dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2022
Data di pubblicazione – 28 giugno 2022

La monetizzazione dei dati personali: applicazione e rischi relativi al trattamento dei dati inerenti la salute

di
Lorenzo Maria Lucarelli Tonini*

1. *Introduzione*

Nel contesto economico moderno, caratterizzato da una incessante produzione automatizzata ed interconnessa, i dati, quali beni dematerializzati, rivestono un ruolo centrale, ancor di più quando si tratta di dati personali, ossia tali da rendere identificabile una persona fisica. I dati, soprattutto quelli personali, sono oggi una delle maggiori fonti di ricchezza[1], tanto da essere pacificamente definiti come "petrolio digitale", visto il significativo valore patrimoniale che questi hanno assunto, di fatto, negli ultimi decenni.

* *Dottorando di ricerca, Università degli Studi "Roma Tre".*

[1] J. LITMAN, *Information Privacy/Information Property*, in *52 Stan. Law Rev*, 2000, p. 1283; R. PARDOLESI, C. MOTTI, *L'Informazione come bene*, in G. DE NOVA (a cura di), *Dalle Res alla new properties*, Franco Angeli, Milano, 1991, p. 37 ss.

Contributo sottoposto a referaggio

In tal senso, esemplare è il noto "Caso Facebook"[2], affrontato dal Consiglio di Stato[3] dopo un lungo procedimento volto ad accertare se il *social network* fornisse il proprio servizio gratuitamente o, invece, dietro il pagamento non di una somma di denaro ma di una (incerta) quantità di dati personali degli utenti iscritti.

In concreto, infatti, sono molteplici le fattispecie che vedono il dato personale acquisire un proprio ed autonomo valore patrimoniale, tale da consentirne l'utilizzo quale moneta di scambio per pagare un determinato servizio. Si pensi, ad esempio, proprio alle piattaforme *social* le quali, nella maggioranza dei casi, sono totalmente gratuite, oppure all'iscrizione e utilizzo di caselle email o ad altri servizi Internet[4] i quali, spesso, prevedono il pagamento di un prezzo solo per usufruire di contenuti o servizi *premium*. In questi casi, sovente, le piattaforme godono di un ritorno economico nello svolgere attività di *targeting*[5], veicolando, per le aziende dalle quali vengono remunerate, pubblicità mirata in base all'elaborazione dei dati acquisiti dai propri utenti. Si pensi, ancora, ai contratti di assicurazione automobilistica i quali, sovente, prevedono il pagamento di un prezzo inferiore nel caso in cui venga installata la c.d. "*black box*" dalla quale è possibile estrarre dati di circolazione dell'utente/automobilista[6].

Sempre di patrimonializzazione, o ancor più specificamente di monetizzazione del dato personale si può parlare rispetto a quella attività posta in essere tra i titolari del trattamento e i *data broker*, ove i primi cedono ai secondi, dietro il pagamento di una somma di denaro, i dati acquisiti nello svolgimento della propria attività, solitamente con lo scopo, per i *data broker*, di svolgere attività di marketing.

[2] Per una attenta disamina della questione si veda: G. SCORZA, *Facebook non è gratis?,* in *Dir. di Internet*, 3, 2021, pp. 561-571, il quale, differenziando nettamente tra "patrimonializzazione" dei dati personali e "monetizzazione" dei dati personali, afferma che «I dati personali che gli utenti forniscono a Facebook per utilizzare il servizio sono o non sono un corrispettivo del servizio? Neppure la lettura della sentenza in commento consente di rispondere alla domanda. La contestazione dell'Autorità Garante della concorrenza e del mercato relativa all'ingannevolezza della qualificazione del servizio come gratuito da parte di Facebook sembra, a ben vedere, ritenuta dai Giudici del Consiglio di Stato, fondata più sul fatto che, per un verso o per l'altro, Facebook trarrebbe un beneficio economico dallo sfruttamento commerciale dei dati degli utenti che sul fatto che tali dati personali rappresentino il corrispettivo del servizio».

[3] Si fa riferimento alla sentenza del Consiglio di Stato del 29 marzo 2021, n.2631, in *Dir. di Internet*, 3, 2021, pp. 547-561.

[4] Per una approfondita analisi del contratto di accesso ad Intenet si veda E. BATTELLI*, Il contratto di accesso ad Internet*, in *Media Laws*, 1, 2021, pp. 129-157.

[5] Per un approfondimento sull'attività di *targeting* si vedano le *Linee Guida 8/2020 sul targeting degli utenti di social media*, pubblicate dall'EDPB il 13 aprile 2021.

[6] E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e rischi,* in *Il Corriere giuridico*, 12, 2019, p. 1517 ss.

Se da una parte, quindi, occorre prendere atto del valore patrimoniale attualmente acquisito dai dati personali, ormai oggetto di una specifica disciplina omogenea in tutta l'Unione europea[7], dall'altra occorre sottolineare come tale assunto non sia stato, e non sia tuttora, sempre pacifico dal punto di vista giuridico, riscontrando invece forti limitazioni e perplessità, come si vedrà in particolare nel settore sanitario, ove i dati trattati, relativi alla salute, richiedono *ex lege* una tutela rafforzata.

2. *I limiti alla "monetizzazione": dalla concezione "morale" a quella "negoziale"*

Dirimente per affrontare il tema della monetizzazione dei dati personali è il valore[8] che si riconosce al dato personale e, quindi, alla possibilità di una sua commercializzazione.

A tal riguardo si fa riferimento a due contrapposte teorie, l'una improntata ad un approccio "morale" è preclusiva della commercializzazione dei dati personali e attenta alla tutela della sfera giuridica della persona fisica, l'altra, invece, più propriamente "negoziale", prende atto dell'esistenza di un vero e proprio "mercato del dato" e, pur con le necessarie cautele, ammette il diritto dell'interessato a sfruttare economicamente i propri dati personali.

A sostegno di una "concezione morale" del dato personale viene da molti[9] evidenziato che esso è una esplicazione dell'identità e della personalità del soggetto interessato, tale da qualificare il diritto al corretto trattamento dei dati personali come un diritto fondamentale, in quanto tale inalienabile e indisponibile. Una tale configurazione prende le mosse, inoltre, dalla previsione del diritto alla protezione dei dati personali, distinto e solo in parte sovrapponibile al diritto alla riservatezza,

[7] Regolamento Ue 679/2016, recepito in Italia con il D. Lgs. 101/2018 che ha modificato il D. Lgs. 196/2003.

[8] Sul valore dei dati personali si vedano: J. LITMAN, *Information Privacy/Information Property*, cit., 1283; Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers, No. 220, 2013; G. MALGIERI, B. CUSTERS, *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017.

[9] Al riguardo si vedano le posizioni di S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 397 ss.; F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995; A. SCALISI, *Il valore della persona nel sistema e i nuovi diritti della personalità*, Giuffrè, Milano, 1990; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati personali e tutela della persona*, Giuffrè, Milano, 1998, p. 25 ss.

quale diritto costituzionalmente garantito in quanto esplicazione dell'art. 2 Cost. e, a livello sovranazionale degli artt. 8 della Carta dei diritti fondamentali dell'Unione europea e 16 del TFUE. Tale tesi, che è stata supportata per lungo tempo dalla dottrina prevalente[10], impegnata a garantire la tutela della sfera giuridica dell'interessato sulla base del connotato di "sacralità" della persona fisica, risulta però essere stata in parte sconfessata dalla prassi commerciale.

Più recenti, invece, sono gli interventi della dottrina[11] che si è espressa a sostegno della patrimonializzazione dei dati personali, sulla base di un "approccio negoziale" che ha preso atto dell'esistenza di una florida economia dei dati e volto a garantire una più efficace protezione dei dati personali in quanto bisognosi di una tutela rafforzata.

Sulla base dell'approccio negoziale, quindi, ai dati personali si riconosce uno specifico valore economico nell'ambito dei più disparati scambi commerciali nei quali questi vengono in rilievo.

Non viene meno, tuttavia, l'importanza del diritto alla protezione dei dati personali quale diritto fondamentale ma viene sottolineata la necessità di garantire la tutela della persona fisica non solo in quanto tale ma anche quale soggetto contraente. Infatti, quotidianamente si compiono attività, soprattutto online, che richiedono di fornire dati personali e, ormai, si è abituati a farlo di *default* con un semplice *click* o *scroll*, senza nemmeno domandarsi a cosa serviranno i dati forniti con queste azioni, come questi verranno trattati e se questi siano effettivamente pertinenti rispetto al servizio offerto. L'interessato, pur di usufruire di un servizio online, spesso non si rappresenta minimamente la possibilità che, conferendo i propri dati, stia concludendo un vero e proprio contratto con effetti giuridici[12]. Questo è ancor più evidente nell'ambito dei servizi digitali apparentemente gratuiti e offerti da società di rilevanza globale, le quali difficilmente potrebbero giustificare la propria

[10] Si veda, *ex multis*, G. ALPA, M. BESSONE, L. BONESCHI, *Il diritto all'identità personale*, Cedam, Padova, 1981; F. MACIOCE, *Tutela della persona e identità personale*, Cedam, Padova, 1984; A. SCALISI, *Il valore della persona nel sistema e i nuovi diritti della personalità*, Giuffrè, Milano, 1990; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583.

[11] A riguardo si vedano le posizioni di V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 23-59.; A. DE FRANCESCHI, *Il pagamento mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1381-1411.

[12] E. BATTELLI, *Il contratto di accesso a Internet*, cit., p. 147 ss.

ricchezza a fronte dei servizi offerti gratuitamente se non sottolineando come, in realtà, il prezzo pagato risieda nei dati personali degli utenti.

Stando così le cose, al fine di legittimare (e tutelare) tale rapporto sinallagmatico che vede un soggetto fornire un determinato servizio e l'utente "pagare" con i propri dati personali, i fautori dell'approccio negoziale rinvengono in questo la struttura causale tipica del rapporto contrattuale.

Gli iniziali approdi all'approccio negoziale, qualificando i dati personali quali "beni immateriali", simili all'immagine e al nome[13], propongono l'estensione anche ai primi della lettura dualistica[14] ormai riconosciuta ai secondi. In altre parole, se per un verso l'ordinamento riconosce un diritto della personalità primario, caratterizzato dalla non patrimonialità e indisponibilità, dall'altro garantisce anche un autonomo diritto patrimoniale di utilizzazione economica degli attributi della personalità. Dunque, così come è ormai riconosciuta la possibilità di sfruttare economicamente il nome o l'immagine, sarebbe anche possibile sfruttare economicamente i dati personali, utilizzandoli quale merce di scambio a fronte della fornitura di un servizio[15].

3. *Il consenso alla "monetizzazione" dei dati personali*

Sostegno all'approccio negoziale viene rinvenuto anche nel Regolamento Ue 679/2016, il quale espressamente prevede, all'art. 1[16], che la libera circolazione dei dati personali non possa essere limitata per motivi attinenti alla protezione delle persone fisiche. In tale previsione viene rinvenuta la volontà del legislatore europeo di «porre sullo stesso piano l'approccio morale e quello negoziale,

[13] Per approfondimenti si rimanda a F. G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, ESI, Napoli, 2008, p. 20 ss.

[14] V. ZENO-ZENCOVICH, voce *Personalità (diritti della),* in *Dig. Disc. Priv.,* vol. XIII, Utet, Torino, 1995, p. 441.

[15] Sul punto di veda V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. Inf.*, 1993, p. 545 ss.; F. G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, cit., pp. 20-26.

[16] Art. 1, Reg. Ue 679/2016: «Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione dei dati.

Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»

mirando ad un loro bilanciamento costante»[17].

La "nuova" normativa europea, dunque, non rivestirebbe solo una funzione di garanzia di un diritto fondamentale quale la protezione dei dati personali ma, coerentemente con l'intero ordinamento europeo, realizzato con il fine di favorire un mercato unico europeo, avrebbe anche la duplice funzione di regolare «un'economia dei dati dell'Unione che tuteli i diritti e le libertà fondamentali dei cittadini europei, favorisca e incentivi la libera circolazione dei dati all'interno dell'Unione e, soprattutto, costruisca una società digitale a misura di persona umana»[18].

Nell'analisi della negoziabilità dei dati personali, il consenso si pone quale specifica base giuridica legittimante il trattamento dei dati comuni, ai sensi dell'art. 6 del GDPR, in quanto elemento strutturale della fattispecie tipica di un contratto sinallagmatico nel quale una parte fornisce un servizio e l'altra acconsente al trattamento dei propri dati personali, questi considerati quale controprestazione seppur diversa dalla dazione di denaro. All'interno di tale rapporto sinallagmatico, tuttavia, è necessario distinguere diversi momenti: da una parte vi è la comunicazione dei dati personali da parte dell'interessato al fornitore del servizio; dall'altra vi è il consenso al loro trattamento.

Occorre poi distinguere tra i dati forniti perché necessari alla fornitura del servizio, dagli ulteriori dati richiesti e non necessari alla fornitura del servizio stesso, quindi dati "eccedenti", e in determinati casi potenzialmente lesivi del principio di "minimizzazione"[19]. I primi, necessari alla fornitura del servizio, troveranno diretta tutela nella normativa europea e nazionale sulla base dell'approccio morale volto alla protezione dell'interessato nella sua sfera giuridica personale. I secondi, quali dati eccedenti e oggetto del contratto, troveranno invece tutela non solo nella normativa a protezione dei dati personali ma anche nella normativa contrattuale e,

[17] G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Il diritto dell'informazione e dell'informatica*, 4, 2020, p. 656.

[18] Così G. D'ACQUISTO, F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi Giuridica dell'Economia*, n.1, 2019, ai quali si rimanda per un approfondimento sul "mercato dei dati" europeo.

[19] Art. 5, c. 1, lett. c) del Regolamento Ue 679/2016.

specificamente, in quella consumeristica[20], sulla base dell'approccio negoziale.
Distinto, invece, è il momento in cui l'interessato autorizza il trattamento dei suoi dati personali, poiché solo in seguito a ciò gli ulteriori dati forniti ed eccedenti rispetto a quelli necessari all'esecuzione del contratto (in quanto «necessari all'esecuzione del contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali»[21]), nonché quelli trattati *ex lege*[22], potranno essere oggetto di trattamento e quindi acquisire per il fornitore quel valore patrimoniale necessario a renderli merce di scambio rispetto al servizio offerto.

4. *Il ruolo del diritto alla limitazione del trattamento e la funzione del consenso quale autorizzazione all'utilizzo dei dati personali*

Ponendo attenzione all'approccio negoziale si potrebbe dunque ritenere, così come alcuni affermano[23], che l'interessato, acconsentendo al trattamento dei propri dati personali, li ceda al fornitore in qualità di proprietario di tali beni, quindi mediante un negozio traslativo. Tuttavia, una simile ricostruzione si scontra inevitabilmente con l'assunto per cui i dati personali, ormai pacificamente ritenuti un bene, seppure immateriale e bisognoso di una tutela rafforzata, appartenendo alla sfera più intima e personale dell'interessato, difficilmente possono essere in concreto ceduti. Infatti, è innegabile che il trasferimento della proprietà dei dati personali comporterebbe per l'interessato l'impossibilità di utilizzarli e, quindi, il venir meno di elementi descrittivi della propria persona. Inoltre, se i dati personali costituissero oggetto di proprietà dell'interessato, il cessionario, dopo averli ricevuti ed esserne

[20] Un simile approdo trova ragione nella possibilità di rinvenire nel rapporto interessato-fornitore l'elemento tipico alla base dell'applicazione della disciplina consumeristica, ossia quell'asimmetria informativa e contrattuale che rende il consumatore (interessato) una parte debole rispetto al professionista (fornitore), tale per cui l'interessato è il più delle volte portato ad accettare le condizioni imposte dal fornitore senza alcuna possibilità di contrattare diversamente e quindi a prestare il consenso al trattamento dei propri dati personali al fine di usufruire del servizio fornito. Da quanto detto, deriva, dunque, l'obbligo del fornitore di informare, attraverso una apposita informativa, che i dati personali forniti verranno utilizzati quali prezzo del servizio reso, in adempimento sia degli obblighi informativi previsti dal GDPR, sia di quelli previsti dal Codice del Consumo, il quale impone al professionista l'obbligo di fornire precise informazioni precontrattuali, riguardanti, appunto, anche il prezzo del bene oggetto del contratto. Così, *ex multis*: V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit.; E. BATTELLI, *Il contratto di accesso ad Internet*, cit.; A. DE FRANCESCHI, *Il pagamento mediante dati personali*, cit.;

[21] Art. 6, c. 1, lett. b) del GDPR.

[22] A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, ESI, 2017, pp. 72-73.

[23] Così A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, cit., p. 75: «Qualora i dati personali vengano ceduti a titolo definitivo, si ritiene che alla loro fornitura sia applicabile la disciplina della compravendita».

diventato proprietario, dovrebbe poterli ritrasferire a qualunque altro acquirente liberamente. Sulla base della normativa introdotta dal Reg. Ue 679/2016, invece, per legittimare questo secondo trasferimento occorre un consenso specifico[24] e diverso rispetto a quello legittimante il mero trattamento da parte del titolare, nonché apposita menzione dell'intenzione di trasferirli a terzi all'interno delle informazioni fornite ai sensi degli artt. 13 e 14 GDPR.

Pertanto, in base ad una differente ricostruzione del fenomeno[25], che qui si sostiene, il consenso non avrebbe un'efficacia traslativa. I dati personali, in quanto elementi dell'identità del soggetto interessato, infatti, non gli apparterrebbero in base ad un rapporto di proprietà e, dunque, il consenso non avrebbe l'efficacia di trasferire i dati personali dall'interessato ad un altro soggetto (fornitore del servizio). Si tratterebbe, invece, meramente di un'efficacia autorizzativa con cui egli consentirebbe il mero utilizzo dei suoi dati e la loro consultazione mediante accesso[26], alla stregua dell'efficacia del consenso quale base giuridica che «fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano»[27].

Una simile ricostruzione troverebbe un solido sostegno soprattutto nell'art. 18 del Regolamento Ue 679/2016, il quale riconosce all'interessato, in determinati casi, il diritto di limitare il trattamento dei propri dati personali effettuato dal titolare. Tale previsione, infatti, difficilmente si concilierebbe con la concezione proprietaria di "signoria sul bene". Non sarebbe, difatti, in alcun modo giustificabile la possibilità per l'interessato/venditore di limitare unilateralmente il diritto di proprietà dei propri dati personali acquisito dal fornitore del servizio, il quale avrebbe acquisito il diritto di disporre e godere liberamente dei beni acquistati. L'esplicarsi del diritto

[24] In base al Considerando n. 32 del Reg. Ue 679/2016, «qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste». Dunque, il legislatore europeo richiede che per ogni finalità del trattamento venga espressamente dato un consenso, con la conseguenza che l'interessato dovrà acconsentire, ad esempio, alla registrazione dei propri dati ma anche, con un apposito e separato consenso, alla cessione a terzi.

[25] Si veda V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, p. 48 ss., in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, cit.; C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, Giappichelli 2021, pp. 50-56.

[26] Così F. G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, ESI, Napoli, 2008, pp. 153-175: «I dati personali si configurano come beni giuridici, centro di riferimento di situazioni soggettive plurime e distinte, secondo che si consideri la posizione dell'interessato – titolare istituzionale e organico dei dati -, ovvero la posizione riservata ai terzi qualificati in rapporto al loro interesse alla raccolta dei dati e al relativo trattamento. Proprio sotto questo profilo si differenziano da tutti gli altri beni giuridici: da un lato, si atteggiano come elementi costitutivi dell'identità personale dell'interessato; dall'altro, contengono in sé l'attitudine a rilevare come risorsa oggetto, non di appropriazione bensì di accesso, non di un'attività di godimento bensì di un'attività di trattamento da parte di terzi per specifiche finalità meritevoli»

[27] *Linee guida 5/2020 sul consenso ai sensi del Regolamento (Ue) 2016/679*, adottate dall'EDP il 4 maggio 2020.

alla limitazione del trattamento, così come riportato, sarebbe invece giustificabile affermando che con il consenso l'interessato non trasferisce la proprietà dei propri dati personali ma, più semplicemente, ne autorizza l'uso con la possibilità, prevista *ex lege*, di limitarlo in alcuni casi unilateralmente, quando addirittura revocarlo.

Alle stesse conclusioni, parimenti, si può giungere facendo riferimento al diritto di revoca ex art. 7, par. 3 del Reg. 679/2016 il quale, nel suo concreto esplicarsi, consentirebbe all'interessato di agire unilateralmente nei confronti del titolare del trattamento, inficiandone l'acquisito diritto di proprietà dei dati.

5. *Luci e ombre della Direttiva Ue 2019/770 sulla fornitura di servizi e contenuti digitali*

Quanto sin qui affermato circa la possibilità di riconoscere ai dati personali un valore patrimoniale, tale per cui è oggi possibile parlare addirittura di "monetizzazione", è stato definitivamente positivizzato dalla Direttiva Ue 2019/770, recepita da ultimo con il D. Lgs. n. 173 del 4 novembre 2021.

La Direttiva, emanata con l'obiettivo di omogeneizzare la normativa relativa ai contratti di fornitura di servizi e contenuti digitali tra operatori economici e consumatori, prevede espressamente (art. 3) quale ambito di applicazione quei contratti in cui il professionista fornisca contenuti o servizi digitali e il consumatore fornisca i propri dati personali, quando questi dati siano diversi e ulteriori rispetto a quelli forniti in quanto necessari all'esecuzione del contratto[28] o diversi da quelli trattati per obbligo di legge.

Alla stregua di una tale previsione, dunque, è ormai pacifico, pur rimanendo sempre valide le perplessità in passato avanzate dalla Autorità Garante per la Protezione dei Dati Personali[29] italiana e dall'European Data Protection

[28] Per un approfondimento si veda: A. DE FRANCESCHI, *La Circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura di contenuti digitali*, in A. MANTELERO, D. OLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, pp. 203-218.

[29] Si veda, in proposito, quanto affermato dall'allora Presidente Antonello Soro in occasione della Relazione Annuale per l'anno 2018.

Supervisor[30], che sia possibile concludere un contratto di fornitura di un servizio o contenuto digitale fornendo i propri dati personali (o meglio, come qui si ritiene, autorizzandone l'uso) a titolo di controprestazione, ulteriori e diversi rispetto a quelli necessari per l'esecuzione del contratto o per obbligo di legge.

Occorre, però, procedere con una doverosa precisazione: la legittimità del trattamento dei dati personali, forniti a titolo di "prezzo" del servizio o contenuto digitale, dovrà passare non solo il vaglio della normativa introdotta dalla Direttiva Ue 2019/770, ma, ovviamente, anche quello del Regolamento Ue 679/2016, il quale costituisce la disciplina di riferimento per valutare la legittimità di ogni trattamento di dati personali.

Quindi, trovando legittimità il trattamento dei dati personali quali merce di scambio nella base giuridica del consenso, questo dovrà rispettare quanto previsto dall'art. 6, par.1, lett. a) e dall'art. 7 del GDPR, dovendo essere libero[31] e informato[32], nel senso che l'interessato dovrà aver previamente ricevuto una chiara e semplice informativa che indichi che i suoi dati personali avranno la funzione di moneta di scambio per il servizio offerto.

Sul piano dell'asimmetria contrattuale tipica del rapporto consumatore-professionista[33], l'interessato dovrà ricevere anche adeguate informazioni precontrattuali circa gli elementi essenziali del contratto e quindi, per quanto qui interessa, informazioni circa il prezzo del servizio offerto, il quale dovrà essere qualificato (e auspicabilmente anche quantificato, nel rispetto del principio di minimizzazione) nei dati personali del soggetto interessato. Nella prospettiva negoziale troveranno applicazione anche tutti gli altri istituti rimediali previsti dalla legislazione consumeristica, nonché tutti gli istituti tipicamente contrattuali previsti dalla normativa ordinaria.

Se, è indubbio, che la nuova normativa riguardante la fornitura di servizi e

[30] *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017.

[31] Circa la libertà del consenso all'interno dello scambio servizio digitale-dati personali si veda: C. IRTI, *Consenso negoziato e circolazione dei dati personali*, cit., pp. 90-102.

[32] Artt. 12, 13 e 14 del GDPR.

[33] Si vedano in proposito i provvedimenti dell'Autorità garante per la concorrenza e per il mercato: n. 27432, adottato il 29 novembre 2018 nei confronti di Facebook Ireland Ltd; n. 29890, adottato il 16 novembre 2021 nei confronti di Google Ireland Ltd; n. 29888 del 9 novembre 2021 nei confronti di Apple Distribution International Limited.

contenuti digitali abbia sicuramente avuto il merito di dare un contributo importante al riconoscimento del valore commerciale dei dati personali, attribuendone quindi implicitamente valore patrimoniale, tuttavia non poche incertezze permangono nella sua applicazione pratica.

Si fa riferimento, per quanto oggetto di questa trattazione, alla considerazione che la Direttiva, specificando a quali tipologie di servizi digitali debba trovare applicazione[34], relativamente ai servizi digitali utilizzati nell'ambito sanitario nega l'applicabilità della disciplina qualora si tratti di servizi sanitari strettamente finalizzati a valutare, mantenere o ristabilire lo stato di salute, compreso l'uso dei dispositivi medici[35] strettamente correlati. Non viene fatta menzione, invece, di tutte quelle attività sanitarie accessorie che prevedono comunque l'uso di servizi e contenuti digitali ma non specificamente strumentali a valutare, mantenere o ristabilire lo stato di salute del paziente. Si fa riferimento, dunque, a quegli strumenti, ad uso ancora più massivo rispetto ai "dispositivi medici", comunque utilizzati in ambito sanitario per trasferire regolarmente grandi quantità di dati relativi alla salute e che, quindi, sembrerebbero poter essere remunerati anche mediante l'uso di dati personali dei pazienti.

Questo aspetto problematico, centrale nel presente lavoro al fine di porlo all'attenzione degli studiosi della materia, verrà affrontato analizzando la normativa relativa il trattamento delle "categorie particolari di dati", con l'obiettivo di valutare se sia possibile, e come, utilizzare i dati personali dei pazienti quale moneta di scambio per i servizi e contenuti digitali utilizzati in ambito sanitario diversi da quelli esclusi dalla Direttiva 2019/770. Ipotesi non peregrina ove si prenda in considerazione sia la grave situazione economica di molte realtà sanitarie del Servizio Sanitario Pubblico, sia, soprattutto, la forte impronta commerciale caratterizzante la sanità privata, la quale potrebbe identificare nei dati dei pazienti una nuova e ulteriore fonte di guadagno.

[34] Dir. Ue 2019/770, art. 3, c.5, lett. c).
[35] Così come definiti dall'art. 3, lett. a), della Direttiva 2011/24/UE.

6. *Servizi e contenuti digitali in ambito sanitario: l'eHealth in Italia ed Europa*

Sempre più spesso, anche grazie al rapido progredire della tecnologia e della ricerca scientifica che ne è conseguenza, si fa largo uso in ambito medico di strumenti digitali per differenti finalità, quali una migliore organizzazione e gestione del paziente o la fornitura di cure mediche particolari e innovative (anche nell'ambito di studi medici integrati e finalizzati a progetti di ricerca scientifica) o semplicemente la digitalizzazione di pratiche "analogiche" già in essere.

Negli ultimi due anni, inoltre, la digitalizzazione del settore sanitario ha subito una forte accelerazione dovuta alla pandemia da Covid19, la quale ha richiesto un ingente uso delle tecnologie informatiche in ambito medico per fare fronte sia alle conseguenze derivanti dalla lontananza tra servizio sanitario e paziente, sia alla necessità di tracciamento dei soggetti positivi, la loro gestione, così come la condivisione ed elaborazione dei dati al fine di sviluppare strategie efficaci e condivise con tutti gli operatori del settore medico.

È bene, dunque, sottolineare come il crescente apporto tecnologico nel settore sanitario, se da una parte pone importanti questioni etiche e giuridiche (a cominciare, come si vedrà, dall'impatto sulla protezione dei dati personali dei pazienti), dall'altra acquisisce primaria rilevanza nel perseguire la tutela di un diritto fondamentale quale la tutela della salute, garantito dall'art. 32 della Costituzione.

Un simile riconoscimento è avvenuto anche a livello statale, tanto che la telemedicina e l'innovazione, la ricerca e la digitalizzazione dell'assistenza sanitaria, risultano quali finalità principali del *Piano Nazionale di Ripresa e Resilienza* (PNRR), dopo che il periodo pandemico ha evidenziato chiaramente i limiti del Sistema Sanitario attuale, da una parte esempio di importanti esperienze di eccellenza, dall'altra non ancora pienamente al passo con i tempi[36].

[36] L'Osservatorio *Innovazione Digitale in Sanità* della School of Management del Politecnico di Milano, relativamente all'anno 2021, ha evidenziato un incremento del 5% rispetto al 2019 degli investimenti fatti in sanità, raggiungendo un valore di 1,5 miliardi di euro, pari all'1,2% della spesa sanitaria pubblica complessiva.

Facendo riferimento ai servizi digitali attualmente utilizzati nel settore medico, quindi impiegati anche per trattare dati relativi alla salute dei pazienti, non si può non menzionare il Fascicolo Sanitario Elettronico (FSE) e il Dossier sanitario[37], la cartella sanitaria elettronica[38] ma anche tutti quegli strumenti di comunicazione tra medico e paziente quali i servizi di email, nonché altri servizi o app generiche di comunicazione o piattaforme appositamente create per consentire un'interazione paziente-medico-struttura sanitaria. Così come è necessario fare riferimento a tutti quei servizi che consentono di scaricare *offline* il referto elettronico di un esame (per accedere agli esiti degli esami di ricerca del virus Covid19 questi sistemi sono stati largamente impiegati, potenziati e perfezionati), nonché i servizi di telemedicina, finalizzati a garantire una vigile assistenza sanitaria nei casi in cui i pazienti siano lontani da struttura sanitarie o nel caso di pazienti affetti da cronicità tali da non richiedere la necessità di uno stabile ricovero ospedaliero. Sempre più, infine, sta irrompendo nel settore sanitario l'utilizzo di dispositivi indossabili che servono a monitorare il paziente in maniera continua, l'uso dell'Internet delle cose (IoT), l'utilizzo dell'Intelligenza Artificiale[39], la realtà aumentata ma anche il Cloud Computing[40] (diventato necessario nelle grandi strutture ospedaliere per fare fronte all'enorme quantità di documentazione cartacea presente per legge negli archivi e alla difficoltà di archiviarne nei *data center* fisici i corrispettivi elettronici, in quanto anche essi dotati di spazi esauribili[41]).

Il processo di digitalizzazione che negli ultimi anni sta interessando il nostro Paese, però, per avere una reale e concreta efficacia positiva, necessita altresì di un'integrazione con i sistemi che sono stati adottati dagli altri Stati, per lo meno quelli europei, affinché tutti siano reciprocamente compatibili tra loro in quanto

[37] Sul funzionamento e applicazione del Fse e del Dossier sanitario di vedano le *Linee guida in tema di fascicolo sanitario elettronico (Fse) e di dossier sanitario*, pubblicate dal Garante per la protezione dei dati personali con prov. n. 1634116 del 16 luglio 2009.

[38] Per approfondimenti circa il Fse e la Cartella elettronica si veda F. COVINO, *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in *Federalismi.it*, 5, 2021.

[39] Relativamente all'utilizzo dell'IA in sanità si veda G. VERLATO, M. L. RIZZO, A. GIANNINI, G. ROSATI, A. DELLI PONTI, *La sanità digitale*, in M. IASELLI (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè Francis Lefebvre 2020, pp. 180-185.

[40] Per approfondire i profili applicativi del C*loud* in ambito sanitario si veda L. DEGANI, A. LOPEZ, S. FAMILIARI, *L'applicazione del Gdpr privacy nei servizi sociosanitari*, Maggioli Editore, Santarcangelo di Romagna, 2018, pp.51-53.

[41] Così come previsto nel *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022*, pubblicato dall'Agenzia per l'Italia Digitale e Dipartimento per la Trasformazione Digitale.

basati sullo stesso linguaggio informatico. In termini tecnici si può parlare di interconnessione tra i diversi strumenti digitali, di vecchia e nuova generazione. Se così non fosse, infatti, il complesso delle innovazioni derivanti dalla digitalizzazione dei servizi sanitari rischierebbe di non avere un'efficacia positiva sul sistema sanitario ma, al contrario, di trasformarsi in una limitazione all'accesso alle cure per i pazienti a causa dei problemi tecnico-informatici che gli utenti potrebbero non essere in grado di superare.

Inoltre, a fronte di un sempre maggiore utilizzo della tecnologia in ambito sanitario per migliorare i servizi e le terapie offerte, se da una parte ciò richiede un'integrazione e comunicazione dei sistemi digitali utilizzati, dall'altra occorre prestare maggiore attenzione ai casi di violazione[42] dei dati digitalmente trattati, causa il loro crescente interesse per il fatto non solo di essere in grado di rivelare gli aspetti più intimi dell'interessato ma anche per aver acquisito un importante valore economico tale da spingere terzi ad entrarne illecitamente in possesso.

Della non trascurabile importanza della digitalizzazione del settore medico e sanitario e della considerazione del forte impatto che ciò ha sulla protezione dei dati personali ne è dimostrazione anche l'impegno profuso a livello sovranazionale, in ambito europeo[43], come è possibile rilevare leggendo tra gli obiettivi di transizione digitale previsti nel programma politico adottato dalla Commissione europea per il quinquennio 2019-2024[44], nonché leggendo il *Quadro finanziario pluriennale per il periodo 2021-2027*, approvato dal Consiglio dei ministri dell'Ue, che, prendendo atto delle evidenze poste in essere dal contesto pandemico, ha

[42] Da ultimo si ricordi il *data breach* che ha interessato le infrastrutture telematiche della Regione Lazio, creando molteplici problemi al sistema informatico sanitario e al sistema dedicato alle vaccinazioni contro il Covid19, nonché l'attacco informatico che ha coinvolto l'ospedale S. Giovanni di Roma o la ASL Roma3.

[43] Per una attuale ricostruzione del tema della protezione dei dati personali nel diritto UE nell'ambito emergenziale si veda C. FIORILLO, *La protezione dei dati personali nel diritto UE di fronte all'emergenza*, in S. STAIANO (a cura di), *Nel ventesimo anno del terzo millennio. Sistemi politici, istituzioni economiche e produzione del diritto al cospetto della pandemia da Covid19*, Editoriale Scientifica, Napoli, 2020, p. 435 ss.

[44] Si veda anche la "C*omunicazione sulla sanità e l'assistenza digitali*" dell'aprile 2018 che ha individuato i tre pilastri sui cui si deve fondare la digitalizzazione nel settore sanitario: 1- Accesso ai dati e condivisione sicura; 2- Collegare e condividere i dati sanitari per la ricerca, per una diagnostica più rapida e per una migliore sanità; 3- Rendere più autonomi i cittadini e potenziare l'assistenza individuale attraverso i servizi digitali.

programmato lo stanziamento di 1.074,3 miliardi di euro per i prossimi sei anni a sostegno del processo di digitalizzazione della sanità[45].

Ciò si rileva anche analizzando la definizione data dalla Commissione, la quale, prendendo atto dell'inscindibile connessione presente tra la tecnologia e l'assistenza sanitaria, identifica con i termini «sanità e assistenza digitali» quegli «strumenti e servizi che sfruttano le tecnologie dell'informazione e della comunicazione per migliorare la prevenzione, la diagnosi e il trattamento delle patologie, il monitoraggio e la gestione della salute e degli aspetti dello stile di vita che influiscono sulla salute. La sanità e l'assistenza digitali sono innovative e possono migliorare l'accesso all'assistenza e la qualità delle cure, ma anche aumentare l'efficienza complessiva del settore sanitario»[46].

Prendendo le mosse dalla definizione fornita dalla Commissione europea è possibile poi osservare come l'approccio da questa adottato non sia restrittivo ma aperto all'utilizzo di una molteplicità di servizi digitali in ambito sanitario, che, sembra, non siano individuati solo in quelli previsti (ai fini di escluderli) dalla Direttiva Ue 2019/770. La definizione della Commissione europea comprenderebbe pure tutti quegli strumenti, anche accessori, che migliorano l'efficienza complessiva del settore sanitario, dunque anche tutti quei servizi digitali che sarebbero invece esclusi da quel fenomeno di "patrimonializzazione" dei dati personali nella sanità digitale preso in considerazione dalla Direttiva Ue 2019/770.

Da sottolineare, infine, come per il raggiungimento di un sistema sanitario digitale veramente efficiente sia necessario un lavoro e un dialogo congiunto dei singoli stati membri dell'Ue, viste le limitate competenze in capo all'Unione europea in materia rispetto a quanto riconosciuto ai singoli stati membri i quali ancora mantengono ampi poteri di legiferazione e governo dei sistemi sanitari nazionali[47].

---

[45] Rispetto all'intervento dell'Unione europea a sostegno della digitalizzazione della sanità degli Stati membri si veda R. MICCÙ, *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *Federalismi.it*, 5, 2021, pp. 5 e 6.

[46] Questa la definizione riportata sulla pagina Internet della Commissione europea "*Public Health*", raggiungibile al seguente indirizzo: https://ec.europa.eu/health/ehealth-digital-health-and-care/overview_it#:~:text=Per%20%22sanit%C3%A0%20e%20assistenza%20digitali,vita%20che%20influiscono%20sulla%20salute

[47] Per approfondimenti relativi ai rapporti Ue-Stati membri in relazione le competenze inerenti la sanità pubblica di veda R. MICCÙ, *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, cit., p. 2 ss.; F. ROLANDO, *La tutela della salute nel diritto dell'Unione Europea in risposta all'emergenza*, in S. STAIANO (a cura di), *Nel Ventesimo*

7. *Il trattamento delle "categorie particolari di dati": i dati relativi alla salute*

L'impiego della tecnologia in ambito sanitario, al servizio della tutela del diritto alla salute, pone però la necessità di un attento contemperamento tra diversi interessi giuridicamente rilevanti, quali, appunto, la tutela della salute costituzionalmente garantita, ma anche il diritto all'utilizzo di mezzi tecnologici, più precisamente riconosciuto come "libertà informatica"[48] e, per quanto qui propriamente rileva, il diritto alla protezione dei dati personali[49], nello specifico dati "super sensibili"[50] che, trattati con le modalità e garanzie previste dal Regolamento Ue 679/2016, potrebbero anche divenire, con i relativi rischi e criticità, valore di scambio quale controprestazione, anche parziale, dei servizi digitali forniti in applicazione della Direttiva Ue 2019/770.

Occorre, dunque, delineare come è concretamente possibile trattare i dati relativi alla salute, per poi, una volta chiarito il contesto normativo, verificare se è possibile parlare di "monetizzazione" di questo tipo di dati in riferimento ai servizi digitali impiegati in ambito sanitario, sempre tenendo presente l'espressa esclusione che la Direttiva di riferimento riserva al trattamento effettuato nell'ambito dei servizi sanitari strettamente finalizzati a valutare, mantenere o ristabilire lo stato di salute, compreso l'uso dei dispositivi medici.

Quali *species* del *genus* "dati personali", i dati "relativi alla salute" sono quei dati in grado di rivelare informazioni riguardanti lo stato di salute fisica e mentale dell'interessato, siano esse sotto forma di un numero, un simbolo o di informazioni

anno del terzo millennio. Sistemi politici, istituzioni economiche e produzione del diritto al cospetto della pandemia da Covid -19, cit., p. 417 ss.

[48] Sulla definizione si veda V. FROSINI, *L'orizzonte giuridico dell'internet*, in *Dir. inf.*, 2, 2000, p. 275: «non libertà da, ma libertà di, che è quella di valersi degli strumenti informatici per fornire ed ottenere informazioni di ogni genere».

[49] Sulla necessità di trovare un necessario equilibrio tra tutela della salute e il diritto alla riservatezza personale, si rinvia al lavoro di F. COVINO, *Uso della tecnologia e protezione dei dati personali sulla salute tra pandemia e normalità*, in *Federalismi.it*, 5, 2021, p. 42 ss.

[50] Secondo la giurisprudenza i dati relativi alla salute sono dati "super sensibili" poiché riguardano la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate. Come tali, ad essi va garantita una protezione rafforzata (*ex multis*, Cons. di Stato, Sez. V, Sent. n. 5378, del 27/11/2015; Cons. di Stato, Sez. V, Sent. n. 2511 del 27/05/2008; Cass. civ., Sez. I, n. 14390 del 08/07/2005, in *Pluris*).

riguardanti esami e controlli[51], finanche dati di carattere amministrativo che rivelino la sottoposizione a determinati esami clinici o a ricoveri ospedalieri[52].

Per quanto attiene a questa categoria particolare di dati personali, il legislatore europeo ha espresso chiaramente un divieto di trattamento (art.9, par. 1, Reg. Ue 679/2016), riconoscendo però espresse eccezioni, in questo caso al fine di non paralizzare l'attività sanitaria. L'obiettivo del legislatore, mediante la normativa richiamata, è quello di garantire una protezione rafforzata per questa tipologia di dati personali, nello specifico riconoscendone la legittimità di trattamento nei casi previsti dalle lettere *a*/*c*/*h*/*i)* del paragrafo 2 dell'art. 9 GDPR.

Il trattamento di dati relativi alla salute è quindi legittimo quando l'interessato abbia prestato il proprio consenso, rafforzato dalla caratteristica di dover essere «esplicito»[53], dunque un consenso che sia possibile percepire, sia esso orale o in forma scritta, e che il titolare dovrà dare prova di aver acquisito, ad esempio utilizzando moduli e registrazioni o, come avviene nel contesto digitale, moduli elettronici, email, finanche apposite "caselle da spuntare" e dalle quali sia chiaramente evincibile la funzione e le conseguenze dell'azione digitale posta in essere.

Il trattamento di dati relativi alla salute è parimenti legittimo quando è necessario per tutelare l'interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'impossibilitò fisica o giuridica di prestare il proprio consenso; per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali; per motivi di

[51] Secondo il considerando 35 del Reg. Ue 679/2016: «nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro».

[52] Per la rilevanza di tali dati già attualmente in campo di assicurazioni sulla vita e sanitarie si veda E. BATTELLI, *Insurtech ed evoluzione dell'offerta di polizze sanitarie: tra innovazione tecnologica e nuovi servizi assicurativi in campo medico*, in *Contratto e impresa*, 1, 2022, p. 52 ss.

[53] A riguardo si vedano le *Linee guida 5/2020 sul consenso ai sensi del regolamento (Ue) 2016/679*, adottate dall'EDPB il 4 maggio 2020.

interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri di elevata qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici. Sempre, ovviamente, previa informativa prestata ai sensi degli artt. 13 e 14 del GDPR.

Quanto alle basi giuridiche appena richiamate, al fine di verificare se è possibile utilizzare i dati relativi alla salute come vera e propria moneta di scambio, nei limiti dei dati non esclusi già dalla Direttiva, risulta di immediata evidenza come solo il consenso e i motivi di interesse pubblico nel settore della sanità pubblica potrebbero, in astratto, essere presi in considerazione. Ciò in quanto le altre basi giuridiche previste dalla normativa a legittimazione del trattamento dei dati relativi alla salute (trattamento necessario per tutelare un interesse vitale; trattamento necessario per esercitare/difendere un diritto in sede giudiziaria; trattamento necessario per finalità di medicina preventiva…) sono limitate dal legislatore a specifiche finalità di trattamento, non essendo quindi possibile "piegarle" a finalità diverse da quelle predeterminate, quale potrebbe essere, invece, la "finalità di monetizzazione".

8. *Consenso e interesse pubblico nel settore della sanità pubblica quali basi giuridiche legittimanti la monetizzazione dei dati relativi alla salute?*

Quanto alla base giuridica del consenso[54] esplicito dell'interessato, questo ha rappresentato in passato[55] (in applicazione del D. Lgs. 196/2003, c.d. "Codice Privacy"), prima dell'introduzione del nuovo Regolamento Ue 679/2016 e dell'emanazione del relativo decreto legislativo di attuazione (D. Lgs. 101/2018), la

[54] Quanto al valore riconosciuto al consenso in ambito sanitario prima dell'introduzione del GDPR, si veda: S. VICIANI, *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. crit. dir. priv*., 2007, p. 321 ss., per il quale il consenso si presenta come «il mezzo tecnico per esprimere quella libertà di autodeterminazione insito nel riconoscimento del valore giuridico di una persona» e si sostanzia in operazioni di significato transattivo essendo tendenzialmente lasciata al soggetto «la facoltà di scegliere se instaurare una relazione con il destinatario dell'atto autorizzativo e al tempo stesso di prefissare le condizioni a cui tale relazione deve conformarsi»;

[55] Sullo sviluppo storico della tutela dei dati relativi alla salute nella normativa italiana ed europea e nella giurisprudenza della Corte di Giustizia Ue si veda il prezioso studio di G. FARES, *Il dati relativi alla salute e i trattamenti in ambito sanitario*, in *Federalismi.it* - Osservatorio di Marzo 2018, pubblicato anche in L. CALIFANO e C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, p. 441 ss.

principale fonte di legittimazione del trattamento dei dati relativi alla salute, tanto che era generalmente praticata in ambito sanitario la somministrazione al paziente, insieme al modulo relativo al consenso informato al trattamento sanitario, di una dichiarazione precostituita con la quale egli acconsentiva al generale trattamento dei propri dati, compresi quelli relativi alla salute. Ciò, nella pratica, comportava che in mancanza del consenso al trattamento dei propri dati (spesso perché il paziente non era in grado di prestarlo in quanto in stato di incoscienza), il personale medico non potesse intervenire, comportando ciò gravi conseguenze sul diritto alla tutela della sua salute[56] (salva la prassi per cui in questi casi il consenso veniva acquisito successivamente, non appena possibile, operandosi il personale sanitario *in primis* per salvare la vita dell'interessato).

Proprio per superare una simile deriva, dovuta all'applicazione della normativa precedente, il legislatore, nel valorizzare la definizione riportata dall'art. 4 n. 11 del Reg. Ue 679/2016 in materia di consenso, così come specificato anche dal Considerando 42, ha fortemente affievolito l'ambito di applicazione del consenso quale base giuridica per il trattamento dei dati relativi alla salute. Infatti, come dimostrato dalla prassi, in questo caso il consenso non sarebbe mai libero poiché preclusivo dell'accesso all'assistenza sanitaria, costituendo così condizione essenziale per l'esecuzione della prestazione (come previsto dall'art. 7 n.4[57] del GDPR ai fini della valutazione della libertà del consenso).

Tale principio, fatto proprio anche dal D. Lgs. 101/2018, a modifica del D. Lgs. 196/2003, è stato infine chiarito dal provvedimento del 7 marzo 2019, n. 9091942 dell'Autorità Garante per la protezione dei dati personali, recante «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario»[58] e con il quale è stata introdotta la c.d. "finalità di

[56] Contrarietà al consenso per accedere ai servizi sanitari, in quanto non libero, è stata espressa, ad esempio, da G. FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in *Sanità pubblica e privata*, n. 2, 2009, p. 10 ss.

[57] L'art. 7, n.4 del Reg. Ue 679/2016, per valutare la libertà del consenso, prevede di prendere considerazione «l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».

[58] Si vedano anche le *Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19,* adottate il 21 aprile 2020 dall'EDPB.

cura" a legittimazione di tutti, e solo, quei trattamenti di dati relativi alla salute necessari a garantire la cura del paziente/interessato[59].

Il consenso, dunque, non può generalmente essere considerato una valida base giuridica legittimante il trattamento dei dati relativi alla salute in ambito sanitario, ad eccezione di quei casi in cui esso sia effettivamente libero in quanto non condizionato e preclusivo dell'accesso alle cure.

Se non è possibile utilizzare il consenso come base giuridica per trattare i dati personali relativi alla salute, come sopra descritto, bisogna tuttavia segnalare come tale principio valga solo per i trattamenti che siano strettamente finalizzati a garantire le cure al paziente, mentre non trovi applicazione, come espressamente sancito dal Garante[60], in tutti quei trattamenti "accessori" per i quali il consenso esplicito ritornerà ad essere la regola principale. Si fa riferimento, ad esempio, ai dati trattati mediante l'utilizzo di App mediche, trattamenti finalizzati alla fidelizzazione dei pazienti relativi al settore farmaceutico-sanitario o trattamenti effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali, così come l'utilizzo dei servizi di refertazione online o l'invio di dati relativi alla salute tramite posta elettronica. Fino all'utilizzo di strumenti quali l'archiviazione in cloud o l'uso di servizi di analisi dei dati mediante Intelligenza Artificiale creati e implementati da imprese fornitrici.

Si tratta, in effetti, di una moltitudine di attività che comportano, ugualmente, il trattamento di enormi quantità di dati relativi alla salute e che, dunque, dovranno soggiacere alla regola del consenso libero ed informato.

Per quanto qui di interesse, rispetto a queste attività, che non rientrano all'interno della definizione di "sanità" presa in considerazione dalla Direttiva 2019/770 per la quale il legislatore europeo ha espressamente vietato la monetizzazione dei dati personali, il soggetto interessato potrebbe, senza violare alcuna norma o

[59] Quanto previsto è motivato anche considerando che colui che chiede assistenza medica ad un medico professionista stia implicitamente acconsentendo al trattamento dei propri dati, sempre nei militi dell'attività di cura richiesta. In base a tale ricostruzione, dunque, il consenso non sarebbe stato espunto dalle basi giuridiche legittimanti il trattamento dei dati relativi alla salute, al contrario esso non richiederebbe più di essere prestato in quanto implicito nel comportamento concludente messo in atto dal paziente.

[60] Come riporta il provvedimento del 7 marzo 2019, n. 9091942 dell'Autorità Garante, «Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento)».

provvedimento, legittimare il trattamento dei propri dati relativi alla salute al fine di utilizzarli come valore di scambio per usufruire del servizio "accessorio" (quale l'iscrizione e l'utilizzo di app mediche, di solito apparentemente gratuite), così come autorizzare la struttura sanitaria ad utilizzare i propri dati come controprestazione per i servizi o contenuti digitali forniti da un terzo e poi messi a disposizione dei pazienti.

Oltre che tramite il consenso e la "scriminate di cura" (così come descritta nella sua definizione omnicomprensiva delle basi giuridiche previste dalle lettere *c* e *h* dell'art. 9, par.2 del GDPR), i dati relativi alla salute sono spesso trattati anche per «motivi di interesse pubblico nel settore della sanità pubblica[61]», in assenza del consenso dell'interessato. Si tratta, dunque, di una base giuridica volta non a tutelare la dimensione individuale dell'interessato di tutela della salute ma quella collettiva che legittima il trattamento dei dati al di là del consenso del paziente.

Tale base giuridica[62] rileva nel contesto di questo lavoro, volto ad indagare la possibilità e i rischi legati alla monetizzazione dei dati personali relativi alla salute, se si considera che per il significato da attribuire all'«interesse pubblico nel settore della sanità pubblica», il Considerando n. 54 richiama non solo gli elementi strettamente collegati con l'assistenza sanitaria ma, anche, le «risorse destinate all'assistenza sanitaria», la «spesa sanitaria e il relativo finanziamento». Prendendo le mosse dalla definizione appena riportata sarebbe dunque possibile, apparentemente, trattare i dati personali relativi alla salute anche per finalità che possiamo definire "economiche del settore sanitario pubblico". Se tale approdo viene calato nel contesto normativo sorto a seguito del recepimento della Direttiva Ue 2019/770 che, come è stato in precedenza sottolineato, consentirebbe l'utilizzo anche dei dati personali relativi alla salute come controprestazione dei servizi e contenuti digitali, ormai ampiamente utilizzati nel settore sanitario, e che non rientrino nella categoria dei servizi strettamente sanitari, è possibile pericolosamente affermare che il SSN potrebbe finanziare tali attività con i dati

[61] Art. 9, c.2, lettera i) del Reg. Ue 679/2016.

[62] Per approfondimenti sull'argomento si veda G. FARES, *Il dati relativi alla salute e i trattamenti in ambito sanitario*, cit., p. 441 ss.

personali dei propri pazienti, utilizzandoli come controprestazione, totale o parziale, rispetto al servizio o contenuto digitale fornito.

Se ad una simile ipotesi, non difficile da immaginare nella sua concretezza considerando le precarie condizioni economiche di molte strutture sanitarie pubbliche, si aggiunge che proprio tramite la base giuridica dell'interesse pubblico nel settore della sanità pubblica il SSN ha trattato una grandissima quantità di dati per fare fronte all'attuale contesto pandemico, si può immaginare come questi dati, applicando la Direttiva 2019/770 e nel rispetto delle informazioni previamente rese ai sensi degli artt. 13 e 14 GDPR (che dovranno dunque aver previsto fin dall'inizio la possibilità di utilizzo dei di quei dati anche per finalità di finanziamento) potrebbero, alla stregua dell'interpretazione normativa prospettata, essere utilizzati in futuro per finanziare, anche nell'interesse pubblico, quei servizi e contenuti digitali, che non siano strettamente medici, resi necessari per far fronte all'emergenza (quali, ad esempio, le App di *contact tracing*[63] "e simili"). Una simile conclusione, invece, non sarebbe possibile rispetto ai servizi sanitari offerti da strutture private in quanto la base giuridica prevista dall'art. 9, par.2, lettera *i*), trova applicazione esplicitamente solo nel settore della sanità pubblica, diversamente, invece, dall'«interesse pubblico rilevante», previsto dalla lettera *g)* della medesima disposizione, il quale trova applicazione, come riconosciuto[64], anche nei confronti delle strutture sanitarie private

9. *Conclusioni*

Le esigenze di efficientamento e sviluppo del settore sanitario, finalizzate a garantire un migliore servizio assistenziale al paziente lungo l'iter che lo vede passare dalla fase di ingresso e accertamento fino alle sue dimissioni, ha visto negli ultimi anni l'affermarsi del fenomeno della sanità digitale, caratterizzata da un

[63] Per approfondimenti relativi alle App di *contact tracing* e il loro impatto sulla protezione dei dati personali si veda C. COLAPIETRO, A. IANNUZZI, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, 2, 2020, p. 772 ss; A. BERNES, *Regolare la tecnologia di digital contact tracing alla luce della protezione dei dati personali*, in *Ius Civile*, 5, 2020, p. 1279 ss.

[64] Si veda in proposito la *Nota del Presidente del Garante, Antonello Soro, al Presidente del Consiglio dei Ministri, al Presidente della Conferenza delle regioni e delle province autonome e al Presidente dell'ANCI, in tema di trattamenti di categorie particolari di dati personali per motivi di interesse pubblico rilevante*, doc. web n. 9065601 del 27/11/2018.

sempre maggiore utilizzo delle tecnologie per lo svolgimento di attività sia strettamente di cura sia accessorie.

Si pensi, ad esempio, ai macchinari utilizzati per la diagnostica, spesso collegati con pc e appositi programmi per l'elaborazione dei dati, alle app, piattaforme e dispositivi indossabili impiegati nei progetti di telemedicina ma anche agli strumenti digitali (a partire dalla posta elettronica) usati per la gestione della comunicazione con il paziente. Si tratta di una molteplicità di strumenti differenti, che impiegano diverse tecnologie, tutti generalmente accomunati dallo svolgimento della necessaria attività di trattamento dei dati personali degli interessati/pazienti.

Nella prospettiva di indagine affrontata si è potuto rilevare come i contratti di fornitura di servizi e contenuti digitali siano stati interessati dalla recente riforma introdotta dalla Direttiva Ue 2019/770 al fine di dotare il settore di una disciplina uniforme che garantisca le parti contraenti, il consumatore e il professionista, ma allo stesso tempo tuteli la concorrenza all'interno del mercato europeo. La normativa, però, è intervenuta anche a legittimare quei contratti che prevedono l'utilizzo dei dati personali del consumatore (ulteriori rispetto a quelli necessari per fornire il servizio o per obbligo di legge) quale controprestazione rispetto al servizio o contenuto digitale oggetto del contratto, pur non riconoscendone espressamente la funzione di prezzo da pagare ma facendo chiarezza su una questione su cui dottrina e giurisprudenza si sono negli ultimi anni confrontati in maniera non unanime.

Numerosi sono i settori nei quali la disciplina trova espressamente applicazione. Vengono invece esplicitamente esclusi i "servizi sanitari[65]", ossia quei servizi finalizzati a valutare, mantenere o ristabilire lo stato di salute, così come i "dispositivi medici[66]" impiegati a tal fine.

Non vengono, invece, presi in considerazione tutti quei servizi accessori e collaterali alle attività strettamente mediche ma che hanno ugualmente

[65] Dir. Ue 2019/770, art. 3, c.5, lett. c).

[66] Così come definiti dall'articolo 3, lett. a), della Direttiva 2011/24/UE.

implementato l'utilizzo di tecnologie digitali, ancor di più durante l'attuale periodo pandemico.

A ben vedere, dunque, i servizi e i contenuti digitali accessori all'attività prettamente medico-sanitaria dovrebbero rientrare nell'applicazione della Direttiva Ue 2019/770, potendo dunque essere forniti contro l'uso dei dati personali dei pazienti.

Tuttavia, potendo rientrare nel trattamento non solo dati comuni ma anche dati appartenenti a "categorie particolari", quali quelli relativi alla salute dei pazienti, ciò potrà avvenire solo in presenza delle basi giuridiche previste dall'art. 9 del Reg. Ue 679/2016 e ritenute idonee a tal fine (consenso e interesse pubblico nel settore della sanità pubblica), tenendo sempre ben presente il principio generale di divieto di trattare dati relativi alla salute.

Quanto al consenso al trattamento, quale base giuridica potenzialmente più utilizzata a tal fine, vista la natura economica e contrattuale delle operazioni prese ad esame, la monetizzazione dei dati personali relativi alla salute potrà riguardare solo un'operazione economica che, in un'ottica funzionale, si realizzi tramite un accordo negoziale atipico di trasferimento in uso ai fini di trattamento dei dati (sanitari). Con a fondamento, quindi, un interesse negoziale meritevole di essere perseguito (la tutela della salute), sulla base dell'assunto che il limite al non utilizzo dei dati personali non sia inviolabile, bensì superabile tramite un consenso rafforzato e procedimentalizzato come tecnica circolatoria delle situazioni esistenziali diverse da quelle patrimoniali.

Vista l'importanza che i dati personali rivestono nell'attuale società digitale e viste le criticità peculiari dei dati relativi alla salute, la possibilità di riconoscere a questi valore e funzione economica nei termini fin qui riportati richiede una attenta riflessione circa la sua opportunità, finanche un intervento del legislatore teso a regolare il fenomeno se non addirittura, valutati i rischi, un intervento correttivo atto a vietarlo espressamente intervenendo sulla lettera della legge al fine di non lasciare, così come sembra attualmente possibile, eventuali possibilità di monetizzazione dei dati sanitari trattati per fini che non sono strettamente sanitari

così come già escluso dalla Direttiva 770/2019, evitando, quindi, che siano gli operatori del settore a segnare la strada da percorrere in un mondo, quello digitale, dove tutto è permesso e ciò che è vietato non sempre è facilmente perseguibile.