea in cui trova applicazione la normativa sovranazionale sulla protezione dei dati, è certamente quello avviato nel 2016 e concluso tre anni dopo dall'Autorità Nazionale della Concorrenza tedesca contro Facebook, società imputata di realizzare un illecito concorrenziale attraverso condizioni contrattuali per l'accesso al *network*, che subordinavano l'utilizzo del *social*, rendendo di fatto non libero il consenso dell'utente, alla circostanza che l'impresa potesse raccogliere dati e informazioni (relativi all'utente stesso ed al suo dispositivo) anche grazie ad altri servizi facenti sempre capo all'azienda (nella specie, in particolare, *WhatsApp* ed *Instagram*) o a soggetti terzi; dati e informazioni che sarebbero poi stati in un secondo momento combinati ed elaborati, a fini di profilazione, senza il consenso degli interessati[154]. La vicenda è estremamente interessante per il fatto di rappresentare il caso più evidente ed esplicito di contatto tra le due discipline, poiché la violazione delle regole a protezione della privacy è individuata come il mezzo stesso per eludere la normativa concorrenziale[155]. Ma un non minore interesse risiede nel fatto che il provvedimento ha avuto un seguito giudiziario travagliato[156], che da ultimo ha portato l'*Oberlandesgericht* di Düsseldorf a sollevare, nel marzo del 2021, una questione incidentale alla Corte di Giustizia dell'Unione europea, il cui verdetto sarà decisivo per l'avallo o il definitivo abbandono della strada intrapresa verso un'integrazione delle discipline della protezione dei dati e della concorrenza.

Peraltro, a ben vedere, anche il GDPR mostra già qualche timido tentativo di regolazione in questa direzione, come testimonia la norma di cui all'art. 20 sul diritto alla portabilità dei dati, ai sensi del quale, quando il trattamento, che avvenga in forma automatizzata, ha come base giuridica il contratto o il consenso, «l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti». Ora, certamente la norma è ispirata (anche) ad una logica pro-concorrenziale, nel tentativo di impedire che il fornitore di un servizio digitale "blocchi" di fatto l'utente paventando il rischio che il passaggio ad altro operatore comporti la perdita di dati o anche solo la difficoltà di trasferirli[157]. Tuttavia, è piuttosto evidente

---

[154] Tra i vari commenti a questa vicenda, nei sui diversi passaggi, si vedano almeno M. MIDIRI, *Privacy*, cit., 220 ss.; C. OSTI – R. PARDOLESI, *L'antitrust ai tempi di Facebook*, in *Mercato Concorrenza Regole*, 2019, 195 ss.; A. GIANNACCARI, *Facebook e l'abuso da sfruttamento al vaglio del* Bundesgerichtshof, in *Mercato Concorrenza Regole*, 2020, 403 ss.; e C. KOENIG, *Exploit to Exclude: Federal Court of Justice Considers Facebook's Data Policy to Violate Competition Law*, in *European Competition and Regulatory Law Review*, vol. 4, n. 4/2020.

[155] Per dirla con le parole di M. MIDIRI, *Privacy*, loc. cit., «non rientra nella concorrenza basata sui meriti un'attività imprenditoriale che viola discipline legali, pur estranee al diritto della concorrenza […] Vi è dunque una strada per utilizzare la normativa sulla protezione dei dati come *benchmark* normativo».

[156] Il provvedimento amministrativo, infatti, è stato sospeso in via cautelare con una decisione giudiziale annullata tuttavia in sede di appello dal *Bundesgerichtshof* (con argomentazioni, però, diverse da quelle che sorreggevano l'atto dell'Autorità per la concorrenza), e la questione è oggi in attesa della decisione di merito (di primo grado).

[157] Un cenno in tale direzione si legge in L. BIANCHI, *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di), *Circolazione*, cit., 223 ss., la quale evidenzia come esso dovrebbe agire, in ipotesi, da stimolo per implementare *best practices* in tema di trattamento quale elemento di concorrenzialità sul mercato. Sul rapporto tra diritto alla portabilità e disciplina *antitrust* v. G. M. RICCIO – G. SCORZA – E. BELISARIO, *GDPR e normativa privacy*, Milano,

che essa offre un arsenale non troppo rifornito, anche perché, come è stato osservato, non solo quanto maggiore è il numero di informazioni conferite ad un fornitore di servizi tanto maggiore sarà (almeno percepito) il costo del passaggio ad un altro, così che, nei casi in cui il meccanismo potrebbe operare, vi sono ostacoli di fatto che spingono in direzione contraria, ma soprattutto non va trascurato l'effetto *network*, per cui la migrazione ad altro fornitore potrebbe far perdere quei vantaggi in termini di integrazione di servizi prestati dallo stesso fornitore[158].

Se la legislazione *antitrust* sembra oggi rappresentare uno dei fronti più avanzati, nel tentativo di colmare la strutturale inadeguatezza del quadro normativo vigente in tema di privacy tanto da costituire una via da percorrere, da parte dello Stato, per offrire una maggiore e più effettiva tutela alle situazioni soggettive di cui parliamo[159], un percorso analogo e strettamente collegato a quello avviato in Germania merita di essere ricordato nel nostro Paese per quanto riguarda la disciplina della tutela dei consumatori, ugualmente utilizzata "in combinato disposto" con quella sulla protezione dei dati personali. Ciò che, del resto, non stupisce se si pensa, per un verso, alle molte analogie esistenti tra la posizione del consumatore e quella dell'interessato, entrambi tutelati come soggetti vulnerabili attraverso normative di derivazione eurounitaria, nonché, per altro verso, al legame ben noto tra promozione della concorrenza e tutela del consumatore[160], non a caso affidate al medesimo soggetto regolatore, di modo che se la prima può essere utilizzata a fini di garanzia della privacy non è sorprendente che anche la seconda possa esserlo[161].

In questa prospettiva, una vicenda particolarmente significativa è quella che ha visto l'Autorità Garante della Concorrenza e del Mercato sanzionare, con provvedimento 29 novembre 2018, n. 27432, la società Facebook in quanto, da un lato, la gratuità dell'iscrizione al *social* veniva considerata pratica ingannevole, giacché all'interessato era fornita un'informativa sul trattamento dei dati personali talmente poco chiara che all'utente non sarebbe risultato evidente che la cessione dei dati avrebbe rappresentato una controprestazione per il servizio, mentre, dall'altro lato, veniva qualificata come pratica aggressiva quella già oggetto del provvedimento tedesco, in quanto il consenso dell'interessato finiva per essere condizionato dall'avere come unica alternativa all'accettazione della condivisione dei dati la rinuncia totale al servizio. Ora, appare di grande interesse il fatto che una stessa pratica, lesiva della protezione dei dati, abbia ricevuto tutela in due

---

2018, 209 ss., anche per la confutazione di alcune tesi volte a sminuire l'efficacia dell'art. 20 GDPR ai fini qui considerati; nonché, ampiamente, M. BORGHI, *Portabilità*, cit., 223 ss.

[158] Così M. BORGHI, *Portabilità*, cit., spec. 240 ss., il quale invero esprime dubbi sull'effettivo impatto della norma. Non a caso, del resto, come si vedrà *infra*, nel paragrafo 5.3., la proposta di *Digital Market Act*, volta ad introdurre maggiore ed effettiva concorrenzialità nei mercati digitali, interviene (anche) su questo diritto, cercando di migliorarne l'incisività.

[159] Secondo un auspicio espresso in modo assai argomentato da G. DE MINICO, *Big Data*, cit., 99 ss.

[160] In dottrina l'auspicio che nei mercati digitali operassero congiuntamente le tre discipline della concorrenza, della *data protection* e della tutela dei consumatori era stato avanzato, per esempio, da W. KERBER, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, in *Journal of Intellectual Property Law & Practice*, vol. 11, 11/2016, 856 ss. In tema anche M. MIDIRI, *Privacy*, cit., 212, che parla di «tre settori distinti, ma uniti da "legami di famiglia". Questi legami sono i principi del diritto europeo e delle costituzioni nazionali».

[161] L'uso della normativa consumeristica in "combinato disposto" con quella in tema di protezione dei dati è oggetto di analisi da parte di C. ALVISI, *Dati personali*, cit., 673 ss.

Stati europei differenti ricorrendo a due normative afferenti ad ambiti diversi (ma entrambe pur sempre con forti origini nel diritto sovranazionale), sancendo così un quadro in cui le misure di garanzia si intrecciano e laddove quelle dirette non bastano, altri rami dell'ordinamento soccorrono.

Questa integrazione (verrebbe da dire, giustapposizione) di tutele, nel caso italiano, ha inoltre ricevuto un importante avallo dalla giurisprudenza, giacché il ricorso avverso il provvedimento amministrativo dell'*Antitrust* è stato accolto, ma solo limitatamente al secondo dei presunti illeciti sanzionati, da parte del TAR Lazio – Roma con le sentenze sez. I, 10 gennaio 2020, nn. 260 e 261[162], confermate poi, in appello, dalla recente statuizione del Consiglio di Stato, sez. VI, 29 marzo 2021, n. 2631. Quest'ultima pronuncia, in uno con le decisioni impugnate, prima ancora che per il merito, assume una particolare importanza per il fatto di dare corpo ad una nuova prospettiva, laddove essa, a monte del *decisum*, fa riferimento all'«esigenza di garantire "tutele multilivello" che possano amplificare il livello di garanzia dei diritti delle persone fisiche, anche quando un diritto personalissimo sia "sfruttato" a fini commerciali, indipendentemente dalla volontà dell'interessato-utente-consumatore»[163]. Insomma, nel tentativo di conciliare l'assunto della indisponibilità dei diritti della personalità, tra cui evidentemente rientra quello in esame, con la indubitabile assunzione di valore economico dei dati, senza per questo ritornare ad una concezione di tipo proprietario di essi, il giudice amministrativo postula una sorta di scissione tra l'esercizio dei diritti dell'interessato, che risponde alla logica personalistica e trova disciplina nel GDPR e nelle norme interne di attuazione e integrazione, e lo sfruttamento del dato da parte della società che fornisce il servizio, per la quale esso non rappresenta altro che un *asset* economico, oggetto di negozi di scambio, nei quali tuttavia la imperfetta informazione dell'interessato ridonda in pratica commerciale scorretta[164], potendo così trovare parallela ma autonoma applicazione la disciplina consumeristica. Un ragionamento analogo, del resto, era già stato proposto in dottrina[165], nel sottolineare come attraverso la profilazione il titolare produca in effetti un nuovo bene giuridico, sganciato dalla dimensione personale e possibile oggetto di diritto esclusivo di sfruttamento e cessione, secondo il tipico regime proprietario. Il che, in effetti, sembra a mio avviso trovare anche un riscontro normativo, e precisamente nella esclusione dal diritto alla portabilità dei dati diversi da quelli che siano stati forniti direttamente dall'interessato, come appunto le elaborazioni che su di esse abbia compiuto il titolare.

La problematicità di questa prospettiva, per le questioni di vasta portata che implica, in primo luogo sulla ammissibilità, dal punto di vista dogmatico, dell'utilizzo di dati come corrispettivo

---

[162] Su cui A. L. TARASCO, *"Facebook" è "gratis"? "Mercato" dei dati personali e giudice amministrativo*, in *Dir. econ*, 2020, 265 ss.; e M. MIDIRI, *Privacy*, cit., 226 ss.

[163] Punto 8 della parte motiva della decisione.

[164] Per dirla ancora con le parole del Collegio, «nell'appena descritta accezione non viene in emersione la commercializzazione del dato personale da parte dell'interessato, ma lo sfruttamento del dato personale reso disponibile dall'interessato in favore di un terzo soggetto che lo utilizzerà a fini commerciali, senza che di tale destino l'interessato conosca in modo compiuto le dinamiche».

[165] Per esempio da V. RICCIUTO, *La patrimonializzazione dei dati personali*, in in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 48 ss.

negoziale, è evidente[166]. Tuttavia, se è vero che la posizione del Consiglio di Stato, nel separare il dato, per quanto concerne la sfera di disponibilità dell'interessato, come elemento della personalità, dal dato, in possesso del Titolare, come bene economico, può sembrare eludere, più che risolvere, il problema, a me pare che, *rebus sic stantibus*, essa rappresenti l'ottica più idonea tanto a descrivere la realtà attuale del mondo virtuale[167] quanto ad offrire un immediato strumento, in attesa di eventuali significativi interventi che spettano al decisore politico[168], di risposta alle esigenze di tutela effettiva per i diritti oggetto della nostra indagine[169]. Non solo, ma la prospettiva del giudice amministrativo appare, al contempo, promettente di ulteriori sviluppi, alla luce della complementarietà tra due discipline differenti, ma di fatto convergenti nell'offrire una più completa garanzia ad un medesimo interesse, intaccato (accerchiato, verrebbe quasi da dire) da minacce di natura diversa.

In questa stessa ottica, potrebbero rinvenirsi soluzioni ulteriori, ad esempio, a salvaguardia dell'autodeterminazione informativa in senso più ampio[170]. L'inserimento, a tacer d'altro, nell'art. 26, comma 1, lett. c) del d. lgs. n. 205 del 2006 (Codice del consumo), tra le pratiche commerciali aggressive, idonee a limitare la libertà di scelta o di comportamento del consumatore, dell'ipotesi di ripetute sollecitazioni commerciali, appare significativo, tanto più per il fatto che la stessa norma, non a caso, richiama espressamente anche il Codice della privacy come disciplina di cui è fatta salva la parallela applicazione. Di modo che appare evidente come sia già presente nel diritto positivo (almeno) un caso in cui esplicitamente la normativa consumeristica si presenta come complementare a quella posta a garanzia della privacy.

5.2. Una proposta *de jure condendo*

In ottica *de jure condendo*, ma pur sempre muovendoci all'interno delle coordinate che caratterizzano il *corpus* normativo vigente, credo che vi sia un aspetto interessante su cui l'attenzione della dottrina – e ancor più del legislatore – non è stata adeguata[171]: il tema dei mezzi di tutela collettivi per la protezione dei dati.

---

[166] La questione è stata rilevata subito da G. SCORZA, *Si può fare commercio di dati personali?*, in *Agendadigitale.eu*, 30 marzo 2021, che giustamente sottolinea come si aprano anche altri interrogativi, fondamentalmente legati alla necessità di individuare l'Autorità competente e le modalità procedurali in tutte le ipotesi di "concorrenza di competenze".

[167] Giacché, come scrive V. RICCIUTO, *La patrimonializzazione*, cit., 45, negare che la fornitura di dati sia la controprestazione di uno scambio negoziale sarebbe «una lettura "ipocrita" del fenomeno» che potrebbe sostenere solo chi viva bendato in una stanza buia.

[168] Di cui le proposte descritte *infra*, al paragrafo 5.3 rappresentano un esempio, sebbene non nella prospettiva di superare il meccanismo alla base dell'attuale sistema, ovvero quello del dato come bene economico (anche) di scambio.

[169] Così lo stesso G. SCORZA, *Si può fare*, cit., il quale sottolinea come nei fatti si assista proprio al paradosso per cui i dati personali rappresentano l'identità di un individuo, ma al contempo sono oggetto di rapporti commerciali.

[170] Suggerimenti in questa direzione possono leggersi in C. ALVISI, *Dati personali*, cit., spec. 688 ss.

[171] Con alcune eccezioni, tra cui quella, come sempre formulata con lungimiranza, di S. RODOTÀ, *Tecnopolitica*, cit., spec. 156 ss., ove l'A. intuiva già molto tempo addietro, con riferimento ad azioni collettive ed al

Il GDPR, in effetti, al riguardo, dimostrando indubbiamente un certo *favor* per siffatti strumenti[172], prevede all'art. 80 che «l'interessato abbia il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto» i rimedi amministrativi e giurisdizionali sia nei confronti dell'Autorità di controllo che del titolare o del responsabile, oltre che di agire in via risarcitoria ove previsto dall'ordinamento.

Ora, a me pare che si tratti di una previsione importante, che offre uno strumento in più di cui avvalersi per dare maggiore effettività di tutela alle plurime situazioni soggettive che il Regolamento intende garantire. Non è certo raro, a ben vedere, il caso in cui il singolo interessato si trovi in una difficoltà di fatto ad esercitare i propri diritti, vuoi per ignoranza degli stessi, vuoi per incapacità di fare ricorso ai mezzi di tutela all'uopo predisposti, vuoi ancora per il carattere bagatellare (a livello del singolo rapporto, ma verosimilmente non a livello aggregato) degli interessi in gioco. In tutte queste ipotesi, l'affidamento dell'esercizio dei diritti ad un soggetto, privo di scopo lucrativo, può dare sostanza ad interessi, altrimenti lasciati privi di una tutela effettiva. E, se è vero che sulla base del dettato normativo ciò è già possibile, è pur vero, a mio avviso, che si renderebbe opportuno un intervento normativo integrativo, almeno a livello nazionale, che sostenesse e fornisse un quadro regolativo più preciso a questi enti collettivi[173], prevedendo misure volte a favorirne l'istituzione ed a sostenerne lo svolgimento delle funzioni (non necessariamente con interventi di carattere finanziario). Del resto, da tempo è stato rilevato come sia andato maturando, in generale, un modello costituzionale di promozione attiva dell'associazionismo proprio in correlazione ad interessi diffusi emergenti in campo sociale contro il potere privato dei grandi gruppi di interesse[174]: modello che, *optimo jure*, meriterebbe di trovare espansione anche con riferimento alla tutela della privacy.

Se poi guardiamo alle analoghe branche dell'ordinamento in cui, attraverso enti collettivi di rappresentanza, si cerca di rimediare allo squilibrio tra un singolo individuo ed enti di dimensioni e forza (anche contrattuale) incommensurabili, quali il diritto del lavoro ed il diritto dei consumatori, si potrebbe forse ipotizzare l'introduzione di previsioni ancor più incisive. Ad esempio, la consultazione delle parti interessate ai fini della redazione della valutazione di impatto, ovvero uno dei documenti nei quali si sostanzia l'*accountability* del titolare, il quale deve provvedervi «quando un tipo di trattamento, allorché prevede *in particolare l'uso di nuove*

---

possibile intervento di associazioni di consumatori o di utenti, che «le strategie di tutela della *privacy* […] esigono molteplici strumenti, tra loro non incompatibili, e che, almeno in talune situazioni, possono operare congiuntamente».

[172] Sul punto v. G. M. RICCIO – G. SCORZA – E. BELISARIO, *GDPR*, cit., 588 ss., i quali evidenziano come la norma rappresenti una delle novità più rilevanti del GDPR.

[173] Tra le (assai poche) indicazioni che possono trarsi in via interpretativa dal Regolamento, secondo A. CANDINI, *Gli strumenti di tutela*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento*, cit., 590, vi è quella per cui, non essendo richiesta la protezione dei dati come finalità esclusiva dell'ente, anche Associazioni con finalità più ampie – *in primis* la difesa dei consumatori – potrebbero rientrare nel novero di essi.

[174] Cfr. G. GEMMA, *Costituzione ed associazioni: dalla libertà alla promozione*, Milano, 1993, spec. 190 ss.

tecnologie […] può presentare un rischio elevato per i diritti e le libertà delle persone fisiche»[175] potrebbe essere introdotta, almeno per alcuni casi in cui le situazioni soggettive al nostro esame siano in pericolo, come obbligatoria e magari delegabile (anche) a soggetti collettivi di rappresentanza. Allo stesso modo, la consultazione delle parti interessate per l'adozione dei codici di condotta da parte da parte di organismi rappresentanti le categorie degli interessati, suggerita dal *Considerando* n. 99, potrebbe essere prevista come necessaria misura procedimentale, coinvolgendo anche dal lato delle categorie di interessati le associazioni di rappresentanza. Od ancora, se è vero, come ho cercato di dimostrare, che il consenso si rivela in diverse ipotesi uno strumento di garanzia meramente formale di autodeterminazione informativa, a causa delle circostanze fattuali che circondano il suo rilascio, si potrebbe ragionare, limitatamente ai casi più delicati, di un consenso validamente espresso solo "in sede protetta", per mutare una terminologia del diritto sindacale, ovvero solo con una qualche forma di assistenza, compatibile con lo sviluppo dell'economia digitale, da parte di uno di questi enti collettivi, anche solo incanalando l'acquisizione dello stesso in una procedura concordata, magari nel contesto di un codice di condotta[176], con enti di rappresentanza degli interessi…degli interessati.

Peraltro, l'analogia con altri settori ordinamentali non si arresta qui, se si considera che il secondo paragrafo della medesima disposizione del GDPR prima riportata già prevede altresì la facoltà per gli Stati membri di stabilire un'autonoma legittimazione degli stessi enti collettivi ad agire a difesa di interessi collettivi[177].

Si tratta, in questo caso, di una opzione di cui il legislatore italiano non ha ritenuto di avvalersi[178], benché non manchino certo nell'ordinamento attuale ipotesi di tal fatta, ad esempio in materia ambientale o, ancora una volta, consumeristica. Epperò, a mio avviso è stata persa l'occasione per offrire uno strumento di difesa che potrebbe rivelarsi estremamente utile[179], specialmente laddove dovessero crearsi *network* europei, analoghi a quello delle Autorità di controllo, anche tra questi organismi di rappresentanza, la cui forza collettiva potrebbe tentare di esercitare pressioni e proporre azioni anche verso colossi della società digitale, di fronte ai quali abbiamo visto come la debolezza strutturale del GDPR stia proprio nell'aver immaginato un tradizionale rapporto bilaterale, che non corrisponde più alla realtà attuale. Ma se quella, in sé debole, previsione, viene proiettata su più ampia scala, sommando, per così dire, le frantumate

---

[175] Cfr. art. 35, par. 1, GDPR. Il corsivo è mio.

[176] Per la cui elaborazione, del resto, il *Considerando* n. 99 già prevede che gli organismi di rappresentanza dei titolari e dei rappresentanti dovrebbero consultare le parti interessate.

[177] In tema A. MANTELERO, *La* privacy, cit., 1202 ss., ove l'A. sottolinea come, per un verso, l'analogia sia più forte con l'ambito consumeristico di quanto non lo sia con quello lavoristico, stante l'indeterminatezza del gruppo costituito dagli interessati, non immediatamente identificabile *a priori*, sebbene, per altro verso, nel contesto della protezione dei dati azioni collettive rischierebbero di incontrare un limite nella difficoltà di reazioni tempestive, per la difficoltà stessa degli interessati di venire a conoscenza della lesione che stanno subendo.

[178] Invero non certo in modo isolato, giacché nella stessa direzione si orientata la maggior parte dei Paesi UE, come rammaricato dal Parlamento europeo nella *Risoluzione* citata del 25 marzo 2021, al cui punto 18 si invitano gli Stati membri ad avvalersi dell'opzione offerta dal GDPR.

[179] Analogamente G. DE MINICO, *Big Data*, cit., 98, che invero critica il legislatore europeo per non avere introdotto una «*class action*, la cui spersonalizzazione del legittimato all'azione processuale ben si combina col concetto di danno diffuso».

situazioni soggettive individuali, allora potrebbe prendere corpo una forma di garanzia in grado forse di rappresentare un'arma più efficace. Di modo che, occorrerebbe sul punto sia un'azione a livello europeo di sostegno alla creazione di reti tra enti di rappresentanza collettiva, sia un intervento normativo a livello nazionale per creare il rimedio giudiziale necessario al fine di mettere in grado, anche nel nostro Paese, questi soggetti di procedere nel senso auspicato[180].

5.3. Volgendo lo sguardo all'orizzonte

Seppure in una prospettiva di (ben) più lungo termine, ed ancora *de jure condendo*, c'è a mio parere una terza via, che mi sembra indirizzata verso una direzione meritevole di essere percorsa. Mi riferisco, in questo caso, al ripensamento complessivo della *governance* dei dati, che, sulla base della *Strategia europea per i dati* elaborata dalla Commissione[181], si è tradotta in una proposta di Regolamento, destinato a comporre, con il GDPR e altri due atti normativi presentati in materia di servizi e di mercati digitali[182], un *corpus* normativo, dal cui complesso potrebbero trovare almeno un principio di soluzione anche quelle nuove esigenze di tutela che la privacy richiede nella sua dimensione attuale, ancora una volta mutate a seguito del nuovo contesto tecnologico[183].

Un'analisi, seppure per sommi capi, di alcuni contenuti essenziali di questi atti normativi mi pare a questo punto opportuna, in quanto essi testimoniano di una sensibilità volta ad un approccio al tema decisamente più in linea con i tempi e in grado di indicare una strada che merita di essere percorsa, con la finalità di superare le criticità più strutturali che ho rilevato nell'attuale impianto di protezione dei diritti di cui ci stiamo occupando.

(A) Il primo – e certamente più rilevante ai nostri fini – atto di cui vale la pena trattare è la proposta di "Regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati" (c.d. *Data Governance Act*) presentato dalla Commissione il 25 novembre 2020[184]. Si tratta di un provvedimento che ha come obiettivo generale quello di massimizzare, nel rispetto della privacy, la disponibilità dei dati e lo scambio sia nella direzione pubblico-privato che

---

[180] Per l'ammissibilità di una *class action* in materia di privacy, in analogia a quella presente in ambito consumeristico, v. G. M. RICCIO – G. SCORZA – E. BELISARIO, *GDPR*, cit., 591 ss., i quali (contrariamente a A. CANDINI, *Gli strumenti*, cit., 589) ritengono che a ciò non osti il fatto che l'art. 80 sembri alludere ad azioni per la tutela di interessi pur sempre individuali, giacché il *Considerando* n. 142, cui esso fa rinvio, curiosamente utilizza una diversa formulazione in cui viene utilizzato il plurale.

[181] Cfr. Comunicazione della Commissione europea del 19 febbraio 2020 *Una strategia europea per i dati*, COM(2020) 66 final, reperibile sul portale Eur-lex.

[182] Per un primo commento, in prospettiva integrata, del pacchetto proposto dalla Commissione nel dicembre 2020 v. M. LEISTNER, *The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A critical primer*, 23/02/2021, reperibile nella repository SSRN, https://ssrn.com/abstract=3789041.

[183] Sottolineo, per inciso, che il sistema descritto nel testo quanto alla sua componente giuridica presuppone, tuttavia, *a latere*, per poter adeguatamente funzionare, anche il perseguimento di due politiche pubbliche, come peraltro l'Unione europea sembra avere ben presente, ovvero adeguati investimenti nella infrastruttura digitale pubblica e nell'alfabetizzazione informatica, quali *conditio sine qua non* affinché la tutela offerta dal diritto trovi condizioni fattuali adeguate alla sua concreta realizzazione.

[184] La proposta è naturalmente reperibile sul portale Eur-lex, con l'identificativo COM(2020) 767 final.

in quella speculare, in modo tale da contrastare l'egida delle *Big Tech* e consentire a nuovi soggetti privati, in ottica pro-concorrenziale, di potersi avvalere del plusvalore in termini di sviluppo della disponibilità di importanti raccolte di dati, ma anche agli organismi pubblici di disporre di informazioni fondamentali per la definizione dei propri indirizzi politici.

In questa direzione, è anzitutto rilevante quanto la proposta prevede in tema di riutilizzo dei dati nella disponibilità di organismi pubblici[185], valorizzando, per un verso, l'anonimizzazione e altre tecniche volte ad assicurare che i vantaggi derivanti dalla maggiore disponibilità dei dati non si traduca in una retrocessione nella tutela dei diritti dei singoli, ma assicurando, per altro verso, non solo la diffusione di dati utili a fini di statistica e ricerca e sviluppo, ma anche differenziando il ritorno economico che i soggetti pubblici possono ottenerne, fino ad azzerarlo ove il riuso vada a beneficio delle PMI o di altri soggetti con maggiori difficoltà a disporre di *Big Data* o comunque persegua finalità di natura non commerciale[186]. Insomma, una sorta di democratizzazione dell'accesso ai dati, nel tentativo di conciliare lo sviluppo tecnologico con esigenze di natura sociale.

In secondo luogo, non mi pare nemmeno da trascurare l'obiettivo di rendere trasparente l'intermediazione dei dati, attraverso previsioni volte ad istituzionalizzare il ruolo dei soggetti che svolgono questa attività, con l'obbligo di notifica e soprattutto con la loro corresponsabilizzazione nella funzione di controllo sugli utilizzatori finali. Tra questi soggetti, poi, di particolare interesse sono le cooperative di dati, come enti «che aiutano interessati o imprese individuali, microimprese o piccole e medie imprese, che sono membri della cooperativa o che conferiscono alla cooperativa il *potere di negoziare i termini e le condizioni per il trattamento dei dati* prima di dare il loro consenso, a compiere scelte informate prima di acconsentire al trattamento dei dati»[187]. Seppure il testo precisi che l'esercizio dei diritti resta appannaggio del singolo individuo[188], si tratta di una previsione che, per un verso, prende atto della debolezza del consenso lasciato a se stesso ed affianca un opportuno sostegno, mentre, per altro verso, attribuisce un vero e proprio potere negoziale agli interessati, in forma associata in quanto l'unica ad attribuire un reale peso contrattuale, sulla falsariga di quanto peraltro a mio avviso già si potrebbe – e dovrebbe – fare anche solo modificando ed integrando il GDPR.

Da ultimo, il provvedimento dedica alcune disposizioni agli organismi che, previa iscrizione in apposito registro pubblico, intendano attuare una vera e propria forma di volontariato in ambito di dati personali. Questi ultimi, infatti, vengono ad essere possibile oggetto (anche) di donazione con finalità altruistica tramite soggetti che all'uopo, sotto l'opportuno controllo delle Autorità preposte, onde evitare che dietro di essi si realizzi confusione con realtà imprenditoriali che vogliano surrettiziamente appropriarsi di informazioni personali, ne assumono il compito di raccolta e diffusione previo rilascio di idonee garanzie di protezione dei singoli. Del resto, se la

---

[185] Integrando, in questo senso, le previsioni della direttiva 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[186] Su questi passaggi si vedano i *Considerando* 6 e 20 nonché l'art. 6 della proposta.

[187] Art. 9 della proposta (corsivo mio), a corredo del quale si veda anche il *Considerando* 24.

[188] Salvo che lo Stato, sfruttando la facoltà offerta dal GDPR e delle quale ho detto poc'anzi, abbia già previsto rimedi collettivi, deve intendersi.

regolazione parte dal presupposto che i dati hanno valore patrimoniale – fino a rappresentare un *asset* strategico dello sviluppo economico[189] – non appare a quel punto incoerente consentire che essi, oltre che di cessione retribuita (anche con la fruizione di un servizio), possano altresì essere oggetto di atti di disposizione a titolo (realmente e consapevolmente) gratuito, al fine di essere utilizzati per finalità di interesse generale.

(B) Una seconda proposta di "*Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*" (cd. *Digital Services Act*) è stata presentata il 15 dicembre 2020 dalla Commissione[190], al fine di rivedere la disciplina dei servizi digitali e incidere sulla *governance* della rete. Non si tratta, quindi, propriamente, di un atto normativo che interviene sul trattamento dei dati personali; tuttavia, poiché disciplina l'ambiente stesso in cui le situazioni soggettive al nostro esame trovano il loro ordinario terreno di sviluppo e le loro principali insidie, non stupisce che si possano rinvenire previsioni direttamente rilevanti anche per il nostro oggetto di indagine.

In particolare, le misure riguardanti la pubblicità sulle piattaforme *on line* suscitano interesse in quanto, integrando le norme del GDPR in tema di profilazione (ivi incluso il necessario consenso dell'interessato ed il diritto di questi di opporsi al trattamento), danno più completa attuazione al principio di trasparenza, imponendo alle piattaforme stesse di rendere note, tra l'altro, le «informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità»[191]. In questo modo, l'interessato ha maggiori *chances* di acquisire effettiva consapevolezza sulla profilazione cui è assoggettato e, per l'effetto, vi è una maggiore probabilità che egli eserciti in concreto i suoi diritti. Si tratta, insomma, di una disposizione utile nell'ottica in particolare dell'autodeterminazione informativa e dell'identità personale, nella misura in cui essa cerca di evitare che le proprie preferenze vengono (subdolamente) eterodirette cristallizzando, quando non guidando, le scelte negoziali o, più genericamente, di vita.

(C) Sempre al tema della profilazione sono peraltro dedicate alcune previsioni, sebbene forse meno incisive dal punto di vista della tutela della privacy di quanto non lo siano in prospettiva *antitrust*, dell'altro atto presentato dalla Commissione il 15 dicembre 2020, nel medesimo quadro della *Strategia europea per i dati* e di fatto complementare al precedente, ovvero la proposta di "*Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*", ovvero il cd. *Digital Markets Act*[192].

---

[189] «The oil of the digital era», per ricorrere alla significativa – e divenuta celebre – espressione utilizzata nell'articolo *The wordl's most valuable resource is no longer oil, but data*, apparso su *The Economist* del 6 maggio 2017.

[190] La proposta è reperibile su Eur-Lex con l'identificativo COM(2020) 825 final. In essa si dà conto anche delle Risoluzioni del Parlamento cui essa intende fornire risposta, sulle quali tuttavia sarebbe ultroneo qui soffermarsi.

[191] Art. 24, lett. c) della proposta della Commissione. Analoga è la previsione di cui all'art. 30, par. 2, lett. d) che, per le piattaforme di grandi dimensioni, stabilisce l'obbligo di tenuta di un registro che rechi anche «un'indicazione volta a precisare se la pubblicità fosse destinata ad essere mostrata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine».

[192] Il testo è pubblicato su Eur-Lex con l'identificativo COM(2020) 842 final. Una rassegna delle previsioni recate da esso può leggersi in P. IBÁÑEZ COLOMO, *The Draft Digital Markets Act: A Legal and Institutional Analysis*; e G. MONTI, *The Digital Markets Act – Institutional Design and Suggestions for Improvement*, TILEC Discussion

L'articolato normativo, infatti, ad integrazione della lacuna rilevata nel GDPR, pone proprio specifica attenzione sulla raccolta dei *Big data* e la loro elaborazione algoritmica per finalità di profilazione[193]. Una sorta di presa d'atto di questo meccanismo di funzionamento del mercato digitale, infatti, si rinviene nell'*incipit* del *Considerando* 61, ove si legge che «gli interessi degli utenti finali in materia di protezione dei dati e di privacy sono rilevanti ai fini di qualsiasi valutazione degli effetti potenzialmente negativi della pratica adottata dai gatekeeper, consistente nel raccogliere e nell'accumulare grandi quantità di dati provenienti dagli utenti finali», laddove con il termine *gatekeeper* si allude al fornitore di servizi di piattaforma di base (come un motore di ricerca, un *social network*, un *cloud*, ecc.) che abbia una posizione consolidata nel suo settore e rappresenti una porta di accesso privilegiata attraverso cui gli utenti commerciali possono raggiungere quelli finali (in tal senso la definizione recata dall'art. 3 del testo). Tuttavia, il divieto stabilito per i *gatekeeper* di combinare i dati ricavati dall'uso della piattaforma con quelli provenienti da altre sue attività o da terzi non è configurato come assoluto, potendo essere superato, come precisa l'art. 5, con uno specifico consenso dell'interessato. Previsione, questa, che ripropone la già vista criticità più generale della effettività della tutela offerta dall'istituto del consenso in ottica di protezione dell'interessato, e la cui problematicità non viene mitigata dalla espressa previsione (nell'art. 11) dell'obbligo di garantire la effettiva osservanza delle statuizioni regolamentari.

Più significativo, invece, è quanto l'atto prevede in tema di trasparenza, laddove il *Considerando* n. 61 chiarisce che «è opportuno che i gatekeeper forniscano quanto meno una descrizione della base su cui è realizzata la profilazione, indicando anche se si avvalgono dei dati personali e dei dati derivati dall'attività dell'utente, il trattamento applicato, lo scopo per il quale è preparato e in ultima analisi utilizzato il profilo, l'impatto di tale profilazione sui servizi del gatekeeper e i provvedimenti adottati per consentire agli utenti finali di essere a conoscenza dell'uso pertinente di tale profilazione, nonché per chiedere il loro consenso» e, più incisivamente, l'art. 13 stabilisce l'obbligo di ottenere un *audit* indipendente sulle tecniche di profilazione utilizzate, di cui è previsto un aggiornamento annuale. Si tratta di disposizioni che sembrano introdurre in modo esplicito il diritto per l'interessato di poter comprendere la logica che guida il funzionamento dell'algoritmo, la cui mancanza – almeno in termini espliciti – nel GDPR[194] non sembra porsi in coerenza con il principio fondamentale della trasparenza.

Paper, n. 4/2021, entrambi del 22 febbraio 2021 e reperibili nella *repository* SSRN, rispettivamente https://ssrn.com/abstract=3790276 e https://ssrn.com/abstract=3797730

[193] Sul contributo della proposta in esame ad una migliore e più completa attuazione del GDPR, v. S. VEZZOSO, *The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU*, 25 gennaio 2021, reperibile nella repository SSRN, https://ssrn.com/abstract=3772724, spec. 5 ss.

[194] Il Regolamento, infatti, sul punto, si limita a stabilire, nel *Considerando* n. 71, che l'interessato deve ricevere «specifiche informazioni», mentre l'art. 13, par. 2, lett. f), oltre ad indicare che lo stesso deve essere reso edotto dell'esistenza di una decisione automatizzata, prescrive che, in tal caso, gli siano fornite «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento». L'esistenza di un "diritto alla spiegazione" o di un "diritto alla leggibilità" dell'algoritmo, alla luce principalmente di questa disposizione, è stata oggetto di un interessante dibattito, in cui vale la pena segnalare, su posizioni opposte, S. WACHTER – B. MITTELSTADT – L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, n. 2/2017, 76 ss.; e G. MALGIERI – G.

La proposta, peraltro, prevede altresì che spetti ai *gatekeeper* garantire l'osservanza degli obblighi previsti dalla normativa UE in materia di protezione dei dati personali da parte degli utenti commerciali che la utilizzano, ai quali la piattaforma deve consentire, per un verso, di acquisire direttamente il consenso dell'interessato con la stessa facilità con cui ne è previsto il rilascio per i servizi offerti dalla piattaforma stessa, nonché, per altro verso, di assicurare agli interessati strumenti effettivi per l'esercizio del diritto di portabilità dei dati[195]. Insomma, ciò che si intende evitare è che il *gatekeeper* tenti di mantenere solo per sé i dati, abusando così della propria posizione a danno degli utenti commerciali della piattaforma allorché si pongano quali suoi possibili concorrenti. Di modo che, specularmente a quanto abbiamo visto sta avvenendo oggi, con questo atto normativo non sarebbe tanto la disciplina della concorrenza a tutelare i diritti oggetto della nostra indagine, quanto piuttosto la normativa sulla protezione dei dati ad assicurare una concorrenza sui mercati digitali[196]. Il che, sia pure a ruoli invertiti, conferma lo stretto legame tra i due ambiti.

6. Nota conclusiva

Il progresso tecnologico – lo rilevavo nell'aprire questa indagine – ha da sempre plasmato protezione dei dati e identità personale, di cui ha fatto apparire, in un processo senza sosta, nuovi profili, che rispondono a bisogni emergenti di tutela a fronte di nuovi pericoli e minacce che lo sviluppo delle tecnologie porta con sé. Ma se nel periodo considerato all'inizio dell'analisi il ritmo dell'evoluzione era piuttosto lento, tanto da essere compatibile con i tempi di risposta di un legislatore mediamente pronto a cogliere le nuove istanze provenienti dal contesto sociale, lo stesso si è fatto con il fluire del tempo sempre più incalzante, fino ad arrivare ad un'epoca – quella attuale – in cui gli atti normativi corrono fortemente il rischio di nascere già inidonei a rispondere al continuo mutamento tecnologico. Non solo, ma la diffusione di una realtà digitale pervasiva e atopica, destinata sempre più a fondersi con quella *off line*, in un legame in cui tendono ad assottigliarsi fino a svanire i confini tra l'una e l'altra, porta con sé lo smarrimento di coordinate spaziali, che complicano non poco il compito del regolatore.

In questo contesto, a me pare che l'unica soluzione per offrire una efficace tutela ai due diritti fondamentali a protezione della personalità umana, che hanno costituito l'oggetto delle presenti note, sia quello di un approccio integrato, che possa cercare di portare a sintesi coerente diverse strade, che vanno percorse simultaneamente.

COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, n. 3/2017, 243 ss. Per la posizione favorevole all'esistenza di un siffatto diritto, cui mi sembra preferibile aderire alla luce del preciso richiamo, nel testo, alla logica del processo decisionale, si vedano da ultimo le argomentazioni portate da G. DE MINICO, *Towards*, cit., 397 ss.

[195] Rispettivamente art. 11, par. 2 ed art. 6, par. 1, lett. h. Quest'ultima disposizione è apprezzata da S. VEZZOSO, *The Dawn*, cit., 10, per il fatto di costituire un mezzo efficace per dare quell'effettività al diritto alla portabilità, che il GDPR non è in grado di assicurare.

[196] Analogamente, S. VEZZOSO, *The Dawn*, cit., 8 ss.

Da un lato, infatti, è quanto mai necessaria una integrazione tra fonti di livello internazionale e sovranazionale e fonti interne, che possa rispondere alla diffusione della rete ed alla sua mancanza di riferimenti a luoghi fisici corrispondenti al concetto di territorio quale noto agli studi costituzionalistici[197], pur senza obliterare le ineliminabili specificità nazionali[198]. Da questo punto di vista, l'"accentramento" a livello di UE determinatosi con il passaggio dallo strumento della direttiva a quello del Regolamento[199] per la protezione dei dati (ma in realtà, come abbiamo visto, a tutela di molti aspetti delle situazioni soggettive qui esaminate) trova piena giustificazione e non può che salutarsi con favore[200], così come il tentativo che l'atto euronitario compie di dispiegare i propri effetti, per quanto possibile, al di fuori dei confini unionali[201], nella consapevolezza della dimensione mondiale della rete e dei *player* del settore[202]. Lo stesso aggiornamento della Convenzione n. 108 del 1981 del Consiglio d'Europa, cui ho fatto cenno in precedenza[203], è indirizzato in questa stessa prospettiva.

D'altro lato, però, l'approccio integrato cui facevo riferimento va inteso anche nel senso che le situazioni soggettive di cui parliamo richiedono di essere ripensate e adeguate al quadro di una realtà digitale nella quale sono immerse e dalla quale, pertanto, vengono le principali minacce. Ed allora fondamentale e imprescindibile appare il tentativo di sistematizzare le discipline del "mondo digitale" e di considerare la protezione dei dati e l'identità, attraverso la specifica normativa a loro tutela, come uno dei cardini di un più ampio *corpus*, in via di costruzione, per la regolazione dei mercati digitali, ma che sarebbe auspicabile si estendesse alla regolazione della rete nel suo complesso. Anche se, sul punto, assume particolare rilievo il timore che, come in diversi recenti precedenti (non ultimo il GDPR), le resistenze e le pressioni degli operatori del mercato digitale (*Big Tech* per prime) prolunghino l'*iter* per un tempo assai dilatato, durante il quale l'evoluzione tecnologica facilmente scompiglierebbe nuovamente le carte.

Una ulteriore forma di approccio integrato, tra discipline volte a regolare ambiti differenti, si palesa già, peraltro, opportunamente nell'uso combinato delle normative consumeristica,

---

[197] Tra le analisi volte a indagare l'effetto di smarrimento spaziotemporale conseguente alle tecnologie comunicative in genere, ed alla rete in particolare, v., *ex plurimis*, P. COSTANZO, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in *Costituzionalismo e globalizzazione*, Atti del XXVII Convegno annuale Salerno, 22-24 novembre 2012, Napoli, 2014, spec. 53 ss. Il tema è peraltro oggetto della relazione a questo Convegno di Cristina Napoli.

[198] È questo un punto su cui insiste F. PIZZETTI, *Riflessioni metodologiche allo studio dei diritti "nella rete della rete"*, in ID. (a cura di), *Il caso*, cit., 2 ss.

[199] In relazione al quale, ampiamente, L. DURST, *Oggetto*, cit., spec. 52 ss.

[200] Benché, nella prassi, la Commissione, con la *Comunicazione al Parlamento europeo e al Consiglio del 24 giugno 2020 sulla protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati (COM(2020)0264)*, 8 ss., abbia rilevato come, nei fatti, il ricorso alle clausole di specificazione contenute nel GDPR sia stato ampiamente utilizzato dagli Stati membri ed abbia condotto al mantenimento di una non secondaria frammentazione normativa.

[201] Sarebbe qui ultroneo soffermarmi sull'ambito di applicazione territoriale del Regolamento; per questo profilo, v., *ex plurimis*, G. M. RICCIO – G. SCORZA – E. BELISARIO, *GDPR*, cit., 18 ss.

[202] Consapevolezza che, come rileva V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, in in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali*, cit., 21 ss., si evince anche dal riferimento al fatturato mondiale come parametro previsto dall'art. 83 per la quantificazione delle sanzioni.

[203] V. *supra*, nota 67.

concorrenziale e a protezione dei dati, le quali, pur nella loro specificità, possono apportare a loro volta una tutela assai preziosa in contesti non sufficientemente presidiati od in cui comunque i confini tra ciò che è regolazione del mercato e ciò che è garanzia per i diritti fondamentali della persona tende molto a sfumarsi. Il che, peraltro, comporta l'ampliamento dei soggetti preposti alla garanzia dei diritti della personalità qui in esame[204]: se, infatti, precedentemente l'intervento statale si esplicava attraverso il binomio giudice ordinario – Garante per la protezione dei dati, ora esso vede coinvolta anche l'Autorità Garante della Concorrenza e del Mercato, e, conseguentemente, il giudice amministrativo, titolare di giurisdizione esclusiva in sede di eventuali impugnazioni, con la necessità di trovare forme di coordinamento ed integrazione anche sotto il profilo istituzionale per i soggetti che presidiano la tutela della privacy e dell'identità.

Da ultimo, se una minaccia significativa è oggi rappresentata da forti poteri privati, non mi sembra da trascurare la maggiore garanzia che anche formazioni collettive di natura privatistica, ma prive di finalità lucrative e sorte con lo scopo di assicurare maggiore garanzia alle situazioni soggettive al nostro esame, possono offrire attraverso una tutela collettiva, invero in gran parte ancora da costruire e possibilmente da elevare a livelli territoriali più ampi possibili. Un approccio che integra, in buona sostanza, strumenti di natura pubblicistica con altri di natura privatistica.

Tutto ciò richiede, in ogni caso, una previa condizione, ovvero la consapevolezza e la volontà politiche di intervenire per cercare di guidare e indirizzare lo sviluppo tecnologico, anziché subirlo, così da evitare che il sistema di regole giuridiche ed ancor prima valoriali che sta alla base della società resti travolto da quei fenomeni epocali che più volte il progresso delle tecniche ha segnato nel corso della storia[205]. Occorre, in buona sostanza, che la politica (ri)affermi il proprio primato sulla tecnologia[206] e che i soggetti regolatori (legislatori sovranazionali e interni *in primis*) non si affidino a questa con una fiducia di stampo positivistico, ma si adoperino piuttosto nel tentativo di governare il fenomeno tecnologico, assumendosi la responsabilità (politica, per l'appunto) delle scelte regolatorie in materia ed effettuando adeguati investimenti infrastrutturali, al fine di evitare che l'assenza (o, quanto meno, il ritardo) nell'innovazione finisca per aumentare l'attuale distanza tra la capacità tecnologica dei poteri privati e quella dello Stato[207]. I diritti, infatti, nel mondo

---

[204] Attuandosi quel "pluralismo processuale" di cui parlava M. MEZZANOTTE, *Il diritto*, cit., 265, per il quale, se nell'attuale società sono aumentate le insidie per la privacy, ciò «ha indotto lo Stato a riallocare le funzioni al suo interno al fine di moltiplicare gli strumenti di intervento ed i mezzi di tutela».

[205] Così già F. PIZZETTI, *Riflessioni*, cit., 8 ss. In termini analoghi anche C. COLAPIETRO, *Il diritto*, cit., 36, il quale parla di una «deriva tecnologica […] a cui non è possibile non reagire, dal momento che l'uso della tecnica deve essere al servizio dei diritti».

[206] Su cui, in relazione all'emergenza pandemica, insiste particolarmente G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *laCostituzione.info*, 1° aprile 2020.

[207] Di una «stretta interrelazione tra *governance* politica ed infrastruttura tecnologica, non senza ricadute sui diritti fondamentali (legati, in particolare, alla sfera della *privacy*)» ragiona L. TRUCCO, *App Immuni*, cit. Nella stessa prospettiva si pone M. PLUTINO, *"Immuni"*, cit., 555, allorché rileva come la necessità per gli Stati di ricorrere alle tecnologie delle *Big Tech* sia tra le ragioni che spiegano talune normative statali, le quali, celando in realtà politiche industriali fortemente sollecitate da questi soggetti privati, si manifestano come eccessivamente compressive delle medesime situazioni soggettive in nome di esigenze di sicurezza, latamente intesa.

digitale si possono tutelare solo con la tecnologia[208], a condizione che questa sia indirizzata dal decisore politico, il quale è chiamato ad assumere le proprie responsabilità affinché sia il diritto a stabilire le regole ed alla tecnica si faccia ricorso per darvi attuazione. Del resto, da tempo è stato evidenziato come la tecnologia sia plasmata da istanze culturali e il suo stesso sviluppo, prima ancora dell'utilizzo, può ben essere indirizzato attraverso l'introduzione di limiti di carattere etico e giuridico[209]. In questa direzione, il GDPR ci offre già una *best practice* rappresentata dalla privacy *by design*, laddove l'aver previsto l'obbligo di implementare misure di protezione fin dalla fase di progettazione di un processo (aziendale, produttivo, ecc.) che comporti il trattamento di dati è un buon esempio di vincolo che incide sul momento genetico stesso di nuove tecnologie, costrette a "fare i conti" con la privacy come loro componente essenziale[210].

Parallelamente, credo non sia meno necessario prendere atto che, contrariamente a quella che mi sembra ancora la visione dominante, la privacy va letta (e dovrà sempre più essere letta) come una libertà *nello* Stato e non (solo e non tanto) *dallo* Stato, per usare un paradigma ben noto al diritto costituzionale[211].

Chiunque, infatti, navigando in rete, lascia, per ciò solo, inevitabilmente dietro di sé, in modo più o meno consapevole, scie di informazioni sul proprio conto, prontamente raccolte da soggetti privati, "moligopolisti" di dimensioni colossali, che attraverso di esse riescono, tramite profilazione[212], a conoscere le sue preferenze e pertanto a proporgli, durante la navigazione o sui *social*, solo i contenuti graditi (sempre gli stessi) "ingabbiandolo" in una sorta di bolla, dalla quale discendono, per la società operante nel *web*, ampi profitti pubblicitari ed invece, per l'interessato, una forte limitazione della propria libertà di informazione, a dispetto delle originarie promesse della rete. Non solo, ma quegli stessi soggetti privati, con tali dati, arrivano ad influenzare, quando non a determinare, le politiche pubbliche, a censurare soggetti politici[213] e fin anche, più in generale, ad esercitare prerogative di fatto sovrane. Se questo è, come rilevato da più parti, un pericolo per la democraticità del sistema[214], è allora opportuno un nuovo e forte intervento pubblico, non solo, in generale, a regolazione della rete, ma anche, più nello specifico, a garanzia,

---

[208] Sottolinea giustamente L. FLORIDI, *La quarta rivoluzione*, cit., 131, che le «ICT digitali offrono già alcuni strumenti per controbilanciare i rischi e le sfide che rappresentano per la privacy», giacché esse «non erodono inevitabilmente la privacy, possono anche migliorarla e proteggerla».

[209] In questo senso, v., per esempio, le riflessioni di U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008, 218 ss.

[210] Osserva, analogamente S. CALZOLAIO, *Protezione*, cit., 610, che, se il diritto può essere neutro rispetto alla tecnica, non necessariamente vale anche l'opposto, così che la codificazione della privacy *by design* appare il mezzo principale per veicolare il diritto.

[211] Sulla privacy come libertà positiva, per assicurare la quale è necessario un *facere* da parte di un'Autorità pubblica v. G. DE MINICO, *Towards*, cit., spec. 389

[212] Evidenzia, sul punto, S. CALZOLAIO, *Protezione*, cit., 603, che «nel contesto tecnologico dato, la profilazione (in modo e gradi diversi) della persona è una condizione strutturale e inevitabile. La produzione incessante di dati comporta quasi automaticamente la possibilità e l'esigenza di creare profili individuali e collettivi. La profilazione definisce l'individuo […] nel contesto sociale, poiché consente a chi profila di prevederne le attività».

[213] Ovvio il riferimento alla censura, seppure in quel caso non del tutto priva di ragioni, che ha colpito l'ex Presidente statunitense Donald Trump, sulla quale, per tutti, v. M. MANETTI, *Facebook, Trump e la fedeltà alla Costituzione*, in *Forum di quaderni costituzionali – Rassegna*, n. 1/2021, 194 ss.

[214] Una posizione analoga è espressa con forza da B. CARAVITA, *Davanti ad un mondo che cambia chi è più pericoloso tra Trump e Zuckerberg?*, in *Federalismi.it*, n. 1/2021, 5 ss.

delle situazioni soggettive di cui qui ci siamo occupati[215], sia quando ciò comporti un potenziamento delle sfere di intervento delle Autorità Garanti, a supporto di diritti il cui mero riconoscimento normativo non può risolversi in una tutela effettiva[216], sia quando ciò significhi rendere disponibile un'ampia quantità di dati in mano pubblica a preferenza di un soggetto privato[217].

Resta, è vero, la necessità che la risposta avvenga al livello territoriale più ampio possibile, laddove, se quello nazionale non appare nemmeno in ipotesi poter essere reputato sufficiente, anche quello europeo non può essere pienamente adeguato, a fronte di poteri di livello planetario. Di modo che, pur con tutte le criticità che ciò comporta, rimane di piena attualità il tema della ricerca di modalità per opporre anche a poteri diversi dallo Stato, ma che con esso condividono prerogative di fatto sovrane, il riconoscimento ed il rispetto di quei diritti fondamentali, tra cui appunto la privacy e l'identità personale, che nell'esperienza costituzionale, anche multilivello, si sono andati consolidando ed hanno trovato esplicita affermazione[218]. E se in questo l'attività della Corte di Giustizia è stata, in alcune circostanze, sicuramente meritoria per lo sforzo di attribuire efficacia orizzontale alle previsioni di cui agli artt. 7 ed 8 della Carta dei diritti fondamentali[219], mi pare che le proposte normative sul campo, in Europa, pur nell'evidente difficoltà di affermare una sovranità digitale a livello continentale e soprattutto con la consapevolezza, stante la centralità per l'economia digitale, della posta in palio e di come ci si muova su un terreno minato in cui la possibilità di ingenerare, a livello internazionale, contrapposizioni tra blocchi regionali con visioni tra loro alquanto difformi, è assai forte, possano offrire un contributo ulteriore nella direzione auspicata. Il tutto, però, a condizione che i tempi per giungere a nuove regolazioni siano adeguatamente brevi; dal momento che, in difetto, ci ritroveremo ancora una volta di fronte al

---

[215] In questa direzione condivido appieno i rilievi, ancor più autorevoli per il fatto di provenire da una studiosa che è stata anche componente dell'Autorità Garante, di L. CALIFANO, *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO – C. COLAPIETRO, *Le nuove frontiere*, cit., 53 ss., la quale ricorda come la riservatezza subisca interferenze quotidiane che «si rivelano spesso operazioni svolte da soggetti spregiudicati, che si avvalgono di banche dati massive». Di modo che – continua l'A. – «le tendenze degli ultimi anni hanno dimostrato come siano questi i pericoli più tangibili e allarmanti per i cittadini comuni; è quindi avverso questi comportamenti che diviene cruciale irrobustire gli sforzi e affinare gli strumenti per la protezione della privacy».

[216] È in questa prospettiva che V. CUFFARO, *Il diritto europeo*, cit., 22, legge le norme del GDPR sui poteri delle Authorities.

[217] L'importanza per il decisore pubblico di disporre di dati che spesso oggi sono di esclusiva pertinenza di enti privati è evidenziata anche nella Comunicazione del 19 febbraio 2020 citata *supra*, alla nota 181, 8 ss.

[218] Del resto, come scrive T. E. FROSINI, *Costituzionalismo 2.0*, in Id., *Liberté, égalité, internet*, Napoli, 2019, 189, «la sfida che nel Ventunesimo secolo attende il costituzionalismo è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà […] in un contesto sociale profondamente mutato dall'innovazione».

[219] Sulla protezione della privacy in ambito digitale come terreno privilegiato in cui si è mosso il giudice di Lussemburgo per assicurare, anche nei confronti di soggetti privati, un'efficace tutela dei diritti fondamentali, v. O. POLLICINO, *L'efficacia orizzontale dei diritti previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *Medialaws*, 2018, 138 ss., il quale peraltro rileva come l'efficacia orizzontale delle disposizioni costituzionali sui diritti, non universalmente riconosciuta a livello comparato, sembra però essere ormai sdoganata a livello europeo. Peraltro, l'Autore evidenzia, in modo pienamente condivisibile, come i fattori determinanti del riconoscimento di una tutela estensiva della privacy e dei dati personali siano stati, da un lato, la dimensione a-territoriale delle nuove tecnologie e, dall'altro, l'intento della Corte di assoggettare anche i soggetti privati al rispetto delle prerogative costituzionali previste dalla Carta.

rischio che, pur con diverse (e ben più vaste) coordinate geografiche, *dum Romae consulitur, Saguntum expugnatur*.