Le *Femtech*: quando la fuga dei dati sanitari lede il «right to intimate privacy»

di Maria Vittoria Malinconi

Abstract: *Femtech: when the leak of health data undermines the «right to intimate privacy»* – The article aims to focus on the Femtech-phenomenon: Health-app addressing an array of "female" health needs that seems poisoned by risks in terms of privacy and personal freedom. In the United States, millions of women-users urgently need protection because of an almost total lack of regulation and the risk of criminalization in the new post-Dobbs world. Through comparison with the European Union legal framework, I intend to stimulate a general reflection: the new technologies' "regulatory challenges" to the traditional right to privacy not only make clear that GDPR is not a panacea, but also the need to change approach.

Keywords: Femtech; Health-app; United States of America; Women's health data; Privacy

1. La salute digitale: una panoramica

La pervasività delle nuove tecnologie ha ormai plasmato anche il settore sanitario, al punto che è stato coniato un nuovo archetipo di sanità: la cd. sanità digitale (*eHealth*). Un «broad umbrella term»[1], come chiarisce l'organizzazione mondiale della sanità, in cui è compresa anche la cd. sanità mobile (*mHealth*), che a sua volta qualifica «la pratica della medicina e della sanità pubblica supportata da dispositivi mobili, quali telefoni cellulari, dispositivi per il monitoraggio dei pazienti, computer palmari (PDA) e altri dispositivi senza fili»[2].

È questa la cornice che inquadra applicazioni sanitarie (d'ora innanzi: *Health-app*) progettate per essere installate e utilizzate sui più comuni *devices* e capaci di monitorare la salute dell'utente. Nello specifico, queste applicazioni *software*, attraverso la richiesta costante di inserimento dati – sanitari, comportamentali, personali – elaborati dall'intelligenza artificiale, restituiscono *outputs* che possono incidere sul benessere psico-fisico e/o sullo stile di vita del destinatario del servizio digitale, anche senza specifico controllo medico.

Da esse è possibile, e opportuno, distinguere le applicazioni (d'ora innanzi: app) utilizzate dalla telemedicina che tendono a ripristinare, seppur a distanza, il rapporto medico-paziente nell'ambito della prevenzione, diagnosi

[1]OMS, *Global Strategy on digital health 2020-2025*, 2021.
[2]OMS, *mHealth-New horizons for health through mobile technologies*, *Global Observatory for eHealth series*, V.3, 6.

DPCE online
ISSN: 2037-6677

e assistenza medica[3]. Le più generiche *Health-app* si basano, infatti, su una forma di interazione a carattere esclusivo tra il *software* e il "paziente", il quale si troverà ad agire nella più ampia veste di "utente" di un servizio digitale di tipo medico collocato al di fuori del tradizionale rapporto terapeutico[4].

La capillare diffusione di suddette app se, da una parte, incoraggia anche la costruzione di un'inedita autodeterminazione sanitaria della persona, dall'altra, basandosi sul trattamento quasi esclusivamente automatizzato di dati sensibili, crea fonti di rischio altrettanto inedite[5].

La digitalizzazione e l'impego di sempre più sofisticate tecnologie in un settore critico come quello sanitario ha determinato una "datizzazione" dei pazienti senza precedenti ed è proprio la nuova centralità del *dato sanitario* nell'esercizio dell'attività di cura a richiedere una riconsiderazione delle tradizionali categorie di settore[6]. In tale contesto, le *Health-app*, il cui funzionamento si basa sulla raccolta ed elaborazione di dati sensibili, unitamente alle peculiarità del *mobile-ecosystem* – come l'ubiquità e continuità della comunicazione –, sollevano significative problematiche, di cui il diritto deve farsi carico. Tra di esse, si rileva, in particolare, la tutela della *privacy* nella cd. "*third party request*" e, quindi, nel possibile utilizzo dei dati da parte di soggetti estranei al rapporto terapeutico o per finalità non terapeutiche[7].

Il presente contributo è volto all'analisi del recente fenomeno della "*mHealth-femminile*", che offre occasioni di riflessione in considerazione delle peculiarità che lo denotano. L'analisi giuridica riguarderà in particolar modo il quadro normativo statunitense che meglio evidenzia, data l'assenza di un'adeguata regolamentazione giuridica, le criticità in punto di lesione dei diritti fondamentali legati all'uso di specifiche *Health-app*. Il fine ultimo sarà

[3]Si tratta di applicazioni *software* volte alla raccolta e allo scambio di dati sanitari per consentire una visita medica e/o un confronto a distanza con il medico oppure il monitoraggio da remoto dei parametri vitali di un paziente affetto da patologie croniche (come il diabete). La pandemia da Covid-19 ne ha decretato un aumento esponenziale. Sul tema, cfr. L. Ferraro, *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, in *Dir. informaz.*, 2022, 837-866.

[4]I. Rapisarda, *La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche*, in *Nuove leggi civ. comm.*, 1/2023, 186. A titolo d'esempio, si citano alcune app disponibili sulle piattaforme iOS e Android che promettono di: suggerire programmi nutrizionali personalizzati e finalizzati al controllo del peso o alla riduzione della massa grassa (come *Lifesum)*, supportare l'utente nella gestione delle proprie emozioni e del proprio benessere mentale (come *Mindspa)*, migliorare la salute dell'occhio con *workout*-personalizzati (come *Ginnastica oculare*), monitorare l'andamento del diabete (come *MySugr* nella versione base).

[5]Sul binomio sanità digitale e protezione dei dati personali e sulla centralità del dato sanitario nella funzione di cura oltreché nel progresso scientifico ed economico, v. i significativi approfondimenti presenti nel recente volume di G. Cerrina Feroni (a cura di), *Le nuove frontiere della medicina. Assetti istituzionali e gestione dei dati*, Il Mulino, 2024, e, segnatamente, lo scritto di F. Mattei, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie*, 125 ss.

[6]C. Di Costanzo, *L'impiego delle nuove tecnologie nel settore della salute: problematiche e prospettive di diritto costituzionale*, in *Consulta Online*, I/2023, 218. L'autrice sottolinea come la (cyber)sicurezza sanitaria, la tutela dei dati sanitari, il consenso informato, la responsabilità-responsività sanitaria «sono attualmente soggette a importanti modificazioni e trasformazioni in atto in quanto operanti nel settore della salute digitale».

[7]CNB, *"Mobile-health"e applicazioni per la salute: aspetti bioetici*, 28-05-2015, 10.

quello di stimolare, per il tramite della comparazione con il quadro normativo dell'Unione europea, una riflessione generale.

2. La salute femminile *a prova di* app: il caso "*Femtech*"

«What female health needs through technology is Femtech»[8].

Descrive così il fenomeno Ida Tin, imprenditrice danese e ideatrice della prima applicazione per il tracciamento e il monitoraggio del ciclo mestruale femminile[9]. Nel 2013, non appena messa in commercio, quest' app decolla, creando un nuovo mercato definito dal neologismo «Femtech». Un termine che, oggi, qualifica un'intera industria in cui sono comprese *startup* progettate per monitorare oltre novanta condizioni diverse di salute femminile[10] e a cui risponde un valore di mercato che si stima possa raggiungere la soglia di 60 miliardi di dollari entro il 2027[11]. Non solo app per il tracciamento del ciclo mestruale, ma, più in generale, tecnologie finalizzate a una più efficace gestione di condizioni sanitarie psico-fisiche tipicamente femminili[12] come l'infertilità, la gestazione, la menopausa finanche coadiuvare la diagnosi precoce di patologie oncologiche[13].

Il filo rosso che accomuna le *Femtech-apps*, in particolare, è il trattamento di informazioni personali plurime[14] richieste con regolarità alla donna-utente e che, elaborate dall'intelligenza artificiale, sono restituite in

[8]I. Tin, *The rise of a new category: Femtech*, 15-09-2016, Blog, in www.helloclue.com.

[9]Nel 2011 a Berlino progetta "*Clue*": la donna, mese dopo mese, inserisce informazioni che, elaborate dall'AI e visualizzate sottoforma di calendario, sono restituite in chiave di *output* e tradotte nella previsione dell'andamento ovulatorio e mestruale del ciclo successivo.

[10]C. Tarabbia, *L'evoluzione tecnologica digitale per la salute della donna: luci ed ombre in medicina*, in *BioLaw Journal*, 3/2023, 16.

[11]Emergen Research, *Femtech Market by Type, by End-Use, by Application, by Region, Forecasts to 2027*, giugno 2021, in www.emergenresearch.com (è prevista una crescita annua del 15.6 percento a livello globale, il cui 40 percento arriva dal Nord America). Tale indice è ancor più di rilievo quando si considera che la maggior parte delle *Femtech-apps* è ad uso gratuito: l'alto profitto deriva dalla vendita dei dati sanitari riproduttivi a terze parti (cfr. *infra* par. 2.2).

[12]D. K. Citron, *A New Compact for Sexual Privacy*, in 62 *William & Mary Law Review*, 2021, 1774 («Far more extensive, however, is the tracking of women's health. The term "femtech" describes apps, services, products, and sites that collect information about women's period cycles, fertility, pregnancies, menopause, and sexual and reproductive histories»). Il termine richiama un'industria caratterizzata da varie soluzioni di AI applicata alla salute femminile. Pur nel riconoscimento dell'ampiezza e specificità del settore, questo articolo si concentrerà maggiormente sulle *Femtech-apps*.

[13]Alcune *startup* hanno progettato *software* a fini diagnostici: come "EVA-COLPO", lanciato sul mercato nel 2022 da *MobileODT* per il carcinoma del collo uterino e "MIA" il software AI creato da *Kheiron Medical Technologies Ltd.* per il carcinoma mammario.

[14]Per l'accesso e l'utilizzo di queste app sono richieste eterogenee informazioni di carattere "personale". Tra queste: i dati anagrafici; gli "indicatori" biologici (come la temperatura basale, il flusso mestruale e lo stato del muco cervicale o della cervice uterina); i dati cd. *"sensibili"*, come l'orientamento, l'attività e la vita sessuale, l'assunzione di droghe/alcool, ma anche i dati sanitari, in generale, e, nello specifico, i dati sanitari riproduttivi (come "la storia abortiva" o la gravidanza, ove si registrano anche i dati fisiologici del feto). Cfr. K. Levy, *Intimate Surveillance*, in 51 *Idaho L. Rev.*, 2015, 679.

DPCE online
ISSN: 2037-6677

veste di informazioni nuove che influenzano le scelte della donna sul proprio corpo e, quindi, sul proprio benessere psico-fisico.

2.1 [Segue] Poche luci…

Attorno all'industria *Femtech* gravita la retorica del cd. "*empowerment*-femminile": la promessa è quella di assicurare alle donne il controllo sulla propria salute e sul proprio corpo. D'altronde, il motivo per cui questo fenomeno, in tempi brevissimi, ha avuto un successo di portata mondiale[15] è attribuibile, in particolare, al fatto che le nuove tecnologie hanno soddisfatto un bisogno comune a milioni di donne.

Femtech nasce come vera e propria arte *tecnica*, richiamandone il cuore etimologico greco, dove "*téchne*" è in generale la capacità di operare usando la propria perizia per risolvere un problema concreto. E, infatti, la prima di queste app è stata progettata da una donna *per* le donne al fine di soddisfare una comune necessità: garantire il diritto all'autodeterminazione sanitaria femminile. Un prezioso strumento per tutte le donne, ma specialmente per quelle che vivono in Paesi il cui retaggio culturale e sociale impedisce loro di cercare assistenza sanitaria ogniqualvolta ce ne sia il bisogno[16].

Il funzionamento delle *Femtech-apps*, basandosi sulla regolare richiesta di inserimento dati alla donna-utente, permette un monitoraggio quotidiano traducibile in "dato scientifico" utile ai medici nell'effettuare diagnosi complesse e nell'implementare la ricerca in un settore, quale quello della salute riproduttiva, storicamente «under-funded» e «under-studied»[17]. Al riguardo, in America, fino agli anni Settanta, le donne erano escluse da *trial* clinici a causa della diffusa convinzione che il ciclo mestruale potesse influenzarne in modo imprevedibile i risultati[18]. La drammatica sotto-rappresentanza femminile negli studi sulla progressione e il trattamento delle malattie influisce, oggi, negativamente sulla capacità del medico di fornire cure di alta qualità basate su dati empirici. L'utilizzo così diffuso di queste app (un terzo delle donne americane ne fa quotidiano utilizzo[19]) fornisce ai professionisti

[15]A partire dal 2016, lo sviluppo di *Femtech* ha interessato l'intero globo: la maggior diffusione si registra in Nord America, in Europa e in Asia. Gli Stati Uniti e il Regno Unito, in particolare, sono i Paesi leader con il maggior numero di aziende a livello mondiale. V. *FemTech Industry*, agosto 2022, in www.femtech.health.

[16]M. Sommer et al., *Period Poverty and Promoting Menstrual Equity*, in *Jama Health Forum*, 2021.

[17]A. Scatterday, *This is no Ovary-action: Femtech Apps Need Stronger Regulations to Protect Data and advance Public Health Goals*, in 23 *N.C. J.L. & Tech.*, 2022, 642.

[18]R. B. Merkatz, *Inclusion of Woman in Clinical Trials: A Historical Overview of Scientific, Ethical, and Legal Issues*, in 27 *J. Obst., Gyn. & Neonatal nursing*, 1998, 78-84.

[19]D. Rosato, *What Your Period Tracker App Knows About You*, 28-01-2020, in www.consumerreports.org. Nello specifico, le app di tracciamento del ciclo mestruale sono la IV app per la salute più popolare tra gli adulti e la II tra le adolescenti. Cfr. M. L. Moglia et al., *Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System*, in 127 *Obstetrics & Gynecology* 6, 2016, 1153.

del settore una quantità di dati aggregati utile a concorrere al soddisfacimento del *"gender-gap"* nella ricerca medica[20].

Nonostante quanto appena detto, il fenomeno presenta molte ombre: le *Femtech-apps*, se prive di adeguata regolamentazione giuridica, rappresentano una temibile fonte di rischio in termini di *privacy* e di libertà personale. In realtà, sebbene sia incontestabile il carattere sensibile e personale dei dati sanitari riproduttivi, questi sono regolarmente raccolti, aggregati, condivisi e venduti a terze parti.

Nei fatti, l'industria *Femtech*, forgiata sulla retorica dell'*empowerment* femminile, finisce per trasformare la donna in una "massa di dati preziosi".

2.2 [Segue] … molte ombre

Le *Femtech-apps* alimentano l'ecosistema digitale con un flusso significativo di dati sensibili venduti e/o condivisi a terze parti; nello specifico, ai *data brokers*, alle aziende di *data analytics*, alle agenzie pubblicitarie, finanche alle *Big-Tech* (come *Google* e *Facebook*).

I dati sono utilizzati per alimentare ed educare algoritmi destinati a prevedere i bisogni dell'utente al fine di strutturare politiche di pubblicità mirata attraverso la profilazione. Una profilazione finalizzata non solo al *marketing* aggressivo, ma anche a orientare delicati processi decisionali. Così, i dati sanitari di una donna infertile e affetta da gravi patologie potranno tradursi in pubblicità su costose tecniche di procreazione assistita, da un lato, nell' aumento degli oneri assicurativi e degli interessi sui prestiti, dall'altro, nell'impossibilità di ottenere l'assicurazione sulla vita, infine[21]. Interesse economico che, parimenti, induce i proprietari di queste app a raccogliere e aggregare quante più informazioni possibili: in un mondo in cui i dati personali sono diventati «the coin of the realm»[22], quelli riproduttivi sono tra i più redditizi[23].

Nell'era digitale, questo scenario preoccupa nei termini di protezione dei dati personali. Un timore certamente comune a tutte le app che partecipano alla creazione del nuovo ecosistema digitale, ma che si fa più forte in considerazione di *Health-app* che trattano dati di tal genere. I più recenti studi empirici sul tema evidenziano che il flusso dei dati avviene nella quasi totalità dei casi all'oscuro della donna-utente. Ebbene, quando i proprietari delle app vendono queste informazioni senza il consenso della donna compiono una lesione del cd. «right to intimate privacy»[24]. Tale declinazione del tradizionale «right to privacy» coglie l'unicità dei dati che le utenti, più o

[20]In proposito, v. A. Nowogrodzki, *Inequity in medicine*, in *Nature*, 2017, 550, e C. Moskowitz, *Fertile Ground: The Long-Neglected Science of Female Reproductive Health*, 1-05-2019, in www.scientificamerican.com.

[21]M. E. Gilman, *Feminism, Privacy and Law in Cyberspace* in D. Brake, M. Chamallas, V. L. Williams (Eds.), *Oxford Handbook of Feminism and Law in the U.S.*, Oxford, 2021, 552-572.

[22]D. K. Citron, *op. cit.*, 1767.

[23]In particolare, il dato di una donna in gravidanza in USA ha un valore quindici volte superiore rispetto a qualsiasi altro dato. Cfr. *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*, 9-09-2019, in www.privacyinternational.org.

[24]A. Scatterday, *op.cit.*, 643; D. K. Citron, *op. cit.*, 1768.

DPCE online
ISSN: 2037-6677

meno consapevolmente, condividono e che si inseriscono nel più intimo substrato della sfera personale femminile. Unicità che necessita soluzioni di diritto in grado di bilanciare l'esigenza di tutela senza incidere sul progresso scientifico ed economico.

3. Le *Femtech* nell'ordinamento americano: alcune criticità

Negli Stati Uniti è urgente la necessità di regolamentare il fenomeno a causa della mancanza di identità di tutela di questi dati sensibili tanto nella dimensione analogica quanto nella dimensione digitale. Si rifletta su un esempio di vita concreta: una donna, desiderosa di avere un figlio, si rivolge al ginecologo dopo aver sofferto aborti spontanei. Durante l'appuntamento lo specialista vorrà ricevere dalla paziente informazioni sul suo stato di salute, e non solo. Ebbene, nella realtà analogica la protezione di tali dati sensibili è assicurata dal segreto professionale e dall'obbligo di previa autorizzazione scritta in caso di divulgazione. Inoltre, se l'ufficio li trascrivesse nel *database*-digitale sarebbero comunque garantiti dalle misure di sicurezza informatica a cui deve adeguarsi. Si pensi, poi, alla stessa donna che, una volta a casa, inserisca nella *Femtech-app* le informazioni rivolte al medico poco prima. Nonostante queste siano le medesime – e medesima è l'esigenza di tutela – molto probabilmente – senza il suo consenso e senza notifica – saranno vendute a terze parti.

Tale scenario crea un'inedita fonte di rischio in termini di *privacy* e di libertà personale per milioni di donne americane a causa di una pressoché assente regolamentazione giuridica, da un lato, e del cd. "rischio di criminalizzazione" sorto nello scenario *post-Dobbs*, dall'altro.

3.1 Il *deficit* normativo

L'asimmetria di tutela richiamata poc'anzi è, in parte, causata dall'assenza di una legge organica atta a garantire la riservatezza dei dati personali. La disciplina statunitense in tema *privacy* appare estremamente complessa e disomogenea: a differenza di quella europea – compatta attorno al Regolamento per la protezione dei dati personali (d'ora innanzi: GDPR)[25] –, essa è frammentata non solo a livello verticale, tra Federazione e Stati[26], ma anche a livello orizzontale, essendo presenti leggi settoriali finalizzate alla regolamentazione di specifiche categorie di dati, come i dati commerciali e, appunto, sanitari.

Con riguardo al tema oggetto di questo articolo, sono da ricordare tre leggi federali.

[25]Regolamento (UE) 2016/679 (GDPR). In generale, in dottrina, cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; V. Zeno-Zencovich, *Data protection in the Internet*, in *Ann. dir. comp.*, 2018, 106 ss; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.
[26]D. K. Citron, *op. cit.*,1804 ss.

Anzitutto, il *Federal Trade Commission Act* (FTCA)[27] che, per il tramite della *Federal Trade Commission* (FTC), controlla le *Femtech-companies*. Nello specifico, l'art. 45, lett. a) FTCA, vieta ogni atto o pratica commerciale sleale o ingannevole. In tal senso, impone alle *Femtech-companies* di costruire informative *privacy* complete, intellegibili e non contraddittorie circa l'uso e la destinazione dei dati ivi raccolti. Inoltre, ai sensi di quanto previsto dall'*Health Breach Notification Rule* (HBNR)[28] dell'FTC, ogniqualvolta i dati sanitari siano stati oggetto di *"data-breach"* sussiste l'obbligo di notificarlo al consumatore. E, secondo l'interpretazione estensiva data dall'FTC del termine "*breach*" che qualifica nei termini di *violazione* anche la condivisione di dati sanitari senza l'autorizzazione dell'interessato[29], l'HBNR potrebbe disincentivare il costante flusso di dati sanitari a favore di terze parti.

Nonostante queste prescrizioni, il diritto di *privacy* delle consumatrici non sembra essere garantito sostanzialmente: da un lato, perché non sono previste misure di sicurezza informatica a cui quella particolare infrastruttura tecnologica deve adeguarsi per garantire la tutela dei dati ivi trattati; dall'altro, perché la sola notifica *ex post* non rappresenta per l'utente soddisfazione del danno causato dalla violazione. Sicché, l'FTC non è in grado di risolvere i rischi che gravitano attorno alle *Femtech-apps* in termini di «privacy e data security»[30].

La seconda legge da ricordare è il *Federal Food, Drug, and Cosmetic Act* (FDCA)[31], che, sotto il controllo del *Food and Drug Administration* (FDA), regolamenta i dispositivi medici. Tra questi rientrano, per qualificazione recente, i cd. *software application for contraception*: applicazioni che, attraverso l'utilizzo di sofisticati algoritmi, forniscono un servizio digitale di fertilità predittiva che giustifica la qualifica di "strumenti contraccettivi digitali"[32]. Suddetti *software*, appartenendo ai dispositivi medici di II Classe[33], devono adeguarsi a una serie di requisiti, compreso un complesso sistema di etichettatura, affinché sia garantita accuratezza, effettività e affidabilità in riferimento alla prestazione di un servizio digitale medico, quale quello di prevenire una gravidanza. Solo due app del panorama *Femtech* hanno ottenuto

[27] 15 U.S.C. §§ 41-58. Legge federale sulla protezione dei consumatori, adottata nel 1914 e da ultimo emendata nel 2022.

[28] 16 C.F.R. § 318 (2009). Implementa la s. 13407 dell'*American Recovery and Reinvestment Act* del 2009. Tutela, in linea generale, i dati sanitari che restano al di fuori dell'ambito applicativo dell'HIPAA (*v. infra*). La disposizione finale prevede, inoltre, un obbligo di notifica a favore dei *media* in caso di *data-breaches* che interessino almeno 500 utenti.

[29] *Complying with FTC's Health Breach Notification Rule*, 2022, in www.ftc.gov. Si veda anche la definizione di "*breach of security*" in 16 C.F.R. §318.2 (a).

[30] C. Rosas, *The future is femetch: Privacy and data Security Issues Sorrounding femtech Applications*, in 15 *Hastings Business Law Journal*, 2019, 334.

[31] 21 U.S.C. ch.9 § 301. *"Set of laws"* approvate nel 1938 dal Congresso al fine di attribuire all'FDA autorità di regolamentazione e controllo sulla sicurezza di alimenti, farmaci, dispositivi medici e cosmetici.

[32] 21 C.F.R. §884.5370 (2022).

[33] L'FDA classifica i dispositivi medici in base al "livello di rischio" per la salute pubblica: la I Classe comprende i dispositivi a basso rischio, la II Classe a rischio intermedio e la III Classe ad alto rischio. Per ognuna è prevista una forma di controllo a intensità graduale, molto lieve per i dispositivi di I, fino alla richiesta di PMA (*premarket-approval*) per quelli di III. Cfr. 21 U.S.C. §360c (a).

DPCE online
ISSN: 2037-6677

dall'FDA tale riconoscimento[34]; tutte le altre che restano al di fuori di suddetta regolamentazione: la legge esclude dalla qualificazione di dispositivo medico un prodotto che abbia come destinazione d'uso «mantenere o incoraggiare uno stile di vita sano»[35]. Pertanto, l'FDA non controlla centinaia di *Femtech-apps* prima che siano messe in commercio. Come evidenziato in dottrina[36], l'attività di controllo esercitabile dall'Agenzia federale potrebbe essere maggiore, in teoria, ma, in pratica, risulta improbabile a causa del tradizionale approccio "*hands-off*" nella regolamentazione delle applicazioni sanitarie. Un approccio che, in effetti, risponde alla più generale intenzione del Congresso di diminuire gli oneri normativi a carico delle emergenti app sanitarie al fine ultimo di incoraggiare il progresso[37].

Infine, le *Femtech-companies* sono potenzialmente soggette all'*Health Insurance Portability and Accauntability Act* (d'ora innanzi: HIPAA)[38], una risalente legge federale che tutela le cd. *Protected Health Information* (PHI), ovvero le informazioni sanitarie individuali e identificabili in ogni forma (inclusa quella elettronica), registrate o trasmesse esclusivamente da una "*covered entity*". In questa categoria, secondo quanto previsto dal *Code of Federal Regulation*, sono compresi unicamente: gli «health care providers and health care plans», le «clearinghouses», e i «business associates»[39]. Solo un ristretto numero di *Femtech-apps* rientra in quest'ultima categoria e, quindi, nell'ambito applicativo di suddetta legge[40]. Di conseguenza, la quasi totalità delle stesse resta al di fuori di questa regolamentazione.

Lo scenario così descritto fa emergere quanto sia auspicabile un'inversione di tendenza che, per il tramite di un controllo più stringente esercitabile dalle Agenzie federali competenti[41] o di un intervento legislativo, sia volta alla protezione di dati a tal punto intimi e condivisi *volontariamente* dalle donne stesse.

[34]«Natural Cycle» e «Clue birth control». Cfr. *FDA allows marketing of first direct-to-consumer app for contraceptive use to prevent pregnancy*, 10-08-2018, in www.fda.gov e, *FDA device summary*, 18-02-2021, in www.accessdata.fda.gov.

[35]*21st Century Cures Act*, Pub. L. No. 114-255, § 3060(a), (2016), codificato in 21 U.S.C. § 360j(o).

[36]Cfr. L.R. Fowler, M.R. Ulrich, *Femtechnodystopia*, in 75 *Stanford Law Review*, 2023, 1279; A. Taylor, *Fertile Ground: Rethinking Regulatory Standards for Femtech*, in 54 *UC Davis Law Rev.*, 2021, 2283-86 (l'autrice evidenzia che l'FDA dovrebbe qualificare come "SAC" ogni *Femtech-apps* che tratti dati riproduttivi, suggerendo inoltre una modifica nella classificazione – dalla II alla III Classe – al fine di garantire maggior controllo).

[37]Il «21st Century Cures Act» (2016) e il «Digital Health Innovation Action Plan» (2017) stabiliscono che l'FDA debba regolamentare come dispositivi medici solo le "*mobile medical apps*" ad alto rischio. Cfr. A. Scatterday, *op.cit.*, 654.

[38]Pub. L. n. 104-191-Aug.21, 1996.

[39]Cfr. C. Rosas, *op.cit.*, 330; 45 C.F.R. §160.103 (2014).

[40]L'app *Glow*, qualificata come *"business associate*", rientra nell'ambito applicativo HIPAA. Il programma *"Glow Fertility program Patient Services Agreement"* permette lo scambio di informazioni sulla fertilità con l'operatore sanitario.

[41]Si veda la recente azione portata avanti dall'FTC contro «Flo» volta a notificare a favore delle utenti la costante condivisione dei loro dati a terze parti senza consenso o notifica. Le *policies* dell'app sancivano chiaramente che i dati non sarebbero stati oggetto di condivisione e che "*would only use Flo App users' data to provide the Flo App's services*". Cfr. «Flo Health, Inc.» in www.ftc.gov.

3.2 Il rischio di criminalizzazione nel "mondo" *post-Dobbs*

A seguito della sentenza *Dobbs v. Jackson Women's Health Organization*[42],la U.S. *Supreme Court*, operando l'*overrulling* della storica *Roe v. Wade*[43], ha stabilito che l'autorità di regolamentare l'aborto debba tornare nelle mani del popolo e dei suoi rappresentanti. In ragione di tale pronuncia, l'interruzione di gravidanza è oggi vietata in almeno quattordici Stati[44].

Sorge, quindi, un'ulteriore fonte di rischio legata al fenomeno oggetto di questo articolo: il facile accesso all'ecosistema digitale dei dati sanitari riproduttivi innalza il rischio di criminalizzazione. Se le forze di polizia e i pubblici ministeri hanno già utilizzato estrazioni di dati digitali per l'accertamento di fatti di reato[45], non sorprenderebbe che le analisi forensi su dispositivi digitali diventino parte integrante delle indagini su aborti illegali[46]. Ai fini del presente contributo, preme citare, in particolare, due casi giudiziari: una donna, residente in Mississippi, è stata accusata di omicidio di II grado a seguito di cure ospedaliere richieste nel 2017 per un aborto spontaneo. Le autorità di polizia hanno utilizzato le ricerche effettuate dalla donna *online* e, nello specifico, l'acquisto di un farmaco abortivo per provare la di lei *intenzione* ad abortire[47]. Ancora, nel giugno del 2022 le forze di polizia in Nebraska – attraverso l'emanazione di un *"search warrant"* – hanno ottenuto direttamente da *Facebook* i messaggi personali scambiatesi *online* tra una madre e la figlia minorenne. In questa fattispecie, l'acquisizione di dati digitali si è rivelata cruciale per accusare – e in seguito condannare – le due donne di aver occultato il cadavere di un feto abortito illegalmente[48]. Tali casi dimostrano l'utilizzo dei dati personali digitali a fini probatori, una pratica che potrebbe diventare un protocollo *standard* negli ordinamenti giudiziari in cui l'aborto è vietato[49].

In tale contesto, le *Femtech-apps* sembrerebbero essere la fonte primaria verso cui indirizzare le indagini finalizzate alla persecuzione dell'aborto. È verosimile, infatti, che le autorità competenti facciano richiesta formale alle *Femtech-companies* di accedere ai dati sanitari ivi trattati. Trova così giustificazione l'attuale tendenza che vede molte donne, residenti negli Stati "*trigger*", a eliminare dai propri dispositivi tali app nel timore di una divulgazione dei dati non desiderata.

[42]597 U.S. 215 (2022).
[43]410 U.S. 113 (1973).
[44]V. *Tracking Abortion Bans Across the Country*, last update: 13-06-2024, in www.nytimes.com.
[45]L. Koepke et al., *Mass Extraction: the Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 4, 2020, in www.upturn.org.
[46]C. Conti-Cook, *Surveilling the Digital Abortion Diary*, in 50 *University of Baltimore Law Review* 1, 2020, 36.
[47]*Ivi*, 3-4.
[48]M. Kaste, *Nebraska cops used Facebook messages to investigate an alleged illegal abortion*, 2022, in www.npr.org; S. Mansoor, *What Nebraska's Sentencing of a Teen Who Used Abortion Pills Might Mean in Post-Roe America*, 2023, in www.time.com.
[49]A. Prince, *Reproductive Health Surveillance*, in *Boston Collage Law Review*, No. 2022-36, 1110.

DPCE online
ISSN: 2037-6677

Nel "mondo" dell'America *post-Dobbs*, l'esercitare o il non esercitare il «right to intimate privacy» può in concreto ostacolare o, al contrario, rafforzare la capacità delle forze dell'ordine nel perseguire l'aborto.

Al riguardo, il IV Emendamento alla Costituzione degli Stati Uniti riconosce e garantisce il diritto di ogni individuo a essere protetto da irragionevoli e arbitrari perquisizioni e/o sequestri da parte di autorità governative. Sembrerebbe, dunque, offrire immediata protezione costituzionale alle donne utenti delle *Femtech-apps* laddove i diritti e le libertà riproduttive siano venute meno. Ma, la pretesa di tutela in termini di *privacy* dei dati raccolti e trattati da tali app nei confronti di estrazioni operate da autorità governative è "limitata" alla luce della «third party doctrine»[50] tradizionalmente formatasi sull'interpretazione del IV Emendamento. Per giurisprudenza costante[51], la Corte Suprema, a partire dal caso *United States v. Miller*[52], nega l'estensione di tale protezione costituzionale alle informazioni e ai dati che l'individuo *volontariamente* condivide a terzi, compresi i fornitori di servizi digitali. La prodromica volontà nella condivisione è il motivo che fa venir meno la legittima aspettativa di *privacy* su dati personali scientemente condivisi. Ne consegue che il IV Emendamento non forgia un diritto alla *privacy* di matrice costituzionale né garantisce alle donne utenti delle *Femtech-apps* di pretendere un'aspettativa legittima sulla riservatezza dei dati condivisi in tali app il cui tratto distintivo è proprio l'intenzionalità della condivisione al fine di ricevere la prestazione del servizio digitale.

Le app sulla salute femminile dopo *Dobbs* rivelano come il fenomeno *Femtech* abbia ormai superato i confini normativi entro cui è stato ideato: la dinamicità del panorama statunitense in punto di diritti riproduttivi è in grado di riscrivere i rischi tradizionali in problemi molto più gravi. Così, il divario che sussiste nel contesto americano tra le nuove domande di tutela e gli strumenti normativi in vigore dimostra la necessità di un nuovo approccio[53].

3.3 Nuove proposte di regolamentazione

Al fine di accrescere la tutela in materia, diverse sono le strade potenzialmente percorribili dal Congresso. Quest'ultimo, come evidenziato in

[50]Si tratta di una dottrina di *common law* sviluppatasi in seno alle corti americane.

[51]A ragion del vero, a partire dal caso *United States v. Jones* (2012) il giudice Sotomayor evidenzia nella *concurring opinion* la necessarietà di rivedere il principio dell'aspettativa ragionevole di privacy nella sua diversa declinazione nell'era digitale. Ancora, nelle sentenze *Riley v. California* (2014) e *Carpenter v. United States* (2018), la Corte Suprema dimostra un'inversione di rotta: nel primo caso dichiara l'incostituzionalità delle perquisizioni volte all'estrazione dei dati digitali contenuti negli *smartphones* senza mandato del giudice; nel secondo caso sostiene che la dottrina della terza parte non operi nei confronti dei dati di localizzazione registrati dagli *smartphones* in considerazione del carattere "involontario" della raccolta.

[52]425 U.S. 435, 436-37 (1976). Dove si legge che "*The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities*".

[53]Ai fini di un approfondimento sul tema, v. A.Z. Huq e R.Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, in 97 *N. Y. U. L. Rev.*, 2022, 555-646.

dottrina[54], potrebbe, anzitutto, emendare il testo dell'HIPAA incidendo sulla definizione di *"covered entity"* al fine di farvi comprendere anche le *Femtech-companies*. Se così fosse, dovrebbero adeguarsi alle «privacy, security and breach notification rules» previste, principalmente, nel Titolo II; e, quindi, dovrebbero: (a) ottenere il consenso scritto e informato della donna *ante* divulgazione dati; (b) assicurare alla donna il "diritto d'accesso"; (c) notificare alla donna la *data-breach;* (d) imporre misure di sicurezza e gestione del rischio per l'archiviazione e trasmissione dei dati sanitari protetti, aggiornate secondo il progresso tecnologico. Invero, il Congresso, attraverso l'*Health Information Technology for Economic and Clinical Health* (HITECH) *Act*, ha già rafforzato la risalente disciplina HIPAA, riconoscendone flessibilità e assicurando protezione ai dati sanitari nel nuovo panorama della sanità digitale[55]. La rapida diffusione di *Femtech* dovrebbe incentivare il Congresso a rispondere a questa nuova "sfida normativa" senza partire da zero, intervenendo su un *corpus* normativo che ha dimostrato negli anni di essere in grado di tutelare – nella difficile opera di bilanciamento – la riservatezza dei dati sanitari protetti pur garantendone la condivisione in un regime di sicurezza.

Se tutto questo è vero, non meno vero è che la sola estensione del concetto di "*covered entity*" alle *Femtech-companies* non sia sufficiente[56]. Al fine di garantire tutela sostanziale alle utenti sarebbe necessario emendare il testo normativo intervenendo anche sui requisiti tecnici di sicurezza informatica. In particolare, i dati crittografati – ora soluzione a discrezione dell'azienda – dovrebbero essere «the commercially-reasonable standard» imposti come requisiti obbligatori per tutto il panorama delle *mobile medical apps* comprese, quindi, le *Femtech-apps*[57].

Il Congresso, inoltre, potrebbe adottare nuove normative finalizzate alla tutela federale della riservatezza dei dati personali, in generale, o dei dati sanitari riproduttivi, in particolare. In tal senso, si cita primariamente l'*American Data Privacy and Protection Act*[58] che, se approvato, istituirebbe la prima regolamentazione della *data privacy* di livello federale negli Stati Uniti[59]. Secondariamente, è anche da ricordare il *My Body My Data Act*[60] che, a seguito delle problematicità sollevate dal caso *Dobbs*, creerebbe un *"federal standard"*[61] a tutela dei dati sanitari riproduttivi prevedendone limiti alla registrazione, archivio, condivisione e riconoscendo alla donna un «private right of action» affinché le entità regolamentate siano considerate responsabili delle violazioni incorse.

4. Le *Femtech* nell'ordinamento dell'Unione europea: cenni

Diverso, almeno formalmente, si presenta il quadro europeo in materia.

[54]C. Rosas, *op.cit.*; A. Scatterday, *op.cit.*
[55]A. Scatterday, *op.cit.*, 667.
[56]C. Rosas, *op.cit.*; L.R. Fowler, M.R. Ulrich, *op. cit.*, 1273-1312.
[57]C. Rosas *op.cit.*, 324.
[58]H.R. 8152, 117th Cong., 2022.
[59]A. Prince, *op.cit.*, 1140 ss (*"It would have established a comprehensive data privacy regime at the federal level for the first time"*).
[60]H.R. 8111, 117th Cong., 2022.
[61]A. Prince, *op.cit.*, 1138.

DPCE online
ISSN: 2037-6677

Anzitutto, i prodotti *Femtech* – sia app che *devices* – sono potenzialmente soggetti alla disciplina delineata dal Regolamento sui dispositivi medici (d'ora innanzi: MDR)[62]. La normativa europea considera, infatti, dispositivo medico, in generale, e dispositivo medico di rischio medio-alto (Classe IIb), in particolare, anche i dispositivi – compresi i *software* – «per il controllo del concepimento o il supporto al concepimento»[63]. Alcuni prodotti *Femtech* sono così qualificati dai rispettivi "fabbricanti"[64], i quali devono rispettare stringenti requisiti di certificazione e sicurezza ai fini della commercializzazione del prodotto all'interno dell'Unione[65].

Tuttavia, la qualificazione di un *software* come dispositivo medico dipende dalla destinazione d'uso impressa *ab origine* dal fabbricante. Pertanto, è dispositivo medico unicamente il s*oftware* specificamente destinato dal fabbricante a essere impiegato per una o più delle destinazioni d'uso mediche di cui all'art. 2 MDR, al contrario del *software* destinato a finalità generali o a fini associati allo stile di vita e al benessere, nonostante l'utilizzo in contesto sanitario[66].

In riferimento alle app sanitarie, la specificità del tema oggetto del presente contributo rende necessario evidenziare che la distinzione tra le *Medical Mobile-app*, qualificate come dispositivi medici e sottoposte a rigide forme di controllo, e le generiche *Health Mobile-app* di libera commercializzazione risiede in un'espressa destinazione d'uso del fabbricante[67]. Questo criterio induce a ritenere che i fabbricanti abbiano immesso – e immettono – nel mercato europeo *Femtech-apps* formalmente associate allo stile di vita e al benessere, ma sostanzialmente in grado di svolgere le finalità mediche di controllo e supporto al concepimento, al fine di eludere la stringente regolamentazione di settore e le conseguenti responsabilità. La maggior parte di queste app non è qualificata, infatti, come dispositivo medico e, di conseguenza, i rispettivi *software* sono progettati, prodotti e, infine, commercializzati senza il rispetto delle specifiche tutele previste dall'MDR, nonostante il trattamento di dati sanitari e le finalità perseguite.

La scelta compiuta dai fabbricanti non esclude, comunque, l'applicabilità della disciplina delineata dal GDPR. Una regolamentazione che, seppur in termini generali, segue l'impostazione della tutela offerta dall'MDR soprattutto alla luce del principio di *accountability* di cui all'art. 24 GDPR[68]. Più specificatamente, le app non qualificabili come strumento di telemedicina o, indipendentemente dalla finalità, a cui abbiano accesso soggetti diversi dal professionista sanitario tenuto al segreto professionale, necessitano del consenso esplicito dell'interessato ai fini della liceità del trattamento[69]. La quasi

[62]Regolamento (UE) 2017/745 (MDR).
[63]Art. 2 e All. VIII-7.2, MDR.
[64]Cfr. la definizione del termine "fabbricante" di cui all'art. 2(30) MDR.
[65]Art.10 MDR.
[66]19° *considerando* MDR.
[67]C. Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e Mercato*, 1/2023, 35.
[68]Sul principio dell'*accountability* o – come definito dall'A. – della "responsabilizzazione", criterio che informa l'intero testo del GDPR, cfr. G. Finocchiaro, *GDPR tra novità e discontinuità – Il principio di accountability*, in *Giur.it.*, 12/2019, 2778 ss.
[69]Provv. n. 55 GPDP, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7-03-2019, in www.garanteprivacy.it.

totalità delle *Femtech-apps* risponde a questa definizione. Lo strumento del consenso, quindi, è la base giuridica che legittima il trattamento dei dati – anche i più intimi – delle utenti.

Il consenso, però, svolge funzione legittimante solo se risulta «manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato»[70]. Sono proprio questi requisiti che fondano dubbi sulla liceità del trattamento dati[71] nelle *Femtech-apps* nell'Unione.

Sulla base di quanto emerso da studi empirici recenti e, in particolare, da uno studio del 2021[72], i dati personali delle utenti non sembrano essere garantiti almeno tanto quanto sarebbe atteso a fronte del quadro normativo in vigore: la legge è elusa con espedienti definitori[73] e con la prestazione di un consenso le cui modalità esplicative appaiono di dubbia liceità. Degno di nota il fatto che il quaranta per cento delle app prese in considerazione nello studio non fornisce al primo accesso l'informativa *privacy*, mentre, il sessanta per cento di queste prevede come unica modalità di accettazione delle *policies* l'opzione binaria "accetta o rifiuta". Inoltre, nei casi in cui la gratuità dell'app crea un meccanismo per cui l'utente è portato a cedere il proprio consenso come fosse il "prezzo" da pagare per ottenere il servizio[74], si discute su quanto possa dirsi effettivamente libero. Il rischio è che le donne mettano in secondo piano valutazioni consapevoli sulla propria *privacy* rispetto al bisogno di accedere al servizio digitale. Peraltro, le informative, laddove presenti, appaiono fornite esclusivamente in lingua inglese attraverso l'utilizzo di vocaboli tecnici e poco intellegibili. Tale profilo preoccupa soprattutto in considerazione che sono, *in primis*, rivolte a giovanissime utenti. Infine, in media, ognuna delle suddette app attiva, subito dopo l'installazione, 3.8 *trackers* ovvero programmi nascosti che tracciano l'attività dell'utente e che raccolgono dati *extra* rispetto a quelli adeguati e pertinenti al tipo di servizio prestato, in violazione del principio di minimizzazione dei dati.

Dunque, la disciplina generale del GDPR non sembra essere in grado, da sola, di fornire tutela.

Per completezza, volgendo lo sguardo verso normative in attesa di attuazione, si citano due Regolamenti: il *Cyber Resilience Act*[75], che impone nuovi requisiti di sicurezza cibernetica per i prodotti con elementi digitali a cui non si applichino già specifiche normative (come l'MDR), per un verso; e

[70] 32° *considerando* GDPR.

[71] Sulle condizioni di liceità del trattamento dei dati personali e sulle criticità in punto di prevalenza di interessi "altri" rispetto a quelli del *data subject*, cfr. D. Poletti, *GDPR tra novità e discontinuità – Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 12/2019, 2783 ss.

[72] M. Mehrnezhad e T. Almeida, *Caring for Intimate Data in Fertility Technologies*, in *Conference on Human Factors in Computing Systems (CHI '21)*, May 8-13, 2021, Yokohama, Japan, ACM, New York, USA.

[73] 24 app, su un campione di 30, sono catalogate negli *app-store* come *"health e fitness"* anziché *"medical"*.

[74] Sul tema della "commercializzazione" dei dati personali, cfr. 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*, Torino, 2019, 40.

[75] Testo approvato dal Parlamento europeo il 12-03-2024.

DPCE online
ISSN: 2037-6677

l'*Artificial Intelligence Act* (d'ora innanzi: AI Act)[76], volto a stabilire regole armonizzate sull'AI, per altro verso. In particolare, l'AI Act rafforzerà la sicurezza dei prodotti *Femtech* qualificati come dispositivi medici: definibili come sistemi ad alto rischio, dovranno soddisfare stringenti requisiti prima di ottenere il marchio CE di conformità. Tra questi, l'aderenza a più alti indici di sicurezza informatica utili per prevenire l'indebito accesso alle informazioni raccolte nel dispositivo. Inoltre, si può pensare che l'AI Act si applicherà anche alle più generiche *Health-app* in quanto potenzialmente qualificabili come «sistemi di AI per finalità generali».

5. Alcune osservazioni conclusive

Diversi sono gli spunti di riflessione che il fenomeno specifico delle *Health-app*, nel panorama più generale delle *Femtech*, offre, soprattutto se analizzato in prospettiva comparata.

Anzitutto, è possibile notare che nell'Unione europea, nonostante l'ordinamento sia dotato – sia nello specifico che nel generale – di un solido quadro normativo di tutela, si rilevano lesioni al «right to intimate privacy» potenziali e simili a quelle riscontrate nel contesto americano. Le sfide lanciate dall'AI applicata in un settore critico come quello sanitario, evidenziano sempre più le criticità del GDPR. Da qui, l'esigenza di maturare nuovi approcci normativi a tutela della *privacy* sanitaria a fronte delle inedite peculiarità dell'ecosistema della sanità mobile.

Inoltre, quanto emerge dal contesto europeo stimola una riflessione sul contesto americano: se il Congresso modificasse il testo dell'HIPAA o adottasse una legge federale sulla *data privacy* più completa, il grado di tutela normativo così ottenuto non sarebbe comunque paragonabile a quello offerto – da anni – dal GDPR in seno ai confini dell'Unione. E se anche il GDPR non sembra essere una panacea, la vittoria che si otterrebbe negli Stati Uniti sarebbe, comunque, una vittoria imperfetta.

Necessaria sembrerebbe, piuttosto, una regolamentazione che assicuri alle donne la condivisione dei propri dati sanitari in un regime di assoluta sicurezza, oggi quasi del tutto assente nel contesto americano, e in quello europeo garantito in modo fragile dal consenso. Una regolamentazione idonea a responsabilizzare in modo proattivo tutti gli attori del fenomeno, dal fabbricante alla donna stessa, perché solo una consapevolezza responsabile delle utilizzatrici può garantire loro l'esercizio del «right to intimate privacy» nella declinazione di autodeterminazione informativa.

Maria Vittoria Malinconi
Dipartimento di Scienze Giuridiche
Università degli Studi di Firenze
mariavittoria.malinconi@unifi.it

[76]Testo approvato dal Parlamento europeo il 13-03-2024.