Roberta Catalano

PANDEMIA E *PANOPTICON*: PROFILI EVOLUTIVI DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

1. Il *Panopticon* o *Panottico* (parola di etimologia greca per significare *che fa vedere tutto*) è una ideale struttura carceraria progettata alla fine del diciottesimo secolo dal filosofo e giurista Jeremy Bentham[1]. Essa si connota per la particolare disposizione degli ambienti, grazie alla quale tutti i prigionieri si trovano ad essere costantemente controllati da un unico guardiano, che può osservarli senza essere visto[2]. Secondo Bentham i vantaggi offerti dal *Panopticon* derivano dalla speciale condizione in cui versano i detenuti: la consapevolezza della costante esposizione allo sguardo del sorvegliante, unita all'impossibilità di sapere a chi quello sguardo è rivolto, induce i carcerati ad una condotta disciplinata e, con il prolungarsi della detenzione, condiziona la loro mente fino al punto di piegarla ed abituarla al rispetto delle regole (il filosofo descrisse il *Panopticon* come "un nuovo modo per ottenere potere sulla mente, in maniera e quantità mai vista prima"[3]).

L'idea del *Panopticon* ha profondamente influenzato l'immaginario collettivo, tant'è che nel mondo diverse strutture carcerarie e ospedali psichiatrici sono stati edificati sull'impronta di quel progetto[4]. Innumerevoli

1 J. Bentham, *Panopticon, or the ispection-house*, Londra, 1791; tr. it. M. Foucault, M. Perrot (a cura di), *Panopticon ovvero la casa d'ispezione*, Venezia, 1983. La denominazione assegnata al carcere ideale evoca il nome del gigante *Argo Panoptes* (in greco *Ἄργος Πανόπτης*, *Argo che tutto vede*) che, secondo il mito, era dotato di innumerevoli occhi e, pertanto, veniva considerato un ottimo guardiano.

2 Il Panottico si compone di una torre centrale, sede del guardiano, circondata da un edificio di forma circolare o semi-circolare in cui sono situate le celle dei detenuti, illuminate dall'esterno e divise da spessi muri. Le celle sono dotate di due finestre ciascuna, una rivolta verso l'esterno per far entrare la luce, e l'altra posta sul versante interno, in direzione della torre centrale, per consentire il controllo del custode.

3 M. Foucault, M. Perrot (a cura di), *Panopticon ovvero la casa d'ispezione*, p. 36.

4 Lo stesso Bentham osservava che il suo progetto ben si adattava ad essere utilizzato "sia che si tratti di punire i criminali incalliti, sorvegliare i pazzi, riformare i viziosi, isolare i sospetti, impiegare gli oziosi, mantenere gli indigenti,

racconti cinematografici[5] e televisivi[6] si sono ad esso ispirati, così come molti libri di narrativa, tra i quali *1984* di George Orwell che ipotizza una società nella quale il controllo dell'ordine pubblico è rimesso ad una organizzazione paramilitare, la Psicopolizia, in grado di sorvegliare chiunque attraverso dei teleschermi[7]. Il carcere ideale di Bentham è stato, altresì, oggetto delle riflessioni di studiosi e filosofi tra i quali Michel Foucault che, nel suo saggio *Sorvegliare e punire. Nascita della prigione*, rileva che il *Panopticon* riproduce la struttura attualmente assunta dal potere, che non si cala più dall'alto ma pervade la moderna società dall'interno, per il tramite di una complessa serie di meccanismi e relazioni volte a garantire un controllo costante, pervasivo e invisibile[8].

In effetti, la struttura del *Panopticon* dimostra, in modo plastico e quanto mai efficace, che un regime di controllo accentrato sulla vita delle persone è in grado di manipolarne la condotta, comprimerne la dignità e, se trattasi di controllo diffuso, compromettere l'assetto democratico della società. Ma l'accostamento del *Panopticon* alla pandemia da Covid-19 nasce dalla ulteriore considerazione che il carcere ideale di Bentham implica l'idea

---

guarire i malati, istruire quelli che vogliono entrare nei vari settori dell'industria, o fornire l'istruzione alle future generazioni" (cfr. M.Foucault. M. Perrot (a cura di), *Panopticon ovvero la casa d'ispezione,* p. 36).
Tra gli edifici ispirati al *Panopticon* di Bentham si possono ricordare, in Italia, il *Padiglione Conolly* dell'*ex* ospedale psichiatrico di San Niccolò di Siena, originariamente destinato all'isolamento dei malati più gravi; ed il carcere dell'isolotto di Santo Stefano (contiguo all'isola di Ventotene) edificato dai Borbone nel 1795. Anche nel mondo ricordiamo le strutture del *Panopticon* di Ibaguè, in Colombia, inizialmente adibito a carcere; dell'*Ashley Building* a Birmingham; del *Presidio Modelo* a Cuba dove fu detenuto Fidel Castro; dell'*ex* ospedale psichiatrico Miguel Bombarda a Lisbona, in Portogallo, edificato nel 1896 su progetto dell'architetto Jose Maria Nepomuceno e attualmente sede di un museo psichiatrico.

5 Oltre all'omonimo film del 2016 per la regia di Tarsem Singh, si possono ricordare diverse pellicole appartenenti al genere della fantascienza tra le quali *Minority report* del 2002 per la regia di Steven Spielberg, e *Anon* del 2018 per la regia di Andrew Niccol.

6 La nota serie Netflix *Black mirror* mette in luce i pericoli ed i paradossi connessi al progresso tecnologico, ai *social*, ai mezzi di comunicazione di massa e, per questo motivo, dedica molti episodi ai problemi derivanti dal graduale assottigliamento della sfera di riservatezza delle persone a causa di situazioni di controllo informatico accentrato, più o meno invisibile.

7 G. Orwell, *Nineteen Eighty-Four*, London, 1949; trad. it. G. Baldini (a cura di), *1984*, Milano, 1950.

8 M. Foucault, *Sorvegliare e punire. Nascita della prigione,* trad. it. A. Tarchetti (a cura di), Torino, 1976, pp. 222 ss.

che l'instaurazione di un controllo accentrato può essere giustificato, nonostante i gravi effetti che ne derivano, al ricorrere di interessi sovraordinati (come, nel caso considerato, quelli di sorvegliare e rieducare i rei). Sicché diviene necessario chiedersi se ed in che misura l'attuale stato di pandemia può giustificare, in nome dell'emergenza sanitaria, l'edificazione – proprio come un carcere – di un sistema di tracciamento e prevenzione del contagio attuato a mezzo del trattamento automatizzato e massivo dei dati personali e sensibili di tutti cittadini[9].

Il delicato e complesso tema del rapporto tra interessi fondamentali della persona e diritto emergenziale non è compito precipuo dello studioso del diritto civile, ma la peculiare situazione creatasi in conseguenza della pandemia offre al civilista un punto di osservazione privilegiato sulle nuove limitazioni al diritto alla protezione dei dati personali, sulle conseguenze che ne derivano sull'assetto complessivo dei diritti fondamentali e, quindi, sul grado di compatibilità di una tale evoluzione con l'ordito dei valori di vertice delle moderne democrazie occidentali.

2. Sul sito dell'Autorità Garante per il trattamento dei dati personali, nella parte dedicata al Covid-19, v'è una ampia rassegna delle numerose misure derogatorie apportate, nel giro degli ultimi mesi, alle tutele ordinariamente riconosciute ai dati personali[10]. Allo stesso modo, molte ordinanze regionali hanno introdotto prescrizioni più o meno stringenti volte a controllare e tracciare gli utenti di servizi pubblici ovvero di attività commerciali private (come ristoranti o palestre)[11].

Qui, evidentemente, non è possibile analizzare questo vasto contesto normativo nella sua interezza, ma ciò non toglie che si possano trarre utili spunti di riflessione, bastevoli all'indagine che ci si è proposti di svolgere, dall'esa-

9 Si sono interrogati sul punto, e sulle problematiche connesse, V. Cuffaro, *La protezione dei dati personali ai tempi dell'epidemia*, in "Corr. Giur.", 2020, pp. 729 ss.; P. Benanti, J.P. Darnis, A. Sciarrone Alibrandi, *Per una resilienza con la tecnologia. Appunti per il post Covid-19*, in *Pandemia e resilienza. Persona, comunità e modelli di sviluppo dopo la Covid-19*, pubblicazione della Consulta Scientifica del Cortile dei Gentili, Roma 2020, pp. 113 ss.; P. Gremigni, *Coronavirus e privacy: le Faq del Garante sul rapporto di lavoro*, in "Guida al lavoro, Il Sole 24 ore", n. 21/22, 2020, pp. 31 ss.; A. Natalini, *Covid-19 e privacy: contact tracking tra diritti e libertà*, in "Guida al diritto, Il Sole 24 ore", n. 16, 2020, pp. 8 ss.; N. Urbinati, *La democrazia ai tempi del Covid-19 Sopportare i limiti, a quale prezzo?*, in "Civiltà delle macchine", n. 2, 2020, pp. 29 ss., in part. p. 33.

10 Cfr. la pagina web *https://www.garanteprivacy.it/temi/coronavirus*.

11 Per i testi di queste ordinanze v. le pagine *web* delle varie autorità regionali ovvero il sito *regioni.it*.

me di alcune regole soltanto, individuate come particolarmente significative. Tra queste senza dubbio si segnala l'art. 6, d.l. n. 28/2020, convertito in legge con modificazioni, dalla l. n. 70/2020, sull'introduzione di un unico sistema informatizzato di prevenzione della diffusione del virus Covid-19.

Detto articolo prevede l'istituzione presso il Ministero della Salute di una piattaforma unica nazionale volta al tracciamento dei contatti tra persone che abbiano scelto di installare sui propri telefoni cellulari un'applicazione denominata *Immuni*. Quest'applicazione, a mezzo del trattamento dei dati relativi alla salute, alla posizione ed agli spostamenti, è in grado di tracciare i contatti degli utenti e segnalare loro il pericolo rappresentato dalla vicinanza prolungata con una persona infetta.

Il trattamento dei dati da parte di *Immuni* avviene su base volontaria ed in forma anonima, ma le peculiarità del mezzo tecnologico e la natura delle informazioni trattate implicano inevitabilmente un elevato rischio di intrusione nella vita privata degli utenti. Di ciò il legislatore è ben consapevole, tanto che all'art. 6, c. 2, d. l. n. 48/2020, impone al Ministero della Salute, nella sua qualità di titolare del trattamento, gli obblighi di effettuare una speciale valutazione periodica dell'impatto di *Immuni* sui dati degli utenti, e di adottare (ed aggiornare costantemente) misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli elevati pericoli per i diritti e le libertà degli interessati.

Anche il Garante della *privacy*, pur autorizzando l'avvio della sperimentazione, ha segnalato diverse importanti criticità dell'applicazione[12]. Tra queste, anzitutto, la necessità di chiarire meglio il ruolo di alcuni soggetti coinvolti nel trattamento dati e, segnatamente, di *Bending Spoons spa* che ha realizzato *Immuni*, e di *Apple* e *Google* le quali forniscono la piattaforma tecnologica su cui transitano i dati dell'applicazione. Il Garante ha riscontrato, altresì, rilevanti profili di vulnerabilità costituiti dal fatto che: a) il sistema *bluetooth*, indispensabile al funzionamento di *Immuni*, è esposto all'azione di *malware* idonei a captare in modo fraudolento i dati personali e sensibili; b) tali dati potrebbero essere facilmente intercettati anche a mezzo di peculiari apparati di scansione (cd. *sniffer*); c) i mezzi utilizzati per garantire l'anonimato dei positivi al Covid-19 potrebbero essere aggirati da diversi sistemi di re-identificazione operanti allorché sia possibile associare informazioni personali aggiuntive al *device* connesso al *bluetooth* (come accade, ad esempio, allorché l'utente si trova in prossimità del

12 Garante privacy, "Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato *Immuni*, Nota sugli aspetti tecnologici", 3 giugno 2020, in *garanteprivacy.it*.

proprio domicilio ovvero quando, in un negozio, paga con la propria carta di credito). Secondo il Garante, poi, un ulteriore *vulnus* è rappresentato dal fatto che il sistema potrebbe, per svariati motivi, veicolare dati erronei (es., di un soggetto ritenuto, per sbaglio, positivo al virus), così creando infondate situazioni di allarme.

Infine, il Comitato europeo per la protezione dei dati personali, sin da prima dell'emanazione del d. l. n. 48/2020, si è reso autore delle Linee Guida n. 04/2020 del 21 aprile 2020 sul trattamento dei dati relativi alla salute ai fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19, nelle quali, a fronte delle varie analoghe disposizioni in corso di elaborazione in tutti i Paesi membri per consentire l'uso di applicazioni preordinate al tracciamento per motivi sanitari, ha mosso il rilievo che il controllo continuo e sistematico della posizione e dei contatti delle persone costituisce una grave interferenza nella loro vita privata, sicché può giustificarsi solo in base all'adesione volontaria e consapevole degli utenti ovvero a comprovati motivi di interesse pubblico[13].

Ebbene, non par dubbio che la disciplina dettata dall'art. 6, d. l. n. 48/2020, così come quelle non dissimili varate dagli altri Paesi europei, siano conformi ai principi ed alle cautele fissate nelle Linee Guida europee, dal momento che si ispirano all'esigenza di tutelare la salute pubblica in una situazione di emergenza sanitaria e rimettono alla libera scelta dei cittadini l'uso delle applicazioni di tracciamento. Inoltre, le limitazioni alla riservatezza in esse contenute sono coerenti con la riserva di legge disposta all'art. 23 del GDPR (reg. n. 16/679/UE)[14], alla cui stregua è consentito allo Stato membro, in presenza di obiettive esigenze di tutela della sanità pubblica, di limitare mediante specifiche misure legislative "la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 […] nonché all'art. 5 nella misura in cui le disposizioni ivi contenute corrispondano ai diritti ed agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica"[15].

---

13 Il testo delle Linee Guida è reperibile su "Guida al diritto, Il Sole 24" ore, n. 21, p. 53, ma anche sul sito *garanteprivacy.it*.

14 Più ampiamente sul punto vedasi A. Natalini, *Sistema di allerta digitale Covid-19: passa la riserva di legge per l'app*, in "Guida al diritto, Il Sole 24 ore", n. 22, 2020, pp. 61 ss.

15 Inoltre, va ricordato che il *Considerando* 52 del GDPR prevede "la deroga al divieto di trattare categorie particolari di dati personali dovrebbe essere consentita anche quando è prevista dal diritto dell'Unione o degli Stati membri, fatte salve adeguate garanzie, per proteggere i dati personali e altri diritti fondamentali, laddove ciò avvenga nell'interesse pubblico [ ] e per finalità di sicurezza sanitaria, controllo e

Sono coerenti, altresì, con le riserve di legge in materia di riservatezza dei dati personali, anche sanitari, desumibili in Italia dagli artt. 2, 15, 32, e 117, c. 2, lett. l), m), q), r), Cost., e in Europa dall'art. 8 CEDU e dagli artt. 7 e 8 della Carta di Nizza.

Infine, il trattamento in forma anonima dei dati e il fatto che l'applicazione può essere facilmente disinstallata dai *devices* sui quali è scaricata, induce a prevedere (e sperare) che al termine dell'emergenza sanitaria le piattaforme di tracciamento cadano in disuso eliminando i rischi connessi al loro impiego.

Ciononostante, rimane il fatto che la pandemia sta costituendo un'occasione irripetibile per attuare, come mai prima, un trattamento massivo e combinato di dati sensibili – come quelli relativi alla salute, agli spostamenti ed ai contatti – ad opera di soggetti pubblici e privati (nel caso di *Immuni*, da parte del Ministero della Salute, *Google* ed *Apple*). Infatti – e senza considerare le eventualità, pure segnalate dal Garante per la *privacy*, di recepimento fraudolento dei dati –, questi soggetti si trovano nella condizione di raccogliere – seppur in forma anonima – moltissime informazioni che, combinate con quelle quotidianamente desumibili dall'uso generalizzato di telefoni, computer e *tablet*, favoriscono l'aggiramento della garanzia dell'anonimato e pertanto ampie e generalizzate operazioni di profilazione[16].

---

allerta, la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute. Tale deroga può avere luogo per finalità inerenti alla salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria". Inoltre, l'art. 9, par. 2, lett. i), consente il trattamento quando "necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale".

16 Nel 2019 il *New York Times* ha svolto un'indagine volta a verificare quali e quante informazioni possono essere tratte dai dati, raccolti anche in forma anonima, relativi agli spostamenti e alla geolocalizzazione dei cittadini americani. I risultati, esposti in un *reportage* intitolato *How your phone betrays democracy*, hanno evidenziato l'esistenza di un reale pericolo per la democrazia derivante dall'uso di tecniche sempre più invasive della sfera privata delle persone. È emerso, infatti, che persino la semplice rilevazione effettuata a mezzo dei dispositivi di geolocalizzazione dei dispositivi mobili consente, a mezzo di tecniche automatizzate di analisi su larga scala della *routine*, di identificare le singole utenze e, quindi, le persone intestatarie. Analogamente, D. Cautela, *La privacy tra controllo della pandemia e mantenimento dell'equilibrio democratico*, in "privacy.it", 6 aprile 2020, p. 4, ricorda che "uno studio dell'*Imperial College* di Londra, pubblicato su *Nature Communications,* ha dimostrato come l'uso di algoritmi *machine learning*, di

Da questo angolo visuale, emergono chiare le similitudini tra la struttura reale del *Panopticon* e quella virtuale delle piattaforme informatiche di raccolta e gestione dei dati. Con la differenza, molto inquietante, che in queste ultime il *cyber*-controllo si trova, per lo più, in capo a grandi multinazionali private operanti per scopi di lucro (come appunto *Apple* e *Google*).

Dato il pericolo che il *cyber*-controllo invisibile, accentrato e diffuso comporta per la democrazia e la dignità della persona, occorre predisporre adeguate garanzie a presidio del diritto alla protezione dei dati personali[17]. Tuttavia, la tendenza in atto è di segno opposto. Infatti, le recenti norme in materia di tracciamento in funzione di contrasto alla pandemia da Covid-19 costituiscono solo l'ultima tessera di un mosaico normativo alla cui stregua il diritto alla protezione dei dati personali sembra essere considerato – più che un presidio essenziale per la libertà e la dignità della persona – un ostacolo allo sviluppo economico e tecnologico ovvero alla tutela della salute[18].

---

retro-ingegnerizzazione e il ricorso ai cd. *generative models* rendano possibile ricondurre dati considerati anonimi ai rispettivi interessati, con il potenziale effetto – tipico delle tecniche applicate ai trattamenti operati sui *big data* – di produrre *output* di profilazione comportamentale, i cui risultati si prestano ai più svariati utilizzi, leciti o illeciti, palesi od occulti". Ma già in precedenza G. Faggioli, *Big-data e privacy: la protezione dei dati personali è possibile?*, in "Osservatori.net Digital innovation", 1 febbraio 2018, osservava che "attraverso la fusione di diverse banche dati [...] si può riuscire a 're-identificare' un interessato attraverso informazioni apparentemente anonime. In molti casi, dunque, l'anonimizzazione di singoli identificatori univoci non è sufficiente per escludere le re-identificazioni (un dato considerato 'anonimo' può essere successivamente attribuito a una determinata persona). Inoltre, gli algoritmi che vengono applicati nell'analisi dei *Big-data* permettono di analizzare in modo autonomo e automatizzato banche dati di grandi dimensioni, anche nelle loro connessioni reciproche. Queste procedure di analisi generano nuove informazioni e spesso nuovi dati personali". Sul punto v. anche l'attenta analisi di A.C. Nazzaro, *L'utilizzo dei Big-data e i problemi di tutela della persona*, in "Rass. dir. civ.", 2018, pp. 1239 ss.

17 Papa Francesco nella sua Enciclica *Fratelli tutti* del 3 ottobre 2020, Capitolo primo, paragrafo *L'illusione della comunicazione*, rileva che "paradossalmente, mentre crescono atteggiamenti chiusi e intolleranti che ci isolano rispetto agli altri, si riducono o spariscono le distanze fino al punto che viene meno il diritto all'intimità. Tutto diventa una specie di spettacolo che può essere spiato, vigilato, e la vita viene esposta a un controllo costante. Nella comunicazione digitale si vuole mostrare tutto ed ogni individuo diventa oggetto di sguardi che frugano, denudano e divulgano, spesso in maniera anonima. Il rispetto verso l'altro si sgretola e in tal modo, nello stesso tempo in cui lo sposto, lo ignoro e lo tengo a distanza, senza alcun pudore posso invadere la sua vita fino all'estremo".

18 Anche il Garante si duole di questa percezione di cui sembra ormai essere oggetto il diritto alla protezione dei dati personali: P. Stanzione, *La privacy non*

3. A conferma di ciò, si osservi il percorso evolutivo seguito dalla disciplina in materia di diritto alla protezione dei dati personali.

Elaborato dai giuristi anglosassoni come diritto alla *privacy,* esso è stato inizialmente modellato sullo schema dominicale e, quindi, strutturato come diritto *ad excludendum omnes alios* dagli spazi intimi e privati della vita personale e familiare[19]. A partire dalla fine degli anni '80 del XX secolo, con l'avvento e la diffusione delle nuove tecnologie informatiche e telematiche, quel diritto è stato sottoposto ad un processo di graduale revisione. Ciò in quanto le logiche di appartenenza alle quali era ispirato mal si conciliavano con il progresso tecnologico (ed economico), poiché impedivano l'uso di molte delle informazioni (dati personali) necessarie al più efficace funzionamento delle comunicazioni, specie di quelle elettroniche. Il diritto alla *privacy* è stato, quindi, gradualmente spogliato della sua struttura dominicale e le tutele riconosciutegli sono state finalizzate, più che ad escludere *omnes alios* dal trattamento delle informazioni, a contemperare i contrapposti interessi per fare in modo che, nel rispetto di determinate modalità e limiti normativamente determinati, i dati personali e/o sensibili (non solo quelli relativi alla vita privata) potessero essere conosciuti ed utilizzati da terzi[20].

L'originario diritto alla *privacy* ha, così, ceduto il passo al diritto alla protezione dei dati personali il cui nucleo di tutela è stato incentrato sul consenso informato e consapevole del titolare in ordine al trattamento dei suoi dati da parte di terzi.

La logica del consenso impone, però, soprattutto quando il trattamento avviene con l'ausilio di strumenti informatici e telematici, che il titolare disponga delle risorse e delle conoscenze necessarie all'impiego di que-

---

è un ostacolo alla gestione della pandemia, Intervento apparso sul quotidiano "Domani" del 26 ottobre 2020 e pubblicato altresì sul sito *garanteprivacy.it*.

19 In questo modo risulta recepito in Italia dalla dottrina, tra gli anni '50 e '60 del XX secolo, e, poco dopo, dalla giurisprudenza di legittimità. Al riguardo cfr. l'analisi, in prospettiva storica, del dibattito dottrinale e giurisprudenziale di quegli anni svolta da M. Prosperi, *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento*, in "privacy.it", n. V, 2002, poi, le pagine dei primi studiosi che si occuparono del diritto alla riservatezza come A. De Cupis, *Il diritto alla riservatezza esiste*, in "Foro it.", parte I, 1954, pp. 116 ss.; G. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in "Riv. trim. dir. proc. civ.", parte I, 1958, I, p. 465; G. Pugliese, *Il diritto alla "riservatezza" nel quadro dei diritti della personalità*, in "Riv. dir. civ.", parte I, 1963, pp. 615 ss.

20 Su questo percorso evolutivo cfr., per tutti, A. Di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in "Appendice a La tutela dei diritti", Milano, vol. 3, 2001, pp. 393 ss.

gli strumenti[21]. Il che non sempre si verifica, o perché il titolare non può avvalersi di mezzi informatici e telematici (ad esempio, non ha le possibilità economiche necessarie a procurarseli o vive in un'area geografica non dotata di infrastrutture adeguate a garantire l'accesso alla rete *internet*), o perché non ha le conoscenze e le competenze per utilizzarli (come può avvenire per le persone anziane o non sufficientemente scolarizzate), o semplicemente perché ha tali impegni o difficoltà da non poter verificare tutti i trattamenti che lo riguardano (si pensi al frettoloso consenso dato, nel corso della navigazione in *internet*, alle segnalazioni sull'uso di *cookies* da parte dei siti visitati)[22].

Ne è derivato, pertanto, un progressivo indebolimento del diritto alla protezione dei dati personali che si è accentuato quando, a fronte della globalizzazione della *net economy* e dell'accentramento del trattamento dei dati in capo a poche multinazionali situate in paesi lontani, ci si è avveduti dell'insufficienza delle tutele meramente locali.

Anche al fine di contrastare queste difficoltà, l'Unione europea nel 2016 ha emanato un Regolamento unico in materia di trattamento dei dati personali (reg. n. 16/679/UE meglio noto come GDPR) che, tuttavia, non ha impresso un mutamento di rotta alla deriva intrapresa[23]. Anzi, se possibile, l'ha accentuata dal momento che, in più punti, chiarisce espressamente di

21 Una delle prime voci a segnalare i problemi che l'impiego degli strumenti informatici e telematici possono generare in relazione alla riservatezza delle persone è stato S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, pp. 120 ss. In qualità di Garante della *privacy* si è, poi, molto impegnato su questo fronte e, in particolare, ha curato l'elaborazione della *Carta dei diritti in Internet* approvata nel novembre del 2015 dalla Camera dei Deputati.

22 I *cookies* sono stringhe di testo collocate all'apertura di una pagina *web* per memorizzare i dati di navigazione dell'utente e, talvolta, tracciare il suo comportamento in rete (*tracking cookies*) al fine di consentire la personalizzazione della pubblicità sul *browser*. Secondo le vigenti norme di origine comunitaria, gli utenti della rete *internet* devono essere informati in modo semplice e comprensibile dell'uso di *cookies* da parte dei siti *web* che visitano, e devono prestare il loro consenso. I *cookies* possono essere utilizzati senza il previo consenso degli utenti solo qualora siano necessari per motivi tecnici come, ad esempio, per memorizzare le preferenze linguistiche ovvero i dati di *login* e del carrello acquisti. È noto però che, nella pratica, la tutela così offerta è del tutto inadeguata dal momento che il consenso, per motivi di tempo o per inconsapevolezza, viene spesso dato in modo frettoloso e senza consultare le specifiche tecniche dei *cookies*.

23 Per l'esame del testo normativo del GDPR vedasi, tra gli altri, F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in "Nuove leggi civ. comm.", 2017, pp. 369 ss.; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna 2019.

non voler impedire o limitare la circolazione dei dati personali, ma piuttosto di volerla agevolare purché con modalità sicure e controllate[24]. Inoltre, il GDPR non tiene adeguatamente conto dei rilevanti problemi connessi alla sempre maggiore diffusione della tecnologia informatica denominata *blockchain* che, connotandosi per la sua idoneità a garantire l'immodificabilità dei dati archiviati in registri diffusi, mal si concilia sia con la logica del controllo sul trattamento sia con le norme a tutela del diritto all'oblio[25].

In questo già problematico contesto sono intervenute, infine, le nuove regole volte a fronteggiare l'emergenza pandemica, che di nuovo danno prova dell'ormai spiccata propensione del legislatore a comprimere il diritto alla protezione dei dati personali ogniqualvolta vengano in gioco altri interessi generali, siano essi di carattere sanitario, economico, tecnologico.

---

24 Ad esempio, nel *Considerando* 4 del GDPR si legge che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità". Il *Considerando* 6 aggiunge che "la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso Paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali". Pertanto, il regolamento si pone gli obiettivi di creare un *clima di fiducia* in ordine ai trattamenti di dati personali e fare in modo che "le persone fisiche abbiano il controllo dei dati personali che li riguardano" (*Considerando* 7). Al riguardo, P. Perlingieri, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in "Foro nap.", 2018, pp. 481 ss., osserva che il GDPR sancisce il passaggio da una concezione fondata esclusivamente sul consenso informato ad una concezione caratterizzata anche dal controllo sul trattamento, ma comunque rileva l'inidoneità del consenso a garantire adeguata tutela ad interessi di natura personale.

25 La tecnologia *blockchain* si struttura in un *sofware* che genera un *database*, decentralizzato e condiviso dagli utenti in rete, funzionalmente volto alla gestione e memorizzazione di dati che vengono resi immodificabili. I dati immessi nel sistema vengono automaticamente crittografati, dotati di marcatura temporale e memorizzati in un *database* condiviso (c.d. registro diffuso), composto da blocchi tra loro collegati e distribuiti tra gli utenti. Pertanto, ogni transazione avviata tra due o più *client* autorizzati all'accesso è subito nota all'intera *community* perché i blocchi condividono l'archivio, chiedendo ai partecipanti di mettere a disposizione le loro risorse di memoria e di calcolo per effettuare il controllo, la validazione e la marcatura temporale delle nuove informazioni immesse nel sistema (c.d. controllo e consenso diffuso). Ne deriva che l'autenticità e l'immutabilità dei dati è garantita dalla combinazione di tecniche di firma digitale e marcatura temporale che assicurano l'identificazione dei *client* e la datazione irreversibile del documento annotato nel registro di tutti i nodi della rete, nonché l'archiviazione definitiva e irrevocabile dei dati validati da tutti i nodi della rete.

4. A fronte di ciò verrebbe da chiedersi, in funzione anche un po' provocatoria, se il diritto alla protezione dei dati personali possa ancora essere qualificato come diritto soggettivo. Però non par dubbio che la risposta a tale interrogativo debba essere affermativa, sia perché la tutela dei dati personali è un presidio essenziale per lo svolgimento della personalità degli individui *ex* art. 2 Cost. (la metafora del *Panopticon* sta a dimostrarlo); sia perché è ampiamente condivisa l'affermazione che, nei rapporti interprivati, gli interessi personali dotati di rilievo costituzionale non si attuano in modo assoluto, ma si bilanciano tra loro poiché, trovandosi in una situazione di attuazione costante e contemporanea per tutti i consociati, entrano giocoforza in conflitto tra di loro e, quindi, incorrono in un'azione di continuo contemperamento[26]. È, appunto, in tale prospettiva che si spiegano le limitazioni apposte al diritto alla protezione dei dati personali nel caso della pandemia, giacché fondate sull'esigenza di tutelare la salute; così come quelle previste in relazione al *cyberspazio*, giustificate dall'intento di garantire a tutti nuove possibilità di esercizio di libertà personali e nuove occasioni di partecipazione democratica.

Queste limitazioni, però, nel loro insieme, stanno determinando, di fatto, la graduale concentrazione di un'enorme massa di dati in capo a entità statali o extrastatali, talvolta operanti con scopo di lucro, con il conseguente pericolo che tutti i valori di vertice dei moderni ordinamenti occidentali vengano ad essere svuotati per il tramite del graduale assottigliamento del contenuto del diritto alla protezione dei dati personali. La metafora del *Panopticon* ammonisce proprio su tale pericolo: all'instaurazione di un controllo invisibile e generalizzato consegue, oltre alla compressione del diritto alla protezione dei dati personali, l'erosione degli altri diritti e libertà fondamentali che, non essendo più schermate dalla sorveglianza del potere centrale, risultano esposte alle sue pressioni e condizionamenti.

Esemplare, al riguardo, è il caso del trattamento di dati personali e biometrici per fini di promozione commerciale attualmente consentito, seppur con cautele, dal GDPR. Anche in questa ipotesi le limitazioni apposte al

26 In tal senso, seppur con diversità di sfumature, nel quadro della dottrina civilistica vedi, *ex multis*, D. Messinetti, *Personalità (diritti della)*, in "Enc. dir.", XXXIII, Milano, 1983, pp. 359 e 377; ma anche L. Mengoni, *Diritto e valori*, Bologna, 1985, pp. 6 ss.; P. Perlingieri, *Il diritto civile nella legalità costituzionale*, V. I, Napoli 2020, pp. 1 ss.; tra i giuspubblicisti, v. G. Zagrebelsky, *Il diritto mite*, Torino, 1992, pp. 170 ss., ma anche R. Bin, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992, pp. 60 ss.; G. Scaccia, *Il bilanciamento degli interessi come tecnica di controllo costituzionale*, in "Giur. cost.", n. I, 1998, pp. 3956 ss.

diritto alla riservatezza trovano il loro fondamento nell'esigenza di contemperarlo con un altro valore di rilievo costituzionale, qual è l'iniziativa economica privata. Tali limitazioni, però, mostrano una notevole capacità espansiva a carico delle altre libertà personali del titolare perché l'imprenditore, facendo leva sulle informazioni raccolte, può mettere in atto una complessa serie di efficaci strategie (ad esempio, di *neuromarketing*) idonee a condizionarne le scelte, le opinioni ed i comportamenti[27].

In definitiva, il diritto alla protezione dei dati si ascrive alla categoria dei diritti della personalità ma, al tempo stesso, funge da baluardo per tali diritti dal momento che ogni limitazione ad esso apportata immancabilmente si riflette sull'intera categoria. Per questo motivo, e diversamente da quanto fatto finora, l'introduzione di nuove limitazioni al diritto in esame andrebbe ponderata con attenzione[28], in una prospettiva ampia, cioè in modo da tener conto anche delle conseguenze pregiudizievoli per gli altri diritti fondamentali e, quindi, evitando di considerare il diritto alla protezione dei dati come una monade isolata, avulsa dagli altri valori essenziali della persona.

Se valutato da siffatta prospettiva, il diritto alla protezione dei dati personali non appare più come un orpello, o un inutile ostacolo alla piena realizzazione di questo o di quell'altro interesse, ma piuttosto come un argine essenziale a preservare la dignità della persona e l'ordine democratico. Pertanto, le garanzie offerte dalla logica del consenso e del controllo del trattamento da parte dei titolari dei dati o dei Garanti nazionali potrebbero apparire non sempre bastevoli a garantire un grado di tutela sufficiente ed effettiva[29].

Qui non è possibile definire adeguatamente il ruolo che l'evoluzione tecnologica può giocare (non solo per favorire il trattamento massivo dei

27 Sia consentito rinviare a R. Catalano, *Neuromarketing e tutela civile dei dati personali biometrici*, in "Comp. e dir. civ.", aprile 2019; ma v. anche A. Santosuosso, *Neuroscienze e diritto*, Pavia 2009, pp. 11 ss.; M. De Caro, A. Lavazza, G. Sartori, *Siamo davvero liberi? Le neuroscienze e il mistero del libero arbitrio*, Milano 2010, pp. 5 ss.

28 In questa direzione sembra orientarsi anche la Corte di Cassazione che di recente, con l'ordinanza del 21 ottobre 2019, n. 26778, in "Nuove leggi civ. comm.", in G. Alpa (a cura di) *Numero speciale Casebook I diritti della persona*, 2020, pp. 107 ss., con nota di R. Mattera, ha rilevato che l'applicazione della vigente disciplina in materia di protezione dei dati personali va in ogni caso improntata al principio della minimizzazione, alla cui stregua ogni trattamento può avere ad oggetto solo "i dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati".

29 P. Perlingieri, *Privacy digitale e protezione dei dati personali tra persona e mercato*, cit., pp. 481 ss.

dati, ma anche) in funzione di controllo e limitazione del trattamento stesso. Così come non è possibile analizzare i casi in cui, superata la logica del consenso individuale, sia possibile recuperare aree di divieto assoluto di trattamento ovvero stabilire forme di tutela collettiva a presidio di coloro che non siano in condizione di proteggere adeguatamente la propria riservatezza. È, però, almeno necessario rilevare che l'attuale situazione di pandemia e le misure adottate per contrastarla, qualora non assistite da adeguate misure di sicurezza e se non rimosse al cessare dell'emergenza sanitaria, possono contribuire ad accelerare notevolmente il processo di indebolimento di cui è oggetto da qualche anno il diritto alla protezione dei dati personali e, conseguentemente, a consolidare una situazione di progressiva erosione degli altri diritti fondamentali.

Il *Panopticon* virtuale che sta sorgendo dall'emergenza sanitaria reca, però, alcuni semi di speranza. Bisogna constatare infatti che, proprio grazie alla pandemia ed alla conseguente necessità di creare piattaforme comuni di tracciamento delle persone infette, si sono stabilite, come mai prima, delle proficue sinergie tra molti Stati. Tali sinergie, una volta estinta l'emergenza pandemica, possono ben costituire il fondamento di una collaborazione internazionale rivolta all'elaborazione di un nuovo sistema globalizzato di tutele per il diritto alla protezione dei dati personali inteso come presupposto essenziale della dignità delle persone. Il che, a fronte della dimensione ormai globalizzata dei soggetti che raccolgono e trattano enormi quantità di dati grazie al monitoraggio delle reti di comunicazione, sembra costituire l'unica strada per riconoscere al diritto alla riservatezza forme di tutela individuale e collettiva realmente idonee a contrastare il consolidarsi di concentrazioni di potere in capo ad enti privi di legittimazione democratica.