RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0203 • articolo sottoposto a peer review • pubblicato in anteprima il 29 apr. 2025

Leonardo Marchesin

Oltre il consenso. I limiti dell'*Individual Control Model* e prospettive per un approccio collettivistico alla sorveglianza contemporanea

La sorveglianza contemporanea non ha portato soltanto vantaggi alle società post-moderne. Le attività di *dataveillance*, *data mining* e *profiling* rappresentano un pericolo reale nella maggior parte delle comunità umane odierne. Tale rischio riguarda non soltanto gli individui, vittime quotidiane di discriminazioni o visioni distorte della realtà, ma anche la collettività democratica in cui essi vivono, esposta alla progressiva erosione dei suoi principi fondamentali e delle pratiche dialogiche di cui si nutre. L'approccio tradizionale alla privacy e alla sua tutela (c.d. *Individual Control Model*) tenta, come dimostrato soprattutto dalla logica del consenso insufflata dal legislatore europeo nella disciplina del GDPR, di reagire a tale situazione di allarme riponendo tutte le proprie speranze nel rafforzamento del singolo e dei suoi diritti. Tuttavia, prassi quotidiane e studi scientifici hanno dimostrato l'inefficacia di un simile orientamento, il quale, da solo, rischia di peggiorare una condizione già emergenziale. Si rende, dunque, necessario un mutamento di paradigma, ovvero l'elaborazione di un sistema complessivo che, affiancandosi a quello già esistente, riesca a garantire una protezione effettiva delle persone e della loro privacy. Poiché, infatti, i pericoli generati dalla *dataveillance* riguardano non soltanto il soggetto ma anche la comunità intera, è necessario iniziare a pensare a delle risposte alla sorveglianza contemporanea che si avvalgano anche e soprattutto della forza collettiva del *demos* (c.d. *Societal Structure Model*).

Sorveglianza – Dataveglianza – Riservatezza – Individual Control Model – Societal Structure Model

Beyond the consent. The limits of the Individual Control Model and prospects for a collectivist approach to contemporary surveillance

Contemporary surveillance has not only brought benefits to post-modern societies. Dataveillance, data mining and profiling pose a real danger in most of today's human communities. This risk affects not only individuals, who are daily victims of discriminations or distorted views of reality, but also the democratic community in which they live, exposed to the progressive erosion of its fundamental principles and the dialogical practices on which it is nourished. The traditional approach to privacy and its protection (the so-called Individual Control Model) attempts, as demonstrated above all by the logic of consent insufflated by the European legislator in the GDPR regulation, to react to this situation of alarm by placing all its hopes in the empowerment of the individual and his rights. However, daily practices and scientific studies have demonstrated the ineffectiveness of this orientation, which, on its own, risks worsening an already emergency situation. What is needed, therefore, is a paradigm shift, i.e., the development of an overall system that, by complementing the existing one, is able to guarantee effective protection of individuals and their privacy. In fact, since the dangers generated by dataveillance concern not only the individual but also the entire community, it is necessary to start thinking of responses to contemporary surveillance that make use, also and above all, of the collective strength of the *demos* (so-called Societal Structure Model).

Surveillance – Dataveillance – Privacy – Individual Control Model – Societal Structure Model

L'Autore è tirocinante ex art. 73 l. 98/2013 presso il Tribunale Ordinario di Venezia

1. *Your browsing is being watched*

La routinaria vita di tutti i giorni pare procedere in uno stato di quieta normalità, tanto per chi si affaccenda nelle più svariate attività lavorative o di studio, quanto per chi ancora gode degli ultimi attimi di festivo riposo. Eppure, tale idilliaco spaccato di quotidianità è destinato a subire una brusca e inquietante interruzione.

Dalla parete di un edificio pubblico, una telecamera si desta e, dispiegate le proprie ali metalliche, si distacca dal muro nel quale era stata precedentemente installata, planando rapidamente in prossimità di un individuo per osservarlo più da vicino. Dapprima uno solo, ma presto decine e decine di occhi elettronici compiono ammutinamento, abbandonano le rispettive posizioni all'interno dello scacchiere cittadino e si lanciano in una asfissiante persecuzione delle più svariate persone nelle quali hanno la ventura di imbattersi. A casa e in ufficio, nei parcheggi sotterranei e nelle fermate dei mezzi pubblici, addirittura nel lungomare e in un peschereccio al largo, nessuno può dirsi al riparo da questo stormo di telecamere che, come uccelli o pipistrelli, virano in picchiata verso qualsiasi soggetto capiti entro il loro campo visuale. L'obiettivo degli occhi elettronici è chiaro: spiare non tanto (o meglio, non solo) la persona in carne ed ossa, quanto piuttosto le attività che essa sta svolgendo attraverso l'iPhone che tiene costantemente nel palmo della propria mano.

A nulla sembrano valere la fuga, le urla di terrore, il getto a mare del proprio dispositivo o il tentativo velleitario di colpire le telecamere scagliandogli contro anche gli oggetti più improbabili. Gli occhi elettronici sono ovunque, e da essi non è dato trovare sicuro riparo.

Il quadro dalle tinte orwelliane dipinto da Apple nei pochi secondi dello spot che pubblicizza il motore di ricerca installato nei suoi dispositivi restituisce con poche ma incisive immagini uno stato dell'arte ben noto nell'ambito dei *surveillance studies*[1].

La dilagante presenza di CCTV e sistemi di videosorveglianza pubblici e privati all'interno dei tessuti urbani rappresenta una realtà radicata e persistente oramai da diversi decenni, tanto che già agli inizi del secolo Hille Koskela aveva modo di sostenere senza tema di smentita che "surveillance cameras are commonly used to protect high-class private premises – 'gated communities' – but also semi-public places such as shopping malls, underground and mainline train-stations, police stations and even churches" e "to monitor city streets"[2].

1. V. lo spot pubblicitario integrale.
2. Koskela 2000, p. 245. Negli stessi anni, in Italia, Stefano Rodotà parimenti affermava che "il semplice camminare per strada diventa un atto implacabilmente registrato da una telecamera, le informazioni vengono conservate ed ogni nostro passaggio in una piazza o in una strada, in una stazione, in un grande magazzino può essere ritrovato": Rodotà 2004, p. 173. E la diffusione dei sistemi di videosorveglianza che veniva rilevata a inizio secolo pare non accennare a diminuire o decelerare. In Italia, il *Rapporto Nazionale sull'attività della Polizia Locale* del 2023 ha infatti attestato che nel 2022, presso i 145 comandi analizzati, risultavano installate complessivamente 29.137 telecamere di videosorveglianza, in media 202 per ogni città,

Analogamente, non costituisce una recente novità la diffusione presso larga parte della popolazione mondiale di dispositivi elettronici in grado di perpetrare forme di monitoraggio destinate ad andare ben oltre la sola captazione di parole e condotte resa possibile dalla tradizionale videosorveglianza. Come noto, infatti, pressoché la totalità degli apparecchi tecnologici e dei software informatici quotidianamente utilizzati dalla maggior parte delle persone risulta essere capace di raccogliere, immagazzinare, assemblare ed elaborare dati e metadati emessi dagli utenti medesimi, ora volontariamente ora inconsapevolmente[3]. Non è, dunque, un caso che già sul finire del secolo scorso Roger Clarke avesse rilevato la presenza, accanto alla "classica" *surveillance*, di una *dataveillance*[4].

Tuttavia, come dimostrato dal summenzionato *spot* pubblicitario di Apple, il consolidamento nel tempo e nello spazio delle anzidette dinamiche di controllo e delle tecnologie che le rendono possibili non ha implicato una diminuzione dei timori connessi agli effetti di una sorveglianza che appare sempre più fluida, subdola e pervasiva.

Negli ultimi decenni, infatti, numerosi sono i giuristi, gli informatici, i sociologi e gli economisti che, nei rispettivi ambiti di studio, hanno levato incessantemente la loro voce specialistica per denunciare i rischi individuali e collettivi connessi alla vigilanza contemporanea, nonché per provare ad approntare soluzioni teoriche e pratiche volte ad arginarne le conseguenze maggiormente dirompenti e pregiudizievoli. E non è, dunque, un caso se oramai da tempo anche i legislatori di numerose nazioni e organizzazioni internazionali hanno deciso di intervenire normativamente per (provare a) regolare un contesto, quello della sorveglianza, tanto dannoso in potenza quanto diffuso nella pratica[5].

In questo articolo si procederà innanzitutto alla riepilogazione critica di quelli che, nell'ambito dei *surveillance studies*, sono notoriamente ritenuti gli effetti maggiormente pericolosi delle attuali forme di monitoraggio. L'attenzione verrà posta in particolar modo su quelle modalità di controllo che, ben più invasive rispetto alla mera videosorveglianza, hanno riguardo alla dimensione digitale della persona anziché al suo corpo fisico. In tale contesto, si avrà modo di evidenziare come simili conseguenze attentino non solo alle libertà e ai diritti del singolo individuo ma anche, e conseguentemente, ai valori e ai principi che fondano le società oggigiorno rette da una logica democratica.

Successivamente, e prendendo a modello anzitutto la regolamentazione racchiusa nel GDPR (*General Data Protection Regulation*, o Regolamento 2016/679), si darà spazio a una sintesi dei principali rimedi accolti e applicati a livello dottrinale prima e legislativo poi, evidenziando come questi ultimi si muovano entro un orizzonte perlopiù individualistico e scarsamente incline a considerare soluzioni di natura più marcatamente collettivistica. Sulla base di ciò, si avrà modo di riscontrare i patenti limiti che affliggono tale approccio fondato sull'esaltazione del potere e del controllo del singolo soggetto, i quali risulteranno manifesti una volta evidenziati i vizi logici e pratici che inficiano il concetto cardine in cui tale approccio si incarna, ovverosia quello del consenso.

Per concludere, si cercherà di mostrare come, al fine di provare ad arginare le conseguenze più

il che segna un netto aumento rispetto all'anno precedente, quando la media registrata è stata di 192 telecamere per ogni città.

3. L'esempio più celebre è dato dalla localizzazione operata dagli smartphone: "a meno di disattivarla esplicitamente all'interno del menù impostazione del vostro dispositivo […] la localizzazione non cessa di lasciare traccia di ogni vostro spostamento nel mondo […]. Algoritmi applicati alla velocità a cui vi muovete sono utilizzati per dedurre se siete a piedi o in macchina, o persino in quale tipo di veicolo vi trovate […]": Greenfield 2017, pp. 27-28.
4. Cfr. Clarke 1998, p. 499.
5. Tra le più celebri normative internazionali che si sono occupate della sorveglianza dei dati si ricordano le Linee Guida OCSE del 1980, la Convenzione 108 del Consiglio d'Europa (o Convenzione di Strasburgo) del 1981, il General Data Protection Regulation (GDPR), successore della Direttiva 95/46/CE (c.d. Direttiva Madre), e l'Asia-Pacific Economic Cooperation (APEC) del 2004. Di tutela della privacy, più in generale, si occupano anche la Dichiarazione universale dei diritti umani del 1948 (art. 12), la CEDU del 1950 (art. 8), il Patto internazionale sui diritti civili e politici del 1966 (art. 17) e la Carta di Nizza del 2000 (artt. 7, 8 e 52).

preoccupanti di una sorveglianza alla quale la logica dell'assenso risulta non essere stata in grado di porre freni tangibili e realmente efficaci, si renda necessario un mutamento di paradigma, quantomeno parziale. Se, infatti, non appare opportuno abbandonare *in toto* il modello consensuale attualmente prevalente sul piano normativo, è altrettanto necessario ammettere che continuare a fare affidamento esclusivamente sul medesimo rischia di dimostrarsi una scelta poco azzeccata alla luce dei risultati finora raggiunti. Appare, pertanto, opportuno iniziare a volgere lo sguardo anche verso misure di natura maggiormente collettivistica per far fronte a delle dinamiche di controllo che, in fin dei conti, non attentano soltanto alla persona ma anche alla società in cui essa vive.

2. Il lato oscuro della sorveglianza

Benché essa presenti taluni profili di favore per la società e di vantaggio per l'individuo[6], la sorveglianza, sia essa generalmente intesa ovvero considerata con specifico riferimento all'odierna epoca post-moderna, appare in grado di produrre effetti nocivi tali, per portata e propagazione, da dover essere – come sono stati e continuano ad essere – resi oggetto di attenta analisi.

L'ambiguità insita nel concetto stesso di monitoraggio[7], già evidente nelle consolidate pratiche di videosorveglianza[8], non pare affievolirsi o venire meno neppure allorquando la sorveglianza abbia ad oggetto non tanto le condotte materiali dell'individuo quanto piuttosto i dati virtuali che lo riguardano[9]. Anzi, le innovative modalità di controllo del corpo elettronico e dell'identità digitale della persona paiono, se possibile, accentuare i lati negativi della sorveglianza, benché i profili positivi della stessa continuino ad essere più appariscenti[10].

Come noto, la quotidianità della maggior parte dei soggetti che vivono nelle società contemporanee si dipana sempre più di frequente anche attraverso una dimensione virtuale[11]. Numerose sono le attività giornaliere che odiernamente si possono (o, addirittura, si devono) svolgere non più materialmente, bensì con l'ausilio di Internet e di dispositivi elettronici ad esso connessi[12]. Ed è altrettanto riconosciuto che nel momento in cui un individuo si trova ad agire all'interno della Rete

6. Ne sono un esempio paradigmatico i benefici apportati in ambito medico-sanitario dall'utilizzo dei dati: cfr. Orefice 2018, pp. 152-154.
7. L'ambiguità della sorveglianza è tema più volte sottolineato da David Lyon: cfr., tra gli altri, Lyon 2020, p. 91 ss. La natura ambivalente del monitoraggio pare addirittura accentuarsi se considerato in relazione al carattere altrettanto sfumato delle tecnologie che oggigiorno lo rendono possibile. Sull'ambiguità delle odierne tecnologie cfr. Stiegler 2023.
8. Da un lato, infatti, l'installazione di telecamere all'interno dei tessuti urbani viene giustificata, non senza sollevare perplessità, quale misura di tutela della sicurezza personale e cittadina (cfr. Svendsen 2017 e Lyon 2020, *passim*). Dall'altro lato, tuttavia, non è più un mistero che, qualora scorretto, sfuggente e orientato da pregiudizi, l'uso di occhi elettronici possa portare all'insorgenza di trattamenti discriminatori a danno di singoli soggetti o interi gruppi sociali, nonché alla disincentivazione finanche di pratiche tutt'altro che illecite e, anzi, funzionali all'esercizio di libertà democratiche (cfr. Greenfield 2017, p. 248, e Pin 2022, p. 7).
9. Cfr. De Kerkhove 2016, p. 36, e Orefice 2018, pp. 106-107.
10. In generale, David Lyon ritiene, riprendendo un linguaggio in uso già da tempo presso alcuni hacker, che oggi si possa parlare di *neofilia*: tale è la propensione delle persone a essere entusiaste delle novità apportare dalle nuove tecnologie, la quale le induce a dimenticare o sottovalutare i rischi che esse portano con sé, sorveglianza inclusa: cfr. Lyon 2020, p. 100 ss.
11. Celebri sono i due neologismi ideati da Luciano Floridi per indicare l'attuale dispiegarsi della vita umana tra dimensione analogica e dimensione digitale, ovverosia *inforg* (*informational organism*) e *onlife* (crasi di *online* e *life*): cfr., tra gli altri, Floridi 2020. Le due dimensioni sembrano destinate a fondersi con un grado di compenetrazione ancora maggiore a seguito dell'avvento del c.d. Metaverso, ovverosia la "possibilità di elevare il livello di interazione tra il mondo 'reale' e quello 'virtuale' fino al punto (ideale) in cui le esperienze vissute in essi siano totalmente coerenti e interscambiabili": Sarra 2024, p. 4.
12. Cfr. Delmastro–Nicita 2019, pp. 8-9, e Marchesin 2024-a, p. 31.

esso, volontariamente o meno, cede un gran numero di dati e rilascia un'ingente quantità di metadati (c.d. *big data*), prontamente raccolti, incasellati, assemblati e utilizzati non solo da istituzioni pubbliche ma anche da imprese private[13].

La realtà che è andata consolidandosi in anni recenti difficilmente potrebbe considerarsi del tutto negativa, in quanto foriera anche di possibilità e comodità di indubbio vantaggio[14]. Tuttavia, occorre ricordare che simili facilitazioni della vita individuale e collettiva implicano una ingente raccolta di informazioni da parte di attori pubblici e privati, i quali, pertanto, si avvalgono a tal fine di algoritmi e software in grado di controllare tutte le attività dell'utente e di tradurle in preziose strisce alfanumeriche dalle quali estrarre conoscenza (*data mining*, o *data analysis*)[15].

Come evidenziava già nella decade precedente Eli Pariser, l'attività di reperimento e conservazione di dati e metadati tramite algoritmi risulta essere funzionale al *profiling* della persona, ovverosia alla schedatura delle sue preferenze, idee ed opinioni e alla sua conseguente classificazione entro categorie predefinite (*data segments*)[16]. Ed è proprio una simile dinamica a suscitare, tra i *surveillance scholars*, i maggiori allarmi.

Dal punto di vista individuale, infatti, la targetizzazione implica una vera e propria reificazione del soggetto. La riduzione della multiforme personalità umana a un neutro coagulo di stringe alfanumeriche rappresenta un chiaro svilimento della dignità dell'individuo, il quale vede appiattite le proprie idee ed emozioni entro gli angusti spazi di un database elettronico atto alla sua successiva manipolazione[17].

E forse tale prassi potrebbe ancora considerarsi tollerabile qualora fosse funzionale alla mera facoltà di personalizzare le *app* e la grafica dei dispositivi. Tuttavia, il *profiling* non risulta essere fine a se stesso. Esso, infatti, rappresenta il principio sulla base del quale vengono prese decisioni destinate a incidere più o meno pesantemente sulla vita della persona (*data-driven society*)[18]. Non si tratta soltanto della possibilità di inoltrare messaggi pubblicitari personalizzati o di effettuare delle perfette discriminazioni di offerte e prezzi tra gli utenti (*behavioral retargeting*)[19]. In base al credito sociale che emerge dai dati raccolti, le decisioni assunte dagli algoritmi possono incidere sulla vita lavorativa e pubblica di un soggetto[20]. Sicché è evidente non solo la progressiva perdita di controllo sulle proprie vite da parte di utenti spesso inconsapevoli di tali

13. Sulla quantità di dati rilasciati da un utente medio ogni giorno cfr. Greenfield 2017, p. 29; Delmastro–Nicita 2019, pp. 10-11; Perri 2020, pp. xi-xii; Maestri 2021, p. 56; Pin 2021, p. 51; Paolucci 2021, p. 205; Sarra 2022-a, pp. 21-22; Pietropaoli 2024, p. 4; Marchesin 2024-a, pp. 31-32.
14. A livello collettivo, ad esempio, vale la pena notare che taluni reati difficilmente potrebbero essere perseguiti e, conseguentemente, sanzionati come per legge in assenza della possibilità, per le forze dell'ordine e per i pubblici ministeri, di acquisire file di log e di traffico telefonico incamerati dai dispositivi tecnologici impiegati dai rei. Sul piano individuale, analogamente, le amenità garantite dalle odierne tecnologie implicanti un certo grado di vigilanza risultano essere sin troppo evidenti.
15. Sulla definizione di *data mining* cfr. Maestri 2021, p. 60, e Sarra 2022-a, p. 84.
16. Cfr. Pariser 2012. Sulla profilazione e sul suo funzionamento cfr. anche Greenfield 2017, pp. 214-215, e Delmastro–Nicita 2019, p. 27.
17. Sugli effetti reificanti della sorveglianza contemporanea e sulla possibile correlazione tra essi e le conseguenze disumanizzanti e spersonalizzanti discendenti dal monitoraggio panottico di epoca moderna cfr. Marchesin 2024-b. Sulla reificazione dell'utente provocata dalla riduzione dell'essere umano in dati e dalla sorveglianza che li riguarda cfr. anche Orefice 2018, p. 79; Becker 2019, p. 311; Maestri 2021, p. 63; Han 2021, pp. 20-21; Paolucci 2021, p. 208; Han 2023, p. 13; Sarra 2024, p. 18; Pietropaoli 2024, p. 4.
18. Cfr. Sarra 2022-a, p. 85, e Sarra 2022-b, *passim*.
19. Cfr. Orefice 2018, pp. 105-106; Delmastro–Nicita 2019, pp. 11 e 81-83; Bazzoni 2019, p. 639; Pin 2021, p. 52; Di Corinto 2022, pp. 32-33; Ferraris–Saracco 2023, p. 46; Han 2023, pp. 27-28; Pietropaoli 2024, p. 4; Doctorow 2024, p. 20.
20. Cfr. Delmastro–Nicita 2019, p. 123, e Pin 2021, p. 56.

dinamiche[21], ma anche il pericolo di perpetrazione di pratiche discriminatorie e sperequative[22], posta la asserita non neutralità degli algoritmi utilizzati[23].

Da una prospettiva aperta all'intero consorzio umano, i rischi anzidetti non paiono affievolirsi.

La profilazione, infatti, permette di avvalersi delle preferenze personali emergenti dall'analisi dei dati per selezionare non solo le occasioni di lavoro e di acquisto, ma anche le notizie che ciascun individuo avrà modo di visualizzare, nonché l'ordine in cui esse appariranno ai suoi occhi (*self-sorting*). In un mondo dove il web e i social network costituiscono sempre più di frequente la principale fonte di informazione per un gran numero di persone[24], queste ultime sono destinate a venire a contatto pressoché esclusivamente con notizie che, secondo le previsioni di un algoritmo opaco, più si confanno alle loro idee e preferenze, ovverosia con informazioni che tendono a confermare – o, quantomeno, a non mettere in discussione – le loro opinioni originarie, giuste o errate che siano[25].

È innegabile che tale dinamica possa, entro certi termini, essere utile per mettere in comunicazione tra loro individui che condividono i medesimi interessi ma che vivono in luoghi tra loro assai distanti; tuttavia, essa cela pericoli estremamente elevanti per la collettività.

Divenute destinatarie pressoché in via esclusiva di informazioni sartorialmente ritagliate sulla base dei dati e metadati rilasciati in Rete, le persone corrono il rischio di entrare in possesso di una visione della realtà soltanto parziale o comunque ideologicamente orientata in base alle loro preferenze aprioristiche[26]. Il nocumento determinato da una simile situazione non riguarda soltanto i singoli soggetti, che sono esposti al pericolo di non poter accedere alla verità dei fatti e di essere privati del diritto a un'informazione imparziale e completa. A essere danneggiata è l'intera società, la quale dovrà sopportare gli effetti pregiudizievoli prodotti dalle decisioni prese dai suoi membri sulla base di notizie deficitarie, parziali e incomplete, se non addirittura del tutto false[27].

Non solo. Come sostiene Cass R. Sunstein, la reclusione degli individui entro impercettibili *filter bubbles* rischia di produrre effetti di "polarizzazione" e "frammentazione"[28] delle varie frange della popolazione. Se attraverso i più usati mezzi di informazione le persone rinverranno pressoché esclusivamente notizie confermative dei loro pensieri e pregiudizi, esse si trincereranno e radicalizzeranno attorno alle loro posizioni, divenendo sempre meno propense all'accoglimento o anche solamente all'ascolto di idee e opinioni diverse provenienti da gruppi sociali differenti[29] (c.d. autismo informativo[30]).

In questi termini – e ben al contrario rispetto a quanto si prospettava all'epoca dell'avvento di Internet[31] –, è evidente il pericolo corso dagli attuali regimi democratici, chiamati non solo a fronteggiare la disinformazione dei singoli soggetti ma anche a far fronte alla progressiva perdita di efficacia della pratica dialogica, da sempre collante del tessuto sociale.

21. Cfr. Solove 2021, p. 39, e Pietropaoli 2024, p. 5.
22. Cfr. Pin 2021, p. 57, e Pietropaoli 2024, p. 2.
23. Cfr. Greenfield 2017, pp. 239-240; Perri 2020, p. 132; Sarra 2022-a, p. 93; Kienke 2023, p. 49; Coniglione 2023, p. 3.
24. Cfr. Delmastro–Nicita 2019, pp. 91-93, e Han 2022, p. 32.
25. Cfr. Sunstein 2017, pp. 11-14; Delmastro–Nicita 2019, pp. 94-102; Bazzoni 2019, pp. 639-640; Sarra 2022-a, p. 94; Han 2023, p. 28.
26. Cfr. Pin 2021, pp. 52-53.
27. Sulla diffusione delle fake news e sulle sue conseguenze cfr. Moro–Fioravanzi 2022.
28. Sunstein 2017, p. 15.
29. Cfr. Sunstein 2017, pp. 21-22 e 37; Delmastro–Nicita 2019, pp. 101, 111; Bazzoni 2019, p. 641; Han 2023, pp. 39-40; Kienke 2023, pp. 42-43; Coniglione 2023, p. 10; Pietropaoli 2024, p. 5; Solove–Hartzog 2024, p. 1029. Tale pericolo si innesta, peraltro, nel contesto generale attuale, il quale, contraddistinto dalla rapidità delle informazioni, sovente priva del tempo necessario per instaurare dibattiti seri e approfonditi: cfr. Han 2023, p. 25.
30. Cfr. Kienke 2023, p. 46.
31. Cfr. Scorza 2022.

3. Lo stato dell'arte: l'*Individual Control Model*

Pur a fronte di uno scenario inquietante e apparentemente privo di speranza per la riservatezza degli individui, il summenzionato *spot* pubblicitario di Apple termina con un lieto fine. Cliccando sull'icona di Safari, infatti, le persone perseguitate dalle telecamere volanti riescono ad annientarle, sfuggendo così al loro penetrante e infaticabile sguardo. Il messaggio conclusivo è chiaro: *Safari. A browser that's actually private*.

È evidente il tentativo dello *spot* pubblicitario del motore di ricerca impiegato da Apple di esporre al pubblico la volontà della multinazionale statunitense di attuare forme di *privacy by design e privacy by default*. Tuttavia, esso dipinge un suggestivo quadro ben indicativo di un certo approccio alla tutela della riservatezza: soggetti consapevoli di essere costantemente sorvegliati da dispositivi implacabili – rappresentati dagli occhi elettronici muniti di ali –, preoccupati se non addirittura terrorizzati da tale situazione complessiva, decidono scientemente di adottare comportamenti volti alla protezione della loro privacy – esemplificati in estrema sintesi dal gesto di cliccare sull'icona di Safari.

Nell'ambito dei *surveillance studies* è frequente imbattersi in proposte che mirano a osteggiare le più invasive forme di monitoraggio e i loro effetti maggiormente intollerabili attraverso pratiche che fanno affidamento sul singolo, ovvero su circoscritti gruppi di soggetti mossi da iniziative individualistiche.

In riferimento alla videosorveglianza, ad esempio, Cossutta e Mainardi ritengono lodevole ed efficace l'attività politico-artistica di collettivi quali i *Surveillance Camera Players*, un gruppo i cui membri "organizzano performance-protesta di fronte alle camere di sorveglianza situate in luoghi pubblici e […] usano la loro visibilità, le loro apparizioni pubbliche, le loro interviste e il loro sito per sfatare il luogo comune che 'solo chi è colpevole di qualcosa si oppone alla sorveglianza'"[32]. Relativamente al contesto digitale, invece, è nota la proposta di Brunton e Nissenbaum, divenuta celebre come "offuscamento": incentivati a cliccare su qualsivoglia *banner* sia presente nelle pagine web visitate (*AdNauseam*) o a rilasciare un'ingente quantità di like a prescindere dal contenuto dei post pubblicati nei social network (*like-farming*), gli individui vengono invitati, attraverso queste e altre condotte analoghe, all'"aggiunta deliberata di informazioni ambigue, confuse e ingannevoli per interferire con la sorveglianza e la raccolta di dati personali"[33].

Analogamente, e sempre avuto riguardo alla sorveglianza dei dati, a livello normativo si riscontra oramai da decenni una generale adesione dei legislatori a quello che, in letteratura, viene definito *Individual Control Model*, ovverosia un'impostazione generale che – per usare le parole del suo più noto teorizzatore, Alan F. Westin – considera 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"[34]. In altri termini, a fronte di un generale depotenziamento (*disempowerment*) dell'individuo causato dalle nuove tecnologie e dalla sorveglianza che esse permettono, lo scopo perseguito da numerosi legislatori è quello di adottare misure normative volte a favorire un rafforzamento (*empowerment*) del singolo soggetto, garantendogli diritti specifici e, in generale, un maggiore controllo sui suoi dati[35].

Tale approccio alla riservatezza e alla sua tutela, invalso anche negli Stati Uniti a partire dagli anni Settanta del secolo scorso[36], trova oggi la sua

32. Cossutta–Mainardi 2018, p. 173.

33. Brunton–Nissenbaum 2016, p. 10.

34. Westin 1967, p. 7. Come rileva Julie Zahle, la visione secondo cui il miglior strumento di tutela della privacy è rappresentato dal consenso informato ha avuto un notevole successo, tanto da continuare ad essere perorata ancora in tempi recenti: cfr. Zahle 2017, p. 1.

35. Cfr. Hartzog 2018-a, pp. 423-425; Richards–Hartzog 2019, p. 1462; Becker 2019, pp. 308-309; Solove–Hartzog 2024, pp. 1023-1025; Elvy 2024, p. 644.

36. Già nel 1973 lo U.S. Department of Health, Education, and Welfare decise di trasfondere la logica dell'*individual control model* in un report poi rivelatosi assai influente, secondo il quale gli individui avrebbero dovuto avere "a right to participate in deciding what the content of the record will be, and what disclosure and use

massima espressione nella normativa in materia di privacy più celebre a livello internazionale, ovverosia nel GDPR entrato in vigore il 25 maggio 2018 nel contesto eurounitario[37].

Coerentemente con il dichiarato intento di assicurare un maggior controllo all'individuo sui dati che lo riguardano (Considerando 7 GDPR)[38], il Regolamento 2016/679 riconosce un'ingente numero di diritti al singolo soggetto, garantendogli la possibilità non solo di cederli, ma anche di accedervi (art. 15, parr. 1 e 3, GDPR), rettificarli/integrarli (art. 16 GDPR), richiederne la cancellazione (art. 17 GDPR) ovvero il trasferimento (art. 20 GDPR).

Non solo. La massima espressione dell'adesione del *General Data Protection Regulation* a un'ottica ispirata all'*Individual Control Model* è data dal notevole affidamento che esso compie nei confronti del consenso individuale quale "potente strumento di controllo e partecipazione del singolo nella gestione delle proprie informazioni"[39].

Come noto, l'assenso individualmente prestato non rappresenta la sola base giuridica in grado di legittimare il trattamento dei dati da parte di titolari e responsabili dello stesso[40]. Sono previste, infatti, altre cinque condizioni di legittimità del trattamento, le quali prescindono totalmente dal consenso individuale e devono ritenersi analoghe ad esso per valenza. Sicché, soprattutto con l'avvento del GDPR, è possibile affermare che oggi l'assenza dell'assenso individualmente prestato non preclude necessariamente la liceità del trattamento dei dati, qualora ricorra nel caso concreto una diversa base giuridica[41]. Anzi, è possibile affermare, con Andrea Maria Garofalo, che tale condizione di liceità del trattamento deve ritenersi astrattamente residuale, in quanto destinata a trovare attuazione laddove non sia possibile dare applicazione alle altre previste dal Regolamento 2016/679[42].

Tuttavia, proprio in virtù della sua natura residuale, il consenso individuale costituisce in concreto la base giuridica più di frequente impiegata nella prassi quotidiana; sicché non deve meravigliare che essa emerga complessivamente dal *General Data Protection Regulation* quale prima e principale condizione di legittimità delle pratiche volte alla raccolta, all'immagazzinamento e all'utilizzo di dati relativi alla persona[43]. Da un lato, vale sottolineare che il consenso dell'interessato è menzionato dall'art. 6, par. 1, GDPR quale prima base giuridica

will be made of the identifiable information in it": cfr. U.S. Department of Health, Education & Welfare 1973, p. 41.

37. Come sottolinea Fausto Caggia, la decisione di sostituire la previgente Direttiva Madre 95/46/CE con un Regolamento si spiega anche alla luce della volontà del legislatore europeo di unificare le normative statuali in materia di privacy, nonché le prassi commerciali e i codici di condotta concernenti attività svolte con l'ausilio del web: cfr. Caggia 2019, pp. 431-432.
38. Cfr. Maestri 2021, p. 66, e Sarra 2022-b, p. 45.
39. Meneghetti 2021, p. 276. Cfr. anche Solove–Hartzog 2024, p. 1030, e Marchesin 2024-a, pp. 33-34. In tale frangente, il GDPR si pone in continuità rispetto alla previgente Direttiva 95/46/CE: cfr. Meneghetti 2021, pp. 268-269.
40. L'art. 6, par. 1, GDPR prevede altre cinque basi di legittimità del trattamento dei dati: l'esecuzione di contratti e misure precontrattuali di cui l'interessato è parte; l'adempimento di un obbligo legale da parte del titolare del trattamento; la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica; l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri da parte del titolare del trattamento; il perseguimento di interessi legittimi dello stesso. Cfr. Bravo 2017, p. 138 ss.
41. Come nota Dianora Poletti, "la possibilità di (facile) revoca [del consenso individuale], espressamente indicata dall'art. 7, par. 3, Regolamento […], impedisce la prosecuzione del trattamento che su di esso si fondava, a meno che il titolare non faccia valere una condizione di liceità alternativa": Poletti 2019, p. 2785.
42. Cfr. Garofalo 2021, p. 121, nota 8.
43. Cfr. Seminara 2021, pp. 860-861; Meneghetti 2021, p. 267; Coniglione 2023, p. 6; Solove 2024, p. 596; Sarra 2024, p. 20. Sulla posizione di chi ritiene che il legislatore europeo, pienamente consapevole del funzionamento delle odierne economie di rete, abbia inteso, attraverso il GDPR, sminuire il ruolo centrale rivestito dal consenso individuale in materia di privacy cfr. Caggiano 2017, p. 15, e Caggia 2019, pp. 405-410.

funzionale alla legittimità del trattamento dei dati, e che esso soltanto tra le basi giuridiche riceve una definizione specifica *ex* art. 4 GDPR[44]. Dall'altro lato, come osserva acutamente Alessandro Purpura, "la manifestazione di consenso ad opera dell'interessato basterebbe ad escludere una valutazione di necessità del trattamento prevista invece in tutti gli altri casi"[45]; con ciò dimostrando la volontà del legislatore europeo di riconoscere una forza quasi insindacabile all'assenso dell'interessato. Inoltre, come ricorda Dianora Poletti, non solo "il consenso sembra rafforzarsi nella sua modalità di manifestazione, divenendo 'esplicito' e 'inequivocabile'", ma esso "riveste un ruolo decisivo nel caso (rilevante soprattutto per le applicazioni di intelligenza artificiale) del trattamento automatizzato dei dati personali (art. 22)"[46].

Benché si sia, dunque, cercato di prendere progressivamente le distanze dalla logica del trattamento dei dati basata in via esclusiva sulla nozione di consenso individuale, *in primis* prevedendo nuove e più stringenti basi giuridiche, l'assenso dell'interessato continua a ricevere notevole attenzione da parte del legislatore europeo – certamente più di quanta ne ricevano le altre condizioni di legittimità[47]. Sicché, se da un lato ciò dipende dalla diffusione spazio-temporale della prassi consensuale, dall'altro lato una simile scelta legislativa non può che finire per conservare – se non addirittura implementare – tale stato dell'arte.

La fiducia ancora riposta dal GDPR nel consenso individuale ben si evince, poi, dall'attenzione dedicata dal legislatore europeo alla sua disciplina, tanto da pervenire al punto di dedicarvi una definizione assai puntuale e articolata.

Per consenso, infatti, il Regolamento 2016/679 intende "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (art. 4, n. 11, GDPR). Benché non sia chiamato a integrare una forma specificamente predeterminata[48] – fatta eccezione, soprattutto, per le ipotesi concernenti dati sensibili, nelle quali se ne richiede la natura esplicita (art. 9, par. 2, lett. a, GDPR) –, il consenso deve integrare quattro requisiti per potersi dire valido e legittimante: a) la libertà, sinonimo di consapevolezza del consenso da parte dell'utente e di assenza di coartazione al momento della sua prestazione (Considerando 42 GDPR)[49]; b) la specificità, collegata al principio di minimizzazione dei dati, in virtù del quale il consenso deve essere "limitato, pertinente ed adeguato a quanto necessario rispetto alle finalità per le quali [i dati] sono trattati" (art. 5 GDPR)[50]; c) l'informazione, che

44. Alessandro Purpura, inoltre, evidenzia come l'attenzione riservata dal legislatore europeo alla disciplina della validità del consenso individuale sia sintomo della sua perdurante centralità nel quadro del GDPR: cfr. Purpura 2022, p. 904.
45. Purpura 2022, p. 901. Ciò deve considerarsi vero anche allorquando si tratti di derogare ai divieti al trattamento di dati personali e genetici previsto dall'art. 9, par 1, GDPR, purché il consenso individuale sia esplicito. Sulla centralità del consenso emergente dalla disciplina dell'art. 9 GDPR cfr. Tuccari 2024, p. 517.
46. Poletti 2019, p. 2785. Sulla rilevanza del consenso individuale nel trattamento automatizzato di dati personali cfr. anche Troisi 2019, p. 45.
47. Se da un lato il GDPR, ammettendo anche altre basi giuridiche, dà prova della consapevolezza del legislatore europeo che non sempre gli individui sono effettivamente capaci di tutelare i propri dati, dall'altro lato continua a riconoscere la rilevanza del consenso individuale, permettendo ai singoli soggetti di disporre delle informazioni che li riguardano: cfr. Garofalo 2021, p. 119.
48. Così risulta dalla lettura del considerando 32 e dell'art. 7 GDPR. Tale profilo rappresenta oggetto di consolidata dottrina in questo senso: cfr. Caggiano 2017, p. 10; Caggia 2019, pp. 414-416; Seminara 2021, p. 864. In questi termini, il GDPR ha innovato quanto precedentemente previsto dal Codice privacy italiano, che, prima dell'entrata in vigore del Regolamento europeo, faceva ambiguamente riferimento alla forma scritta del consenso all'art. 23, co. 3, Codice privacy (oggi abrogato).
49. Cfr. Seminara 2021, p. 865, e Meneghetti 2021, p. 274.
50. Connesso alla specificità del trattamento dei dati è il principio che ne richiede la granularità: cfr. Seminara 2021, p. 863.

deve essere fornita all'interessato dal titolare del trattamento in maniera accessibile, chiara e comprensibile non solo in merito alle finalità e al contenuto del processamento dei dati raccolti (artt. 13 e 14 GDPR) ma anche relativamente ai diritti esercitabili dall'interessato stesso (artt. 15-22 GDPR)[51]; d) l'inequivocabilità, connessa alla necessità di espressione del consenso attraverso un comportamento attivo e positivo da parte dell'interessato (considerando 32 GDPR)[52].

La disciplina generale del consenso individuale è poi rifinita da due ulteriori norme: quella che ne sancisce la natura revocabile (art. 7, par. 3, GDPR) e quella che impone al titolare del trattamento di darne prova una volta rilasciato dall'utente (art. 7, par. 1, GDPR).

Nell'ambito dell'Unione europea, le più recenti normative relative allo sviluppo delle nuove tecnologie e al trattamento dei dati ad esse correlato dedicano senz'altro meno spazio alla definizione e alla disciplina dell'assenso individualmente prestato. Tuttavia, il frequente richiamo al *General Data Protecion Regulation* in esse presente impone di considerare la logica del consenso individuale – così come emergente dal medesimo – anche in relazione alla loro applicazione[53].

Il Regolamento 2023/2854 (c.d. *Data Act*), ad esempio, subordina il trattamento dei dati relativi all'utente – soprattutto se egli è persona fisica coincidente con la figura dell'interessato, e qualora i dati siano generati dall'uso di prodotti connessi e servizi correlati – alla disciplina prevista dal GDPR (considerando 34), il quale si pone addirittura in regime di prevalenza sul predetto regolamento in caso di conflitto (art. 1, par. 5)[54]; sicché, sebbene nella presente disciplina i riferimenti all'assenso individualmente prestato siano alquanto tenui, il rinvio esplicito al Regolamento 2016/679 fa rivivere anche in tale contesto normativo le pratiche consensuali che, come si è visto, ne costituiscono un rilevante fulcro. Il Regolamento 2024/1689 (c.d. *AI Act*), invece, non solo lascia distinta e impregiudicata la regolazione del consenso individuale degli interessati al trattamento dei loro dati personali dettata nel *General Data Protecion Regulation* (considerando 141), ma ad essa assomma un'ulteriore ipotesi di assenso, quello informato, da intendersi quale "espressione libera, specifica,

51. In merito alla forma dell'informazione fornita all'interessato, l'art. 12, par. 1, GDPR precisa: "il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato".

52. Così era già stato specificato da Article 29 Data Protection Working Party 2010, p. 13. Anche la Corte di Giustizia dell'Unione europea si è pronunciata sul punto, correlando l'inequivocabilità del consenso alla sua prestazione attraverso un comportamento (materiale o verbale) positivo, attivo e deliberato dall'utente: cfr. Corte di giustizia dell'Unione europea, 1 ottobre 2019, C-673/17, *Planet49*, e Corte di giustizia dell'Unione europea, 11 novembre 2020, C-61/19, *Orange România SA* c. *Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP)*. Cfr. anche Caggiano 2017, p. 9.

53. Si ricorda, preliminarmente, che l'art. 8, par. 2, della Carta di Nizza, pur aprendo alla forza legittimante di altre e differenti basi giuridiche, dispone in via generale che il trattamento dei dati di carattere personale debba svolgersi non solo secondo i principi di lealtà e finalità determinata, ma anche nel rispetto del "consenso della persona interessata", unica condizione di legittimità espressamente menzionata dalla Carta dei Diritti Fondamentali dell'Unione europea.

54. Nel Regolamento (UE) 2023/2854, il riferimento al consenso diventa esplicito nella parte centrale del considerando 34, parte nella quale si afferma che "se l'utente non è l'interessato ma un'impresa, ivi incluso un imprenditore individuale, ma non nei casi di uso domestico condiviso del prodotto connesso, l'utente è considerato un titolare del trattamento. Di conseguenza tale utente che, in qualità di titolare del trattamento, intenda richiedere dati personali generati dall'uso di un prodotto connesso o di un servizio correlato, deve disporre di una base giuridica per il trattamento dei dati come previsto dall'articolo 6, paragrafo 1, del Regolamento (UE) 2016/679, come il consenso dell'interessato o l'esecuzione di un contratto di cui l'interessato è parte".

inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare" (art. 3, par. 1, n. 59).

L'adesione all'approccio teorico che va sotto il nome di *Individual Control Model*, peraltro, non è propria soltanto del legislatore europeo. Come osservano Daniel J. Solove e Woodrow Hartzog, infatti, "in the United States, many laws sought to implement the Individual Control Model through the notice-and-choice approach, where organizations posted notices about their privacy practices and individuals could opt out if they objected"[55].

Addirittura, dunque, in molte normative sulla privacy elaborate ed emanate da legislatori di oltreoceano non si richiede nemmeno che il consenso dell'individuo sia espresso attraverso un comportamento attivo (*opt-in*). Esso si desume sovente per *facta concludentia*, ovverosia sulla base delle condotte materialmente tenute dall'utente durante la navigazione sul web, pur potendo sempre essere revocato da quest'ultimo istantaneamente o in un momento successivo (*opt-out*)[56].

In generale, pertanto, traspare un'evidente adesione da parte dei legislatori europei e statunitensi a un modello di contrasto alla *dataveillance* e ai suoi effetti più nocivi fondato sulla libera scelta di ciascuna persona. Elargendo in gran quantità facoltà e diritti al singolo soggetto, si cerca di porre costui nella posizione ottimale per poter controllare e gestire i propri dati. Attraverso la libertà e l'informazione che dovrebbero dare fondamento a ciascun consenso rilasciato da ogni individuo, quest'ultimo dovrebbe vedere rinforzata la propria posizione nei confronti di istituzioni pubbliche e imprese private, e dovrebbe riuscire a fuoriuscire dallo stato di minorato potere a cui lo relega l'asimmetria informativa rispetto ad esse.

Tuttavia, come si evidenzierà nel paragrafo successivo, tale approccio non pare da solo sufficiente a fronteggiare i pericoli insiti in forme di monitoraggio capaci di arrecare danno non solo al soggetto ma anche alla società in cui esso vive ed opera quotidianamente.

4. Consenso senza senso

Il quadro normativo che ritrae il consenso quale prima forma di contrasto al controllo oggi reso possibile dai dispositivi tecnologici appare assai suggestivo. Esso tenta di bilanciare la perdita di potere e conoscenza generata dalla vigilanza contemporanea in capo all'individuo tramite il riconoscimento di strumenti tecnico-giuridici in grado di riaffermarne la capacità di libera autodeterminazione. Tuttavia, gli accesi e scintillanti colori di tale disegno legislativo non devono distogliere l'attenzione del critico dai limiti tecnici da cui esso è intrinsecamente affetto.

Nelle pratiche quotidiane, infatti, è estremamente raro rinvenire consensi rilasciati in adesione al *gold standard* fissato dal GDPR e dalle normative ad esso affini o ispirate.

La necessità di fondare il trattamento dei dati personali su un consenso pienamente informato e consapevole si scontra sovente con delle informative privacy assai prolisse, difficilmente intellegibili per linguaggio e riferimenti, nonché contraddistinte da un elevato grado di vaghezza[57]. Il tempo necessario alla lettura materiale delle *privacy*

55. Solove–Hartzog 2024, pp. 1025-1026. Un esempio è rappresentato dal *California Consumer Privacy Act* (CCPA), una delle prime normative complete in materia di privacy emanata negli Stati Uniti, entrata in vigore il 1° gennaio 2020 e successivamente modificata ed estesa nel 2023 dal *California Privacy Rights Act* (CPRA). In parte ispirato al GDPR, il CCPA guarda ancora con attenzione prevalente all'individuo e tende a fare affidamento perlopiù sulle sue decisioni personali quanto a tutela della riservatezza: cfr. Cal. Civ. Code § 1798.120(a).

56. Daniel J. Solove riassume efficacemente la dinamica: "organizations create a privacy notice (also called a 'privacy policy' or 'privacy statement') to inform people about the collection and processing of personal data. Individuals are given a 'choice' to opt out of certain uses and disclosures, such as sharing or selling personal data to third parties. At its most basic, the choice is take-it-or-leave-it—either do business with an organization or do not. In other instances, organizations present ways to opt out of certain data uses; if people fail to opt out, then they are deemed to consent": Solove 2024, pp. 599-600.

57. Cfr. Orefice 2018, p. 105; Custers–Dechesne–Pieters et al. 2019, p. 249; Maestri 2021, p. 69; Di Corinto 2022, p. 33; Coniglione 2023, p. 6.

policy[58] e la mancanza di conoscenze tecnico-giuridiche di base per poterle comprendere[59] – e, conseguentemente, per riuscire a prendere sulla base di esse decisioni realmente ragionate – rappresentano due ostacoli per ora ancora ampiamente insormontabili.

Peraltro, non deve dimenticarsi che le informative privacy concernono il trattamento di dati da parte di sistemi informatici in rapida e continua evoluzione. Sicché nessuna *privacy policy* può considerarsi definitiva e immutabile nel tempo[60]. Irrealisticamente, ciò comporta che a ogni (necessaria) modifica dell'informativa privacy da parte del titolare del trattamento dovrebbe seguire una comunicazione all'interessato, il quale, pur essendo spesso sprovvisto di entrambi, dovrebbe impiegare ulteriori tempo e competenze per riconsiderare un consenso già preventivamente prestato e decidere se confermarlo o no[61].

Benché numerosi siano stati i moniti della dottrina e i tentativi da parte delle autorità competenti volte a una sensibile mitigazione della complessità che caratterizza le *privacy policy*[62], ancor oggi la gran parte degli utenti risulta essere scarsamente incentivata alla lettura di informative privacy tutt'altro che accessibili[63]. Con il risultato che molte persone finiscono per acconsentire alla cessione e al trattamento dei propri dati personali senza (poter) avere la minima idea di quali siano i termini destinati a regolare tali operazioni nel caso concreto[64].

Anche la specificità del consenso pone problematiche di difficile risoluzione.

Affinché tale requisito possa dirsi pienamente integrato, è necessario che le richieste formulate all'utente siano granulari, ovverosia puntuali e circoscritte. Tuttavia, l'esigenza di specificità dell'assenso e delle domande che lo precedono rischia di avere quale unico esito la proliferazione di informative e richieste, così tecniche e numerose da non sortire alcun effetto se non quello di confondere ulteriormente l'utente[65].

Quanto alla libertà del consenso, essa è chiamata a fare i conti con il crescente valore pecuniario dei dati, i quali sono divenuti in breve tempo il nuovo oro nero nelle economie mondiali[66].

È noto, nell'ambito dei *surveillance studies*, che molti dei beni e servizi (perlopiù online) che

58. Cfr. Custers–Dechesne–Pieters et al. 2019, p. 253. Già nel 2008 Aleecia McDonald e Lorrie Cranor rilevavano che soltanto per leggere le informative privacy gli utenti avrebbero dovuto spendere 201 ore ogni anno (poco più di 8 giorni): cfr. McDonald–Cranor 2008. Recenti studi dimostrano che negli ultimi vent'anni la lunghezza media delle *privacy policy* è notevolmente aumentata, e con essa anche i tempi di lettura: cfr. Schwab 2018; Litman–Navarro,2019; Stokel–Walker 2022.
59. Cfr. Custers–Dechesne–Pieters et al. 2019, pp. 251 e 253; Solove 2021, p. 5; Solove 2024, pp. 618-619. Su pregiudizi ed errori che, più in generale, contraddistinguono le decisioni degli individui in materia di privacy e cessione dei dati cfr. Kesan–Hayes–Bashir 2016.
60. Cfr. Custers–Dechesne–Pieters et al. 2019, 251.
61. Tale dinamica, infatti, molto spesso non si verifica: cfr. Solove 2024, p. 609.
62. Sulla necessità, manifestata in dottrina, di un'informativa privacy dettagliata e completa, ma al contempo accessibile e comprensibile cfr., ad esempio, Hintze 2017; Orefice 2018, *passim*; Custers–Dechesne–Pieters et al. 2019, pp. 248-249. Tale esigenza è stata ribadita dalla giurisprudenza della Corte di Giustizia dell'Unione europea nelle sentenze: Corte di giustizia dell'Unione europea, 1 ottobre 2019, C-673/17, *Planet49*, e Corte di giustizia dell'Unione europea, 11 novembre 2020, C-61/19, *Orange România SA* c. *Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP)*. A livello normativo, l'invito a formulare informative privacy concise, comprensibili e basate su un linguaggio chiaro e semplice si rinviene, ad esempio, in: considerando 58 GDPR, e Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-574(C).
63. Cfr. Becker 2019, p. 310, Solove –Hartzog 2024, p. 1026; Solove 2024, p. 597.
64. Cfr. Solove 2024, p. 614.
65. Cfr. Solove 2024, pp. 622-623. In generale, sulla natura controproducente della prassi di fornire all'utente una quantità eccessiva di informazioni (*information overload*) cfr. Bawden–Robinson 2020.
66. Sul valore economico dei dati cfr. Orefice 2018, p. 176; Bazzoni 2019, p. 642; Lyon 2020, p. 82 ss.; Paolucci 2021, p. 207; Di Corinto 2022, p. 31.

vengono presentati come gratuiti lo sono soltanto in termini strettamente monetari. In verità, essi vengono pagati dagli utenti con una moneta molto più duttile e potenzialmente fruttuosa, ovverosia la cessione di informazioni[67].

Se tale realtà risulta essere ampiamente riconosciuta negli ambienti specialistici, non pare che al riguardo vi sia altrettanta consapevolezza in coloro che, come la maggior parte dei soggetti che conducono la loro vita nelle società contemporanee, fanno un uso quotidiano di Internet e dei dispositivi ad esso connessi. La mancanza di consapevolezza circa il valore economico dei dati personali e il loro utilizzo come merce di scambio da parte di entità pubbliche e private rende gli individui disposti a cedere a cuor leggero un'ingente quantità di informazioni, anche di molto maggiore rispetto a quella strettamente necessaria, pur di ottenere in cambio un bene o un servizio per il quale non è richiesto alcun esborso di denaro[68].

La prestazione del consenso alla cessione dei dati, dunque, non può considerarsi mai del tutto libera in quanto rappresenta frequentemente la condizione necessaria e sufficiente per poter fruire di un vantaggio che altrimenti non si potrebbe ricevere o per il quale sarebbe altresì necessario il pagamento di una somma di denaro[69].

L'assenso concretamente prestato dall'individuo risulta essere il più delle volte soltanto una "fiction", una copia sbiadita e infedele di un modello normativo di consenso tanto ideale quanto astratto, in quanto "the conditions for meaningful consent mainly exist [only] in a fairy tale"[70].

Più in generale, attraverso le loro pratiche quotidiane i soggetti dimostrano di non avere piena coscienza delle conseguenze derivanti a livello individuale e collettivo dalla cessione di ingenti quantitativi di informazioni a terzi[71].

In parte ciò è dovuto alla capacità dei programmatori di sfruttare a proprio favore il grado di irrazionalità insito in ogni decisione umana: la richiesta di consenso viene formulata all'utente secondo tempi e modalità e sulla base di *design* che lo incentivano a rispondere affermativamente (*nudge*)[72], nonché in contesti che lo inducono a sottovalutare la portata delle scelte che sta compiendo (*gamification*)[73]. D'altro canto, è chiaro che i benefici derivanti dalla prestazione del consenso risultano essere, agli occhi dell'utente, ben più tangibili e immediati dei pericoli connessi alla cessione dei dati, i quali si palesano soltanto come un'ombra remota e indeterminata[74].

Dunque, benché in generale le persone affermino di avere un'alta considerazione della riservatezza e di avere a cuore la sua tutela, in concreto esse non paiono particolarmente preoccupate dei rischi annessi alla cessione di dati personali a entità pubbliche e private. Nondimeno, esse non esitano a riporre informazioni personali nelle mani di terzi, anche a fronte di vantaggi estremamente esigui, e

67. Sulla presunta gratuità di beni e servizi che, in realtà, vengono "pagati" dall'utente attraverso la cessione dei suoi dati personali cfr. Delmastro–Nicita 2019, pp. 24-25; Fioriglio 2021, p. 89; Battelli 2022, p. 355; Di Corinto 2022, p. 33; Ferraris–Saracco 2023, pp. 57-58; Pietrangelo 2023, p. 939; Capilli 2024, p. 3.

68. Cfr. Greenfield 2017, p. 28; Delmastro–Nicita 2019, p. 43; Perri 2020, pp. 13-14; Di Corinto 2022, *passim*, Coniglione 2023, p. 2.

69. Cfr. Orefice 2018, pp. 110-113; Custers–Dechesne–Pieters et al. 2019, p. 253; Solove 2021, p. 36; Solove 2024, p. 607.

70. Solove 2024, p. 596. Cfr. anche Pin 2021, p. 48.

71. Cfr. Sarra 2024, p. 11.

72. Cfr. Hartzog 2018-a, pp. 427-428; Hartzog 2018-b, pp. 21-23; Mathur–Acar–Friedman et al. 2019; Waldman 2020, p. 105; Solove 2021, p. 21.

73. Sul modo, appunto, giocoso con cui la dimensione digitale viene presentata e accolta anche in riferimento alla privacy cfr. Greenfield 2017, p. 34; Delmastro–Nicita 2019, p. 105; Maestri 2021, p. 62; Han 2022, p. 16; Han 2023, p. 20.

74. Sulla difficoltà degli individui di considerare correttamente i possibili rischi derivanti dalle decisioni assunte in un contesto complesso e sulla tendenza a cogliere perlopiù i vantaggi immediati anziché i costi di lungo termine cfr., quale studio autorevole, Acquisti–Grossklags 2004, pp. 172–173. Cfr. anche Solove 2021, pp. 19 e 43-44, e Solove 2024, p. 620.

non sono disposte a investire denaro per salvaguardare la propria riservatezza[75]. Tale fenomeno risulta essere talmente diffuso e scientificamente comprovato da aver assunto, a partire dal 2007, la denominazione di *privacy paradox*[76]. Non v'è dunque da meravigliarsi se "surveillance isn't just hoisted upon people; many people eagerly sign up for it […] embrace and normalize the fruits of the digital age, no matter how poisonous they might be [and] will often make choices that are not in their own best interest"[77].

Il progresso tecnologico, a sua volta, non ha favorito la salubrità della pratica del consenso.

In un mondo dove la Rete è diventata il principale mezzo per svolgere attività individuali e collettive, l'individuo viene insistentemente sommerso da richieste di assenso, le quali, pertanto, vengono percepite più come un noioso impiccio del quale sbarazzarsi al più presto anziché come un utile strumento con il quale potersi difendere da indebite invasioni della propria sfera privata (*consent fatigue*)[78]. Senza dimenticare il fatto che con l'avvento dell'*Internet of Things* ogni persona si ritrova quotidianamente circondata da dispositivi che raccolgono dati senza che ciò avvenga necessariamente sulla base di un preventivo consenso[79].

Per quanto vaste siano, poi, le possibilità di scelta messe a disposizione dell'utente circa la cessione dei propri dati, esse saranno sempre limitate e predeterminate da parte dei programmatori, sicché non sarà mai possibile una reale personalizzazione della quantità di dati trasmessi e delle modalità della loro cessione[80].

In definitiva, il consenso non pare poter rappresentare uno strumento da solo capace di permettere all'individuo di fronteggiare le molteplici insidie lanciate dalle odierne forme di monitoraggio. I rilevanti pericoli per i soggetti e per la società passibili di essere creati dalla sorveglianza contemporanea difficilmente possono essere fronteggiati attraverso un assenso sbrigativamente prestato da una persona condizionata nelle sue decisioni e incapace di avere piena contezza delle conseguenze delle sue scelte.

Applicato nei termini anzidetti, il consenso rischia di essere non tanto uno scudo a difesa degli individui e delle comunità che essi compongono, bensì una spada con la quale entità pubbliche e private possono più agevolmente penetrare laddove si annidano i dati di cui necessitano per trarre profitto.

5. Agire, ma in quale direzione?

I rischi individuali e collettivi connessi alla sorveglianza in generale e alle odierne forme di monitoraggio in particolar modo non possono essere negati, né tantomeno possono essere svalutati o dimenticati.

I pericoli derivanti dalla trasparenza totale dei soggetti e dalla loro reclusione all'interno di *echo*

75. Cfr. Barth–De Jong–Junger et al. 2019. Cfr. anche Solove 2021, p. 21.
76. Cfr. Norberg–Horne–Horne 2007. Benché sia assodato in letteratura il fatto che sovente gli individui non siano coscienti dei rischi a cui la collettività e loro stessi si espongono attraverso la cessione dei dati, e che, in ogni caso, tali pericoli siano oggetto di una generale sottovalutazione, vale la pena ricordare che il concetto di *privacy paradox* non è del tutto pacifico in dottrina. Daniel J. Solove osserva al riguardo: "because behaviour and attitudes regarding privacy are about different things, the fact that they do not align is not a discrepancy. It is not even clear that they can be brought into alignment. Depending upon which side one takes, it can be tempting to view behaviour or attitudes as a more fixed reflection of people's true preferences, with the other being false or skewed. But behaviour and attitudes are highly malleable and are quite different. Behavior involves risk decisions within specific contexts; it is always context dependent. Attitudes are more general views about value and can exist beyond specific contexts. The fact that attitudes and behaviour about privacy diverge is not a paradox or even an inconsistency": Solove 2021, p. 4.
77. Solove–Hartzog 2024, p. 1032.
78. Cfr. Hartzog 2018-a, p. 429, Custers–Dechesne–Pieters et al. 2019, pp. 247 e 253; Solove 2021, p. 45; Solove 2024, p. 597. Per una panoramica del numero di richieste di consenso ricevute mediamente da un utente cfr. Olmstead–Atkinson 2015.
79. Cfr. Hartzog 2018-a, pp. 429-430. Sul funzionamento dell'IoT cfr. Greenfield 2017, p. 32 ss.
80. Cfr. Hartzog 2018-a, pp. 426-427.

chambers costituite da dati suggeriscono, al contrario, di trattare della sorveglianza attuale con ancora maggior impegno. I valori umani e sociali in gioco allorquando ci si occupa di privacy devono ritenersi talmente rilevanti e meritevoli di tutela da imporre a tutti i *surveillance scholars* di occuparsene, rimanendo aperti alla possibilità di sondare anche orizzonti finora ignorati o sottovalutati.

Oggigiorno numerose sono le persone, soprattutto di giovane età, che ritengono inutile e velleitario qualsivoglia tentativo di proteggere la propria sfera privata, di controllare le informazioni personali o di prevenire i rischi connessi alle dinamiche di controllo, stante l'ubiquità e la potenza tecnologica dei dispositivi attraverso i quali avviene il trattamento dei dati[81]. Tuttavia, dinanzi a uno scenario tutt'altro che incoraggiante, abbandonarsi all'inevitabilismo appare una soluzione tutt'altro che auspicabile[82]. L'attuale incapacità dell'individuo di fronteggiare i rischi collegati alla sorveglianza tramite i mezzi oggigiorno messigli a disposizione dal legislatore deve essere un incentivo a immaginare strumenti migliori e più efficaci, non una comoda giustificazione per rassegnarsi e disinteressarsi della questione.

D'altro canto, deve ritenersi altrettanto irragionevole l'ipotesi di un atteggiamento totalmente avverso alle odierne forme di vigilanza. Per quanto inquietanti possano essere alcune delle sue derive, infatti, la sorveglianza presenta anche profili positivi meritevoli, per ciò stesso, di essere conservati e valorizzati[83].

In questi termini appare condivisibile la posizione assunta da Daniel J. Solove, secondo il quale "privacy will not always win out"[84]. Le prospettive che parlano delle forme di monitoraggio presentandole perlopiù come un "nemico"[85] o un "avversario"[86] da annientare *in toto* danno prova del loro carattere deficitario, incurante cioè della necessità di preservare talvolta anche la sorveglianza stessa, sebbene ciò implichi una qualche compressione della riservatezza. In altri termini, una teorizzazione finalizzata all'integrale tutela della privacy attraverso la completa eliminazione di qualsivoglia dinamica di controllo rischia di provocare più pregiudizi di quelli che essa intenderebbe rimuovere.

Qualunque sia la possibile soluzione al problema, dunque, essa non potrà che implicare un bilanciamento tra i molteplici valori e interessi in gioco. Quale direzione intraprendere, però, per raggiungere tale equilibrio?

Fare affidamento perlopiù sulla responsabilità dei *big players* e dei loro programmatori appare una prospettiva utile ma tutt'altro che risolutiva.

Innanzitutto, anche ammessa la buona fede delle *big tech*, non sembra logico e realistico credere che la tutela della privacy degli utenti possa essere garantita *in toto* proprio da coloro che più di tutti hanno interesse (economico) allo svelamento della sfera privata degli individui. Successivamente, è necessario evidenziare che i sistemi di *privacy by design* e *privacy by default* elaborati dai programmatori dei *big players* medesimi (anonimizzazione e crittografia su tutti) non possono dirsi del tutto affidabili nella protezione della riservatezza[87].

81. Cfr. Hargittai–Marwick 2016; Hoffmann–Lutz–Ranzini 2016; Solove 2021, pp. 45-46; Maestri 2021, p. 58.
82. Sulla tendenza a considerare la computazione ubiqua e la sorveglianza come fenomeni inarrestabili, passibili soltanto di essere accettati cfr. Zuboff 2019, p. 236.
83. Se, infatti, è innegabile che la *surveillance* rivesta oggi un ruolo di rilievo nella deterrenza e, soprattutto, nella repressione della criminalità, non va dimenticato che è la *dataveillance* a rendere possibili molte delle amenità di cui attualmente è possibile godere, nonché a permettere il buon funzionamento di dispositivi oggi ritenuti essenziali in molteplici contesti.
84. Solove 2021, p. 38.
85. Zuboff 2019, pp. 295-296.
86. Brunton–Nissenbaum 2016, p. 20.
87. Da un lato, la pratica dell'anonimizzazione delle informazioni è resa inefficace dall'alto numero di dati e metadati che ciascun individuo rilascia nel corso della sua routine quotidiana: cfr. Custers–Dechesne–Pieters et al. 2019, p. 255. Anche la crittografia non garantisce una sicurezza assoluta in quanto è possibile, sebbene talvolta con una certa complessità, ricostruire algoritmicamente il testo in chiaro a partire da quello cifrato: cfr. Perri

Del pari, però, non sembra opportuno proseguire esclusivamente sulla via tracciata negli ultimi decenni dai principali legislatori del mondo. E ciò non solo in virtù della natura sfuggente del consenso[88] e delle molteplici problematiche irrisolte messe in luce nel paragrafo precedente.

Come evidenziano Daniel J. Solove e Woodrow Hartzog, insistere su un approccio normativo fondato in via esclusiva sull'*Individual Control Model* appare non solo inutile ma addirittura controproducente[89].

Da un lato, infatti, riconoscere all'individuo facoltà e diritti estremamente rilevanti sulla carta, ma difficilmente esercitabili e scarsamente influenti in concreto, alimenta nei soggetti un senso di controllo sui propri dati che tuttavia è soltanto illusorio[90]. Accreditare ulteriori libertà formali incapaci, però, di garantire una tutela effettiva della privacy altro non permetterebbe se non di far abbassare la guardia alle persone, agevolando così le attività di trattamento dei dati da parte di chi ve ne ha interesse[91].

Dall'altro lato, continuare a fare affidamento prevalentemente su un assenso dato troppo spesso con eccessiva facilità rischia di far ricadere la responsabilità circa gli effetti negativi della sorveglianza sugli utenti stessi. Se, infatti, la normativa vigente ritiene sufficiente il consenso per poter considerare legittimi i trattamenti dei dati, allora a titolari e responsabili degli stessi basterà riuscire ad ottenere formalmente quest'ultimo, indipendentemente dal fatto che esso sia frutto di un ragionamento consapevole o della pura e semplice volontà di sbarazzarsi quanto prima di un "fastidioso" *banner*. Sicché, qualora successivamente emergano delle conseguenze nocive a partire dalla cessione di dati, la responsabilità dovrà riconoscersi non tanto su quanti li hanno trattati a norma di legge, quanto piuttosto in capo a coloro che hanno legittimato il trattamento attraverso il loro assenso[92].

In generale, e alla luce dei più autorevoli studi comportamentali in ambito psicologico e antropologico succedutisi negli ultimi cinquant'anni, sembra quantomeno inopportuno proseguire in una direzione volta prevalentemente all'eccessiva esaltazione del ruolo dell'individuo e delle sue decisioni personali.

Nella seconda metà del secolo scorso, Daniel Kahneman e Amos Tversky sconfessarono l'allora tradizionale e consolidato filone di pensiero che raffigurava l'essere umano come un *homo oeconomicus* perfettamente razionale nelle sue scelte, soprattutto in ambito economico: essi, infatti, dimostrarono che è assai frequente che, nelle pratiche negoziali e di scambio in particolare, i soggetti cadano vittime di molteplici errori provocati perlopiù da euristiche e distorsioni cognitive[93].

2020, p. 108. Per titolari e responsabili del trattamento anche l'obbligo di provvedere alla cancellazione dei dati personali di un utente dietro richiesta esplicita di quest'ultimo potrebbe non essere sempre agevole o potrebbe essere addirittura inefficace, posto che il carattere aperto dell'architettura di Internet mina ampiamente la capacità di controllare i flussi di dati: cfr. Custers–Dechesne–Pieters et al. 2019, p. 252. In generale, poi, va evidenziato che il funzionamento degli algoritmi risulta essere così opaco da non (poter) essere del tutto chiaro nemmeno per le imprese che se ne servono: cfr. Maestri 2021, p. 61; Varoufakis 2023, p. 117; Pietropaoli 2024, *passim*.

88. Sulla difficoltà di stabilire in concreto quando il consenso prestato da un utente possa dirsi realmente rispettoso del *gold standard* preteso dalla maggior parte dei legislatori mondiali cfr. Custers–Dechesne–Pieters et al. 2019, p. 250.

89. Cfr. Solove–Hartzog 2024, pp. 1023-1024 e Solove 2024, p. 596.

90. Cfr. Hartzog 2018-a, pp. 425-426; Solove 2021, pp. 5-6; Solove–Hartzog 2024, pp. 1031-1032 e 1036.

91. Come evidenzia Woodrow Hartzog, "the problem with respecting everyone's personal commitments is that for-profit tech companies have their own agendas. They want users to be maximally forthcoming to monetise all this information. Hence, it is to their advantage to make users believe they have more control than they are actually given": Hartzog 2018-a, p. 426. Tra gli studi più autorevoli in materia cfr. Brandimarte–Acquisti–Loewenstein 2013.

92. Cfr. Solove–Hartzog 2024, p. 1036.

93. Cfr. Kahneman–Tversky 1979. Ben più di recente, Richard H. Thaler e Cass R. Sunstein, nell'ambito dei loro studi congiunti in tema di *nudge*, hanno ripreso e approfondito ulteriormente le rivoluzionarie teorie dei due

Se, dunque, le persone si rendono quotidianamente protagoniste di scelte che, per quanto banali possano essere, si rivelano sovente irrazionali e, talvolta, addirittura nocive per se stesse, è alquanto insensato credere che una simile inclinazione naturale possa trovare redenzione in un contesto estremamente articolato quale quello della *privacy online*. Prendere una decisione razionale e per sé vantaggiosa non è agevole, nemmeno in ambiti di cui gli esseri umani hanno da sempre esperienza materiale; *a fortiori* tale operazione è destinata a essere ben più ardua in un contesto molto meno concreto, ben più ambiguo e assai meno conosciuto come quello della riservatezza, peraltro nell'articolata dimensione digitale e interconnessa[94].

Con ciò non si desidera affatto affermare la necessità di sottrarre agli individui la loro libertà di scelta, né privarli *in toto* della loro facoltà di esprimere opinioni e assensi. Al contrario.

Come osserva opportunamente Stacy-Ann Elvy, "if consent is used to justify data practices, consent should be meaningfully and validly obtained […]"[95]. Tuttavia, come anzidetto, le prassi individuali e le ricerche scientifiche invalse negli ultimi decenni dimostrano inconfutabilmente che il consenso perfettamente aderente al *gold standard* legislativo rappresenta più una lontana chimera che una realtà concreta, sicché può dirsi pervenuto il momento di abbandonare almeno in parte la logica dell'assenso, proprio in quanto incapace, da sola, di assicurare effettività alle decisioni individuali e garantire una tutela piena della privacy. È necessario, cioè, prendere atto della natura *murky* del consenso individuale[96] allo scopo di pianificare soluzioni che consentano di sopperire al suo carattere deficitario.

L'obiettivo, pertanto, è quello di proporre modelli che permettano di istaurare contesti giuridico-sociali ove le scelte dei soggetti possano essere davvero consapevoli e, dunque, realmente incidenti sul trattamento dei dati, senza per ciò stesso dover rinunciare ai vantaggi garantiti dalla sorveglianza.

6. Una prospettiva per il futuro: il *Societal Structure Model*

Nelle sue condizioni attuali, l'individuo non può dirsi in grado di fronteggiare, da solo, le molteplici dinamiche che attentano quotidianamente alla sua sfera privata[97].

Poiché, tuttavia, le misure predisposte finora dai principali legislatori mondiali non hanno sortito appieno gli effetti di *empowerment* che ci si attendeva da esse, sembra opportuno iniziare a porre lo sguardo su soluzioni ancor oggi scarsamente battute a livello normativo, ancorché da tempo caldeggiate, nell'ambito dei *surveillance studies*, da una rilevante componente della dottrina.

Ciò che appare innanzitutto fondamentale è l'istruzione[98].

Il mondo digitale in cui siamo chiamati a vivere e operare quotidianamente offre una quantità di vantaggi e opportunità senza precedenti. Tuttavia, esso risulta essere foriero di rischi altrettanto

psicologi israeliani, affermando che "le previsioni degli esseri umani sono imprecise e distorte" e che "anche il loro processo decisionale presenta numerosi difetti": cfr. Thaler–Sunstein 2014, p. 14. Per un'analisi recente dei principali *bias* incidenti sulle decisioni delle persone in ambito negoziale cfr. Antonazzi 2020.

94. Senza, peraltro, dimenticare che le scelte compiute in materia di privacy da un singolo soggetto possono produrre i propri effetti pratici anche nei confronti di altri individui, assumendo così una dimensione inevitabilmente collettiva. Come Custers e colleghi notano, "the use of Big Data increasingly enables the prediction of characteristics of people who withheld consent on the basis of the information available from people who did consent. When large numbers of people consent to the use of their personal data, it is possible to predict missing values of other people": Custers–Dechesne–Pieters et al. 2019, p. 252.

95. Elvy 2024, p. 644.

96. Sul concetto di *murky consent* cfr. Solove 2024.

97. Sulla vulnerabilità dell'individuo e sulla sua incapacità attuale di reagire da solo alle sfide della sorveglianza contemporanea cfr. Seminara 2018, p. 134, e Zuboff 2019, p. 238.

98. Sull'importanza dell'educazione dell'utente con particolare riferimento alla privacy cfr. Weinberger–Bouhnik–Zhitomirsky-Geffet 2017; Custers–Dechesne–Pieters et al. 2019, p. 255; Pietropaoli 2024, p. 7; Marchesin 2024-a, p. 57.

numerosi e ingenti, ancor più alti proprio perché provenienti da una dimensione intangibile, ubiquitaria e nella quale operano milioni di individui e algoritmi provenienti da ogni parte del globo. Educare al buon utilizzo dei dispositivi tecnologici di uso quotidiano e alla tutela dai pericoli individuali e collettivi che essi necessariamente implicano dovrebbe, pertanto, rappresentare un punto nodale delle politiche di istruzione, un obiettivo minimo che le istituzioni pubbliche potrebbero perseguire anche con la collaborazione di *big tech* e imprese private[99].

Proprio in virtù dei rischi enucleati nei paragrafi precedenti, educare alla tecnologia e alla dimensione digitale dovrebbe implicare anche l'erogazione di un'istruzione di base in tema di privacy.

Nel contesto attuale, dominato dalle richieste di assenso e dal valore legittimante di quest'ultimo, non è pensabile che il soggetto possa approcciare una privacy policy o assumere una decisione cosciente in merito alla cessione di informazioni personali senza avere nel proprio bagaglio culturale delle nozioni elementari concernenti la sorveglianza online, la protezione della riservatezza e il trattamento dei dati. Anche a seguito di un (auspicabile) mutamento di paradigma, tale istruzione si renderebbe comunque fondamentale: essa, infatti, andrebbe in ogni caso a sorreggere un consenso dal quale non è possibile né opportuno prescindere del tutto, e fungerebbe da sostegno per una partecipazione alla difesa della privacy da parte delle persone che si rende pur sempre essenziale.

L'educazione in materia di riservatezza appare tanto più necessaria quanto maggiori sono i valori privati e pubblici che ad essa si accompagnano[100]. In altri termini, fornire un'istruzione basilare relativamente alla privacy non significa soltanto insegnare a leggere correttamente un'informativa privacy o a utilizzare i comandi delle impostazioni delle *app* in maniera adeguata: significa porre le basi per incoraggiare una cittadinanza attiva, consapevole, libera di autodeterminarsi e propensa al dialogo e alla pacifica convivenza.

Per quanto possa essere utile, l'educazione ai media digitali e alla riservatezza che essi chiamano inevitabilmente in gioco non può considerarsi tuttavia sufficiente[101]. Affinché si verifichi un apprezzabile miglioramento nella salvaguardia della privacy e nel suo bilanciamento con altri valori ritenuti imprescindibili, si rende necessario un (quantomeno parziale) mutamento di paradigma.

Come evidenziato da numerosi *surveillance scholars*, la riservatezza costituisce un valore indispensabile non solo per l'individuo ma anche per la società intera, soprattutto se ispirata a principi democratici. Sicché è astrattamente illogico – oltre che concretamente inefficacie, come dimostrato ampiamente dalla prassi diffusa – pensare che la tutela di un diritto sia individuale che collettivo possa passare esclusivamente per le mani di soggetti singolarmente considerati[102]. Se la sorveglianza

99. In generale, il rapporto DESI (*Digital Economy and Society Index*) del 2022 testimonia che, in Italia, soltanto il 46% della popolazione possiede competenze digitali di base, denotando, così, un deficit conoscitivo anche in merito alle principali problematiche connesse alla dimensione tecnologica, privacy inclusa. Come sottolinea Giovanni Ziccardi, riservatezza e *data protection*, unitamente all'intelligenza artificiale, "non sono solo ambiti di studio prettamente tecnici, ma sono strettamente connessi alla cultura, all'essere umano, alla società in cui vive e ai grandi valori giuridici, sociali ed etici del nostro tempo", sicché il loro studio andrebbe incentivato nelle scuole di ogni ordine e grado. Lo stesso legislatore europeo sembra aver compreso la necessità di garantire una maggiore alfabetizzazione digitale, come dimostrato dall'art. 4 del Regolamento sull'Intelligenza Artificiale (Regolamento 2024/1689) entrato in vigore il 1° agosto 2024.

100. Come evidenzia Daniel J. Solove, numerosi sono i valori connessi al concetto di privacy: dalla libertà di pensiero ed espressione alla partecipazione politica, dalla facoltà di autodeterminare il proprio orientamento sessuale al diritto di aderire a un credo religioso. Cfr. Solove 2021, pp. 39-41.

101. Sebbene dipinga un quadro forse sin troppo negativo al riguardo, Daniel J. Solove sottolinea tutti i limiti di un'eventuale educazione degli utenti in materia di privacy, dall'eccessiva complessità della materia all'incapacità delle persone di tradurre in pratica quanto acquisito in linea teorica: cfr. Solove 2024, pp. 617-621.

102. Sulla privacy come valore sociale e non solo come interesse individuale cfr. Orefice 2018, p. 81; Hartzog 2018-a, pp. 430-431; Tufekci 2018; Solove 2021, pp. 5 e 34; Gandy Jr. 2021; Meneghetti 2021, p. 277; Solove–Hartzog 2024, p. 1026; Solove 2024, p. 636.

rappresenta, per taluni aspetti, una minaccia non solo per la libertà della persona ma anche per la democraticità della comunità, è necessario che la risposta alle attuali forme di monitoraggio assuma una sembianza non tanto o non solo individualistica, ma anche e soprattutto collettivistica. È auspicabile, cioè, un progressivo – anche se non definitivo – allontanamento dall'*Individual Control Model* oggi preponderante, in vista di un graduale avvicinamento a ciò che in letteratura viene definito *Societal Structure Model*[103].

Nel 2018, Max Schremes ha trasformato *None of Your Business (noyb)*, l'organizzazione *no profit* di cui è leader, in una piattaforma online avente lo scopo di "to strengthen your right to privacy". Tale obiettivo è perseguito vigilando sulla corretta applicazione delle normative in materia di sorveglianza e riservatezza da parte delle imprese private che sono tenute alla loro osservanza. Ora tramite attività di divulgazione online, ora attraverso la predisposizione di progetti e standard da sottoporre al vaglio dei legislatori europei, ora facendo in modo di "to submit data protection complaints with local authorities and file procedures in national courts", *noyb* mira a essere un punto di riferimento per gli utenti europei e non solo, nonché a garantire un controllo generale su titolari e responsabili del trattamento dei dati[104].

Benché abbia natura privatistica, *noyb* è emblema di una tipologia di piattaforme che possono rappresentare una prima fonte di ispirazione per immaginare una reazione partecipata e collettivistica alle sfide imposte dalle odierne forme di vigilanza. Essa permette di ipotizzare l'esistenza, accanto alle autorità garanti e alla figura del *Data protection officer* (DPO)[105], di un sistema istituzionalizzato che funga da raccordo tra utenti, autorità pubbliche e imprese private. Tali istituzioni intermedie non solo garantirebbero una risposta giudiziaria alle violazioni delle normative in materia di privacy da parte delle *big tech*, ma, prima ancora, assicurerebbero all'utente la possibilità di vigilare sul loro operato in merito al trattamento dei suoi dati attraverso professionisti a ciò preposti, ovvero in prima persona ogniqualvolta lo ritenesse necessario[106].

Sebbene quella delle piattaforme ed istituzioni intermedie sia, ad oggi, soltanto un'idea embrionale, essa certifica l'esigenza di un modello di tutela della riservatezza, e di contrasto agli effetti pregiudizievoli della sorveglianza, che si fondi non più sul debole consenso dell'individuo ma sulla forte partecipazione collettiva di tutti i componenti delle società interessate da tale fenomeno. In altri termini, affinché sia possibile iniziare a immaginare un monitoraggio rispettoso degli ideali democratici e delle persone che concretamente vivono nelle odierne democrazie, è necessario cominciare a ipotizzare e progettare un movimento che prenda le mosse dallo stesso *demos*.

Riferimenti bibliografici

A. Acquisti, J. Grossklags (2004), *Privacy Attitudes and Privacy Behavior. Losses, Gains, and Hyperbolic Discounting*, in "Economics of information security", vol. 12, 2004

103. Sulla necessità di un mutamento di paradigma che, accanto alla libertà di scelta degli individui, preveda la possibilità per i funzionari pubblici di selezionare preventivamente le pratiche da ritenersi sicure per le persone e coerenti con i principi giuridici vigenti cfr. Hirsch 2020.

104. Tutte le informazioni relative al funzionamento e alle attività di *noyb* sono consultabili sul sito.

105. Per Daniel J. Solove, il ruolo dei DPO dovrebbe essere comunque implementato da parte dei legislatori: cfr. Solove 2021, p. 50.

106. Tale ipotesi appare coerente con la prospettiva di stampo sindacalistico caldeggiata da Shoshana Zuboff, secondo la quale, "per quanto possa essere determinato, un individuo isolato non può sostenere il peso della giustizia, così come un singolo lavoratore all'inizio del Ventesimo secolo non poteva combattere da solo per uno stipendio equo e il miglioramento delle condizioni in fabbrica. All'epoca fu necessaria un'azione collettiva, e lo stesso vale oggi. […] Un secolo fa, i lavoratori si organizzarono collettivamente e guadagnarono potere, e allo stesso modo oggi gli utenti si devono mobilitare secondo le 'condizioni d'esistenza' del Ventunesimo secolo. […] Ci vuole un'azione collettiva per imporre finalmente leggi che stabiliscano il diritto al santuario e al futuro come condizioni essenziali per una vita degna": Zuboff 2019, pp. 500-501.

M. Antonazzi (2020), *La negoziazione cognitiva*, in C. Sarra, F. Reggio (a cura di), "Diritto, metodologia giuridica e composizione del conflitto", Primiceri Editore, 2020

Article 29 Data Protection Working Party (2010), *Parere 2/2010 sulla pubblicità comportamentale online*, WP 171, 2010

S. Barth, M.D.T. De Jong, M. Junger et al. (2019), *Putting the Privacy Paradox to the Test. Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources*, in "Telematics and Informatics", vol. 41, 2019

E. Battelli (2022), *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono "gratuiti"*, in "I Contratti", 2022, n. 3

G. Bazzoni (2019), *La libertà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei global social media*, in "Diritto di Internet", 2019, n. 4

D. Bawden, L. Robinson (2020), *Information Overload: An Overview*, in "Oxford Encyclopedia of Political Decision Making", Oxford University Press, 2020

M. Becker (2019), *Privacy in the Digital Age. Comparing and Contrasting Individual versus Social Approaches towards Privacy*, in "Ethics and Information Technology", vol. 21, 2019, n. 4

L. Brandimarte, A. Acquisti, G. Loewenstein (2013), *Misplaced Confidences: Privacy and the Control Paradox*, in "Social Psychological and Personality Science", vol. 4, 2013, n. 3

F. Bravo (2017), *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

F. Brunton, H. Nissenbaum (2016), *Offuscamento. Manuale di difesa della privacy e della protesta*, Eretica Speciale, 2016

F. Caggia (2019), *Il consenso al trattamento dei dati personali nel diritto europeo*, in "Rivista del Diritto commerciale e del Diritto generale delle obbligazioni", 2019, n. 3

I.A. Caggiano (2017), *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in "Diritto Mercato Tecnologia", 2017

G. Capilli (2024), *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in "MediaLaws", 2024, n. 1

R. Clarke (1998), *Information Technology and Dataveillance*, Communications of ACM, 1998

C. Coniglione (2023), *L'utilizzo dei big data in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa*, in "Nomos. Le attualità nel diritto", 2023, n. 1

C. Cossutta, A. Mainardi (2018), *Sorveglianza, soggettività e spazio pubblico*, in C. Cossutta, V. Greco, A. Mainardi, S. Voli (a cura di), "Smagliature digitali. Corpi, generi e tecnologie", Agenzia X, 2018

B. Custers, F. Dechesne, W. Pieters et al. (2019), *Consent and privacy*, eLaw Working Paper Series, 2018/008, 2019

D. De Kerckhove (2016), *La rete ci renderà stupidi?*, Castelvecchi, 2016

M. Delmastro, A. Nicita (2019), *Big data. Come stanno cambiando il nostro mondo*, il Mulino, 2019

A. Di Corinto (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1

C. Doctorow (2024), *Come distruggere il capitalismo della sorveglianza*, Mimesis, 2024

S.-A. Elvy (2024), *Privacy Law Consent Conundrum*, in "Boston University Law Review", vol. 104, 2024, n. 641

M. Ferraris, G. Saracco (2023), *Tecnosofia. Tecnologia e umanesimo per una scienza nuova*, Laterza, 2023

G. Fioriglio (2021), *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in "Journal of Ethics and Legal Technologies", vol. 3, 2021, n. 2

L. Floridi (2020), *Il verde e il blu*, Raffaello Cortina Editore, 2020

O.H. Gandy Jr. (2021), *The Panoptic Sort. A Political Economy Of Personal Information*, Oxford University Press, 2021

A.M. Garofalo (2021), *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in S. Orlando, G. Capaldo (a cura di), "Annuario 2021. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università Editrice, 2021

A. Greenfield (2017), *Tecnologie radicali. Il progetto della vita quotidiana*, Einaudi, 2017

B.-C. Han (2023), *Infocrazia. Le nostre vite manipolate dalla rete*, Einaudi, 2023

B.-C. Han (2022), *Le non cose. Come abbiamo smesso di vivere il reale*, Einaudi, 2022

B.-C. Han (2021), *La società senza dolore. Perché abbiamo bandito la sofferenza dalle nostre vite*, Einaudi, 2021

E. Hargittai, A. Marwick (2016), *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy*, in "International Journal of Communication", vol. 10, 2016

W. Hartzog (2018-a), *The Case Against Idealising Control*, in "European Data Protection Law Review", 2018, n. 4

W. Hartzog (2018-b), *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, 2018

M. Hintze (2017), *In Defense of the Long Privacy Statement*, in "Maryland Law Review", vol. 76, 2017

D.D. Hirsch (2020), *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, in "Maryland Law Review", vol. 79, 2020, n. 2

C.P. Hoffmann, C. Lutz, G. Ranzini (2016), *Privacy Cynicism: A new Approach to the Privacy Paradox*, in "Cyberpsychology: Journal of Psychosocial Research on Cyberspace", vol. 10, 2016, n. 4

D. Kahneman, A. Tversky (1979), *Prospect theory: An analysis of decision under risk*, in "Econometrica", vol. 47, 1979, n. 2

J.P. Kesan, C.M. Hayes, M.N. Bashir (2016), *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, in "Indiana Law Journal", vol. 91, 2016

M. Kienke (2023), *Out of the bubble! Le tecnologie digitali e la politica del futuro*, in "Prospettiva Persona · Prospettiva Civitas", 2023, n. 2

H. Koskela (2000), *'The gaze without eyes': video-surveillance and the changing nature of urban space*, in "Progress in Human Geography", vol. 24, 2000, n. 2

K. Litman-Navarro (2019), *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, in "New York Times", 2019

D. Lyon (2020), *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, 2020

E. Maestri (2021), *Surveillance And Profiling. Online Person's Privacy Between Criminogenic Structures And Legal Paternalism*, in "Journal of Ethics and Legal Technologies", vol. 3, 2021, n. 2

L. Marchesin (2024-a), *L'eredità di Bentham. La sorveglianza post-moderna al cospetto del Panopticon*, in "Journal of Ethics and Legal Technologies", vol. 6, 2024, n. 1

L. Marchesin (2024-b), *One ring to reify them all, one ring to humanize them all. When the human eyes of restorative justice meet the dehumanizing gaze of panoptic surveillance*, in "Mediares", 2024, n. 1

A. Mathur, G. Acar, M.J. Friedman et al. (2019), *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, in "Proceedings of the ACM on Human-Computer Interaction", vol. 3, 2019

A.M. McDonald, L.F. Cranor (2008), *The Cost of Reading Privacy Policies*, in "I/S: A Journal of Law and Policy for the Information Society", vol. 4, 2008, n. 3

M.C. Meneghetti (2021), *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in "MediaLaws", 2021, n. 1

P. Moro, B. Fioravanzi (2022), *Verità digitale. Dalle fake news all'alfabetismo informativo*, in "Calumet", 2022, n. 15

P.A. Norberg, D.R. Horne, D.A. Horne (2007), *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, in "Journal of Consumer Affairs", vol. 41, 2007, n. 1

K. Olmstead, M. Atkinson (2015), *Apps Permissions in the Google Play Store*, in "Pew Research Center", 2015

M. Orefice (2018), *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne editrice, 2018

F. Paolucci (2021), *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in "MediaLaws", 2021, n. 1

E. Pariser (2012), *The filter bubble. What the Internet is Hiding from You*, Penguin Book Ltd, 2012

P. Perri (2020), *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè Francis Lefebvre, 2020

M. Pietrangelo (2023), *Spazio digitale e modelli di regolazione*, in "Consulta Online", 2023, n. 3

S. Pietropaoli (2024), *Dalla sorveglianza al controllo: la parabola della governamentalità algoritmica*, in "Rivista italiana di informatica e diritto", 2024, n. 2

A. Pin (2021), *Diritti costituzionali e intelligenza artificiale*, in P. Moro (a cura di), "Etica, diritto e tecnologia, percorsi dell'informatica giuridica contemporanea", Franco Angeli, 2021

A. Pin (2022), *Nella Rete, anche se Offline. Il ruolo dello spazio pubblico nell'era digitale*, in "Mondo Digitale", vol. 98, 2022, n. 1

D. Poletti (2019), *Le condizioni di liceità del trattamento dei dati personali*, in "Giurisprudenza italiana", 2019, n. 12

A. Purpura (2022), *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*, in "Jus Civile", 2022, n. 4

N.M. Richards, W. Hartzog (2019), *The Pathologies of Digital Consent*, in "Washington University Law Review", vol. 96, 2019, n. 6

S. Rodotà (2004), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, 2004

C. Sarra (2024), *La datificazione della persona nella costruzione del Metaverso*, in "Journal of Ethics and Legal Technologies", vol. 6, 2024, n. 1

C. Sarra (2022-a), *Il mondo-dato. Saggio su datificazione e diritto*, CLEUP, 2022

C. Sarra (2022-b), *L'uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello*, in "Journal of Ethics and Legal Technologies", vol. 4, 2022, n. 2

P.N. Schwab (2018), *Reading Privacy Policies of the 20 Most-Used Mobile Apps Takes 6h40*, in "IntoTheMinds", 28 May 2018

G. Scorza (2022), *In principio era Internet e lo immaginavamo diverso*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A.P. Seminara (2021), *Cookie e libertà del consenso al trattamento dei dati personali*, in "Persona e Mercato", 2021, n. 4

D.J. Solove (2024), *Murky consent: an approach to the fictions of consent in privacy law*, in "Boston University Law Review", vol. 104, 2024

D.J. Solove (2021), *The Myth of Privacy Paradox*, in "The George Washington Law Review", vol. 89, 2021, n. 1

D.J. Solove, W. Hartzog (2024), *Kafka in the Age of AI and the futility of Privacy as Control*, in "Boston University Law Review", vol. 104, 2024

B. Stiegler (2023), *La colpa di Epimeteo*, vol. 1, Luiss University Press, 2023

C. Stokel-Walker (2022), *Privacy policies are four times as long as they were 25 years ago*, in "NewScientist", 3 February 2022

C.R. Sunstein (2017), *#republic. La democrazia nell'epoca dei social media*, il Mulino, 2017

L.Fr.H. Svendsen (2017), *Filosofia della paura. Come, quando e perché la sicurezza è diventata nemica della libertà*, Castelvecchi, 2017

R.H. Thaler, C.R. Sunstein (2014), *Nudge. La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Feltrinelli, 2014

E. Troisi (2019), *AI e GDPR: l'Automated Decision Making, la protezione dei dati, e il diritto alla 'intelligibilità' dell'algoritmo*, in "European Journal of Privacy Law & Technologies", 2019, n. 1

E. Tuccari (2024), *Neuromarketing: un'asistematica disciplina… oltre il consenso?*, in "Persona e Mercato", 2024, n. 2

Z. Tufekci (2018), *The Latest Data Privacy Debacle*, in "The New York Times", 30 January 2018

U.S. Department of Health, Education & Welfare (1973), *Records Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973

Y. Varoufakis (2023), *Tecnofeudalesimo. Cosa ha ucciso il capitalismo*, La nave di Teseo, 2023

A.E. Waldman (2020), *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, in "Current Opinion in Psychology", vol. 31, 2020

M. Weinberger, D. Bouhnik, M. Zhitomirsky-Geffet (2017), *Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior*, in "Oper Information Science", 2017, n. 1

A.F. Westin (1967), *Privacy and freedom*, Atheneum, 1967

J. Zahle (2017), *Privacy, Informed Consent, and Participant Observation*, in "Perspectives on Science", vol. 25, 2017, n. 4

S. Zuboff (2019), *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, 2019