

**SERVIZI DI
MESSAGGISTICA
TRA SOVRANITÀ
DIGITALE E
DATA PRIVACY**





AUTORI

Alessandro Passamonti
Emma Bagnulo
Luigi Iandolo
Virginio Dotto

CURATORI

Marco Baticci

SI RINGRAZIANO

Alessia Sementilli
Federico Muzzati
Fiammetta Del Mancino
Leonardo Spadolini



Indice dei contenuti

Introduzione: le app di messaggistica tra sovranità digitale e <i>privacy</i>.....	4
Sovranità tecnologica e data privacy: l'importanza delle app di messaggistica.....	7
Caratteristiche delle app di messaggistica diffuse e l'esempio di Telegram.....	11
Modelli di Business e Strategie di Monetizzazione.....	12
Il caso di Telegram.....	14
Tirando le somme: il futuro delle app di messaggistica.....	18
L'approccio statunitense e Wickr.....	19
Olvid e Tchap: l'approccio francese.....	23
Tchap: uno strumento istituzionale federato e pilastro della politica pubblica digitale.....	23
Olvid: crittografia radicale e approccio decentralizzato alla riservatezza istituzionale....	24
Un riflesso della sovranità strategica francese.....	26
Il caso italiano: TelsynTouch App.....	26
Conclusioni e proposte di policy.....	29
1. Una piattaforma italiana.....	29
2. Un regolamento per l'utilizzo.....	30
3. Un sostegno alla ricerca.....	30
Bibliografia.....	32

Introduzione: le app di messaggistica tra sovranità digitale e *privacy*

Negli ultimi anni, le applicazioni di messaggistica hanno assunto un ruolo centrale nella comunicazione digitale, sollevando in tal modo crescenti questioni rispetto alla privacy e protezione dei dati, con la questione che si fa ancora più pressante quando l'oggetto delle comunicazioni sono informazioni critiche e riservate a livello nazionale.

Questo paper analizza il fenomeno delle app di messaggistica nel contesto più ampio della sovranità digitale e della data privacy, evidenziando le sfide e le opportunità che tali strumenti pongono per governi, aziende e cittadini. Il lavoro si apre con un'analisi del concetto di sovranità digitale, esplorando il modo in cui la gestione dei dati e delle infrastrutture tecnologiche impatta sulla sicurezza nazionale e sulle politiche di regolamentazione. Successivamente, si esamina il ruolo delle piattaforme di messaggistica nella società moderna, approfondendone l'impatto sociale, culturale e politico, le caratteristiche tecniche e il modello di business e come questi fattori influenzano la dicotomia tra i benefici di tale piattaforme e i rischi ad esse connesse.

Il paper analizza applicazioni e casi studio come Telegram, Wickr negli USA e Olvid in Francia valutandone l'architettura tecnica, il modello di sicurezza, il rapporto con i governi, le modalità di adozione e le eventuali criticità emerse nel tempo. Particolare attenzione è dedicata al bilanciamento tra protezione della privacy e necessità di controllo da parte delle autorità. Il lavoro si conclude con una serie di proposte di policy per il caso italiano, delineando possibili strategie per garantire una maggiore tutela della privacy e della sicurezza digitale, senza compromettere le esigenze di regolamentazione e contrasto agli abusi.

Negli ultimi decenni, le applicazioni di messaggistica hanno rivoluzionato il modo in cui le persone comunicano, integrando funzioni multimediali e interazioni in tempo reale. Queste piattaforme hanno abbattuto barriere geografiche e culturali, influenzando profondamente le dinamiche sociali e facilitando la formazione di comunità virtuali. Tuttavia, questo progresso tecnologico è accompagnato da sfide significative, tra cui la gestione dei contenuti e la protezione della privacy.

Storia e evoluzione della messaggistica

La storia della messaggistica è iniziata con gli SMS, il primo servizio di scambio di messaggi brevi per telefonia mobile. Nel corso degli anni, questo sistema è stato sostituito da tecnologie più avanzate basate su Internet, che offrono comunicazioni gratuite e accessibili globalmente. Le moderne piattaforme di messaggistica utilizzano infrastrutture cloud e offrono una vasta gamma di funzionalità, tra cui videochiamate, servizi di pagamento e condivisione di documenti. Queste piattaforme sono diventate veri e propri ecosistemi digitali integrati, che combinano comunicazione, social networking e servizi finanziari.

L'evoluzione tecnologica ha comportato una migrazione dalle infrastrutture telefoniche tradizionali a quelle di Internet, spostando il controllo dei dati da enti governativi a compagnie private, principalmente straniere. Questo cambiamento ha aumentato il numero di attori



coinvolti nella gestione dei dati e ha complicato il controllo giurisdizionale, poiché i dati possono essere archiviati e gestiti in diverse parti del mondo.

Modelli di monetizzazione e privacy

I modelli di monetizzazione delle piattaforme di messaggistica istantanea creano tensioni con la privacy degli utenti. La sostenibilità economica di molte di queste piattaforme dipende dall'uso dei dati personali degli utenti, che vengono aggregati e analizzati per alimentare sofisticati sistemi di profilazione. Questi profili sono utilizzati per la pubblicità mirata su diverse piattaforme, riflettendo il paradigma del "Capitalismo della Sorveglianza", teorizzato da Shoshana Zuboff. In questo contesto, l'esperienza umana viene trasformata in dati comportamentali, generando un conflitto con la privacy.

Le piattaforme tendono a raccogliere più dati del necessario, e la loro condivisione all'interno di grandi gruppi aziendali, come Meta dopo l'acquisizione di WhatsApp, ha sollevato forti preoccupazioni. La condivisione dei dati tra diverse entità aziendali aumenta il rischio di violazioni della privacy e rende più complesso il controllo dei dati da parte degli utenti.

Sovranità digitale e regolamentazione

La crescente consapevolezza del pubblico riguardo alla protezione della privacy ha portato a una serie di risposte normative volte a garantire una maggiore tutela dei dati personali. Tra queste, un esempio significativo è l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) nell'Unione Europea nel 2018. Questo regolamento ha stabilito un insieme di norme rigorose per la protezione dei dati personali, aumentando la trasparenza nella gestione dei dati da parte delle aziende e rafforzando il controllo dei cittadini sui propri dati.

Il GDPR rappresenta un passo importante verso la standardizzazione delle pratiche di protezione dei dati in tutta l'UE, sostituendo la precedente direttiva 95/46/CE e introducendo concetti come la "privacy by design" e l'approccio basato sul rischio. Inoltre, il regolamento ha introdotto il diritto alla portabilità dei dati, che consente agli individui di trasferire i propri dati personali da un fornitore di servizi all'altro, promuovendo la concorrenza e l'innovazione nel mercato digitale.

Parallelamente a queste iniziative normative, il concetto di sovranità digitale è diventato sempre più rilevante. La sovranità digitale si riferisce alla capacità di uno Stato di regolare ed esercitare il governo della tecnologia e dei servizi all'interno dei propri confini. Questo concetto include diversi aspetti fondamentali, come il controllo sulla residenza, giurisdizione, protezione, indipendenza, mobilità, interoperabilità e portabilità dei dati. In sintesi, lo Stato deve avere il controllo su dove, chi, da chi, con chi, verso dove, per cosa e come i dati dei cittadini vengono gestiti. Ciò è essenziale per garantire che i dati siano protetti e utilizzati in modo trasparente e sicuro, mantenendo al contempo la capacità dello Stato di regolare e governare lo spazio digitale all'interno dei propri confini.

In questo contesto, la sovranità digitale è strettamente legata alla protezione dei dati personali, poiché entrambe richiedono un controllo efficace sulla gestione dei dati e sulla loro circolazione. La capacità di uno Stato di esercitare la sovranità digitale è quindi cruciale per mantenere il monopolio sulla gestione dei dati dei cittadini e per garantire che le norme di protezione dei dati siano applicate in modo coerente e uniforme all'interno dei propri confini.



Questo aspetto è particolarmente rilevante in un'epoca in cui le tecnologie digitali sono sempre più integrate nella vita quotidiana e le informazioni personali sono una risorsa fondamentale per le economie moderne.

Ruolo delle app di messaggistica nella sovranità digitale

Le app di messaggistica svolgono un ruolo fondamentale nella sovranità digitale. Queste piattaforme sono utilizzate dalla maggioranza della popolazione: in Italia, ad esempio, il 78.5% degli italiani ha installato WhatsApp sul proprio telefono, mentre Facebook Messenger e Telegram sono usate rispettivamente dal 40% e dal 36% della popolazione. La centralità della data privacy nella sovranità digitale è stata sottolineata anche dal Piano Italia Digitale 2026, che evidenzia l'importanza di proteggere i dati dei cittadini per mantenere il controllo sullo spazio digitale.

In questo contesto, le app di messaggistica rappresentano un punto critico nella gestione dei dati personali e nella protezione della privacy. La loro diffusione e l'uso intensivo richiedono una regolamentazione efficace per garantire che i dati degli utenti siano protetti e gestiti in modo trasparente e sicuro. La sfida per il futuro sarà quella di bilanciare la libertà di comunicazione con la necessità di proteggere la privacy e la sovranità digitale.

Il presente paper analizza le caratteristiche principali delle app di messaggistica e ne evidenzia il ruolo strategico nella sovranità digitale degli stati. Dopo aver presentato alcune delle iniziative più rilevanti in materia da parte di partner internazionali, il documento offre delle proposte di policy, spunti di miglioramento relativi al contesto regolatorio e strategico nazionale.

Sovranità tecnologica e data privacy: l'importanza delle app di messaggistica

La necessità di una solida guida governativa delle pervasive applicazioni tecnologiche viene, nel discorso comune, descritta con diversi termini. Tra i tanti, emergono sovranità tecnologica e sovranità digitale. Questi due termini, pur simili all'apparenza, presentano in verità alcune differenze sostanziali che è bene rimarcare. La sovranità tecnologica rappresenta infatti la capacità di un'entità statale o sovranazionale di sviluppare, produrre e controllare tecnologie critiche in modo autonomo, riducendo la dipendenza da attori esteri e preservando il controllo strategico su settori chiave. In tal senso, l'Unione Europea ha intensificato gli sforzi per raggiungere un'autonomia tecnologica collettiva, concentrandosi sulla promozione e la difesa di tecnologie strategiche. La Presidente della Commissione Europea Ursula von der Leyen, ad esempio, ha enfatizzato l'urgenza di investire in settori strategici come l'informatica quantistica, l'intelligenza artificiale, la blockchain e la produzione di semiconduttori, considerati elementi cardine per la competitività e la sicurezza economica dell'UE. Questo approccio mira a bilanciare efficienza e indipendenza, evitando dipendenze unilaterali da potenze globali come Cina e Stati Uniti, in un contesto di crescente competizione tecnologica.

D'altra parte, la ricerca di autonomia strategica nel contesto digitale si concretizza nel concetto di **sovranità digitale**, che, pur essendo intimamente connesso alla sovranità tecnologica (quest'ultima abilitante per la prima attraverso lo sviluppo di infrastrutture critiche e tecnologie sicure), ne rappresenta una declinazione più particolare. Infatti, **la sovranità digitale si configura come la capacità di uno Stato di governare e regolamentare l'ecosistema tecnologico entro i propri confini, garantendo il controllo integrale del ciclo di vita dei dati**: dalla residenza alla giurisdizione, dalla protezione alla mobilità, fino all'interoperabilità e alla portabilità.

Questo paradigma impone alle autorità competenti di definire con precisione i parametri chiave del dominio digitale: geografia dei dati (dove risiedono), controllo giurisdizionale (chi li gestisce), sicurezza informatica (da chi sono protetti), autonomia operativa (con quali tecnologie), flussi transnazionali (verso dove si spostano), finalità d'uso (per cosa servono) e standard tecnici (come vengono processati). La mancata padronanza di questi elementi comprometterebbe il monopolio regolatorio statale, esponendo il Paese a rischi di dipendenza tecnologica e vulnerabilità strategica.

In un contesto globale dove la dimensione fisica e digitale della vita individuale e collettiva si intrecciano in modo irreversibile, la sovranità digitale è emersa come priorità trasversale nelle agende politiche nazionali e sovranazionali europee. Questo slancio si è concretizzato nel 2021 con l'appello congiunto di Angela Merkel, Kaja Kallas, Mette Frederiksen e Sanna Marin alla Presidente della Commissione Europea Ursula von der Leyen, sollecitando un'accelerazione nella costruzione di un **mercato unico digitale**¹ basato su standard comuni, interoperabilità e autonomia tecnologica.

¹ Sean Fleming, "What Is Digital Sovereignty and How Are Countries Approaching It?", World Economic Forum, 10 gennaio 2025, <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>.

L'iniziativa dei leader europei ha trovato eco nel 2022 con la conferenza francese "Building Europe's Digital Sovereignty"², evidenziando l'importanza strategica del tema per un'Europa che fatica a rimanere al passo con il cambiamento tecnologico.

La costruzione di una sovranità digitale europea rimane un obiettivo complesso e progressivo, ma il percorso intrapreso da Bruxelles mostra avanzamenti strutturali in ambito normativo e infrastrutturale. Sul piano legislativo, l'UE ha rafforzato il controllo sui contenuti digitali attraverso il Regolamento 2021/784 per contrastare la diffusione di materiale terroristico online e la COM/2022/209 per prevenire gli abusi sessuali su minori online, segnalando una transizione da approcci reattivi a modelli proattivi di governance digitale. Sono poi state incluse sanzioni sostanziali per la non conformità nella DSA, il passaggio a misure regolamentate e lo spostamento dalla lotta ai contenuti illegali e dannosi su base individuale e di gruppo a misure sistemiche.³

Sul fronte infrastrutturale, il progetto Gaia-X (2020) incarna la volontà europea di creare un'infrastruttura di cloud computing sicura, trasparente e interoperabile per aziende e istituzioni in Europa. In particolare, il progetto vuole ridurre la dipendenza dai giganti del cloud statunitensi e cinesi, creare un ecosistema di collaborazione per le piattaforme cloud, favorire la crescita di un'industria europea, e assicurare il rispetto delle normative europee.

L'Italia si configura come hub centrale per la sovranità digitale continentale, grazie alla sua posizione nel Mar Mediterraneo, crocevia del 16% del traffico dati globale attraverso una fitta rete di cavi sottomarini. Questa centralità infrastrutturale, analizzata nello studio⁴ del 2023 dell'AWARE Think Tank, rappresenta un'opportunità strategica per garantire la resilienza delle reti europee.

Il piano Italia Digitale 2026⁵ dettaglia cronoprogramma e obiettivi da raggiungere per portare l'Italia ai primi posti in Europa per il digitale. Per raggiungere gli obiettivi di Italia 2026 sul digitale sono state usate molte delle risorse offerte dal PNRR, circa il 27%. Tra i vari interventi "fisici" vanno considerati la costruzione della rete 5G nazionale, costata quasi 7 miliardi, e gli investimenti in infrastrutture, nonché la digitalizzazione della Pubblica Amministrazione. Per quest'ultimo obiettivo, sono stati predisposti 6.74 miliardi di euro.

Nel 2021 è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN), volta a garantire la cybersicurezza di enti ed organizzazioni nazionali, seguita dal Polo Strategico Nazionale, nato per ospitare i dati delle amministrazioni pubbliche. Si mira infatti a trasferire 12404 enti pubblici italiani in un cloud ad hoc entro la seconda metà del 2026 e ad aumentare l'utilizzo dei servizi SPID e CIE fino ad avere 16500 enti che se ne servano. L'identità digitale inoltre

² France Diplomacy, "Building Europe's Digital Sovereignty", Ministry for Europe and Foreign Affairs, 7 febbraio 2022,

<https://www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-europe/france-and-the-european-union/the-french-presidency-of-the-council-of-the-european-union/article/building-europe-s-digital-sovereignty-7-feb-22>.

³ Flonk, D., Jachtenfuchs, M. e Obendiek, A., 2024. "Controlling Internet Content in the EU: Towards Digital Sovereignty." *Journal of European Public Policy* 31 (8).

⁴

<https://www.awarethinktank.it/wp-content/uploads/2022/05/I-cavi-sottomarini-come-infrastruttura-critica.pdf>

⁵ <https://innovazione.gov.it/italia-digitale-2026/>

dovrà essere utilizzata dal 70% della popolazione entro il 2026. Sistemi informativi e basi dati degli enti pubblici stanno diventando interoperabili grazie alla nuova Piattaforma Digitale Nazionale Dati. In poche parole, l'Italia sta muovendo alcuni fondamentali passi per modernizzare le proprie infrastrutture e formare i dipendenti e i cittadini in modo da massimizzare la sovranità sui dati.

Il dibattito sulle nuove tecnologie è inevitabilmente legato alla questione della protezione dei dati personali, che richiede una chiarificazione terminologica e giuridica. In Italia, il Garante della privacy dice: *“Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..”*⁶ Questa formulazione estensiva consente una giurisdizione dinamica su tecnologie non esplicitamente previste al momento della stesura normativa, garantendo flessibilità interpretativa di fronte a scenari in evoluzione. L'episodio OpenAI-ChatGPT (2023) esemplifica tale approccio: il Garante italiano ha esercitato poteri ispettivi sull'uso di dati di cittadini italiani per l'addestramento del modello, nonostante l'assenza di riferimenti specifici all'IA generativa nella legislazione vigente.

Il concetto di “privacy” è invece ancora più complesso, specie per quanto riguarda l'ordine di priorità da darvi. Il termine si traduce letteralmente con “riservatezza”, ma nell'accezione in cui è concepita nella Dichiarazione dei diritti universali dell'uomo e nella Convenzione Europea per la Protezione dei Diritti dell'Uomo e delle Libertà fondamentali la privacy è in primis un diritto al rispetto della propria sfera privata, che non può essere invasa senza consenso da terzi.

La **data privacy** rappresenta un concetto che va ben oltre la semplice somma delle sue componenti tecniche e normative. In ambito europeo, il GDPR distingue chiaramente tra data protection e data privacy: la prima riguarda la messa in sicurezza dei dati contro accessi non autorizzati, tramite strumenti, tecnologie e policy di sicurezza, si focalizza sull'attribuire agli individui il potere decisionale su chi può accedere, trattare e utilizzare i propri dati personali, nonché per quali finalità⁷.

Come ampiamente dimostrato dal piano Italia Digitale 2026, la data privacy è centrale per la sovranità digitale del bel Paese. Per mantenerla, l'Italia si affida in primo luogo al già menzionato Garante per la Protezione dei Dati Personali, un'autorità amministrativa indipendente nata nel 1996. Il Garante ha numerosi compiti che si possono riassumere sostanzialmente nel farsi controllore della conformità del trattamento dei dati nazionali, nella prescrizione di misure correttive, nel farsi sportello per i reclami, nell'istruire sulla materia e nel formulare pareri e adottare provvedimenti. In sostanza, il garante ha ruolo consultivo, legislativo, esecutivo, e giudiziario per quanto riguarda la privacy. Tuttavia, non è l'unico ente a occuparsi di dati nel Paese. Strategica, infatti, è anche la collaborazione con il settore privato: a livello aziendale, una figura sempre più importante è quella del Data Protection Officer.

⁶ Garante per la Protezione dei Dati Personali, "Cosa intendiamo per dati personali?", Garante Privacy, 2016, <https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali>.

⁷ Wolford, B. "A Guide to GDPR Data Privacy Requirements - GDPR.eu", GDPR.eu, consultato il 9 febbraio 2025, <https://gdpr.eu/data-privacy/>.

In tale contesto normativo e strategico un ruolo fondamentale è svolto dalle app di messaggistica. Queste ultime sono utilizzate ormai dalla maggioranza della popolazione: il 78.5% degli italiani ha installato sul proprio telefono almeno Whatsapp, mentre Facebook messenger e Telegram sono usate rispettivamente dal 40% e il 36% della popolazione⁸. La messaggistica è uno strumento fondamentale anche per le aziende che desiderano comunicare con la clientela: ad esempio, Whatsapp nella sua versione business permette di dare in automatico messaggi di benvenuto, di assenza, risposte rapide, e addirittura di caricare il catalogo prodotti direttamente sull'app più usata nel paese.

Le grandi app di messaggistica appartengono in genere ad imprese estere, il che comporta una serie di problemi a livello europeo e nazionale per quanto riguarda i dati, in particolare il loro trasferimento e la loro conservazione in server allocati oltre confine. Una volta creati, i dati italiani non rimangono, generalmente, in Italia, per cui non è possibile garantire al cittadino di poter controllare chi accede, copia, e trasferisce le proprie informazioni, né a che scopo ciò venga fatto. Non solo; per via della natura transnazionale dei servizi di messaggistica, si complica anche la gestione dell'equilibrio fra diritto alla privacy delle conversazioni personali e la necessità per le forze di sicurezza di prevenire e fermare crimini informatici. Tra gli esempi più famosi vengono in mente i gruppi Telegram utilizzati per lo scambio di materiale pedopornografico o di pornografia non consensuale⁹; ma i contesti criminali che si avvalgono di queste applicazioni sono molto più ampi. La crittografia che dovrebbe garantire la segretezza degli scambi diventa dunque un'arma a doppio taglio, che costringe il legislatore da un lato a chiedere più garanzie sulla sicurezza dei dati alle piattaforme, dall'altro di avere accesso ai dati eventualmente necessari ad indagare su comportamenti illegali online.

Alla luce di questi aspetti, risulta evidente come le app di messaggistica rappresentino una sfida singolare per il raggiungimento della sovranità digitale. Questo paper si propone dunque di indagare diversi modelli di messaggistica, prendendo in considerazione diversi casi studio, nonché analizzando le soluzioni adottate da Stati Uniti e Francia, allo scopo di formulare proposte di policy informate ed efficaci per quanto riguarda la messaggistica in Italia.

8

https://www.ansa.it/canale_tecnologia/notizie/software_app/2023/10/24/whatsapp-messenger-e-telegam-le-chat-piu-usate-dagli-italiani_2bf7684c-3eab-4270-9ca8-c0269a80b8d4.html

⁹ Flora, M. G. P., Monte, N., Beckman, E., 2022, "State of Revenge," *PermessoNegato*, p. 3.

Caratteristiche delle app di messaggistica diffuse e l'esempio di Telegram

Prima di fornire alcuni esempi di soluzioni adottate da altri Stati per regolare le app di messaggistica in una strategia di sovranità digitale, il presente capitolo ambisce, senza pretese di esaustività, a individuare le caratteristiche più importanti delle app stesse. Di queste si cercherà di tracciarne il funzionamento tecnico e i modelli di business sottostanti, portando Telegram come esempio.

I servizi di messaggistica sono, come i social network, servizi di comunicazione di massa, ovvero pensati per coprire una utenza non regionale o particolare, ma globale e il più possibile generica.

Le caratteristiche principali che definiscono un servizio di messaggistica sono, pertanto:

- la scalabilità, ovvero la semplicità di adattamento delle tecnologie e infrastrutture alla base del servizio a numeri di utenti sempre maggiori ed a fasce d'utenti con diverse caratteristiche;
- la quantità, ovvero un rigido e imparziale conteggio degli utenti giornalieri e mensili del servizio.

La scalabilità ha impatto diretto sul costo del servizio: all'aumentare del numero di utenti, una piattaforma con un buon indice di scalabilità riuscirà a contenere i costi operativi, riducendo quindi la spesa complessiva. Un servizio scalabile è, in parole povere, molto efficiente ed ottimizzato per contenere il più possibile i costi dovuti all'espansione della base utente.

La scalabilità dipende da un insieme di scelte, principalmente ingegneristiche, di cui è solo possibile speculare, in quanto esse hanno a che fare con dettagli interni solitamente non divulgati. Quel che è certo è che tutte le piattaforme più famose con milioni di utenti devono avere un certo livello di efficienza ed ottimizzazione, altrimenti perirebbero di costi operativi senza generare margini.

La quantità di utenti è probabilmente la caratteristica più importante, poiché determina direttamente il valore del servizio di messaggistica. La piattaforma più importante è infatti quella con il maggior numero di utenti attivi mensilmente, seguita subito da quella con la seconda utenza più numerosa, e così via a formare una classifica che è tipica dei servizi di comunicazione di massa moderni, per i quali il successo si misura in base all'adozione su larga scala.

Per massimizzare il numero di utenti, le piattaforme di messaggistica lavorano sull'usabilità del servizio, ovvero sulla semplicità d'uso sulle funzionalità offerte. L'usabilità dipende fortemente dalla semplicità dell'interfaccia utente. Un'interfaccia pulita e intuitiva, caratterizzata da un layout semplice e minimalista, guida gli utenti verso le funzionalità essenziali, riducendo la confusione e migliorando l'esperienza complessiva. L'implementazione di elementi familiari come icone standard e interfacce personalizzabili, ad esempio, riduce la curva di apprendimento, permettendo agli utenti di sentirsi a proprio agio nell'utilizzo dell'app.

Sempre nel tentativo di accaparrarsi più utenti possibile, le piattaforme di messaggistica mettono a disposizione diverse funzionalità accessorie. Anzitutto, esse non si limitano a distribuire le loro applicazioni sia su dispositivi mobili che desktop, ma adattano i loro servizi a ogni sistema operativo. Così trasformano le proprie app in "servizi multiplatforma", capaci di funzionare indipendentemente dal dispositivo o dal sistema in uso.

Inoltre, per semplificare la gestione delle conversazioni su più dispositivi, le piattaforme garantiscono anche accesso allo storico delle chat ed ai messaggi da diversi dispositivi sfruttando uno storage cloud, come fanno ad esempio Telegram e Whatsapp

Infine, per far sembrare la comunicazione in tempo reale come una naturale estensione del nostro pensiero, le piattaforme di messaggistica si affidano a colossi dell'infrastruttura digitale: le Content Delivery Network (CDN), veri e propri giganti tecnologici dislocati in ogni area geografica che innervano il mondo "reale" e, come arterie pulsanti, garantiscono una connettività globale con una latenza quasi impercettibile.

Considerando la complessità delle tecnologie impiegate e l'elevato numero di utenti attivi simultaneamente, le applicazioni di messaggistica si trovano a fronteggiare una vasta gamma di minacce, che spaziano dalla compromissione dei server e dei dispositivi, al rischio di violazione della privacy delle comunicazioni, fino all'impersonificazione degli utenti.

Per contrastare queste sfide, le piattaforme moderne adottano un approccio di sicurezza stratificato o multilivello, in cui ogni contromisura è studiata per fronteggiare una specifica categoria di attacco.

Nel contesto odierno, dove la rivoluzione digitale non è solo progresso e numero di utenti ma anche terreno fertile per nuove insidie, il successo di un'app di messaggistica si basa anche sulla sinergia tra sicurezza e semplicità d'uso. Un'interfaccia che, con il suo fascino e la sua semplicità d'uso, si sposi con protocolli e infrastrutture debitamente fortificate (o percepite come tali), diventa l'ingrediente essenziale per catturare quell'utenza moderna sempre più rapita dal mondo virtuale ma altrettanto attenta ai suoi pericoli.

Non è un segreto, infatti, che la capacità di bilanciare semplicità d'uso con robustezza tecnologica consenta alle piattaforme di posizionarsi strategicamente¹⁰. Queste decisioni tecniche si traducono direttamente in narrative di brand, influenzando acquisizione utenti, partnership e modelli di monetizzazione.

Modelli di Business e Strategie di Monetizzazione

E sono proprio i modelli di monetizzazione, essenziali affinché il business di una piattaforma "stia in piedi", ad aver rappresentato nell'ultimo decennio uno dei punti di maggiore frizione tra le piattaforme di messaggistica istantanea e la privacy dei loro utenti. Sebbene servizi come WhatsApp, Messenger, Telegram o Signal offrano connessioni immediate e apparentemente gratuite, la sostenibilità economica di alcuni di essi si basa su strategie che dipendono direttamente dai dati degli utenti, creando una tensione costante con il diritto alla riservatezza¹¹.

¹⁰ <https://www.kaspersky.it/resource-center/preemptive-safety/messaging-app-security>

¹¹ WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app, Dan Goodin, ArsTechnica, 6/01/2021

Questa dinamica rispecchia in pieno i meccanismi del "Capitalismo della Sorveglianza", come teorizzato da Shoshana Zuboff, dove l'esperienza umana viene trattata come materia prima gratuita da trasformare in dati comportamentali¹². Nella tensione costante tra i due poli opposti, la generazione di valore o l'inevitabile estinzione, di un mercato sempre più spietatamente darwiniano, i social network e le app di messaggistica sono sopravvissuti come servizi utente passando dal semplice incremento della base utenti alla monetizzazione attiva su quegli utenti.

Nonostante l'adozione diffusa di sofisticati algoritmi di crittografia, in ultimo della crittografia end-to-end (E2EE), il valore economico degli utenti viene estratto principalmente dai cosiddetti "metadati" e da altre informazioni come dati del profilo, contatti e dettagli del dispositivo¹³. Questi dati, considerabili un "surplus comportamentale" secondo la terminologia di Zuboff, vengono aggregati e analizzati per alimentare sofisticati sistemi di profilazione. Tali profili sono poi utilizzati per la pubblicità mirata su piattaforme diverse o dello stesso ecosistema, rendendo i dati predittivi sul comportamento degli utenti la vera risorsa chiave scambiata nei mercati dei "futures comportamentali".

Tale paradigma, basato interamente sui dati, entra inevitabilmente in conflitto con la privacy. Le piattaforme sono incentivate a raccogliere più dati di quelli strettamente necessari, e la condivisione di queste informazioni all'interno di grandi gruppi aziendali, come nel caso di Meta dopo l'acquisizione di WhatsApp, ha sollevato forti preoccupazioni. Aggiornamenti delle policy sulla privacy, come quello controverso di WhatsApp nel 2021, hanno spesso limitato la capacità degli utenti di opporsi a tale condivisione, presentando scelte binarie del tipo "accetta o rinuncia al servizio"¹⁴.

La crescente consapevolezza del pubblico e le preoccupazioni per la privacy hanno stimolato risposte normative, in particolare l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) in Europa nel 2018¹⁵. Il GDPR ha rafforzato i diritti degli individui e imposto obblighi più severi alle aziende sulla raccolta e l'uso dei dati, portando a indagini e sanzioni da parte delle autorità garanti. Parallelamente, la domanda di maggiore riservatezza ha favorito la crescita di alternative come Signal, sostenuta da una fondazione non-profit e focalizzata sulla minimizzazione dei dati raccolti¹⁶, e Telegram, che ha introdotto modelli di abbonamento premium e funzionalità business per diversificare le entrate¹⁷.

In conclusione, il rapporto tra modelli di business delle piattaforme IM e privacy degli utenti rimane un equilibrio precario, profondamente influenzato dalle logiche del capitalismo della sorveglianza. La necessità di monetizzare servizi gratuiti continua a scontrarsi con le aspettative di riservatezza e i diritti sanciti dalla legge. Il futuro di questo settore potrebbe essere plasmato da nuovi modelli di business (che potrebbero allontanarsi o meno dal modello "estrattivo") e dalla crescente domanda di trasparenza e controllo sui propri dati da parte degli utenti.

¹² The Age of Surveillance Capitalism: the fight for the future at the new frontier of power, Zuboff, 2019

¹³ What You Don't Know About How Facebook Uses Your Data, Natasha Singer, 11/04/2018, The New York Times

¹⁴ WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app, Dan Goodin, ArsTechnica, 6/01/2021

¹⁵ General Data Protection Regulation, Wikipedia

¹⁶ <https://signal.org/>

¹⁷ <https://telegram.org/faq#q-how-are-you-going-to-make-money-out-of-this>

In questo senso la piattaforma Telegram sembra essere una eccezione alla regola: il suo modello di business, infatti, non sarebbe basato sulla profilazione degli utenti ma sui "tradizionali" abbonamenti e su uno schema freemium, diverso da qualsiasi altro servizio di messaggistica diffuso a livello globale.

Nel prossimo paragrafo analizzeremo il business model di Telegram a titolo d'esempio per illustrare in dettaglio i meccanismi di mercato del settore della messaggistica istantanea, mostrando anche perché Telegram è un "outlier" in questo contesto di mercato.

Il caso di Telegram

Tra le app più discusse e scaricate sugli store digitali delle varie piattaforme, Telegram si distingue per diverse caratteristiche che la rendono l'unica app in grado di competere con lo strapotere di Whatsapp, la più importante applicazione di messaggistica istantanea moderna e prima per numero di utenti.

Telegram si configura come una delle piattaforme di messaggistica più innovative e discusse del panorama digitale. Nata nel 2013 dai fratelli Nikolai e Pavel Durov, l'app si è distinta fin dall'inizio per la sua attenzione alla sicurezza e alla privacy, offrendo agli utenti una comunicazione crittografata e funzionalità avanzate che la differenziano dai tradizionali servizi di messaggistica. Con un'utenza che conta 900 milioni di utenti mensili¹⁸, Telegram ha saputo coniugare gratuità e innovazione, offrendo non solo messaggistica istantanea ma anche strumenti di cloud storage, social networking e persino funzionalità di e-commerce.

Il nucleo dell'identità di Telegram risiede proprio nella sua capacità di mettere al centro la protezione della privacy: la piattaforma garantisce chat segrete con crittografia end-to-end e permette agli utenti di nascondere il numero di cellulare e altre informazioni personali. Tale impegno per la sicurezza non solo mira a rafforzare la fiducia degli utenti, ma si pone come elemento distintivo rispetto a quelle piattaforme che, al contrario, traggono profitto dalla profilazione e dalla raccolta dei dati. Inoltre, Telegram abbraccia un modello open source per il software front-end, offrendo trasparenza e la possibilità agli sviluppatori di verificare e contribuire al miglioramento del codice.

Nonostante il successo e l'adozione globale, la piattaforma non è esente da controversie. Le crescenti pressioni normative e le critiche relative alla diffusione di contenuti illeciti hanno messo Telegram in una posizione di equilibrio difficile: da un lato, la necessità di tutelare la privacy e la libertà di espressione, dall'altro, l'obbligo di conformarsi a regolamentazioni sempre più stringenti. Episodi come la sospensione temporanea in alcuni Paesi e l'arresto di figure chiave della società hanno ulteriormente alimentato il dibattito sulla sostenibilità di un modello di business basato sulla sicurezza e sull'anonimato degli utenti^{19,20}.

Questa doppia natura, che mischia innovazione e controversie, rende Telegram un caso studio emblematico nel contesto della trasformazione digitale. L'approccio "freemium", che prevede l'erogazione gratuita della maggior parte dei servizi con l'introduzione di funzionalità

¹⁸ "Telegram hits 900mn users and nears profitability as founder considers IPO", Hannah Murphy, Financial Times, 11/03/2024

¹⁹ "Brazilian Court Orders Suspension of Telegram Over Neo-Nazi Groups", Samantha Pearson, The Wall Street Journal, Aprile 2023

²⁰ "What is Telegram and why was its CEO arrested in Paris?", Barbara Ortutay, APnews, Agosto 2024

premium a pagamento, è solo uno degli elementi della strategia aziendale che ha permesso alla piattaforma di espandersi rapidamente, pur mantenendo un forte orientamento alla tutela dei dati personali. In sintesi, Telegram non è solo un mezzo di comunicazione, ma un laboratorio di sperimentazioni tecnologiche e di modelli di business che sfidano i paradigmi tradizionali.

Analisi della Struttura Societaria e della Dichiarazione d'Intenti

Il modello operativo di Telegram si fonda su una struttura societaria articolata e complessa, composta da diverse entità giuridiche che, pur operando in sinergia, rendono difficile una visione unitaria della responsabilità gestionale²¹. Tra queste, si annoverano Telegram Group Inc., Telegram FZ LLC e Telegram Messenger Inc., società che operano prevalentemente dalle Isole Vergini Britanniche o da centri operativi strategici come Dubai. Questa organizzazione frammentata, sebbene possa apparire opaca, è risultata funzionale, negli anni, alla flessibilità operativa e alla capacità di adattamento della piattaforma ai diversi mercati internazionali.

Alla base di questa struttura vi è una dichiarazione d'intenti che funge da faro guida per tutte le attività della società: fornire un mezzo di comunicazione veloce e sicuro, multiplatforma basato sul cloud²². Tale missione non solo sottolinea l'impegno verso la protezione dei dati e la sicurezza delle comunicazioni, ma evidenzia anche l'ambizione di creare una piattaforma globale, libera da restrizioni nazionali e da pratiche invasive di raccolta dati. In questo senso, Telegram si posiziona come un'alternativa alle tradizionali piattaforme social, puntando su valori etici e su un modello di business che privilegia la privacy degli utenti.

La complessità della struttura societaria, pur rappresentando una sfida in termini di trasparenza, è stata una scelta strategica per garantire autonomia decisionale e per facilitare l'accesso a mercati globali. Allo stesso tempo, questa configurazione solleva interrogativi sul reale controllo della piattaforma e sulla governance interna, elementi che sono diventati oggetto di discussione soprattutto in seguito alle recenti vicissitudini giudiziarie e alle pressioni normative internazionali.

Segmenti di Consumatori e Proposta di Valore

Telegram ha saputo diversificare la propria offerta rivolgendosi a una molteplicità di segmenti di consumatori. La piattaforma non si limita a soddisfare le esigenze degli utenti privati, ma estende il suo raggio d'azione ad aziende, inserzionisti, sviluppatori, content creators e, più in generale, a chiunque ponga una particolare attenzione alla privacy.

La proposta di valore di Telegram si fonda su numerosi pilastri. In primo luogo, la gratuità del servizio per la maggior parte degli utenti costituisce un elemento centrale: la piattaforma offre un'ampia gamma di funzionalità senza richiedere alcun pagamento, permettendo così una diffusione capillare. In secondo luogo, la sicurezza delle comunicazioni – garantita dalla crittografia avanzata e dalle chat segrete – aggiunge un ulteriore livello di affidabilità al servizio, rendendo Telegram particolarmente attraente per chi necessita di un ambiente protetto per scambi di informazioni sensibili.

²¹ <https://telegram.org/privacy/eu#8-2-telegrams-group-companies>

²² <https://telegram.org/faq?setln=en>

Parallelamente, Telegram ha investito nella creazione di funzionalità orientate al business. Canali pubblici, gruppi tematici e strumenti di interazione automatizzata (bot) permettono non solo una comunicazione diretta e personalizzata, ma anche la possibilità per aziende e inserzionisti di instaurare un dialogo diretto con il proprio pubblico²³. L'ecosistema sviluppato attorno alle API gratuite favorisce la creazione di applicazioni e servizi di terze parti, contribuendo a creare un ambiente dinamico e collaborativo²⁴.

Infine, l'adozione di un modello freemium, che prevede l'introduzione di abbonamenti premium per funzionalità avanzate, consente a Telegram di monetizzare senza compromettere il principio fondante della gratuità per la maggioranza degli utenti²⁵. In questo modo, la piattaforma riesce a bilanciare l'obiettivo di espansione globale con la necessità di garantire una sostenibilità economica nel lungo termine, mantenendo al contempo alta la qualità e la sicurezza del servizio.

Strategie di Monetizzazione e Flussi di Entrata

Il modello di business di Telegram ha attirato notevole attenzione proprio per la sua apparente contraddizione: una piattaforma che si vanta di non fare profitti sfruttando i dati degli utenti e che, al contempo, è chiamata a generare ricavi per sostenere l'espansione e il continuo sviluppo dei servizi. Le fonti di monetizzazione si basano su due pilastri fondamentali: i messaggi sponsorizzati e gli abbonamenti premium.

I messaggi sponsorizzati rappresentano una novità che consente agli inserzionisti di promuovere i propri prodotti e servizi inserendo messaggi all'interno delle chat pubbliche. Il modello prevede una distribuzione degli introiti tale per cui Telegram garantisce fino al 50% dell'investimento effettuato dagli inserzionisti per ogni campagna²⁶.

Parallelamente, gli abbonamenti premium costituiscono la prima fonte di guadagno diretta della piattaforma. Introdotti a partire dal 2022, questi abbonamenti offrono una serie di funzionalità aggiuntive quali limiti maggiori nell'utilizzo dei canali, velocità di download migliorata, capacità di upload aumentata e servizi esclusivi come la conversione da voce a testo²⁷. Tale scelta strategica permette a Telegram di mantenere la base gratuita per la maggioranza degli utenti, concentrando la monetizzazione su una minoranza disposta a pagare per funzionalità avanzate.

Una delle peculiarità che distingue Telegram dai competitor è proprio la scelta di non sfruttare i dati personali per attività di profilazione pubblicitaria. Mentre molte piattaforme si affidano al "capitalismo della sorveglianza" per generare profitti, Telegram afferma con fermezza di non raccogliere e monetizzare le informazioni degli utenti, privilegiando invece un modello basato sulla trasparenza e sul rispetto della privacy. Questo approccio, sebbene possa apparire meno redditizio nel breve termine, rappresenta un elemento di forte differenziazione sul mercato e contribuisce a consolidare la reputazione della piattaforma come baluardo della sicurezza digitale.

²³ <https://core.telegram.org/bots/features#bots-for-business>

²⁴ <https://ads.telegram.org/>

²⁵ https://telegram.org/faq_premium

²⁶ <https://telegram.org/tos/content-creator-rewards#2-1-advertisement-revenue-sharing>

²⁷ <https://telegram.org/blog/700-million-and-premium#telegram-premium>

Risorse Chiave, Costi e Partner

Il successo e la crescita di Telegram non sono frutto del caso, ma il risultato di una gestione attenta e di investimenti strategici in risorse tecnologiche e umane. Tra le risorse chiave si annoverano l'infrastruttura tecnologica, il software e il team di sviluppo. Il front-end dell'app, essendo open source, permette a sviluppatori esterni di analizzare, verificare e migliorare il codice, aumentando così la trasparenza e la sicurezza del sistema²⁸. Al contempo, il software back-end rimane proprietario, garantendo a Telegram il controllo esclusivo sulle funzionalità critiche (come la gestione delle chiavi crittografiche) e sui processi di gestione dei dati.

La distribuzione geografica dei data center è un altro elemento cruciale: una rete di server dislocata in diverse regioni del mondo consente di garantire la continuità del servizio anche durante picchi di traffico e di rispettare normative locali relative alla protezione dei dati, come il GDPR^{29,30}. Questa capacità di gestire grandi volumi di traffico a costi contenuti ha permesso a Telegram di mantenere un costo operativo inferiore a 70 centesimi per utente mensile, un dato che evidenzia l'efficienza del modello di business.

Il team di sviluppo³¹, composto da professionisti altamente qualificati selezionati per merito in base a contest di programmazione³², è un ulteriore pilastro fondamentale della piattaforma. L'attenzione alla qualità del software ha permesso a Telegram di lanciare continuamente nuove funzionalità, rispondendo in modo tempestivo alle esigenze di un mercato in rapida evoluzione. Accanto a queste risorse, la leadership di Pavel Durov – figura centrale sia dal punto di vista creativo che finanziario – ha fornito la guida necessaria per navigare le sfide di un settore altamente competitivo. Durov, attraverso investimenti personali e successivi round di finanziamento, ha garantito risorse per oltre tre miliardi di dollari, rafforzando la posizione della piattaforma sul mercato³³.

I partner chiave e gli investitori, sebbene spesso velati da una certa opacità, hanno svolto un ruolo determinante nell'espansione di Telegram. Il sostegno di venture capital e di investitori provenienti da diverse parti del mondo ha consentito alla piattaforma di sviluppare un modello di business scalabile e di affrontare le sfide normative e operative in maniera efficace. Tuttavia, la complessità della struttura societaria e la mancanza di informazioni dettagliate sui singoli investimenti continuano a sollevare interrogativi circa la reale trasparenza della gestione interna, un tema che resta al centro del dibattito pubblico e delle autorità di controllo.

Tirando le somme: il futuro delle app di messaggistica

L'analisi delle caratteristiche delle app di messaggistica diffuse evidenzia come tali strumenti abbiano trasformato radicalmente il panorama comunicativo globale. Grazie all'evoluzione tecnologica, alla capacità di offrire funzionalità multimediali e alla continua attenzione per la

²⁸ <https://telegram.org/apps#codice-sorgente>

²⁹ <https://docs.pyrogram.org/faq/what-are-the-ip-addresses-of-telegram-data-centers>

³⁰ <https://telegram.org/privacy/eu#4-1-storing-data>

³¹ <https://telegram.org/jobs>

³² <https://t.me/s/contest>

³³ <https://www.sec.gov/newsroom/press-releases/2020-146>



privacy e la sicurezza, queste applicazioni sono diventate parte integrante della vita quotidiana di milioni di persone in tutto il mondo.

Il modello di business adottato, che spazia da soluzioni freemium a modelli basati su pubblicità e abbonamenti, rappresenta una risposta efficace alle esigenze di sostenibilità economica senza compromettere l'accessibilità del servizio. Allo stesso tempo, l'integrazione con altri servizi digitali e l'adozione di tecnologie innovative, quali l'intelligenza artificiale e la realtà aumentata, aprono scenari entusiasmanti per il futuro, trasformando le app di messaggistica in veri e propri hub digitali.

Tuttavia, le criticità legate alla gestione della privacy, alla sicurezza e alla moderazione dei contenuti rimangono sfide cruciali che richiedono soluzioni dinamiche e un costante aggiornamento tecnologico. Il futuro vedrà probabilmente una maggiore attenzione alla regolamentazione e alla trasparenza, elementi fondamentali per mantenere la fiducia degli utenti e garantire un ambiente di comunicazione sicuro ed efficiente.

In sintesi, le app di messaggistica rappresentano non solo un mezzo per comunicare, ma un vero e proprio ecosistema in continua evoluzione, in grado di influenzare profondamente la società, la cultura e l'economia globale. La loro capacità di adattarsi alle nuove tecnologie e di rispondere alle esigenze in costante mutamento degli utenti ne farà, senza dubbio, uno degli strumenti più rilevanti del nostro tempo.

L'approccio statunitense e Wickr

Nel rapporto tra sovranità digitale e app di messaggistica, gli Stati Uniti rappresentano un caso particolare, dal momento che nel mainstream non sono molto diffuse le app di messaggistica che spopolano nel resto del mondo. Complice la diffusione di piani con sms illimitati, buona parte degli statunitensi si avvalgono di iMessage e altre app native dei dispositivi per la comunicazione di tutti i giorni. Diverso è, invece, il caso dei funzionari governativi, che non possono scambiarsi informazioni con la stessa leggerezza. Nel 2024, la NARA –National Archives and Records Administration– ha compilato il Transmittal n.33 per aggiornare le direttive riguardo le comunicazioni digitali e la conservazione delle informazioni.³⁴ Innanzitutto, il documento stabilisce come i messaggi scambiati tra funzionari governativi tramite app di messaggistica costituiscano documentazione federale nel momento in cui essi trattino di argomenti pertinenti agli affari federali, indipendentemente dal fatto che il dispositivo da cui siano stati mandati sia personale o meno. Inoltre, è richiesto ai funzionari di mettere agli atti queste comunicazioni inoltrandole entro 20 giorni al proprio indirizzo e-mail ufficiale o utilizzando altri dei metodi approvati per la comunicazione. In generale, le app di messaggistica per la comunicazione ufficiale sono da utilizzarsi solo in via emergenziale. Non solo: la trasmissione di informazioni o documenti riservati tramite queste app è strettamente proibita per motivi di sicurezza. In tal senso, il caso studio relativo all'app Wickr, è sicuramente degno di nota.

Fondata nel 2012 da un gruppo di esperti di sicurezza informatica, Wickr ha rapidamente guadagnato attenzione per le sue caratteristiche di sicurezza avanzate. La piattaforma è stata progettata per offrire comunicazioni sicure attraverso l'implementazione di crittografia end-to-end e funzionalità di autodistruzione dei messaggi. Wickr si è distinta per l'adozione di una crittografia avanzata e per la capacità di autodistruggere i messaggi dopo un periodo predefinito.

Dal punto di vista tecnico, l'app di messaggistica offre funzionalità avanzate come il controllo granulare delle chiavi di crittografia, la protezione dei metadati attraverso la crittografia multilivello e la possibilità di integrare l'archiviazione sicura su server di proprietà dell'utente. Inoltre, il sistema supporta la gestione centralizzata delle policy di sicurezza per le aziende, consentendo di definire criteri di accesso e di conservazione dei dati in linea con le normative internazionali sulla protezione delle informazioni.

Nel panorama delle applicazioni di messaggistica sicura, Wickr si distingue per diverse caratteristiche uniche che la differenziano da concorrenti come Telegram e Signal. A differenza di Signal, che richiede un numero di telefono per la registrazione, Wickr consente agli utenti di creare un account senza fornire informazioni personali identificative, garantendo un ulteriore livello di anonimato. Sebbene sia Wickr che Signal implementino la crittografia end-to-end, Wickr utilizza una combinazione di algoritmi come AES-256 per la crittografia simmetrica e RSA-4096 per quella asimmetrica, insieme al protocollo ECDH521 per lo scambio sicuro delle chiavi, offrendo una robusta protezione dei dati. Una delle funzionalità

³⁴ National Archives and Records Administration, 2025, "The General Records Schedules: Transmittal 33".

distintive di Wickr è la possibilità di impostare un timer per l'autodistruzione dei messaggi, assicurando che le comunicazioni sensibili vengano eliminate automaticamente dopo un periodo specificato. Non sorprende, quindi, che Wickr abbia avuto successo in particolare tra le organizzazioni aziendali e governative.

Grazie alla sua particolare enfasi sulle crittografia dei messaggi e sull'anonimato, Wickr si è subito posta come particolarmente attraente per categorie di utenti che necessitano di un elevato livello di riservatezza, come giornalisti, attivisti e aziende con dati sensibili da proteggere. Nel corso degli anni, la piattaforma si è evoluta attraverso diverse versioni: Wickr Me, destinata agli utenti privati ma poi dismessa nel 2022; Wickr Pro e Wickr Enterprise, pensate per aziende e governi. Queste versioni consentono l'integrazione con sistemi aziendali e forniscono strumenti avanzati di controllo e gestione delle comunicazioni. Quest'ultima è stata adottata in vari settori del settore pubblico Statunitense; agenzie governative come l'FBI, la NSA e il Dipartimento della Difesa hanno utilizzato Wickr per comunicazioni interne, riconoscendo la necessità di proteggere informazioni sensibili. Ad esempio, il Dipartimento della Difesa degli Stati Uniti ha impiegato Wickr per garantire la sicurezza delle comunicazioni tra il personale militare, sfruttando la crittografia di livello militare offerta dalla piattaforma. Inoltre, diverse aziende hanno integrato Wickr nei loro sistemi per salvaguardare la proprietà intellettuale e prevenire fughe di dati. Giornalisti e attivisti, che necessitano di un elevato livello di riservatezza, hanno trovato in Wickr uno strumento prezioso per mantenere riservate le proprie fonti e scambiare informazioni senza timore di intercettazioni.

Uno degli aspetti più significativi dell'adozione di Wickr da parte del governo USA è stato il suo utilizzo in ambienti con requisiti di sicurezza particolarmente elevati, come le comunicazioni tra unità militari schierate in zone di conflitto o le operazioni segrete condotte dalle agenzie di intelligence. In particolare, l'Air Force ha investito milioni di dollari nell'implementazione di Wickr per garantire comunicazioni crittografate tra il personale. Inoltre, il Customs and Border Protection (CBP), l'agenzia di frontiera statunitense, ha fatto uso di Wickr per coordinare operazioni sul campo, sollevando interrogativi sulla trasparenza di tali comunicazioni³⁵.

A dirla tutta, Wickr ha avuto legami con il governo fin dalle sue origini: secondo alcune inchieste, la piattaforma ha ricevuto finanziamenti da In-Q-Tel, il braccio di investimento della CIA³⁶, un dettaglio che ha sollevato leciti dubbi sul grado di indipendenza della società rispetto alle agenzie di intelligence statunitensi. Inoltre, il governo ha stipulato contratti di milioni di dollari con Wickr per l'uso della sua tecnologia in ambito militare e governativo. Nel 2020, Wickr ha creato un comitato consultivo strategico per supportare il suo business federale, coinvolgendo esperti della sicurezza nazionale per consolidare il suo ruolo come fornitore di tecnologie crittografiche alle agenzie statunitensi³⁷.

Interessante è il caso del governatore del Maryland, Larry Hogan, che nel 2021 è stato

³⁵ <https://www.vice.com/en/article/air-force-millions-encrypted-app-wickr/>

³⁶ <https://www.vice.com/en/article/wickr-cia-funding-inqtel/>

³⁷

<https://www.govconwire.com/2020/10/wickr-creates-advisory-board-to-support-federal-business-strategy-joel-wallenstrom-quoted/>

oggetto di critiche per l'uso di Wickr nelle comunicazioni ufficiali della sua amministrazione³⁸. Poiché l'app consente la cancellazione automatica dei messaggi, è emersa la preoccupazione che tali comunicazioni potessero violare le leggi sulla trasparenza e sulla conservazione dei documenti pubblici. Secondo alcune inchieste, i funzionari dello stato avrebbero utilizzato Wickr per discutere di politiche e decisioni governative, evitando così la possibilità di accesso pubblico a queste informazioni. L'uso di applicazioni con crittografia end-to-end e autodistruzione dei messaggi ha sollevato il timore che gli organi governativi possano eludere il Freedom of Information Act (FOIA), limitando la responsabilità e la trasparenza verso i cittadini.

Forse non proprio sorprendentemente, proprio la robusta crittografia di Wickr ha sollevato preoccupazioni tra le autorità, poiché la piattaforma è stata utilizzata anche da gruppi criminali per scopi illeciti, come spaccio di droga e diffusione di materiale pedopornografico³⁹. Il dibattito sulla regolamentazione delle app di messaggistica crittografata è diventato centrale negli Stati Uniti, specialmente in relazione al CLOUD Act, una legge che impone alle aziende americane di fornire dati alle autorità anche se archiviati all'estero. Le richieste di inserire "backdoor" per consentire alle forze dell'ordine di accedere ai contenuti crittografati hanno incontrato forte opposizione da parte di organizzazioni per la tutela della privacy, che temono un uso improprio di tali accessi per attività di sorveglianza di massa. Nel 2022, l'FBI ha segnato un precedente significativo nel campo dell'accesso forzato ai dati crittografati, costringendo un sospetto a sbloccare l'app Wickr tramite riconoscimento facciale. L'operazione è stata possibile grazie a un mandato che imponeva al soggetto di autenticarsi con il proprio volto, consentendo così agli investigatori di accedere alle comunicazioni altrimenti protette dalla crittografia end-to-end. Questo caso ha suscitato ampio dibattito sulle implicazioni legali e sui diritti alla privacy, poiché apre la strada a un maggiore coinvolgimento delle forze dell'ordine nell'accesso ai dati crittografati, sollevando interrogativi sulla protezione delle libertà civili e sull'uso di coercizione tecnologica da parte dello Stato⁴⁰.

Nel 2021, Amazon Web Services (AWS) ha acquisito Wickr, integrando le sue funzionalità di messaggistica sicura nei propri servizi. Tuttavia, nel 2022, AWS ha deciso di interrompere il servizio Wickr Me, la quale è stata dismessa il 31 dicembre 2023, mantenendo attive solo le versioni destinate a aziende e governi. Questa decisione è stata presa in risposta alle crescenti preoccupazioni riguardo all'uso illecito della piattaforma, in particolare nel traffico di droga e altre attività criminali sul dark web. Questa decisione è stata presa per concentrare le risorse sulle soluzioni aziendali e governative, come AWS Wickr e Wickr Enterprise, che continuano a operare *"offrendo servizi di comunicazione sicura con funzionalità avanzate di sicurezza e conformità"*. Wickr Enterprise è stato adottato da diverse agenzie governative statunitensi per garantire comunicazioni sicure e conformi alle normative federali.

38

<https://americanoversight.org/investigation/maryland-gov-hogans-use-of-self-destructing-messaging-app/>

³⁹<https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674> e <https://www.verdict.co.uk/what-is-wickr/>

40

<https://www.forbes.com/sites/thomasbrewster/2022/07/19/fbi-forces-open-amazon-wickr-app-with-a-suspects-face/>



La piattaforma soddisfa e supera le raccomandazioni della National Security Agency (NSA) per la sicurezza delle comunicazioni, offrendo funzionalità di conservazione dei dati e conformità necessarie per le agenzie governative⁴¹. AWS ha inoltre sviluppato una versione personalizzata di Wickr per il DoD USA; Wickr RAM (Recall, Alert, and Messaging). Questa consente al personale militare di collaborare in modo sicuro, sia in patria che all'estero, supportando operazioni tattiche e garantendo la protezione delle informazioni sensibili. La capacità di funzionare su diverse piattaforme e il set di funzionalità avanzate permettono di ridurre i rischi di sicurezza e migliorare l'efficienza operativa.

Per quanto riguarda le aziende, AWS Wickr offre una soluzione di comunicazione sicura che protegge i dati da minacce informatiche e assicura la conformità alle normative vigenti. Wickr Enterprise consente alle organizzazioni di mantenere il pieno controllo sulla propria rete, implementando politiche di sicurezza personalizzate, gestendo le autorizzazioni degli utenti e configurando opzioni di messaggistica effimera. Inoltre, la piattaforma si integra con servizi come Active Directory e Single Sign-On (SSO) tramite OpenID Connect (OIDC), facilitando la gestione degli accessi e migliorando l'efficienza operativa.

L'uso di applicazioni di messaggistica crittografata come Wickr solleva questioni complesse riguardo al bilanciamento tra privacy individuale e sicurezza nazionale. Mentre tali piattaforme offrono protezione contro sorveglianze non autorizzate, possono anche essere sfruttate per attività illecite. Il dibattito continua su come regolamentare efficacemente questi strumenti senza compromettere i diritti fondamentali alla privacy.

In un'epoca in cui la sorveglianza governativa è in aumento, l'importanza di strumenti come Wickr diventa ancora più rilevante. Gli utenti sono chiamati a valutare attentamente le proprie esigenze di sicurezza e privacy, considerando sia i benefici che le potenziali implicazioni dell'uso di tali piattaforme.

⁴¹ <https://wickr.com/secure-collaboration-for-the-federal-government>

Olvid e Tchap: l'approccio francese

L'altro lato dell'Atlantico non è restato comunque a guardare. Negli ultimi anni e nel contesto sempre più cruciale della sovranità digitale europea, la Francia ha adottato un approccio strutturato e proattivo per ridurre la dipendenza da applicazioni di messaggistica straniere e garantire la sicurezza delle comunicazioni istituzionali. Due strumenti emblematici di questa strategia sono **Olvid** e **Tchap**, nati in contesti diversi ma accomunati dall'obiettivo di tutelare la **sovranità digitale** e la **riservatezza dei dati** delle pubbliche amministrazioni e degli alti funzionari dello Stato.

Tchap: uno strumento istituzionale federato e pilastro della politica pubblica digitale

Tchap è stata ideata e sviluppata nel 2018 dalla Direction interministérielle du numérique (DINUM), l'organismo statale francese incaricato della strategia digitale del governo, sotto la guida iniziale di Henri Verdier, allora direttore generale della DINUM. L'iniziativa è nata come risposta diretta a crescenti preoccupazioni relative alla sicurezza delle comunicazioni governative, spesso affidate a piattaforme straniere come WhatsApp o Telegram, particolarmente vulnerabili a rischi di cyberspionaggio e violazioni di dati. Il progetto fu ufficialmente lanciato nell'aprile 2019, con un chiaro obiettivo strategico: recuperare la sovranità digitale francese e garantire una maggiore sicurezza e riservatezza delle comunicazioni istituzionali.⁴²

Dal punto di vista tecnico, la DINUM ha scelto di utilizzare il protocollo open source Matrix, noto per la sua robustezza e la capacità di decentralizzazione, integrando una versione personalizzata del client Element, appositamente adattata per le esigenze della pubblica amministrazione francese. Tchap consente oggi l'accesso esclusivamente ai dipendenti pubblici francesi tramite indirizzi email istituzionali con il dominio "gouv.fr", creando così un ambiente altamente controllato e conforme ai requisiti definiti dal Piano francese per la sovranità digitale del 2018, che stabilisce esplicitamente la necessità di mantenere i dati strategici su server localizzati sul territorio nazionale, certificati dall'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'applicazione è stata integrata nelle **strategie digitali interministeriali**, diventando uno standard raccomandato per le comunicazioni non classificate ma sensibili. Il codice sorgente, essendo basato su Element, è interamente open source e permette verifiche indipendenti da parte della comunità tecnica. Ogni ministero può potenzialmente federare il proprio server Tchap, integrandolo con l'infrastruttura centrale, secondo uno schema simile a quello usato nella posta elettronica.

In termini di diffusione, al 2024 Tchap è utilizzata da oltre 600.000 dipendenti pubblici francesi, inclusi funzionari delle prefetture, delle ambasciate, delle agenzie territoriali e delle forze dell'ordine.⁴³ In linea con questa visione, la roadmap ufficiale del progetto Tchap pubblicata nel 2024 prevede ulteriori sviluppi funzionali: tra questi figurano l'adozione della crittografia end-to-end per i messaggi di gruppo, l'introduzione di un'interfaccia per la

⁴²

https://next.innk/brief_article/la-direction-interministerielle-du-numerique-dinum-lance-un-marche-public-sur-tchap/

⁴³ [Tchap — Tchap](#)

gestione centralizzata dei gruppi da parte degli amministratori, l'integrazione del protocollo di autenticazione FranceConnect+ per rafforzare l'identificazione sicura degli utenti, e un progressivo aumento della compatibilità con ambienti lavorativi collaborativi, come la gestione documentale condivisa e la piena interoperabilità con altri strumenti digitali pubblici.⁴⁴

La piattaforma Tchap è gestita interamente dalla DINUM, assicurando il controllo completo dello Stato sui dati trattati, e garantendo la conformità con tutte le normative nazionali ed europee in materia di protezione dei dati, come il GDPR. Il finanziamento del progetto proviene interamente da fondi pubblici, con significativi investimenti statali destinati allo sviluppo, alla manutenzione e al miglioramento continuo della piattaforma. Secondo il recente rapporto della Cour des comptes, entro la fine del 2023, erano stati investiti circa 5,6 milioni di euro su un totale di 9,3 milioni destinati alla suite numérique de l'agent public, con un costo annuale di manutenzione stimato in 1,85 milioni di euro per il 2024.⁴⁵

Tuttavia, nonostante questi investimenti significativi, il rapporto evidenzia una diffusione limitata: solo il 30% degli agenti pubblici conosceva o utilizzava regolarmente Tchap e gli altri strumenti della suite numérique nel 2022. La *Cour des comptes* critica la strategia della DINUM, suggerendo una maggiore chiarezza nella governance e raccomandando un focus su strumenti con un reale valore aggiunto, evidenziando inoltre che le risorse umane destinate al progetto sono insufficienti, con solo 13 equivalenti a tempo pieno assegnati alla gestione di Tchap.

Questo contesto di uso limitato ed efficacia percepita insufficiente aiuta a comprendere meglio la circolare emessa nel novembre 2023 dalla Prima ministra Élisabeth Borne, in cui si invitavano ministri e membri dei gabinetti a disinstallare le app di messaggistica istantanea di origine straniera – come WhatsApp, Telegram e Signal – e a preferire soluzioni sviluppate in Francia, con una raccomandazione esplicita a utilizzare Olvid.⁴⁶ Se da un lato Tchap rappresenta una soluzione pensata per l'intera amministrazione pubblica, dall'altro la scelta di promuovere Olvid risponde alla necessità di una soluzione con livelli di sicurezza estremamente elevati, particolarmente adatta per ambienti ad alta sensibilità, grazie alla sua architettura decentralizzata e alla certificazione ANSSI.

In definitiva, l'approccio francese alla messaggistica istituzionale mostra la tensione costante tra innovazione pubblica, esigenza di controllo e qualità delle soluzioni. Tchap rimane un simbolo della volontà statale di dotarsi di strumenti sovrani, ma la sua efficacia è strettamente legata alla sua adozione diffusa e alla capacità di evolversi tecnicamente. Olvid, al contrario, rappresenta la risposta a esigenze di sicurezza estrema, complementare al progetto pubblico e oggi punto di riferimento per la comunicazione più sensibile del governo francese.

⁴⁴ <https://tchap.numerique.gouv.fr/feuille-de-route/>

⁴⁵

<https://www.ccomptes.fr/fr/publications/le-pilotage-de-la-transformation-numerique-de-letat-par-la-direction>

⁴⁶

https://www.lepoint.fr/high-tech-internet/les-ministres-francais-invites-a-desinstaller-whatsapp-signal-et-telegram-29-11-2023-2545099_47.php

Olvid: crittografia radicale e approccio decentralizzato alla riservatezza istituzionale

Olvid nasce nel 2019 da un team di esperti in crittografia e sicurezza informatica, provenienti da ambienti accademici di alto profilo come l'École Normale Supérieure e INRIA, con una visione radicale: garantire comunicazioni veramente sicure e decentralizzate, svincolate da qualsiasi server di directory o identificativo personale. A differenza della maggior parte delle app di messaggistica – che richiedono un numero di telefono o un indirizzo email per la registrazione – Olvid permette agli utenti di creare identità completamente anonime, basandosi esclusivamente su meccanismi crittografici di attestazione reciproca. Questo rende l'app particolarmente adatta all'uso in contesti ad alta sensibilità, come quelli governativi e istituzionali.

Dal punto di vista tecnico, Olvid è l'unica applicazione certificata dall'ANSSI per le comunicazioni classificate "Diffusion Restreinte", un livello di classificazione corrispondente alle informazioni sensibili ma non segrete. La sua architettura peer-to-peer elimina la necessità di server centrali per la gestione delle identità, riducendo drasticamente la superficie d'attacco e prevenendo il rischio di compromissioni sistemiche. Il cuore tecnologico di Olvid si basa su una variante avanzata del protocollo Double Ratchet, combinato con un sistema proprietario di gestione delle chiavi e di autenticazione reciproca, garantendo così che solo gli interlocutori legittimi possano accedere alla conversazione – e nemmeno gli stessi sviluppatori dell'app possono accedere ai contenuti scambiati.⁴⁷

L'azienda dietro Olvid, fondata da Thomas Baignères, Vincent Roca, Paul Pujol e Mathieu Cunche, opera come startup indipendente con sede in Francia. Ha ricevuto finanziamenti pubblici nell'ambito del programma France Relance e dal fondo Cybersecurity di Bpifrance, totalizzando circa 4 milioni di euro di investimenti a sostegno dello sviluppo e della scalabilità dell'applicazione. Questi fondi hanno consentito l'espansione delle funzionalità, il rafforzamento del team e l'avvio di collaborazioni con enti pubblici e difensivi.

A partire dal 2021, Olvid ha ricevuto un sostegno crescente da parte delle istituzioni francesi. È stata inclusa nel programma France Relance come tecnologia strategica per la cybersicurezza, ed è attualmente in uso da parte della Gendarmerie Nationale, del Conseil d'État e da diversi ministeri – in particolare Interno, Difesa e Giustizia – per le comunicazioni riservate. La sua adozione si è estesa anche a numerosi enti locali e agenzie semi-governative, grazie a contratti di acquisto pubblico semplificato e a bandi di sperimentazione dedicati alla sicurezza digitale. Inoltre, è in fase di valutazione da parte della NATO per l'uso in scenari classified e restricted, un riconoscimento della solidità tecnica e dell'affidabilità del prodotto (<https://www.olvid.io/>).

A differenza di Tchap, che è una soluzione pubblica centralizzata pensata per l'intera amministrazione e integrata in un ecosistema digitale nazionale, Olvid rappresenta una soluzione di nicchia, indipendente e sviluppata da un'azienda privata, ma fortemente legittimata dall'apparato statale. Il suo modello di business si fonda su licenze professionali e supporto a enti pubblici e imprese private che richiedono livelli di sicurezza avanzati, con un'interfaccia essenziale e un focus esclusivo sulla riservatezza. La società ha inoltre reso

⁴⁷ <https://www.olvid.io/whitepaper.pdf>



disponibile gratuitamente una versione base dell'app per il pubblico, pur mantenendo inaccessibili – per scelta – qualsiasi forma di raccolta metadati o tracciamento dell'attività utente (<https://www.olvid.io/pricing/>).

In sintesi, Olvid si configura come un complemento ideale – non un concorrente – del progetto Tchap. Se quest'ultimo mira a offrire un canale sicuro, integrato e standardizzato per la PA, Olvid soddisfa le esigenze più estreme di riservatezza in contesti politici, investigativi e militari. In un'epoca in cui la cybersicurezza è al centro del dibattito democratico e strategico, la coesistenza di entrambe le soluzioni testimonia un approccio francese articolato, che non rinuncia alla sovranità ma riconosce anche la necessità di flessibilità e di pluralismo tecnologico.

Un riflesso della sovranità strategica francese

L'approccio della Francia si distingue per la chiarezza del legame tra **tecnologia, strategia e sovranità nazionale**. Fin dal **Rapport Bothorel (2020)**, e ancor prima con la legge per una République numérique (2016), Parigi ha cercato di integrare nel discorso pubblico la necessità di dotarsi di strumenti nazionali per la gestione del digitale, non solo per motivi tecnici, ma come **scelta politica di indipendenza strategica**. Le soluzioni come Tchap e Olvid rispondono dunque a una logica di **resilienza istituzionale**, orientata a garantire che le comunicazioni pubbliche restino sottratte a pressioni extraterritoriali, come quelle derivanti dal CLOUD Act statunitense o da normative simili.

Questa strategia mostra come l'infrastruttura della comunicazione digitale non sia neutrale, ma **profondamente geopolitica**. In un'epoca in cui l'integrità del dibattito democratico, la riservatezza degli scambi e la capacità di difendere i dati sono parte integrante della sovranità, strumenti come Tchap e Olvid non rappresentano semplici alternative tecniche, ma **leve di autodeterminazione nazionale e garanzia democratica**.

Il caso italiano: TelsyInTouch App

Guardando all' Italia, TelsyInTouch rappresenta una delle iniziative più avanzate in Italia per una piattaforma di messaggistica nazionale, collocandosi all'interno del crescente dibattito sulla sovranità digitale e sulla protezione delle comunicazioni critiche, sia nel settore pubblico che in quello privato. Questo progetto si inserisce nella missione operativa di Telsy, azienda controllata dal Gruppo TIM e specializzata nella sicurezza delle comunicazioni e nella cybersecurity. Secondo il documento organizzativo dell'azienda⁴⁸, Telsy si occupa della progettazione e realizzazione di sistemi di cifratura destinati sia a usi civili che militari, sviluppando applicazioni per la protezione delle comunicazioni e offrendo servizi di consulenza ICT.

L'analisi del documento evidenzia alcuni spunti di riflessione. Anzitutto, emerge la caratteristica peculiare dell'industria della cybersecurity: l'intersezione tra tecnologie a uso civile e militare. Questa natura dual-use solleva implicazioni sia dal punto di vista della regolamentazione sia in termini di governance tecnologica. Inoltre, il riferimento alla normativa Golden Power sottolinea il valore strategico delle infrastrutture digitali per la sovranità tecnologica nazionale, evidenziando la necessità di sviluppare soluzioni autonome per ridurre la dipendenza da fornitori esteri e garantire un controllo diretto sulle tecnologie critiche.

TelsyInTouch integra la crittografia end-to-end (E2EE) per chat, chiamate, videochiamate VoIP e condivisione di file, consentendo alle istituzioni di mantenere il pieno controllo sulle infrastrutture critiche senza dover ricorrere a provider stranieri. TelsyInTouch si inserisce in un ecosistema più ampio di soluzioni sviluppate da Telsy per la sicurezza delle comunicazioni. Tra queste figurano TelsyATMO, un jammer audio a ultrasuoni che impedisce la registrazione da parte di software malevoli su dispositivi compromessi; TelsyAntares, una piattaforma di web conference basata su crittografia asimmetrica; e TelsyCryptophoneT2, un telefono fisso progettato per garantire chiamate criptate. Tuttavia, il valore strategico di TelsyInTouch va oltre la sua collocazione all'interno del portafoglio aziendale: la sua adozione nel contesto istituzionale italiano avviene in un momento in cui la sicurezza delle comunicazioni è al centro del dibattito pubblico e delle priorità governative. A differenza di Olvid, che opera su server Amazon Web Services e solleva interrogativi sulla sovranità tecnologica francese, la proposta italiana si distingue per la gestione autonoma delle infrastrutture e l'assenza di dipendenze da fornitori esteri⁴⁹. In un panorama geopolitico sempre più instabile e alla luce delle recenti vulnerabilità emerse nei sistemi di messaggistica, l'urgenza di soluzioni affidabili e sicure è sempre più evidente.

Inoltre, qualora si avanzasse concretamente l'ipotesi di un vero e proprio "WhatsApp di Stato", il controllo del Gruppo TIM diventerebbe un tema ancora più delicato di quanto già non lo sia. Eventuali operazioni di vendita o ristrutturazione societaria implicherebbero conseguenze dirette sul destino di Telsy e, di conseguenza, sull'integrità dell'intero sistema di comunicazione istituzionale. Una cessione o un passaggio di proprietà non ponderato potrebbe compromettere la sovranità digitale nazionale e rendere vulnerabili le infrastrutture

⁴⁸ [Telsy-MO-231-Parte-Generale-v.-7.3.pdf](#)

⁴⁹ [Come funziona l'app Telsy vagliata dal governo come alternativa a WhatsApp e Signal - Startmag](#)

di comunicazione governative, esponendole a rischi legati alla governance e alla sicurezza delle informazioni sensibili.

L'evoluzione del panorama geopolitico e i recenti scandali legati alla vulnerabilità dei sistemi di messaggistica⁵⁰ sottolineano l'urgenza di soluzioni tecnologiche affidabili, capaci di coniugare innovazione e protezione delle informazioni sensibili a livello nazionale. Inoltre, il progetto di un'infrastruttura di comunicazione sicura si inserisce in un quadro più ampio di strategie per il rafforzamento della sovranità digitale, coinvolgendo anche aspetti legati alla gestione dell'identità digitale, alla protezione delle reti e alla necessità di una maggiore consapevolezza sui rischi cibernetici. La sfida non è solo tecnologica, ma anche politica e culturale: assicurare un ecosistema digitale sicuro significa costruire un'infrastruttura capace di resistere a pressioni esterne, garantendo al contempo un elevato livello di usabilità e accessibilità per i suoi utenti.

⁵⁰ Riferimenti vari

Conclusioni e proposte di policy

Alla luce delle analisi sviluppate nei capitoli precedenti, è possibile affermare che le applicazioni di messaggistica si collocano oggi al centro di un crocevia tra innovazione, sicurezza e sovranità. Per questo, non possono più essere considerate semplici strumenti di comunicazione: esse rappresentano, a tutti gli effetti, architravi dell'infrastruttura digitale su cui si fonda una parte significativa della vita pubblica e privata contemporanea. Se questo è vero su scala globale, lo è in modo ancora più stringente per contesti nazionali che, come l'Italia, si trovano oggi nella necessità di coniugare trasformazione digitale, protezione dei dati e adattamento alle crisi geopolitiche in corso. È in quest'ottica che si propone, di seguito, una riflessione mirata sul caso italiano, suggerendo alcune traiettorie di policy che possano orientare le scelte future.

Nel caso dell'Italia, la sfida principale non è solo quella di "recuperare terreno" in termini di digitalizzazione, ma piuttosto di costruire una strategia coerente che sappia tenere insieme obiettivi tecnologici, esigenze di sicurezza e diritti fondamentali.

1. Una piattaforma italiana

È prioritario sviluppare una piattaforma italiana di messaggistica, progettata per la comunicazione interna alla pubblica amministrazione e dotata di funzionalità avanzate che rispondano alle esigenze quotidiane della PA. In realtà, una tale iniziativa è già in fase di definizione istituzionale, come dimostrano recenti sviluppi sul fronte nazionale. Ad esempio, il protocollo d'intesa siglato tra l'Istituto Poligrafico e Zecca dello Stato (IPZS) e l'Agenzia per la Cybersicurezza Nazionale (ACN) prevede la creazione di una soluzione specifica per la messaggistica istituzionale, finalizzata al potenziamento della resilienza digitale della pubblica amministrazione. L'utilizzo di questa piattaforma per le comunicazioni della PA potrebbe fungere da apripista per la sua successiva adozione anche nelle comunicazioni tra PA e cittadini.

È auspicabile che tale piattaforma sia pensata, in una prima fase, per l'utilizzo da parte delle amministrazioni centrali – in particolare Presidenza del Consiglio dei Ministri e Presidenza della Repubblica – pur restando scalabile per l'intera PA. Coerentemente con l'articolo 68 del Codice dell'Amministrazione Digitale (CAD), che promuove il riuso e l'adozione di software open source nella PA, e in linea con i requisiti di sicurezza informatica previsti dalla Direttiva UE 2022/2555 (NIS 2), la futura infrastruttura dovrebbe essere sviluppata secondo criteri di sicurezza by design, interoperabilità e sostenibilità giuridica e tecnica, in ogni caso validata dall'Agenzia per la Cybersicurezza Nazionale per garantirne la piena conformità ai più elevati standard di protezione dei dati e resilienza infrastrutturale.

Gli ostacoli all'adozione non sono trascurabili: vi è una forte inerzia culturale nell'uso informale di app commerciali, limitata maturità digitale tra i dipendenti pubblici e timori rispetto alla sovrapposizione con strumenti già esistenti (come PEC o portali regionali). Per superare tali criticità sarà fondamentale un percorso graduale, accompagnato da incentivi, formazione, e da una fase di sperimentazione su scala locale.

Un simile progetto non dovrebbe essere concepito come un'imposizione, né come l'ennesima applicazione calata dall'alto, ma come una piattaforma modulare e adattabile,

sviluppata in collaborazione con attori pubblici e privati, e testata progressivamente a partire da contesti pilota ad alta priorità (come la sanità, l'istruzione, la protezione civile).

2. Un regolamento per l'utilizzo

È necessario introdurre un regolamento nazionale sull'uso delle app di messaggistica nei rapporti tra PA, accompagnato da percorsi formativi obbligatori e da un meccanismo di attuazione chiaro e monitorabile. A tal fine, risulta essenziale che lo sviluppo della piattaforma proceda parallelamente alla definizione di una cornice regolatoria articolata, costruita attraverso determinazioni e decreti direttoriali dell'ACN, in raccordo con AGID. Tali provvedimenti dovranno essere coerenti con i criteri delineati dal Codice dell'Amministrazione Digitale (in particolare l'articolo 68), privilegiando soluzioni open source, interoperabili e sviluppate per conto della pubblica amministrazione. Per garantirne l'adozione effettiva, sarà inoltre necessario prevedere specifici obblighi formativi: inizialmente rivolti ai dipendenti delle amministrazioni centrali, poi – una volta testata e avviata l'applicazione – estesi anche ai cittadini attraverso percorsi formativi accessibili e gratuiti. Quanto al monitoraggio, si suggerisce di evitare la proliferazione di nuovi osservatori e, invece, potenziare l'Osservatorio sulla trasformazione digitale nel territorio italiano, già incardinato presso il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, dotandolo di una sezione dedicata al controllo e alla valutazione della piattaforma di messaggistica. In generale, per garantire coerenza tra regolazione, adozione e vigilanza, sarebbe auspicabile un coordinamento sistematico tra AGID, ACN e AGCOM. Qualora l'utilizzo della piattaforma venisse esteso anche ad ambiti critici quali la difesa o l'intelligence, sarebbe inoltre necessario coinvolgere direttamente il Ministero della Difesa, al fine di garantire la piena aderenza ai requisiti di sicurezza nazionale.

3. Un sostegno alla ricerca

Occorre stimolare la nascita e il consolidamento di un ecosistema italiano per la messaggistica e la sicurezza digitale, sostenendo startup, centri di ricerca e PMI innovative. La maggior parte delle app oggi utilizzate sono sviluppate da aziende americane o asiatiche, spesso caratterizzate da una ampia varietà nei loro modelli di business. In Italia, esistono realtà che lavorano su cifratura, comunicazione sicura, identità digitale decentralizzata – come Telsy (TIM), ma anche startup in ambito universitario – che potrebbero essere sostenute attraverso una pluralità di strumenti. Tra questi, si possono prevedere fondi pubblici dedicati a innovazione digitale, programmi di venture capital pubblico in collaborazione con CDP Venture Capital, e l'estensione di crediti d'imposta per la ricerca e sviluppo applicati a software open-source per la PA. Inoltre, convenzioni tra università, enti pubblici e centri di innovazione potrebbero facilitare la creazione di spin-off accademici e laboratori sperimentali legati alla sicurezza delle comunicazioni. Ad esempio, un protocollo tra i Politecnici italiani e l'Agenzia per la Cybersicurezza Nazionale⁵¹ potrebbe servire a co-sviluppare soluzioni crittografiche certificate. In parallelo, un sistema di gare pubbliche semplificate potrebbe agevolare l'adozione delle tecnologie più promettenti nei comuni italiani con meno di 30.000 abitanti. In Europa, modelli come quello francese di "La

51

https://www.acn.gov.it/portale/documents/20119/87266/ACN_ResearchInnovationAgenda.pdf/f4316f2c-773a-5c9f-92e5-95ea4e7de304?t=1704453683355

French Tech⁵² o il programma tedesco "Digital Hub Initiative"⁵³ mostrano l'efficacia di un supporto pubblico strategico mirato alla nascita di ecosistemi digitali nazionali: l'Italia può ispirarsi a queste esperienze adattandole al proprio tessuto produttivo e istituzionale. Parallelamente, si potrebbe istituire presso ACN un osservatorio nazionale sulla comunicazione digitale, con compiti di analisi delle app in uso, valutazione di rischi emergenti e formulazione di raccomandazioni vincolanti per gli enti pubblici. Va incentivata la creazione di un ecosistema nazionale per la sicurezza e la messaggistica digitale, basato su open source, interoperabilità e autonomia strategica. Lo sviluppo di una piattaforma non è sufficiente se non viene accompagnato da un investimento strutturale nella filiera nazionale dell'innovazione tecnologica. Il sostegno a startup, laboratori universitari e imprese italiane che lavorano su crittografia, decentralizzazione, intelligenza artificiale per la cybersicurezza, deve essere parte integrante della strategia digitale del Paese.

In conclusione, l'Italia si trova oggi di fronte a una sfida duplice: da un lato, proteggere la propria infrastruttura digitale in un contesto internazionale incerto e potenzialmente ostile; dall'altro, recuperare un controllo consapevole, trasparente ed efficiente sugli strumenti quotidiani che regolano la vita dello Stato e dei cittadini. [In tale direzione, si suggerisce di valutare ulteriori misure integrative come l'istituzione di audit periodici, svolti da organismi in seno alle Autorità competenti (quali l'ACN), per individuare tempestivamente eventuali vulnerabilità e garantire la costante conformità dell'infrastruttura digitale alle normative nazionali ed europee – come il Regolamento eIDAS; una revisione triennale del regolamento nazionale e delle linee guida, accompagnata da consultazioni pubbliche, che consenta un aggiornamento continuo e partecipato delle policy e infine la previsione di incentivi economici per le Pubbliche Amministrazioni che adottano la piattaforma statale di messaggistica, rispettando le best practice tecniche e organizzative: tali incentivi potrebbero essere incanalati nell'ambito dell'iniziativa "PA Digitale 2026" prevista dal PNRR. Le app di messaggistica, proprio per la loro apparente neutralità e pervasività, sono al centro di questa sfida. Rendere queste tecnologie coerenti con i valori costituzionali, con la sicurezza nazionale e con la sovranità digitale è una responsabilità che non può più essere rimandata. Le proposte avanzate in questo capitolo intendono offrire un punto di partenza concreto, radicato nel contesto italiano e orientato a un futuro dove tecnologia e democrazia camminino insieme

⁵² [French Tech - Accompagnement et promotion de l'écosystème start-up français](#)

⁵³ [Welcome | de:hub digital ecosystems](#)



Bibliografia

Amazon Wickr. (2025). *Secure collaboration for the federal government*.

<https://wickr.com/secure-collaboration-for-the-federal-government>

American Oversight. (2025). *Maryland Gov. Hogan's use of self-destructing messaging app*.

<https://americanoversight.org/investigation/maryland-gov-hogans-use-of-self-destructing-messaging-app>

ANSA. (2023). *WhatsApp Messenger e Telegram: le chat più usate dagli italiani*.

https://www.ansa.it/canale_tecnologia/notizie/software_app/2023/10/24/whatsapp-messenger-e-telegram-le-chat-piu-usate-dagli-italiani_2bf7684c-3eab-4270-9ca8-c0269a80b8d4.html

ArsTechnica. (2021). *WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app*.

<https://arstechnica.com/gadgets/2021/01/whatsapp-gives-users-an-ultimatum-share-data-with-facebook-or-stop-using-the-app/>

Aware Think Tank. (2022). *I cavi sottomarini come infrastruttura critica*.

<https://www.awarethinktank.it/wp-content/uploads/2022/05/I-cavi-sottomarini-come-infrastruttura-critica.pdf>

Brewster, T. (2022). *FBI forces open Amazon Wickr app with a suspect's face*. *Forbes*.

<https://www.forbes.com/sites/thomasbrewster/2022/07/19/fbi-forces-open-amazon-wickr-app-with-a-suspects-face/>

Direction Interministérielle du Numérique. (2025). *Tchap — Feuille de route*.

<https://tchap.numerique.gouv.fr/feuille-de-route/>

Fleming, S. (2025). *What is digital sovereignty and how are countries approaching it?* *World Economic Forum*.

<https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). *Controlling internet content in the EU: Towards digital sovereignty*. *Journal of European Public Policy*, 31(8).

<https://doi.org/10.1080/13501763.2024.0000000>

France Diplomacy. (2022). *Building Europe's digital sovereignty*. Ministry for Europe and Foreign Affairs.

<https://www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-europe/france-and-the-european-union/the-french-presidency-of-the-council-of-the-european-union/article/building-europe-s-digital-sovereignty-7-feb-22>

French Court of Auditors. (2023). *Le pilotage de la transformation numérique de l'État par la direction*.

<https://www.ccomptes.fr/fr/publications/le-pilotage-de-la-transformation-numerique-de-letat-par-la-direction>



French Tech. (2025). *Accompagnement et promotion de l'écosystème start-up français*. <https://www.lafrenchtech.com/>

Garante per la Protezione dei Dati Personali. (2016). *Cosa intendiamo per dati personali?* <https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali>

GDPR.eu. (2025). *A guide to GDPR data privacy requirements*. <https://gdpr.eu/data-privacy/>

Goodin, D. (2021). *WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app*. *ArsTechnica*. <https://arstechnica.com/gadgets/2021/01/whatsapp-gives-users-an-ultimatum-share-data-with-facebook-or-stop-using-the-app/>

Government of Italy. (2025). *Italia Digitale 2026*. <https://innovazione.gov.it/italia-digitale-2026/>

Kaspersky. (2025). *Messaging app security*. <https://www.kaspersky.it/resource-center/preemptive-safety/messaging-app-security>

Le Point. (2023). *Les ministres français invités à désinstaller WhatsApp, Signal et Telegram*. https://www.lepoint.fr/high-tech-internet/les-ministres-francais-invites-a-desinstaller-whatsapp-signal-et-telegram-29-11-2023-2545099_47.php

Monte, N., Flora, M. G. P., & Beckman, E. (2022). *State of revenge* (p. 3). *PermessoNegato*.

Murphy, H. (2024). *Telegram hits 900mn users and nears profitability as founder considers IPO*. *Financial Times*. <https://www.ft.com/content/1e7277ee-3f08-41f4-bc96-6c3f6319a58d>

National Archives and Records Administration. (2025). *The General Records Schedules: Transmittal 33*. <https://www.archives.gov>

NBC News. (2022). *Wickr, Amazon's child messaging app, has sex abuse problem*. <https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674>

Ortutay, B. (2024). *What is Telegram and why was its CEO arrested in Paris?* *AP News*. <https://apnews.com/article/telegram-ceo-paris-arrest-privacy-2024>

Pearson, S. (2023). *Brazilian court orders suspension of Telegram over neo-Nazi groups*. *The Wall Street Journal*. <https://www.wsj.com>

Pyrogram. (2025). *What are the IP addresses of Telegram data centers?* <https://docs.pyrogram.org/faq/what-are-the-ip-addresses-of-telegram-data-centers>

SEC. (2020). *SEC charges Telegram with conducting unregistered offering of digital tokens*. <https://www.sec.gov/newsroom/press-releases/2020-146>

Signal. (2025). *Signal.org*. <https://signal.org/>



Singer, N. (2018). *What you don't know about how Facebook uses your data*. *The New York Times*. <https://www.nytimes.com>

Startmag. (2025). *Come funziona l'app Telsy vagliata dal governo come alternativa a WhatsApp e Signal*. <https://www.startmag.it>

Telegram. (2025a). *Telegram FAQ*. <https://telegram.org/faq?setln=en>

Telegram. (2025b). *Telegram privacy policy (EU)*. <https://telegram.org/privacy/eu#4-1-storing-data>

Telegram. (2025c). *Telegram's group companies (EU privacy)*. <https://telegram.org/privacy/eu#8-2-telegrams-group-companies>

Telegram. (2025d). *Bots for business*. <https://core.telegram.org/bots/features#bots-for-business>

Telegram. (2025e). *Telegram Ads*. <https://ads.telegram.org/>

Telegram. (2025f). *Telegram Premium*. https://telegram.org/faq_premium

Telegram. (2025g). *Advertisement revenue sharing for content creators*. <https://telegram.org/tos/content-creator-rewards#2-1-advertisement-revenue-sharing>

Telegram. (2025h). *700 million users and Telegram Premium*. <https://telegram.org/blog/700-million-and-premium#telegram-premium>

Telegram. (2025i). *Telegram apps and open-source code*. <https://telegram.org/apps#codice-sorgente>

Telegram. (2025j). *Telegram contest channel*. <https://t.me/s/contest>

Telegram. (2025k). *Telegram job opportunities*. <https://telegram.org/jobs>

Tchap. (2025). *Tchap – Accueil*. <https://tchap.numerique.gouv.fr>

Telsy. (2025). *Telsy-MO-231-Parte-Generale-v.7.3.pdf*. <https://www.telsy.com>

Verdict. (2025). *What is Wickr?* <https://www.verdict.co.uk/what-is-wickr/>

Vice. (2022a). *Air Force spent millions on encrypted app Wickr*. <https://www.vice.com/en/article/air-force-millions-encrypted-app-wickr/>

Vice. (2022b). *Wickr and CIA funding via In-Q-Tel*. <https://www.vice.com/en/article/wickr-cia-funding-inqtel/>



Wickr. (2025). *Wickr creates advisory board to support federal business strategy*.
<https://www.govconwire.com/2020/10/wickr-creates-advisory-board-to-support-federal-business-strategy-joel-wallenstrom-quoted/>

Wikipedia. (2025). *General Data Protection Regulation*.
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Next.ink. (2025). *La Direction Interministérielle du Numérique (DINUM) lance un marché public sur Tchap*.
https://next.ink/brief_article/la-direction-interministerielle-du-numerique-dinum-lance-un-marche-public-sur-tchap/

Olvid. (2025). *Whitepaper*. <https://www.olvid.io/whitepaper.pdf>

ACN – Agenzia per la Cybersicurezza Nazionale. (2025). *Research & Innovation Agenda*.
https://www.acn.gov.it/portale/documents/20119/87266/ACN_ResearchInnovationAgenda.pdf

de:hub digital ecosystems. (2025). *Welcome*. <https://www.de-hub.de>

AWARE

www.awarethinktank.it

info@awarethinktank.it

