

I dati ed i neurodiritti

Data and neuro-rights

EMILIA GIUSTI



Assegnista di ricerca in Diritto dell'Economia
Università degli Studi di Firenze

Abstract

Possiamo ormai distinguere due mondi: quello reale e quello digitale. Due spazi che seppur diversi si legano su di un piano che è quello relativo ai dati degli utenti, che sono diventati il nuovo bene, il nuovo valore di scambio. Proprio per questo però e per la loro capacità di influenzare il mercato sono anche diventati oggetto di attenzione e di riflessione, portando a valutare, anche quanto il loro utilizzo possa, all'opposto, confluire in un abuso ricollegabile al tema dei c.d. neuro diritti. Il saggio vuole focalizzare l'attenzione sui dati, sul loro utilizzo, sui rischi della società moderna e sulla possibile soluzione assicurativa che dovrebbe integrare la già presente assicurazione per la salute aggiungendo un profilo nuovo, più specifico per le applicazioni legate ai social media, al network, a tutte le possibili community in cui il legame si crea attraverso lo scambio di informazioni o la sinergia di attività digitali.



Abstract

We can now distinguish between two worlds: the real world and the digital world. Although different, these two spaces are linked by user data, which has become the new commodity, the new exchange value. Precisely for this reason, however, and because of their ability to influence the market, they have also become the subject of attention and reflection, leading to an assessment of the extent to which their use can, on the contrary, lead to abuse linked to the issue of so-called neuro-rights. This essay aims to focus attention on data, its use, the risks of modern society and the possible insurance solution that should complement existing health insurance by adding a new, more specific profile for applications related to social media, networks and all possible communities in which links are created through the exchange of information or the synergy of digital activities.

Keywords: dati; protezione del dato; rischi; assicurazione del rischio manipolativo

Summary: [1. Introduzione: la protezione del dato.](#) – [2. Applicazioni, dati e rischi.](#) – [3. I neurodiritti.](#) – [4. Conclusione: l'importanza dell'assicurazione.](#)

1. Introduzione: la protezione del dato.

In un mio recente scritto ribadisco come il diritto alla protezione dei dati¹ venga qualificato come un attributo della personalità² e la tutela dei dati personali sia in «primo luogo protezione dei diritti della personalità o in altri termini, tutela dell'autodeterminazione informativa»³.

Come è stato scritto da attenta dottrina, però più che di protezione oggi è meglio parlare di controllo dei dati⁴, questo alla luce del fatto che il termine protezione (pro-tengo) si lega meglio all'idea della necessità di tutelarsi dall'esterno, nel caso dei dati personali invero «il concetto di protezione assume una sfumatura diversa se lo si scruta dal punto di vista delle facoltà connesse e dei mezzi di tutela azionabili: l'utente che impiega alcune proprie informazioni non vuole metterle a riparo ma al contrario le sta offrendo ad altri più o meno consapevole che ne sta perdendo l'esclusività⁵», questo quindi porta a superare il concetto di protezione per far maggior spazio al concetto di controllo⁶ dei dati personali.

¹ E. GIUSTI, *La sanità elettronica: dati personali relativi alla salute, applicazioni e rischi*, in *Riv. It. Med. Leg.*, 2023, I, 93.

² G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, 703.

³ A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 44.

⁴ Questo richiama il concetto di data governance «intendendo con ciò l'insieme di strategie, metodiche e tecnologie per assicurare la qualità, l'integrità, la disponibilità del dato per il suo intero ciclo di vita garantendone al tempo stesso la sicurezza da intrusioni esterne o interne all'organizzazione» Sul punto, si veda I. LISI, *L'impatto de GDPR sulle strategie ICT: il ruolo del DPO oltre la teoria*, in *Guida al Trattamento e alla sicurezza dei dati personali*, in AA.VV., *Manuale per il trattamento dei dati personali*, a cura di G. COMANDÈ e G. MALGIERI, Gruppo 24 Ore, 2019, 384, 215.

⁵ G. GAROFALO, *Trattamento e protezione dei dati personali: spunti rimediali in ambito sanitario*, in *Dir. fam. e pers.*, 2021, III, 1392, 1395.

⁶ S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, 1991, 521 ss.

Controllo che è sempre più indispensabile⁷, soprattutto per i dati sensibili come quelli relativi alla propria salute che con più frequenza affidiamo ai sistemi tecnologici. Questo cambiamento lo abbiamo osservato inizialmente negli interventi del Garante⁸ per la protezione dei dati personali. Nelle sue pronunce, infatti, in un primo momento, analizzando i molteplici sistemi tecnologici che ricorrevano ai dati degli utenti, aveva concentrato il suo lavoro soprattutto nella verifica di tutte quelle misure necessarie affinché fosse mantenuta la privacy del dato⁹ strettamente intesa, magari facendo ricorso a tecniche di pseudoanonimizzazione¹⁰ affinché non fosse possibile legarlo alla persona. Oggi, invece, ha spostato l'attenzione non solo su questo aspetto ma anche sulle autorizzazioni, sul consenso, sull'informativa per l'utilizzo dei dati, sui rischi, sul riutilizzo del dato e sui metadati, sull'età dell'utente, su tutta una molteplicità di argomenti che stanno via via affiorando per poter ampliare e fortificare il controllo sul dato personale. L'attenzione si è allargata spostandosi dall'appartenenza del dato al suo utilizzo¹¹ ed alla possibilità di riuscire ancora a controllarlo, visto che sempre più minori utilizzano la tecnologia e l'intelligenza artificiale.

Dalla lettura della pronunce del Garante, prendiamo atto di come si possono dimostrare insufficienti le competenze tecnico-giuridiche di coloro che realizzano le applicazioni tecnologiche nella gestione dei dati personali¹², e come fattori rilevanti quali il consenso, la sua revoca, la conservazione dei dati ed il loro uso, la proprietà del dato processato, la verifica dell'utente quale persona maggiorenne o meno, ancora non abbiano acquisito l'attenzione e lo spazio che dovrebbero avere quando si predispone un'applicazione. Oggi più di ieri il controllo del dato, dell'applicazione ma soprattutto lo studio delle conseguenze dell'utilizzo dell'applicazione devono diventare il profilo rilevante

⁷ Il concetto di controllo del dato richiama subito quello di autodeterminazione. Sul punto v. A. DEL NINNO, *Diritto all'autodeterminazione sui propri dati e danno da trattamento*, in AA.VV., *Il risarcimento del danno non patrimoniale. Parte Speciale*, a cura di P. CENDON, Torino, 2009, 424, dove si intende la tutela dei dati personali quale protezione del diritto alla autodeterminazione nel trattare e nel far trattare i propri dati.

⁸ Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente italiana istituita dalla legge 31 dicembre 1996, n. 675, per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

⁹ Per quanto riguarda le criticità legate alle modalità di anonimizzazione v. R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0. Una lettura civilistica in chiave comparata*, in AA. VV., *La definizione del diritto*, a cura di F. CORTESE e M. TOMASI, Trento, 2016, 143 ss.

¹⁰ Sulle tecniche di anonimizzazione e pseudonimizzazione v. A. MONREALE *Tecniche di Anonimizzazione e Pseudonimizzazione*, in SAI News. Consultabile al sito: <https://sainews.humnet.unipi.it/documenti/monreale-tecniche-anonimizzazione-e-pseudonimizzazione.pdf>.

¹¹ F. BRAVO, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018. M. BURRI, R. SCHAR, *The Reform of the EU Data Protection Framework. Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, in *Journal of Information policy*, VI, 479.

¹² M. GAMBINI, *Dati personali e internet*, Napoli, 2008, 100. L'Autrice nella nota 24 sottolinea come l'utilizzo dell'espressione "data protection" implica il fatto che si discorra di qualcosa di più ampio del mero diritto ad essere lasciato solo, ossia del diritto dell'individuo a potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo però sempre il controllo sul modo in cui queste circolano e vengono utilizzate dagli altri; v. anche C. ALVISI, *Dati personali e diritti dei consumatori*, in AA.VV., *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 679 ss.

di qualsiasi novità su mercato. Sì, perché, ricorrente ormai è, come già anticipato, la “trasformazione del dato” che in un primo momento viene acquisito, poi viene processato ed infine restituito anche in nuove vesti tanto da dubitare della titolarità dello stesso in capo a chi inizialmente lo ha ceduto.

Il tema dei rischi e dell’informativa all’utilizzo dei dati personali, quindi, si intersecano tra di loro, tanto che, se non si è chiara la presenza dei rischi, delle infrastrutture, dei meccanismi di processo dell’applicazione o tecnologia e quindi delle loro criticità, non potremmo pensare di offrire, a chi ne farà ricorso, un’informativa completa, come, viceversa, se non si ha un’informativa completa non potremo dire di avere un’applicazione sicura da offrire al cittadino¹³. È un argomento, questo del rischio nelle nuove tecnologie, ricorrente ma poco poi analizzato ed approfondito, non si trovano scritti che classifichino i rischi in base all’applicazione che andremo ad utilizzare. Solo tramite l’analisi di alcune pronunce del Garante per la protezione dei dati personali e dell’European Data Protection Board è possibile rinvenire delle linee di indirizzo¹⁴.

2. Applicazioni, dati e rischi.

Iniziando dai rischi analizzati negli anni dal Garante per la protezione dei dati, uno tra i primi casi trattati e che ritengo molto esaustivo è stato quello relativo alla problematica del rischio dell’applicazione legato all’utilizzo del codice QR-code. Il QR-code è un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all’interno di uno schema bianco di forma quadrata, impiegato in genere per memorizzare informazioni destinate a essere lette tramite un apposito lettore ottico o anche smartphone. Nell’ultimo periodo è stato forte il ricorso a tale strumento che ha creato nuovi processi comunicativi: dei collegamenti ipertestuali tra il mondo reale e quello online. Nonostante questa sua funzione non sono mancate le criticità ed i rischi per la protezione dei dati come nel caso dell’applicazione Smart4You. Attraverso l’utilizzo dell’applicazione Smart4You nell’Azienda sanitaria unica regionale Marche era possibile, infatti, leggere il Codice QR presente sul talloncino rilasciato a chiunque era stato sottoposto allo screening per il Covid-19 per poter consultare il proprio dossier medico con le cartelle cliniche, le varie prenotazioni ospedaliere e gli esiti. L’applicazione è risultata, però, vulnerabile nella parte relativa alla gestione dello screening, limitatamente al servizio Screening Covid-19 San Benedetto e la app smart4you connessa con il medesimo screening. Il problema era relativo alla funzione di lettura rapida dell’esito del tampone consegnato ai soli partecipanti alle attività di screening Covid-19 nelle fasi iniziali di accettazione tramite QR-code, generato sequenzialmente e che associava direttamente partecipante-esito tampone.

¹³ S. WACHTER, B. MITTERLSTADT, L. FLORIDI, *Why a Right to explanation of Automated Decision-making Does Not exist in the General data Protection Regulation*, in *International Data Privacy Law*, 2017, 76. L’individuo ha diritto prima e non dopo di conoscere la modalità di funzionamento di un determinato sistema.

¹⁴ Gruppo di Lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, WP 251 rev.01, 6 febbraio 2018, 27.

Il QR non era stato elaborato in modo casuale ma in modo progressivo per cui ad ogni numero corrispondeva un utente e cambiando una cifra era così possibile accedere al profilo di un altro. La violazione si era limitata ai soli dati anagrafici e, ove presente, al numero di cellulare del soggetto. Il rischio per la privacy si sostanzialmente nella decodifica QR-code e quindi nell'acquisizione dei dati personali della singola persona ed anche in questo caso nell'associazione del dato. L'Azienda veniva richiamata dal Garante che si pronunciava il 13 gennaio 2022¹⁵ e per porre rimedio alle violazioni che stavano accadendo prevedeva che il fornitore NSB modificasse la generazione del QR-code con una codifica più complessa di tipo Hash, composta da una prima parte del codice fiscale unita a una sequenza casuale. Inoltre, sono state escluse la funzionalità di decodifica del codice fiscale con il nominativo degli assistiti regionali, la verifica della coerenza tra numero di cellulare con app smart4you e soggetto interrogato, includendo la possibilità di blocco o di alert.

Questo, ci dimostra come, un sistema che all'apparenza potrebbe sembrare corretto, in realtà poi, a causa di errori tecnici, che a volte appartengono all'uomo, a volte a difetti di sistema, possono, se mal gestiti diventare dei fattori lesivi per chi ne faccia uso. Così, come lesivi, progressivamente, stanno diventando i social network che, nonostante un loro iniziale pacifico utilizzo quale "community del dato" hanno man mano acquisito più funzioni e servizi tanto da dover porvi l'attenzione anche da parte delle Autorità per la privacy, raggruppate nella rete internazionale del Global Privacy Enforcement Network (GPEN), che, visto i larghi utilizzi, hanno richiamato le piattaforme che propongono app su smartphone e tablet ad obbligare gli sviluppatori ad informare gli utenti, prima che questi scarichino le app, sugli eventuali dati personali che verranno raccolti e sul loro uso, sui limiti di età. Oggi, nonostante le misure di precauzione avanzate, si riscontrano, anche in questi contesti, forti criticità e come è stato scritto da attenta dottrina si comprende sempre più, guardando la casistica come la causa sia da attribuire in primo luogo al vuoto legislativo: nessuna norma della società dell'informazione e nessun dibattito sull'affidabilità delle nuove tecnologie si occupavano oltre che per la persona adulta anche della particolare posizione del bambino-utente nei servizi e nei prodotti digitali¹⁶.

Un esempio è stato il caso di Tiktok¹⁷, seguito sempre dal Garante della privacy dopo gli eventi che avevano coinvolto minori nell'utilizzo dell'applicazione attraverso la creazione di gare sul social, che purtroppo hanno portato ad esiti terribili per gli stessi ragazzi.

Il garante per la privacy, nelle varie pronunce, provvedimenti ha ribadito l'importanza della tutela del dato in queste applicazioni che espongono anche i ragazzi ma soprattutto, ha ribadito l'importanza della verifica dell'età dell'utente indicando anche strumenti tecnici a cui ricorrere per poter superare questo limite.

¹⁵ Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Azienda sanitaria unica regionale Marche, Provvedimento n. 9 del 13 gennaio 2022 [Doc-Web 9744496].

¹⁶ D. AMRAM, *Non ho l'età, ma... costruire competenze abilitanti per una società dell'informazione a prova di (in)capacità del minore di età*, Giuffrè, 2022.

¹⁷ Garante per la Protezione dei Dati Personali, Provvedimento dell'11 febbraio 2021 [Doc-Web 9554603].

Per questo, proponeva due soluzioni percorribili¹⁸: la prima consentirebbe l'accertamento del superamento di una determinata soglia di età, senza che questa sia però rivelata. Semplificando al massimo, il soggetto sottoposto a verifica - nel nostro caso il minore - dovrebbe dichiarare il superamento della soglia di età ad una infrastruttura di age verification. Quest'ultima dovrebbe essere in grado di riconoscere se il soggetto sottoposto a verifica stia dicendo il vero o il falso.

L'altra soluzione potrebbe essere il ricorso all'intelligenza artificiale che, attraverso algoritmi di machine learning in grado di migliorarsi progressivamente, producono una congettura verosimile dell'età dell'utente. In pratica, la piattaforma dovrebbe estrarre un campione di utenti di partenza, costituito da giovanissimi e da adulti, da sottoporre a scrutinio attraverso la raccolta di parametri di navigazione come, ad esempio, i tempi di permanenza sui vari contenuti, la frequenza dei like e dei click, il percorso che fa il mouse sullo schermo etc.

Questo perché i rischi, quando si tratta di minori, sono maggiori rispetto a quelli in cui può incorrere un adulto ma anche diversi rispetto a quelli da sempre conosciuti. Si passa dal furto di identità, alla violazione della privacy per poi spostarci nell'ambito più profondo con il pericolo di sexting, cioè l'invio, la ricezione e/o la trasmissione di fotografie, messaggi, immagini sessualmente esplicite, con potenziali conseguenze dannose.

Il rischio online più comune affrontato dagli adolescenti è il cyber bullismo, definito come un insieme di azioni aggressive, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, foto, video, e-mail, etc.), il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi.

Il rischio in definitiva è la manipolazione mentale dell'utente, sia attraverso la violazione della sua privacy sia attraverso l'utilizzo dell'applicazione stessa che porta il soggetto a comportamenti del tutto disallineati al suo agire nel mondo naturale.

3. I neurodiritti.

Seguendo quindi, l'ordine di questo saggio, ecco che si apre un'altra parentesi che illustra quanto già sta succedendo in Spagna relativamente alla neurotecnologia e cioè lo studio dell'evoluzione tecnologica attraverso tre aspetti: quello della neuroscienza, quello ingegneristico e quello giuridico¹⁹.

Ci stiamo accorgendo infatti che mentre, come adesso, facciamo di tutto per inquadrare, cristallizzare e definire il fenomeno dell'applicazione, in realtà la stessa si è aggiornata e dalla semplice richiesta di un dato, si è evoluta in un sistema che non si ferma più solo ed esclusivamente a quel dato ma va oltre e sempre attraverso il sistema tecnologico e partendo dal dato, lavora sulla nostra capacità intellettuale e nel corso dell'utilizzo dell'applicazione, non solo

¹⁸ G. C. FERONI, *Le sfide mortali su TikTok e le mani legate* (Il Messaggero, 17.03.2021) [Doc-Web 9563068].

¹⁹ Sui neurodiritti è interessante il libro R. YUSTE ROJAS, *Neuroderechos: Un viaje hacia la protección de lo que nos hace humanos*, Barcellona, 2025.

continuiamo a rendere il dato che inizialmente avevamo deciso di fornire per incominciare ad utilizzare quella tecnologia ma bensì ne forniamo tanti altri, che invece, inizialmente non avremmo fornito perché non interessati a fornirli.

Con l'espansione delle possibilità offerte dalla scienza, si pone la questione del katechon, ovvero della definizione dei limiti di ammissibilità e sostenibilità etica, giuridica e sociale dell'innovazione²⁰.

Nel corso del sistema, siamo così sollecitati che la nostra volontà o meglio consapevolezza viene superata dal desiderio di continuare ad utilizzare il tecnologico e quindi superiamo i problemi di privacy e di una eventuale discriminazione perché magari quel dato che noi cediamo e che potrebbe anche procurarci un disagio se diffuso, in realtà non è neanche garantito, in termini di privacy, dall'applicazione stessa o ancor di più viene ceduto a terzi.

In tal modo tendiamo a superare quella che chiamiamo collaborazione tra macchina e uomo e forse dovremmo iniziare a cercare degli strumenti giuridici che al pari di quelli tecnologici pongano un freno, a quei sistemi, che in qualche modo portano ad una progressiva manipolazione mentale dell'utente tanto da arrivare ad acquisire dati che lo stesso, in condizioni diverse, non avrebbe fornito²¹.

Ed è necessario anche osservare come sia del tutto fuorviante, peraltro, pensare di esaurire la tutela dell'utente online con gli strumenti forniti dalla normativa sulla privacy, considerando l'informazione personale il bene da tutelare al pari del patrimonio²²: la mera revoca del consenso (ovvero l'opposizione) al trattamento dei dati non ha la stessa efficacia del recesso nella fornitura di beni o servizi. Rimanendo, infatti, salvi i trattamenti dei dati personali effettuati prima della revoca/opposizione, di fatto, il rimedio all'eventuale trattamento abusivo del dato personale non ripristina in alcun modo lo stato antecedente al trattamento²³. L'esercizio dei diritti da parte del soggetto interessato non potrà restituire un controllo sull'informazione precedentemente processata ed anche conferita a terzi. Il controllo del soggetto interessato sul flusso di dati generato si perde nel momento stesso in cui si aderisce ad un servizio o si utilizza un prodotto.

Anche questo è doveroso che sia inserito nelle informative che rilasciamo all'utente. Il punto riguarda i suoi "neurodiritti" e quindi i diritti che ha lo stesso nel caso in cui si renda conto che il sistema è riuscito ad arrivare così ben tanto oltre da farsi cedere informazioni che magari non servono neanche per l'utilizzo dello stesso ed a processarle per poi cederle. Siamo andati così avanti che si potrebbe mettere in discussione la stessa sicurezza economica della persona. Questo è un aspetto che maggiormente lo possiamo misurare nei soggetti fragili, appunto ragazzi e anziani oltre che persone portatori di deficit mentali.

Il diritto alla protezione dei dati personali presenta quindi, oggi, una sfida nuova relativa all'impatto della tecnologia, dell'intelligenza artificiale a livello

²⁰ P. STANZIONE, *Privacy e neurodiritti: la persona al tempo delle neuroscienze*, Intervento Giornata europea della protezione dei dati 2021 Convegno "Privacy e neurodiritti: la persona al tempo delle neuroscienze" 28 gennaio 2021 [Doc-Web 9529600].

²¹ C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021.

²² D. AMRAM, *op. cit.* 2022, 32, 260.

²³ E. BACCIARDI, *Il recesso del consumatore nell'orizzonte delle scienze comportamentali*, Torino, 2019; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018.

neurologico che in qualche modo va tutelato. Siccome l'interessato, ossia la persona fisica a cui si riferiscono i dati personali, non è difatti un soggetto che passivamente subisce le operazioni di trattamento effettuate su detti dati, ma, al contrario, vanta un potere di controllo e di intervento sui dati personali, nel momento in cui il controllo del dato viene a mancare perché troppo processato lo stesso individuo dovrà pur ricorrere a nuove tutele ai neurodiritti e cioè quei diritti che vogliono preservare l'intimità celebrale della persona e che oggi dovrebbero diventare tema di discussione anche in ambito assicurativo.

Le tecnologie che influenzano il processo neurale possono compromettere la libertà cognitiva, base del diritto all'autodeterminazione.

Quindi, se parafrasiamo quanto fino ad ora detto e lo osserviamo oggi, alla luce del continuo progresso, non possiamo che pensare che da questo punto vista, vi sono degli importanti vuoti, non solo legali ma anche assicurativi.

In America già si sta affrontando questo tema mettendo in risalto proprio il profilo del danno alla salute.

Dottrina, a riguardo, descrive il tutto come un crescente coro di preoccupazioni sugli impatti dei social media sulla salute mentale, in particolare per i giovani. L'attenzione sui giovani deriva da ricerche che dimostrano il potenziale dei social media di disturbare i percorsi neurali e la chimica nella loro fase unica dello sviluppo neurologico, oltre alle preoccupazioni riguardo all'esposizione a contenuti inappropriati e pericolosi per i bambini su piattaforme minimamente moderate. Diversi rapporti di alto livello hanno evidenziato esiti negativi sulla salute associati all'uso dei social media e all'esposizione a contenuti dannosi, tra cui disturbi del sonno, disturbi dell'immagine corporea, depressione, ansia e comportamenti suicidi. Tre rapporti principali: un consiglio dell'Ufficio del Chirurgo Generale degli Stati Uniti (OSG) (2023), raccomandazioni dell'American Psychological Association (APA, 2023) e un rapporto nazionale delle National Academies of Science, Engineering, and Medicine (NASEM) (Galea et al., 2024) – tutti evidenziano il notevole potenziale di danno nell'uso dei social media tra i giovani, ma anche le complessità e le sfide nello stabilire legami causali e definitivi tra uso e risultati per la salute. Queste preoccupazioni sono rispecchiate in più iniziative locali di salute pubblica, come un avviso del 2024 del Dipartimento della Salute di New York City (NYCDOH) che etichetta i social media come tossina ambientale e mette in guardia sui loro effetti sulla salute mentale dei giovani (Counts et al., 2024). I ricercatori del NYCDOH hanno riconosciuto le particolari difficoltà nel comprenderne gli effetti tossici: oltre ai complessi benefici e danni dei social media, Counts et al. (2024) sottolineano che "la dose che alimenta la tossicità [dei social media] non è nota: è il contenuto, la durata, l'uso o tutto questo?²⁴".

²⁴ J. RICHARDS, K. NIITSU, N. KENWORTHY, *Mental Health v. Social Media: How US pretrial filings against social media platforms frame and leverage evidence for claims of youth mental health harms*, in *SSM-Mental Health*, 2025, VII, 100378.

4. Conclusione: l'importanza dell'assicurazione.

In definitiva e tornando indietro nell'analisi, volendo riprendere la parte relativa alla protezione degli utenti non possiamo che ribadire l'importanza del controllo nell'utilizzo dell'intelligenza artificiale non solo per evitare di incorrere in abusi ma anche per non dover riconoscere l'insorgere di un danno neurologico. Alla luce dei miei neurodiritti e complementando questi alla protezione dei diritti personali oltre che digitali non si può che considerare indispensabile l'intervento assicurativo che non deve oggi, occuparsi solo della salute digitale nel senso dei servizi assicurativi come l'erogazione di servizi di telemedicina e/o home-care²⁵ ovvero la messa a disposizione di dispositivi wearable e/o wireless per cui l'assicuratore può monitorare e assistere, tramite consulti medici da remoto, l'assicurato e riquantificare i premi assicurativi in base allo stile di vita più o meno virtuoso adottato dallo stesso, incentivando l'adozione di condotte sane e così prevenendo l'insorgere di patologici, ma deve considerare i rischi neurologici digitali che possono derivare dall'assenza di informative e condizioni chiare per l'utente nell'uso della piattaforma, nella mancanza di misure a presidio dell'età del consumatore ma soprattutto nell'eccessiva esposizione al processo algoritmico per l'utente che supera la normale tollerabilità per le capacità cognito-comportamentali umane.

Idea, quella assicurativa, già valutata anche dalla dottrina recente che in un magnifico libro ci espone quelle che potrebbero essere le scelte assicurative: e cioè la possibilità di introdurre meccanismi di assicurazione della responsabilità civile contro i danni eventualmente causati dall'uso (improprio o colposo) dei servizi della società dell'informazione e delle nuove tecnologie non solo per gli adulti, ma anche (e soprattutto) da parte di giovani utenti, estendendo esplicitamente la copertura delle polizze chiamate "capofamiglia" oppure, guardando all'assicurazione per responsabilità civile automobilistica, potrebbero essere individuate polizze a tutela degli eventuali danni cagionati dall'uso della tecnologia da parte dell'utente, nella specie equiparato al conducente del veicolo, e del titolare della linea per l'erogazione del servizio o del prodotto, *mutatis mutandis* al pari della posizione del proprietario del veicolo²⁶.

In sintesi, il rischio che è doveroso assicurare è quello legata alla capacità di creare "dipendenza" a quella piattaforma. Un rischio che sicuramente oggi può essere misurato, valutato e normativizzato ma soprattutto evitato attraverso regole, limiti e blocchi automatici da parte dell'user quando si ravvisa un utilizzo fuorviante, continuativo e spasmodico del sistema²⁷.

Forse questo è ancora un lontano orizzonte ma dobbiamo prendere atto che dalla privacy siamo passati al controllo e ora dal controllo siamo passati alla

²⁵ IVASS, Report Analisi Trend Offerta Prodotti Assicurativi, gennaio-giugno 2021, *cit.*, 6 ss.. Consultabile al sito: <https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/altre-pubblicazioni/2021/prodotti-primo-semester-2021/index.html?dotcache=refresh>; ID., Report. Analisi trend offerta prodotti assicurativi, luglio-dicembre 2020, aprile 2021, 8.

²⁶ D. AMRAM, *op. cit.* 2022, 233, 260.

²⁷ Questa strada è in linea anche con il profilo europeo che ha già richiesto la creazione di uno spazio digitale affidabile e sicuro perché obiettivo cardine del Reg. UE n. 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali, di seguito anche "DSA").

salute. Rimarrà sicuramente l'ultima tappa quella legata al valore economico di quanto si viene a creare perché sicuramente un sistema o un'applicazione che ha molti utenti, seppur legati allo stesso da dipendenze mentali, sarà comunque un sistema che non può che definirsi economicamente abile ma è pur vero che quel rapporto economico non può che essere riequilibrato attraverso una buona polizza che analizza l'esposizione tecnologica sull'utente valutandone i rischi che oggi, più di ieri, assumono un importante quadro valoriale.