Emiliano Casalicchio[1], Sebastiano Filetti[2], Sabrina Grigolo[3], Luigi V. Mancini[1], Alessandro Mei[1], Giulio Pagnotta[1], Alice Ravizza[4], Angelo Spognardi[1], Silvia Stefanelli[5]

Privacy e *cybersecurity* nell'ambito delle terapie digitali

1. Profili di tutela dei dati nelle terapie digitali

Le terapie digitali (DTx) sono *software* validati clinicamente che svolgono una funzione terapeutica: attraverso infatti una elaborazione di dati in ingresso restituiscono dati in uscita che hanno la capacità di influenzare il comportamento del paziente, generando un beneficio clinico (ad esempio una App che fornisce indicazioni al paziente migliorandone i problemi di insonnia).

Sotto il profilo della qualificazione giuridica, le DTx rientrano nella definizione di "dispositivo medico" ex art. 1 lett. a della Dir 93/42/CEE (da maggio 2021 nella definizione di dispositivo medico di cui all'art. 1 lett. 2 del nuovo Regolamento UE 2017/745, cosiddetto MDR): la loro produzione e commercializzazione deve pertanto rispettare le suddette discipline.

Le DTx, per le loro modalità di funzionamento intrinseco, svolgono la propria azione trattando dati inerenti lo stato di salute del paziente che rientrano nella nozione di "*particolari categorie di dati*" (ex art. 4 lett. 15 del Regolamento UE 2016/679). Occorrerà quindi analizzare i profili giuridici inerenti tale tipologia di trattamento, alla luce del recente Regolamento UE 2016/679 (cosiddetto GDPR).

Nel presente lavoro - per ragioni di economia di spazi - si analizzeran-

[1]*Dipartimento di Informatica, Sapienza Università di Roma*
[2]*School of Health, UnitelmaSapienza, Roma*
[3]*Accademia del Paziente Esperto EUPATI Onlus*
[4]*Use-Me-D, Torino*
[5]*Studio Legale Stefanelli & Stefanelli, Bologna*

no solo le principali problematiche relative ai profili di trattamento dei dati in relazione alle DTx, tralasciando i profili generali del GDPR.

1.1 Ruoli soggettivi nel trattamento dei dati

Il primo elemento su cui puntare l'attenzione è la determinazione dei ruoli soggettivi nel trattamento dei dati: in altre parole qual è il soggetto che riveste il ruolo di Titolare del trattamento dei dati e quali sono, a cascata, gli altri ruoli soggettivi.

Ai sensi dell'art. 4 punto 7) del GDPR, infatti, il Titolare del trattamento è il soggetto che determina *"finalità e mezzi del trattamento"* ed è colui che ha la generale responsabilità giuridica di garantire il corretto trattamento dei dati.

Alla luce poi della generale interpretazione della disciplina e delle recentissime Linee Guida dell'*European Data Protection Board* "*Guidelines 07/2020 on the concepts of controller and processor in the GDPR*" (*draft* emanato in data 7 settembre 2020) si può affermare che il ruolo di Titolare (ed in generale tutti i ruoli del GDPR) non possono essere definiti in maniera aprioristica, ma devono discendere dai profili concreti di trattamento dei dati.

In sostanza occorre indagare quale soggetto - nella realtà concreta - determina le finalità per le quali i dati vengono trattati, nonché le modalità secondo le quali ciò avviene.

Per quanto riguarda le DTx si ritiene che possano configurarsi due ipotesi:

- la prima vede quale Titolare la struttura sanitaria o il singolo medico che prescrive la DTx.

In questo caso il fabbricante della DTx sarà presumibilmente nominato quale Responsabile del trattamento dei dati ex art. 28 in quanto svolge sui dati operazioni di conservazione ed organizzazione dei dati stessi (senza però, in questo caso, poter definire le finalità di trattamento). Da segnalare che, in questa ipotesi, il soggetto qualificato come fabbricante della DTx, pur rivestendo il ruolo di Responsabile del trattamento dei dati, dovrà comunque mantenere il ruolo di Titolare per tutti quei trattamenti strettamente connessi. Tale soggetto - proprio in quanto *fabbricante del dispositivo medico* - sarà tenuto a trattare i dati per alcune finalità che discendono legislativamente dalla sua qualifica di fabbricante ex MDR, solo a titolo di esempio la sorveglianza *post* commercializzazione (art. 83 MDR) e la vigilanza sul dispositivo medico (art. 89 MDR).

- La seconda ipotesi vede invece come Titolare del trattamento dei dati lo stesso fabbricante della DTx: in questo caso tale soggetto avrà la piena responsabilità di tutti gli adempimenti del GDPR. Ovviamente la struttura sanitaria/medico prescrittore, pur non avendo in questo caso ruoli

specifici in ambito di trattamento dei dati, dovranno poter accedere ai dati di *input* ed ai dati di *output* del paziente ai fini di seguire lo sviluppo e l'andamento della terapia (presumibilmente in qualità di autorizzati al trattamento ex art. 29 GDPR).

1.2 Principi generali del trattamento

Il soggetto che si qualifica come Titolare del trattamento dovrà poi garantire che i dati vengano trattati nel rispetto dei principi del trattamento. Tali principi sono elencati all'art. 5 del GDPR.

Nell'ambito delle DTx il rispetto di tali principi presenta le seguenti peculiarità:

a) *Principio di liceità*

Il trattamento dei dati può avvenire solo ove ci sia una base giuridica che legittima il trattamento stesso.

Nel caso delle DTx il trattamento riguarda dati relativi alla salute (che rientrano nella nozione di "particolari categorie di dati") la cui base giuridica è da ricercare nell'art. 9 del GDPR.

La base giuridica potrà poi cambiare a seconda del soggetto che riveste il ruolo di Titolare.

Ove infatti il ruolo di Titolare sia ricoperto dalla struttura sanitaria o dal medico, la base giuridica di trattamento potrà essere l'art. 9 comma 1 lett. h) che consente il trattamento di dati relativi alla salute ai soggetti che operano in ambito sanitario (art. 9 comma 3) per finalità di "*diagnosi, assistenza o terapia sanitaria*".

Ove invece il Titolare del trattamento sia il fabbricante del dispositivo medico (che non può essere legittimato ai sensi dell'art. 9 lett. h) e comma 3), la base giuridica del trattamento potrà presumibilmente essere il consenso del paziente (art. 9 lett. a).

b) *Principio di limitazione della finalità*

Altro cardine del sistema è il principio di finalità del trattamento.

L'art. 5 lett. b) del GDPR stabilisce infatti che il Titolare è tenuto a definire, prima di iniziare il trattamento, le finalità (cioè gli scopi) per cui tratta i dati ed a trattare i dati solo per le finalità prestabilite (che dovranno altresì essere dichiarate nell'informativa - si veda paragrafo successivo sul principio di trasparenza).

Nelle DTx la finalità principale sarà senza dubbio quella di "*diagnosi,*

assistenza o terapia sanitaria" e quindi di miglioramento dello stato di salute del paziente. Tale finalità peraltro giustifica la destinazione d'uso sanitaria e, quindi, la qualificazione giuridica come dispositivo medico.

I dati raccolti, però, potranno poi essere usati per altre finalità, quali ad esempio la sorveglianza *post*-commercializzazione del dispositivo medico stesso (art. 83 MDR) che - come sopra accennato - troverà la sua base giuridica nella stessa disciplina normativa dell'MDR.

Un'altra finalità di trattamento potrebbe essere poi la ricerca scientifica (nell'ampia nozione del Considerando 159 dell'MDR). In questo caso occorrerà definire (anche in ragione della possibile diversa titolarità) quali possono essere le basi giuridiche di trattamento (ad esempio l'art. 9 lett. h) se il Titolare del trattamento per ricerca scientifica è una struttura pubblica, oppure un separato consenso del paziente se il Titolare è l'azienda privata di produzione della DTx.

Infine un breve accenno al trattamento dei dati (del paziente e/o dei medici e operatori sanitari) per finalità di *marketing*: in questo caso si ritiene che la base giuridica del trattamento dovrà essere (in entrambe le ipotesi di titolarità sopra riportate) il consenso del paziente. Sotto questo profilo si precisa che il consenso dell'interessato (medico e/o paziente) dovrà essere libero (cioè senza pressioni di alcun genere) e consapevole (quindi a seguito di una informativa chiara e comprensibile - si veda il punto successivo sul principio di trasparenza).

Da ultimo alcune considerazioni specifiche collegate proprio al peculiare trattamento attraverso i *software*. Come noto, alcuni *software* possono oggi operare anche in forza di sistemi di autoapprendimento (cosiddetto *machine learning*): in alcuni casi le funzioni di *machine learning* più avanzate possono portare a finalità di trattamento diverse rispetto a quelle definite all'inizio dell'operatività del *software*. Ove questo avvenga ci si potrebbe trovare di fronte all'ipotesi di trattamenti per finalità con assenza di idonea base giuridica.

Sotto questo profilo appare opportuno - specie in casi come quello delle DTx - che i *software* che operano in sistemi di autoapprendimento siano programmati in modo che la loro operatività non sfugga al controllo dell'uomo.

c) *Principio di trasparenza*

Nel sistema del GDPR è data grande importanza al principio di trasparenza. L'interessato infatti (nel nostro caso il paziente che usa la DTx) rimane sempre e comunque il "proprietario" dei suoi dati e deve essere messo nella condizione di poter comprendere con esattezza *come* e *perché* i suoi dati vengono trattati, e quindi poter decidere sui dati stessi.

Il principio di trasparenza indicato all'art. 5 lett. a) trova poi la sua de-

clinazione più precisa negli art. 12 e successivi del GDPR, ed in particolare nell'art. 13 che disciplina la cosiddetta *informativa privacy*.

Tramite l'informativa, infatti, il Titolare deve chiarire al paziente per quali finalità tratta i suoi dati, e come gli stessi vengono trattati (compresa la conservazione dei dati, indicando altresì il Paese in cui i dati sono trasmessi e/o conservati).

Nel settore delle DTx (che operano tramite *software*) si rilevano poi in particolare alcuni profili. In primo luogo si evidenzia che l'art. 13.2 lett. f, stabilisce che il Titolare debba fornire all'interessato le informazioni relative alla "*esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".

Ora, seppure si reputi che la DTx possa non considerarsi strettamente un "processo decisionale automatizzato" secondo la nozione del GDPR (in quando vi è sempre l'intervento di un medico o sanitario), ciò non toglie che la delicatezza della tipologia di trattamento suggerisca un atteggiamento di massima trasparenza in capo al Titolare.

Sotto questo profilo, un aiuto è fornito da una recente guida pubblicata dall'*Information Comunication Officer* - ICO (il Garante inglese) in ambito di Intelligenza Artificiale (AI) "*Explaining decisions made with AI - Draft guidance for consultation"*.

Il documento, chiaramente assunto per i *software* di intelligenza artificiale, può essere comunque considerato un ottimo strumento di *best practice* anche per i *software* non qualificabili come AI.

Molto sinteticamente, nel documento sopra citato, il Garante britannico precisa che il Titolare del trattamento deve decidere come articolare l'informativa tenendo in considerazione i seguenti elementi: 1) il settore nel quale viene impiegato il modello di AI, 2) l'impatto sull'individuo, 3) la tipologia di dati trattati, 4) l'urgenza della decisione, 5) i soggetti a cui è destinata l'informativa.

I contenuti dell'informativa possono, secondo l'ICO, essere divisi in due macro-categorie:

a. spiegazioni "*process-based"*: si tratta di spiegare che nel corso del processo decisionale sono state seguite tutte le *best practices* di *design* e progettazione del *software*;

b. spiegazioni "*outcome-based*": si tratta di chiarire il risultato di una decisione specifica, fornendo, in un linguaggio semplice e comprensibile a tutti, informazioni sul ragionamento seguito.

Infine il Garante elenca sei tipi di informazioni, che a seconda dei casi

possono rientrare nell'ambito del *process-based* o dell'*outcome-based* (fornendo anche indicazioni e *checklist* su come implementarle).

Molto in sintesi:

1) La motivazione del trattamento (*rationale explanation*): è opportuno spiegare le ragioni che hanno portato ad una decisione, pronunciata in un contesto accessibile e in modo non tecnico.

2) La responsabilità del trattamento (*responsibility explanation*): è opportuno indicare chi è coinvolto nello sviluppo, nella gestione e nell'attuazione di un sistema di AI, e chi contattare per una revisione umana della decisione.

3) I dati trattati (*data explanation*): occorre specificare quali dati sono stati utilizzati in una determinata decisione e come sono stati utilizzati.

4) La correttezza nel trattamento (*fairness explanation*): è opportuno spiegare i cardini di funzionamento del *software* e come lo stesso garantisce l'imparzialità nel trattamento.

5) La sicurezza e prestazioni (*safety and performance explanation*): occorre spiegare come funziona il *software* illustrandone l'accuratezza, l'affidabilità, la sicurezza e la robustezza delle sue decisioni.

6) L'impatto (*impact explanation*): occorre chiarire i passaggi compiuti attraverso la progettazione e l'implementazione di un sistema di AI per considerare e monitorare gli impatti che l'uso di un sistema e le sue decisioni hanno, o possono avere, su un individuo, e su una società più ampia.

Come già accennato, le indicazioni sopra riportate non rivestono natura obbligatoria ma sono solo *best practice* che, suggerite da ICO per le informative in ambito di AI, possono trovare applicazione ovviamente anche in *software* non qualificabili come AI.

Infine per quanto attiene alle modalità di somministrazione dell'informativa al paziente, nel caso di DTx che sia una App si suggerisce l'analisi della Linea Guida WP 29 "Linea Guida sulla trasparenza dei dati, parere WP 29 2/2013 sulle Applicazioni per dispositivi intelligenti", nonché il documento della *European Union Agency for Cybersecurity* (ENISA) titolato "*Privacy and Data Protection in Mobile Application*".

d) *Principio di correttezza*

Un altro principio che dovrà essere garantito dal Titolare è quello di correttezza. Il principio di correttezza attiene alla ragionevole aspettativa di trattamento dei dati da parte dell'interessato.

A parere di chi scrive, la "ragionevole aspettativa" dell'interessato sembra racchiudere molti degli aspetti relativi ai profili di eticità del *software*. Ne de-

riva che il rispetto del principio di correttezza dei dati di cui all'art. 5 GDPR comporta - in sostanza - il rispetto dei principi di eticità del trattamento.

Ad avallo di questa tesi si segnala che l'ICO, nella "*Guidance on AI and data protection*" e in particolare nella sezione relativa a "*How do the principles of lawfulness, fairness and transparency apply to AI*?", afferma:

"…. if you use an AI system to infer data about people, in order for this processing to be fair, you need to ensure that:

- *the system is sufficiently statistically accurate and avoids discrimination; and*
- *you consider the impact of individuals' reasonable expectations."*

In relazione a tale aspetto si richiamano anche i contenuti del documento del Comitato Nazionale di Bioetica intitolato "*Mobile - health e applicazioni per la salute: aspetti bioetici*" del 28 maggio 2015.

e) *Principio di minimizzazione dei dati*

Ulteriore principio da rispettare è quello della minimizzazione dei dati. In forza di tale principio possono essere raccolti e trattati solo i dati che appaiono "necessari" in ragione della finalità dichiarata nell'informativa. Il rispetto del principio di minimizzazione quindi non è "astratto" o "predefinito" ma è strettamente collegato alle finalità di trattamento che il Titolare ha dichiarato nell'informativa.

Solo a titolo di esempio le *informazioni raccolte* (e poi trattate) potrebbero essere diverse se le operazioni di trattamento avvengono solo per "*diagnosi e cura"* oppure anche per finalità di "*marketing"*.

Occorrerà quindi fare riferimento alle finalità di trattamento identificate e, alla luce di queste, valutare se le informazioni che vengono raccolte (che sono "dati") sono indispensabili per la finalità stessa.

f) *Principio di esattezza dei dati*

Nell'ambito dei trattamenti effettuati tramite *software*, il principio di esattezza dei dati previsto nell'art. 5 del GDPR appare particolarmente rilevante. Tale principio impone infatti (in via generale) che ogni dato trattato sia "esatto" ed "aggiornato", e che siano pertanto adottate tutte le misure ragionevoli e necessarie per la rettifica dei dati inesatti.

Nello specifico campo dei *software* (e quindi della DTx) l'esattezza del dato deve essere vista sia come necessità iniziale che come obiettivo finale, coinvolgendo quindi anche l'esattezza del "funzionamento del *software*": l'esattezza, in poche parole, deve rappresentare il *fil rouge* dell'intero percorso del dato. È infatti pacifico che se i dati di ingresso non sono esatti o corretti, ne verrà inficiato l'intero processo e il *software* fornirà dati in uscita non precisi.

Tale profilo nell'ambito della DTx si rileva peraltro fortemente anche sotto il profilo della responsabilità da prodotto difettoso del dispositivo medico, nonché sotto il conseguente profilo della responsabilità sanitaria della struttura/medico che somministra la DTx. La non correttezza del dato in uscita potrebbe infatti inficiare le decisioni terapeutiche e quindi compromettere la salute e la sicurezza del paziente.

L'aspetto dell'esattezza dei dati appare poi ancor più impattante ove il *software* lavori in base a sistemi di *machine learning* e di intelligenza artificiale.

g) *Principio di limitazione della conservazione dei dati*

Il GDPR stabilisce infine che i dati devono essere conservati per il tempo limitato al raggiungimento delle finalità per le quali sono stati raccolti. Nel campo delle DTx, trattandosi di dati utilizzati per la terapia, si reputa che la conservazione possa seguire le regole della conservazione della cartella clinica (nell'ipotesi che il Titolare sia la struttura pubblica), oppure possa essere un tempo di conservazione per almeno (se non oltre) i 10 anni, anche allo scopo del mantenimento delle prove ai fini della responsabilità in sede civile, penale ed amministrativa.

1.3 Il processo decisionale automatizzato e la profilazione

Un ulteriore profilo che merita un breve approfondimento è quello relativo all'art. 22 del GDPR sui trattamenti automatizzati e sulla profilazione. Il tema è già stato in precedenza accennato nel paragrafo relativo al principio di trasparenza, per quanto attiene alle informazioni da fornire all'interessato.

In questa sede si intende invece solo precisare gli eventuali adempimenti connessi a tale fattispecie. Più esattamente l'art. 22 stabilisce che l'interessato ha il diritto di non essere sottoposto a una decisione che si basi "unicamente" su un trattamento automatizzato, compresa la profilazione, ove tale trattamento produca effetti giuridici che lo riguardano.

Le Linee Guida dell'*Article 29 Working Party* (WP) "*Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*" stabiliscono poi che si qualifica "processo decisionale automatizzato" il "*processo di prendere una decisione con mezzi automatizzati senza alcun coinvolgimento umano. Queste decisioni possono essere basate su dati reali, nonché su profili creati digitalmente o su dati derivati*".

Si reputa pertanto che, in linea generale, le DTx non rientrino strettamente nella nozione di "processo decisionale automatizzato" in quanto le decisioni assunte (che incidono sulla sfera giuridica del paziente) difficilmente appaiono "automatiche", mentre sembrano essere per lo

più assunte con l'intervento di un sanitario.

Resta inteso che, ove invece si ritenga che l'*output* del *software* sia tale da potersi considerare automaticamente incidente sulla sfera giuridica del paziente, senza un intervento diretto del sanitario, la disciplina dell'art. 22 dovrà trovare piena applicazione. In particolare le modalità di tale trattamento richiedono un consenso *ad hoc*.

Per quanto riguarda invece la profilazione si segnala che si tratta di una operazione di trattamento di cui il GDPR si occupa solo nel sopra citato art. 22, e per la quale sembra quindi che il consenso sia richiesto solo ove vi sia un trattamento automatizzato.

1.4 La valutazione d'impatto

L'art. 35 del GDPR stabilisce che ove i dati vengano trattati attraverso l'uso di nuove tecnologie e tale trattamento possa presentare un rischio elevato per i diritti dell'interessato, il Titolare, prima di procedere al trattamento, deve effettuare una valutazione d'impatto.

Si tratta, nella sostanza, di un documento che deve contenere:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento
- una valutazione della necessità e proporzionalità dei trattamenti tenuto conto della finalità (e quindi in un rapporto fra rischi e benefici)
- una valutazione di come il trattamento potrebbe impattare sui diritti degli interessati (es. diritto alla salute) e dei relativi rischi nel caso di impatto.

Senza dubbio il trattamento dati effettuato da una DTx, proprio perché opera attraverso un *software* e proprio perché può impattare significativamente sulla salute del paziente, richiede una valutazione d'impatto preliminare.

Appare infine rilevante, in questa specifica sede, segnalare che, nello svolgere la valutazione d'impatto, il Titolare del trattamento può decidere di raccogliere le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto.

2. La sicurezza e l'integrità dei dati nelle DTx

I due documenti MDCG[1] e MDRF[2] forniscono una panoramica su quelli che sono i rischi di *cybersecurity* per *medical devices* e indicazioni riguardo le buone pratiche per garantire la sicurezza in fase di progettazione, implementazione e post-produzione di un generico sistema o applicazione medicale. In

particolare, nel primo documento sono presentati i requisiti di sicurezza per i dispositivi medici che devono essere garantiti a livello legislativo europeo, affrontando, in termini puntuali, temi di *cybersecurity*, quali l'efficacia delle misure di sicurezza, l'analisi e la gestione dei rischi durante l'intero ciclo di vita dei dispositivi medici e, come affrontato anche in precedenza, la gestione della protezione della *privacy* e dei dati. Nel secondo documento, invece, sono presentati i principi e le pratiche per gestire la sicurezza dei dispositivi medici, in modo da garantire la completa aderenza ai regolamenti legislativi europei. Entrambi i documenti offrono una sistematica trattazione delle pratiche da seguire, poiché partono dalle definizioni basilari della sicurezza informatica e affrontano in maniera ampia, ma generica, la tematica della gestione dei rischi e delle minacce. Nonostante l'ampiezza dei loro contenuti, i due documenti non forniscono indicazioni specifiche per i requisiti di sicurezza per le terapie digitali, ma si limitano ad elencare requisiti di sicurezza per generici dispositivi medici. Inoltre, i contesti in cui i documenti si muovono sono obbligatoriamente molto indicativi, per poter essere applicati in maniera esaustiva ai diversi possibili tipi di dispositivi medici. Se si vuole, però, contestualizzare maggiormente l'approccio alla sicurezza e, quindi, applicare i principi di sicurezza alle terapie digitali, è fondamentale ridurre il livello di astrazione e cercare di fornire una visione più dettagliata da usare come riferimento. Le terapie digitali, infatti, hanno delle peculiarità specifiche che necessitano di essere trattate approfonditamente e che, in un certo senso, rendono atipico il caso d'uso. Si pensi alle differenze che passano fra un dispositivo medico, come ad esempio una pompa professionale per infusione chemioterapica, e un servizio di terapia digitale che un paziente utilizza sul suo *smartphone*. Senza entrare nel merito della possibile complessità del *software* dei due dispositivi, al produttore della terapia digitale non è data la semplice possibilità di avvalersi di un supporto *hardware* fidato/garantito (*trusted*), poiché lo *smartphone* personale del paziente è esposto ad ulteriori e inevitabili minacce: questo fatto estende in maniera ampia ed evidente la superficie di attacco rispetto ad un classico dispositivo medico. Tale perimetro più ampio di minaccia nel caso di terapia digitale è da considerare durante la fase di sviluppo e dell'analisi e gestione dei rischi.

Per una maggiore comprensione di questa lacuna, nel seguito verrà descritta l'architettura di una generica applicazione di terapia digitale (*Software as Medical Device*, SaMD) e verranno poi analizzate le minacce interne ed esterne (*insider threat* e *outsider threat*), in modo da poter descrivere in maniera più semplice, con un esempio di riferimento, i concetti e le pratiche per la *cybersecurity* nel contesto delle terapie digitali.

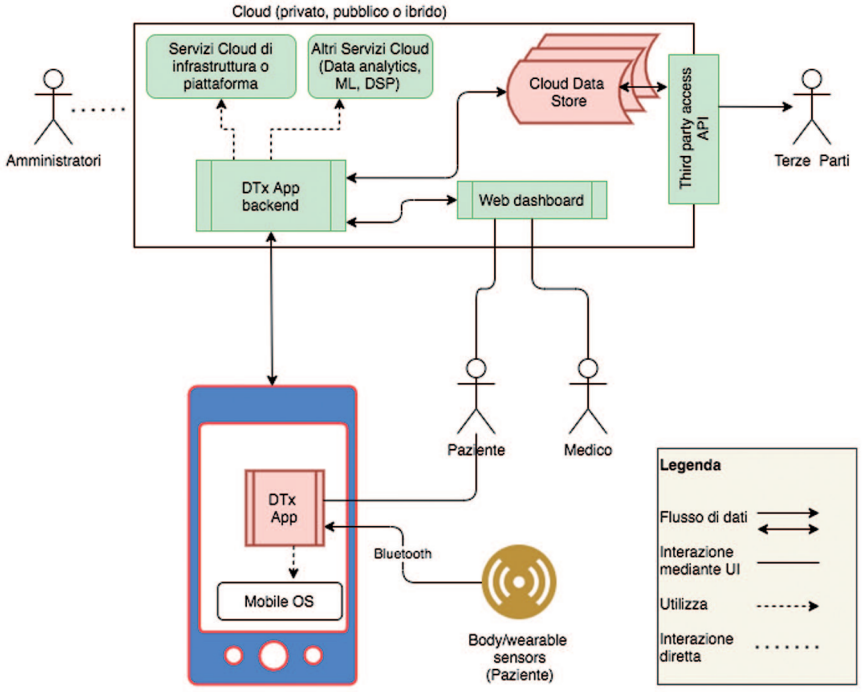
2.1 Architettura di riferimento

L'architettura generale di riferimento per un sistema per l'erogazione di un servizio di Terapia Digitale (nel seguito DTx[3] o SaMD) può essere schematizzata come in *figura 1*.

La DTxApp, ovvero l'*App* che costituisce il principale mezzo di accesso alla terapia digitale, è composta da due macro-componenti principali:

- la prima, *DTxApp*, risiede e viene eseguita sul dispositivo *mobile* del paziente. Nel seguito assumeremo che la *DTxApp* è stata sviluppata usando un *pattern cross-platform* o *hybrid-web*[4]
- la seconda componente, *DTxApp backend*, risiede e viene eseguita su una piattaforma *cloud* e può svolgere diverse funzioni come ad esempio accesso a dati memorizzati nel *Cloud Data Store* (CDS), scrittura di dati nel CDS, analisi o processamento dei dati, esecuzione di algoritmi di *digital therapy* ed esecuzione di algoritmi di *engagement*. La *DTxApp backend* of-

Figura 1 - Architettura di riferimento di un sistema per l'erogazione di un servizio di terapia digitale



fre una serie di *application programming interface* (API) che verranno utilizzate dalla *DTxApp* e dalla *Web dashboard*.

La *Web Dashboard* è un portale *web* che tipicamente permette di accedere ad un sottoinsieme (oppure un soprainsieme, a seconda del ruolo ricoperto dal soggetto che vi accede, ad esempio paziente, *caregiver* oppure medico) delle funzionalità offerte dalla *DTxApp*.

Sul *cloud*, che può essere pubblico, privato o ibrido a seconda delle esigenze, risiedono e vengono eseguiti anche altri servizi di supporto quali, ad esempio, meccanismi di autenticazione, di gestione dei profili utenti (e delle terapie), di accesso/memorizzazione dati dinamici, strumenti di *data analytics*, di riconoscimento vocale e di immagini, di monitoraggio, di *data stream processing* (DSP), solo per citarne alcuni. C'è da porre in evidenza che il *Cloud Data Store* che mantiene i dati dei pazienti e delle terapie dovrebbe essere gestito da un *cloud provider* specializzato nella gestione dei dati sanitari o che sia certificato per tale scopo (ad es. HIPAA, HITRUST CSF, ISO/IEC 27018).

Infine, il sistema DTx/SaMD potrebbe mettere a disposizione ulteriori API (le "*Third party access API*" in *figura*), per consentire a sistemi di terze parti di accedere ai dati raccolti (ad esempio il Ministero della Salute, le farmacie, oppure aziende farmaceutiche che producono e distribuiscono farmaci tradizionali abbinati alla terapia digitale).

Veniamo ora ad analizzare chi sono gli attori che interagiscono con il sistema:

- **Il paziente** è il soggetto che accede alla *DTxApp* mediante il dispositivo *mobile* personale su cui l'*App* è installata. L'*App* mette a disposizione del paziente una interfaccia utente (UI). La *DTxApp* tipicamente consente anche di monitorare alcuni parametri vitali del paziente, attraverso sensori *wireless*, impiantabili o indossabili (*implantable/wearable body sensors*). Il paziente, inoltre, può interagire con la *DTxApp* attraverso la *Web dashboard*, ad esempio attraverso un *personal computer*.
- **Il *caregiver*** è la persona di riferimento che normalmente affianca il paziente nella quotidianità. Rappresenta colui/colei che risponde alle chiamate, che ricorda le terapie, che accompagna il paziente lungo il percorso diagnostico-terapeutico ed assistenziale e che si prende in carico della cura quotidiana. Il *caregiver* accede anch'esso al sistema DTx/SaMD mediante *DTxApp* o *Web dashboard*.
- **Il medico** accede al sistema mediante la *Web dashboard* per controllare lo stato del paziente e l'evoluzione della terapia.
- **Il professionista sanitario** (infermiere, logopedista o altro profilo sanitario) prende in carico, su prescrizione del medico, eventuali bisogni e/o interventi derivanti dalla lettura dei dati trasmessi. Il professionista sanita-

rio accede al sistema DTx/SaMD mediante *Web dashboard*.

• **Le terze parti** sono soggetti che possono accedere ai dati, tipicamente aggregati e anonimizzati mediante apposite API, come ad esempio farmacie o produttori di farmaci abbinati alla terapia digitale, il Ministero della Salute, etc.

• **Gli amministratori,** non considerati in questa trattazione, sono i soggetti incaricati di gestire la piattaforma *cloud* della DTx/SaMD.

Ai fini della comprensione delle possibili minacce *cyber*, è importante anche spiegare brevemente come interagiscono le varie componenti del sistema *DTxApp*. Sempre facendo riferimento all'architettura riportata in *figura 1* (partendo dal basso):

• I sensori forniscono i dati mediante *bluetooth* o altro protocollo *wireless* alla *DTxApp*.

• La *DTxApp*, installata e in esecuzione sul dispositivo *mobile* del paziente, utilizza le funzionalità del sistema operativo (Android o IOS) per quanto riguarda l'accesso alle risorse (ad es. memoria locale) e le operazioni di I/O (ad esempio uso della rete *Internet*, del *display*, dell'audio, della fotocamera).

• La *DTxApp* comunica con *DTxApp backend* per eseguire procedure quali autenticazione, accesso al profilo utente e alla terapia, accesso a dati dinamici, invio di dati generati da sensori o dalla *DTxApp* stessa, etc. L'interazione tra *DTxApp* e *DTxApp backend* avviene attraverso *Internet*, solitamente mediante *web services* (API REST).

• *DTxApp backend* utilizza i servizi della piattaforma *cloud* per garantire prestazioni, affidabilità e sicurezza, come ad esempio bilanciamento del carico, servizi di *scaling* delle risorse, distribuzione geografica, ridondanza, VPN, *firewall*, etc...

• *DTxApp backend*, a sua volta, può anche utilizzare i servizi forniti dal *cloud* quali autenticazione, gestione dei profili utenti, cifratura dei dati, piattaforme scalabili per l'analisi dei dati (ad es. Hadoop) o per il *data stream processing* (ad es. Spark).

• *DTxApp backend* legge e scrive dati da uno o più *Cloud Data Store*.

• La *Web dashboard* utilizza le API fornite dal *DTxApp backend* per l'accesso *web* alle funzionalità della *DTxApp* e alla *Digital therapy*.

2.2 Analisi delle minacce

Nel seguito verranno esaminate le minacce *cyber* del sistema di terapia digitale introdotto nella sezione precedente.

Molte delle componenti del sistema DTx/SaMD in *figura 1* (quelle rappresentate in verde) possono essere messe in sicurezza utilizzando buone pratiche e tec-

nologie *standard*, come anche evidenziato nei documenti MDCG e MDRF. In particolare, sono disponibili soluzioni tecnologiche e controlli di sicurezza per le reti e i protocolli di comunicazione (ISO/IEC 27033 Parti da 1 a 6), per i servizi *cloud* (ISO/IEC 27017) e per le applicazioni che vengono eseguite sul cloud come parte integrante o supporto alla terapia digitale. Viceversa, la *DTxApp* (l'*App* eseguita sul dispositivo *mobile* dell'utente) ed il *Cloud Data Store* (rappresentati in rosso nella *figura 1)* sono i nodi deboli del sistema e richiedono un'analisi particolare.

2.2.1 Principali minacce della componente *Cloud Data Store*

Il *Cloud Data Store* (CDS) è sicuramente una delle risorse più appetibili per chi volesse attaccare il sistema[5]. Come evidenziato da Tang et al.[6], *i Cloud Data Store* possono essere soggetti a vari tipi di minacce, come ad esempio il furto di dati o la loro divulgazione, l'accesso illegale, la corruzione o perdita di dati, e la violazione della *privacy*. Tali minacce possono essere perpetrate da *hacker*, *cloud service provider* curiosi (ovvero che possono accedere ai dati e agli accessi degli utenti) o *cloud service provider* vulnerabili (ovvero che possono perdere o compromettere i dati). Recentemente, la comunità scientifica ha proposto diverse tecniche per rendere sicuri i CDS, ma tali soluzioni non sono ancora mature. Inoltre, le tecniche da utilizzare dipendono strettamente dallo specifico uso del CDS e dai requisiti di sicurezza.

Ad esempio, se è necessario effettuare delle ricerche sui dati preservandone la confidenzialità, viene consigliato l'impiego di tecniche crittografiche che permettano di ricercare un'informazione all'interno di un *database* cifrato (*searchable encryption*)[7]: solo il risultato finale verrà decifrato. Se invece è di interesse garantire la confidenzialità dei dati durante la loro elaborazione per mezzo di un'applicazione (ad esempio DTx *backend* o applicazioni di terze parti), dovrebbero essere utilizzate tecniche crittografiche dette *homomorphic encryption*[8] che permettono di effettuare calcoli sui dati cifrati senza la necessità di decriptare il dato stesso. Nel caso in cui il *provider* di terapia digitale sia interessato a condividere i dati con le terze parti, i medici e i pazienti stessi, è necessario preservare la controllabilità dell'accesso ai dati e l'integrità del dato. Andranno quindi usati innovativi protocolli per il controllo degli accessi, come ad esempio:

- *selective encryption*[9], che consente un accesso selettivo a dati cifrati mediante l'uso di avanzate tecniche di gestione delle chiavi di cifratura;
- *attribute-based encryption*[10], ovvero una tecnica di gestione delle politiche di accesso ai dati cifrati in base ai privilegi degli utenti (ad es. medici, pazienti, terze parti, amministratori);
- *provable data possession*[11], che permette al fornitore del servizio

DTx/SaMD di verificare che i dati memorizzati in un CDS siano corretti (utile nel caso in cui il CDS non sia sotto il controllo di DTx/SaMD *provider* ma affidato a terze parti);

- *proof of retrievability*[12], che permette di verificare che un *file* sia intatto e sempre a disposizione degli utenti legittimi.

Infine, è importante considerare il problema della *privacy* degli utenti che accedono ai dati memorizzati nel CDS e ai servizi *cloud* (DTx/SaMD). Differenti tecniche innovative sono state proposte, come ad esempio:

- *Access pattern protection*[13], per mascherare il comportamento degli utenti che accedono ad un servizio *cloud* (osservando, infatti, tali comportamenti chi attaccasse il sistema può dedurre varie informazioni sensibili dell'utente);
- *Query privacy protection*[14], per mascherare le associazioni tra gli indici e le parole chiave usate per le ricerche e i dati corrispondenti;
- *User identity protection*[15], per mantenere segreta l'identità di un utente che accede ai dati (a seguito della sua autenticazione).

2.2.2 Principali minacce della componente *DTxApp*

Le pratiche di sicurezza introdotte in MDCG e MDRF, benché generalmente riconosciute come efficaci, possono avere piena applicazione in una infrastruttura dove c'è completo controllo di ogni singola componente rappresentata in *figura 1*. La principale differenza tra un *Medical Device* (MD) ed un SaMD è proprio l'infrastruttura ed il controllo che si può avere su di essa. Mentre in un classico MD, come potrebbe essere un *pacemaker*, il produttore ha la possibilità di controllare e certificare ogni aspetto dello sviluppo, dal *firmware* ai protocolli di comunicazione, al sistema di *update* e così via, in una generica SaMD ci troviamo in uno scenario nel quale si affida gran parte del controllo della sicurezza a fattori esterni, legati al sistema operativo (Android oppure iOS) del dispositivo *mobile* del paziente e che risulta essere fuori dal controllo del produttore di DTx/SaMD.

Nello specifico, come affermato nella "*Practice 4 - Secure implementation*" di MDCG, ogni componente del sistema fornito esternamente deve sottostare alle pratiche definite in "*Practice 1 - Security management*", che però sono insufficienti nel mantenere un elevato *standard* di sicurezza nei casi di DTx/SaMD, almeno rispetto alla sicurezza del dispositivo *mobile* del paziente.

Infatti, dato il costante aumento di *malware* su piattaforme mobile, c'è la non remota possibilità che lo *smartphone* del paziente sia già compromesso, prima ancora che il SaMD sia installato. Uno studio dell'Azienda Kaspersky su dati raccolti nell'anno 2019, ad esempio, ha rilevato "*3.503.952 malicious installation packages*", "*69.777 nuovi mobile banking Trojans*" e "*68.362 nuovi*

mobile ransomware Trojans" presenti sui dispositivi mobili dei propri clienti[16].

Questa possibilità non è coperta dai documenti MDCG e MDRF e merita particolare attenzione in quanto rappresenta un rischio evidentemente non trascurabile. Si potrebbe obiettare che un rischio simile si corra anche avendo applicazioni altrettanto sensibili, come ad esempio le applicazioni bancarie in grado di fare transazioni finanziarie, ma è facile dimostrare come le due situazioni siano, invece, gestite in maniera alquanto diversa. Nel caso di una compromissione di uno *smartphone* in cui è presente un'applicazione bancaria, sarà sempre necessario, per perpetrare l'azione malevola di un attaccante, interfacciarsi con i sistemi della banca, poiché tutte le informazioni finanziarie sono conservate e gestite esclusivamente dai sistemi della banca stessa, mentre l'applicazione è solo un'interfaccia per l'utente. Per questo motivo la banca ha sempre modo di accorgersi dell'attività anomala, eventualmente bloccarla e segnalarla all'utente e alle autorità competenti. Questo perché le operazioni bancarie devono essere sempre e comunque approvate dai *server* della banca. Al contrario, in un SaMD, il paziente segue la terapia e fornisce *input* (se richiesti) all'applicazione in completa autonomia, generalmente senza la necessità di una costante validazione da parte della componente "*DTxApp backend*": l'interazione è diretta fra il paziente e l'*App* di terapia digitale installata sul suo dispositivo *mobile*. Questo primo esempio lascia intuire come lo scenario di un SaMD sia differente sia da qualsiasi altro *medical device*, sia da qualsiasi altra *App* utilizzata oggi, da un punto di vista della gestione del rischio da attacchi *cyber*.

Prendiamo adesso in esame altri due casi. Nel primo, il *malware*, già installato e con completo controllo del sistema, fa sì che la terapia somministrata al paziente sia diversa da quella realmente intesa per lui. Avendo il *malware* completo controllo del sistema, esso avrà anche la possibilità di far vedere al sistema *cloud* di controllo come tutto sia nella norma e che il paziente stia migliorando. Dal momento che molti SaMD attualmente sfruttano meccanismi terapeutici simili alle psicoterapie cognitivo-comportamentali, un cambio mirato di queste terapie nel trattamento di seri disturbi, come ad esempio il trattamento di una dipendenza da sostanze stupefacenti, potrebbe causare un peggioramento del paziente.

Nel secondo caso, il *malware*, invece di modificare il contenuto delle terapie somministrate, modifica gli *input* e le risposte che il paziente fornisce all'*App DTxApp*, alterando così, e questa volta in modo passivo (cioè senza alterare il *software* della terapia digitale), il percorso terapeutico seguito dal paziente. Alcuni SaMD, infatti, adattano la terapia ai progressi e cambiano gli obiettivi terapeutici man mano che certi risultati sono o me-

no raggiunti. Indurre questo tipo di sistemi a pensare che certi obiettivi terapeutici sono stati raggiunti modificherà, ad esempio, in modo prematuro la terapia somministrata al paziente, facendo perdere di efficacia il trattamento o addirittura causando un peggioramento del paziente.

Questi esempi dimostrano come nel caso di SaMD non siano sufficienti le normali pratiche di sicurezza descritte nei documenti MDCG e MDRF, ma siano necessarie specifiche azioni di approfondimento per mitigare le minacce e i rischi specifici sopra descritti. Alcune possibili soluzioni potrebbero consistere nell'attestazione sicura del dispositivo *mobile* dell'utente o della *DTxApp*[17], e nell'integrazione di sistemi crittografici per la validazione da parte del sistema *cloud* di controllo delle terapie somministrate dal SaMD al paziente. Bisognerebbe inoltre dotare DTx/SaMD di meccanismi di *anomaly detection* per individuare automaticamente o semi-automaticamente le anomalie nella somministrazione e nella risposta alle terapie come precedentemente menzionato. Va però osservato che, se i dati di un paziente sono compromessi sin dall'inizio della terapia, potrebbe essere impossibile identificare le anomalie mancando dati "corretti" su cui basare le decisioni. Dunque, nei casi sospetti, sembra necessario un canale di comunicazione indipendente, fidato, diretto e frequente con il paziente per confermare lo stato dello svolgimento terapeutico e i reali miglioramenti o peggioramenti ottenuti. Tale canale può essere realizzato estendendo le funzionalità della *control room* in cui operano dei professionisti sanitari che rispondano ai "dubbi" dei pazienti e dei *caregiver* rispetto all'eventuale cambiamento di programma. In questo caso, occorre che gli operatori che rispondono al telefono siano in grado di parlare correttamente le lingue e di comprendere ciò che il paziente/*caregiver* riporta.

2.3 Considerazioni conclusive

In conclusione, le terapie digitali presentano rischi legati alle minacce *cyber* che devono essere specificatamente valutati e limitati, in particolare considerando la specifica caratteristica di DTx/SaMD di essere una commistione fra un dispositivo medico e un *software* distribuito su un'architettura complessa. Benché siano disponibili molte soluzioni tecnologiche in grado di consentire un'adeguata mitigazione dei rischi *cyber* sia per i dispositivi medici che per i prodotti *software*, è proprio la peculiarità di DTx/SaMD che richiede una ulteriore e specifica integrazione alle pratiche e ai principi esposti nei documenti MDCG e MDRF. A mero titolo di esempio, si potrebbe prendere il modello e la struttura della famiglia di *standard* ISO/IEC 27000 che descrive le pratiche per realizzare il sistema di gestione della sicurezza delle

informazioni: a corredo delle linee guida generali e dei requisiti per la gestione della sicurezza delle informazioni che sono obbligatoriamente molto ampi perché pensati per adattarsi ad organizzazioni di qualsiasi tipo e dimensione, gli *standard* forniscono documenti aggiuntivi con linee guida in specifici ambiti/settori (es. per i servizi finanziari, per i servizi in *cloud*, per le comunicazioni intersettoriali e inter-organizzative etc). Inoltre, per rendere più concreto e facilmente applicabile il loro utilizzo, gli *standard* definiscono anche una serie di annessi contenenti i controlli ed i meccanismi specifici per garantire un'adeguata gestione della sicurezza delle informazioni. Anche per il caso di DTx/SaMD sembra fondamentale una trattazione sistematica della loro particolare situazione nei confronti dei rischi *cyber* e lo sviluppo coordinato di un documento specifico con le linee guida per la gestione della sicurezza delle informazioni da loro trattate, e con una serie di controlli dedicati da applicare durante il loro intero ciclo di vita.

What is known:

- Le terapie digitali svolgono la loro funzione trattando dati inerenti allo stato di salute del paziente, che rientrano nella nozione di "particolari categorie di dati" (ex art. 4 lett. 15 del Regolamento UE 2016/679). Occorrerà quindi analizzare i profili giuridici inerenti tale tipologia di trattamento dati alla luce del recente Regolamento UE 2016/679 (cosiddetto GDPR). Il soggetto che si qualifica come Titolare del trattamento dovrà garantire che i dati vengano trattati nel rispetto dei principi elencati all'art. 5 del GDPR, in particolare: principio di liceità - di limitazione della finalità - di trasparenza - di correttezza - di minimizzazione dei dati - di esattezza dei dati - di limitazione della conservazione dei dati
- Dato un sistema DTx/SaMD, sono disponibili soluzioni tecnologiche e controlli di sicurezza per proteggere le reti e i protocolli di comunicazione (ISO/IEC 27033 Parti da 1 a 6), i servizi *cloud* (ISO/IEC 27017) e le applicazioni che vengono eseguite sul *cloud* come parte integrante o supporto alla terapia digitale
- La fruizione della terapia è basata su di una politica *Bring-Your-Own-Device*, ovvero il paziente, per accedere alla cura, deve dotarsi di un dispositivo (ad es. *smartphone*) e della relativa connessione dati.

What is uncertain:

- Il *Cloud Data Store* è sicuramente una delle risorse più appetibili per un attaccante. Le minacce a cui un *Cloud Data Store* è soggetto possono essere, ad esempio, il furto di dati o loro divulgazione, l'accesso illegale, la cor-

ruzione o perdita di dati, e la violazione delle *privacy*. La comunità scientifica ha proposto varie soluzioni, non ancora mature, per garantire la confidenzialità, l'integrità, la disponibilità e la *privacy* dei dati memorizzati in un *Cloud Data Store*. Ciò va attentamente considerato in fase di progettazione ed implementazione di un sistema DTx/SaMD

- Il fatto che una *DTxApp* venga installata su di un dispositivo *mobile* dell'utente per definizione non è *trusted,* e questo comporta implicazioni che possono compromettere l'efficacia della terapia oppure portare a seri effetti indesiderati. Data la loro intrinseca generalità, le linee guida MDCG e MDRF non trattano minimamente questo importante aspetto.

What we recommend:

- È necessario affiancare all'utilizzo delle linee guida di *governance* di alto livello, quali MDCG e MDRF, una specifica analisi tecnica approfondita del nuovo rischio *cyber* prodotto dalla commistione tra il *software* complesso di una *App* per dispositivo *mobile* ed il concetto tradizionale di dispositivo medico, al fine di produrre i controlli di sicurezza specifici per DTx/SaMD, ad esempio seguendo la struttura della famiglia degli *standard* ISO/IEC 27000
- È necessario verificare le competenze digitali di pazienti e di *caregiver* prima di prescrivere una DTX, e fornire *tutorial* o corsi di formazione che considerino come centrale la figura del paziente.

Riconoscimenti

Il lavoro di E. Casalicchio, L.V. Mancini, A. Mei, A. Spognardi è finanziato da Sapienza Università di Roma nell'ambito del progetto "PRISMA - *PRIvacy-preserving, Security, and MAchine-learning techniques for healthcare applications*" e dal MIUR nell'ambito del "Dipartimenti di eccellenza 2018-2022" del Dipartimento di Informatica, Sapienza Università di Roma.

Riferimenti bibliografici

1. Medical Device Coordination Group MDCG 2019-16 - Guidance on Cybersecurity for medical device - December 2019. https://ec.europa.eu/docsroom/documents/41863

2. International Medical Device Regulators Forum - March 2020 - Principle

and practice for medical device Cybersecurity - March 2020 http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

3. https://dtxalliance.org/

4. What is Mobile App Development? https://aws.amazon.com/mobile/mobile-application-development/

5. Akil M, Mancini LV, Venturi D. Multi-covert channel attack in the cloud. *Sixth IEEE International Conference on Software Defined Systems* 2019: 160-5.

6. Tang J, Cui Y, Li Q, et al. Ensuring security and privacy preservation for Cloud Data Services. *ACM Computing Surveys* 2016; 49; Article 13. https://doi.org/10.1145/2906153.

7. Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data. In Proceedings of IEEE 30th International Conference on Distributed Computing Systems (ICDCS'10) 2010: 253–62.

8. Gentry C. A Fully Homomorphic Encryption Scheme. Ph.D. Dissertation. Stanford University, 2009.

9. De Capitani Di Vimercati S, Foresti S, Jajodia S, et al. Encryption policies for regulating access to outsourced data. *ACM Transactions on Database Systems (TODS)* 2010; 35: 12.

10. Sahai A, Waters B. Fuzzy identity-based encryption. In: *Advances in Cryptology (EUROCRYPT'05)* 2005, Springer: 457-73.

11. Ateniese G, Di Pietro R, Mancini LV, Tsudik G. Scalable and efficient provable data possession. *Proceedings 4th Intl. Conf. on Security and Privacy in Communication Networks (SecureComm 2008),* September 2008.

12. Juels A, Kaliski BS Jr. PORs: Proofs of retrievability for large files. In: *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07).* ACM 2007: 584-97.

13. Yang K, Zhang J, Zhang W, Qiao D. A light-weight solution to preservation of access pattern privacy in untrusted clouds. In: *Computer Security (ESORICS'11)* 2011, Springer: 528-47.

14. Cao N, Wang C, Li M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2014; 25: 222-33.

15. Wang B, Li B, Li H. Knox: Privacy-preserving auditing for shared data with large groups in the cloud. In: *Applied Cryptography and Network Security* 2012, Springer: 507-25.

16. Chebyshev V. Mobile malware evolution 2019. Kaspersky https://securelist.com/mobile-malware-evolution-2019/96280/

17. Dushku E, Rabbani M, Conti M, et al. SARA: Secure Asynchronous Remote Attestation for IoT systems. *IEEE Trans Inf Forensics and Security* 2020; 15: 3123-36.