PENALE

La Corte di Strasburgo sull'acquisizione delle chat di Telegram

Fonte: Corte EDU, 13 febbraio 2024, Caso Podchasov c. Russia (ric. n. 33696-19).pdf

Luigi Giordano
25 Luglio 2024

I sistemi di comunicazione elettronica crittografata creano per i governi degli Stati democratici problemi di non poco conto in merito alla protezione dei diritti individuali – tra cui la riservatezza e la libertà di opinione – per consentire, nello stesso tempo, le misure necessarie alla sicurezza nazionale, alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati.

Massima

La legge russa che prevede la conservazione delle comunicazioni internet di tutti gli utenti, l'accesso diretto dei servizi di sicurezza ai dati archiviati senza adeguate garanzie contro gli abusi e l'obbligo di decifrare le comunicazioni criptate pregiudica l'essenza stessa del diritto al rispetto della vita privata previsto dall'art. 8 della CEDU.

Il caso

Secondo **una sezione della legge federale russa** n. 149 del 27 luglio 2006 "sull'informazione", introdotta nel 2014, gli "*organizzatori di comunicazioni via Internet*" sono tenuti ad archiviare **tutti i dati delle comunicazioni** per una durata di un anno e **il contenuto delle stesse** per sei mesi ed a fornire tali dati alle autorità di polizia o ai servizi di sicurezza nelle circostanze specificate dalla legge, insieme con le informazioni necessarie per decodificare i messaggi elettronici se crittografati.

Il 12 luglio 2017, il Servizio di sicurezza federale della Russia, in forza di decisioni giudiziarie fondate su tale legge, ha richiesto a *Telegram* di divulgare le informazioni tecniche per decodificare le comunicazioni relative a sei numeri di cellulare associati agli account *Telegram Messenger*. È stato chiesto, tra l'altro, di fornire **i dati relativi alle chiavi di crittografia** necessarie per decifrare le comunicazioni.

Telegram* ha rifiutato di rispettare l'ordine di divulgazione, sostenendo che era tecnicamente impossibile eseguirlo senza creare una *backdoor, cioè una porta "sul retro" che avrebbe permesso di accedere da remoto al sistema informatico, indebolendo la riservatezza di tutti gli utenti.

La società è stata multata dal Tribunale distrettuale di Mosca il 12 dicembre 2017. Successivamente, con sentenza del 13 aprile 2018, il Tribunale distrettuale di Mosca ha ordinato il blocco dell'applicazione *Telegram* in Russia. Entrambe le sentenze sono state confermate in appello.

Il 12 marzo 2018, **alcuni utenti hanno impugnato l'ordine di divulgazione**, sostenendo che la fornitura delle chiavi di crittografia avrebbe consentito la decifratura delle comunicazioni di tutti gli utilizzatori del sistema di comunicazione, con la conseguente **violazione del loro diritto al rispetto della vita privata**. Dopo aver ricevuto le chiavi di crittografia, infatti, la polizia russa avrebbe avuto la capacità tecnica di accedere a tutte le comunicazioni senza l'autorizzazione giudiziaria richiesta dalla legge russa. Il 22 marzo 2018, il Tribunale distrettuale ha respinto il reclamo. Successivamente, il Tribunale di Mosca ha rigettato l'appello avverso tale decisione.

In seguito, un giudice del Tribunale di Mosca ha rifiutato di valutare un ricorso per cassazione presentato dal ricorrente, non riscontrando violazioni significative del diritto sostanziale o procedurale che avessero influenzato l'esito del procedimento. Un ulteriore ricorso per cassazione del ricorrente è stato respinto il 16 gennaio 2019 dalla Corte Suprema della Federazione Russa.

Telegram, peraltro, nonostante le decisioni giudiziarie intervenute, è ancora funzionante in Russia.

La questione

L'utilizzo di sistemi di comunicazione elettronica crittografata costituisce una risposta alla criminalità informatica e ai timori di sorveglianza di massa. Tali sistemi, tuttavia, creano per i governi degli Stati democratici **un problema di non facile soluzione**: come proteggere i diritti individuali, tra cui la riservatezza e la libertà di opinione, consentendo, nello stesso tempo, le misure necessarie alla sicurezza nazionale, alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati? Quali misure sono compatibili con il rispetto del diritto alla vita privata di cui all'art. 8 Cedu?

Le soluzioni giuridiche

1. La legge federale russa "sull'informazione" stabilisce precisi obblighi per i soggetti forniscono servizi di comunicazione elettronica. Essi sono tenuti a **conservare** sul territorio russo **tutti i dati di comunicazione** generati dagli utenti di internet per una durata di un anno e **il contenuto di tutte le comunicazioni** per una durata di sei mesi; devono fornire le **informazioni alle autorità** di contrasto o ai servizi di sicurezza nelle circostanze specificate dalla legge (entro dieci giorni dalla richiesta), aggiungendo **tutte le informazioni necessarie per de-crittografare** le comunicazioni elettroniche e permettendo l'accesso da remoto a tali dati; devono **identificare gli utenti** di tali servizi di messaggistica tramite i loro numeri di telefono mobile.

Le previsioni di questa legge limitano in modo significativo la riservatezza delle comunicazioni elettroniche che avvengono per mezzo di sistemi che impiegano la crittografia, sebbene **diverse fonti normative sovranazionali ne riconoscono il rilievo come mezzo essenziale per la salvaguardia dei diritti umani**, consistendo in una risposta efficace ai rischi della sorveglianza di massa e della criminalità informatica.

2. Il **Rapporto sul diritto alla privacy** nell'era digitale dell'Ufficio dell'**Alto Commissario delle Nazioni Unite per i diritti umani**, pubblicato il 4 agosto 2022, in particolare, ha riconosciuto che:

- «la crittografia è un **fattore chiave per la privacy** e la sicurezza online ed è essenziale per salvaguardare i diritti, compresi i diritti alla libertà di opinione e di espressione, alla libertà di associazione e di riunione pacifica, alla sicurezza, alla salute e alla non discriminazione»;
- essa garantisce che **le persone possano condividere liberamente le informazioni**, senza timore che le loro informazioni possano diventare note ad altri, siano essi autorità statali o criminali informatici;
- essa è essenziale se si vuole che **le persone si sentano sicure nello scambiare liberamente informazioni con altri** su una vasta gamma di esperienze, pensieri e identità, comprese informazioni sensibili sulla salute o finanziarie, conoscenze sull'identità di genere e sull'orientamento sessuale, espressione artistica e informazioni relative allo status di minoranza.

Secondo l'**Alto Commissario delle Nazioni Unite per i diritti umani,** il conflitto tra la libertà di opinione e di espressione e la protezione delle popolazioni da gravi crimini e minacce alla sicurezza non va risolto limitando l'uso della crittografia, perché sono disponibili **vari altri strumenti e approcci** per acquisire le informazioni necessarie alle investigazioni. Tali misure alternative includono **una polizia tradizionale migliorata** e dotata di maggiori risorse, **operazioni sotto copertura**, **analisi dei metadati** e **il rafforzamento della cooperazione di polizia internazionale**. La criminalizzazione della crittografia, invece, impedirebbe a tutti gli utenti di avere un modo sicuro per comunicare e le *backdoor* obbligatorie nei sistemi di comunicazione che la usano non opererebbero solo nei confronti di utenti specifici identificati come sospettati di crimine o minacce alla sicurezza.

3. Anche l'**Appendice alla Raccomandazione del Comitato dei Ministri del Consiglio d'Europa sulla tutela dei diritti umani per quanto riguarda i servizi di *social networking***, adottata il 4 aprile 2012, ha suggerito agli Stati membri, in cooperazione con il settore privato e la società civile, di adottare misure adeguate a garantire che il diritto degli utenti alla vita privata sia tutelato in rete, in particolare proteggendo i dati personali da accessi illegittimi da parte di terzi, pure quelli concernenti comunicazioni crittografate *end - to-end* tra l'utente e il sito web dei servizi di *social networking*.

4. La **Risoluzione 2045 (2015) dell'Assemblea del Consiglio d'Europa sulla sorveglianza di massa, adottata il 21 aprile 2015**, pur riconoscendo la necessità di una sorveglianza efficace e mirata dei sospetti terroristi e di altri gruppi criminali organizzati, ha espresso preoccupazione per le minacce alla sicurezza di internet derivanti:

- dalle pratiche di alcune agenzie di intelligence, rivelate nei dossier *Snowden*, di ricercare sistematicamente, utilizzare e persino creare "*backdoor*" e altre debolezze negli standard di sicurezza e nell'implementazione che potrebbero essere facilmente sfruttate da terroristi e cyberterroristi o altri criminali;
- per la raccolta di massicce quantità di dati personali da parte di imprese private e per il rischio che tali dati possano essere accessibili e utilizzati per scopi illegali da attori statali e non statali;
- per lo sviluppo in diversi Paesi di un massiccio "*complesso industriale di sorveglianza*" ad opera di strutture le quali, sorte come contromisura per evitare gravi minacce, possono sfuggire al controllo e alla responsabilità democratica e minacciare la natura libera e aperta delle nostre società.

L'Assemblea del Consiglio d'Europa, pertanto, ha esortato gli Stati membri:

- a garantire che le leggi nazionali consentano la raccolta e l'analisi dei dati personali solo con il consenso dell'interessato o a seguito di un'ordinanza del tribunale emessa sulla base del ragionevole sospetto che la vittima sia coinvolta in attività criminali;
- a sanzionare la raccolta e il trattamento illeciti dei dati;
- a vietare severamente la creazione di "*backdoor*" o qualsiasi altra tecnica volta a indebolire o eludere le misure di sicurezza o a sfruttarne le debolezze esistenti;
- a garantire che i loro servizi di intelligence siano soggetti ad adeguati meccanismi di controllo giudiziario e/o parlamentare.

5. In ambito unionale, la sentenza della Corte di giustizia dell'Unione europea (CGUE) dell'8 aprile 2014 nelle cause riunite *Digital Rights Ireland e Seitinger e altri* (C-293/12 e C-594/12, EU:C:2014: 238) ha dichiarato invalida la Direttiva sul trattamento dei dati personali 2006/24/CE. Tale direttiva prevedeva l'obbligo per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare tutti i dati relativi al traffico e all'ubicazione per periodi compresi tra sei mesi e due anni, al fine di garantire che i dati fossero disponibili ai fini della indagine, accertamento e perseguimento di reati gravi, come definiti da ciascuno Stato membro nella propria legislazione nazionale.

La CGUE ha inoltre affermato, nella sentenza del 6 ottobre 2015 nel caso *Maximillian Schrems c. Data Protection Commissioner* (C-362/14, EU:C:2015:650), che una normativa che consente alle autorità pubbliche di avere accesso in modo generalizzato al contenuto delle comunicazioni elettroniche deve essere considerata tale da compromettere la sostanza del diritto fondamentale al rispetto della vita privata.

Sempre in ambito unionale, in una **dichiarazione congiunta di Europol e dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) del 20 maggio 2016 sulle indagini penali legali che rispettano la protezione dei dati del 21° secolo** è stato osservato che «Intercettare una comunicazione crittografata o violare un servizio digitale potrebbe essere considerato proporzionale rispetto al singolo sospettato, ma violare i meccanismi crittografici potrebbe causare danni collaterali». L'obiettivo dovrebbe essere quello di ottenere l'accesso alla comunicazione o alle informazioni, senza provocare la rottura del meccanismo di protezione.

È stato allora osservato come le informazioni devono essere decifrate per essere utili ai criminali. Ciò crea opportunità per alternative come **operazioni sotto copertura**, **infiltrazione in gruppi criminali** e **accesso ai dispositivi di comunicazione oltre il punto di crittografia**, ad esempio mediante intercettazione legale su tali dispositivi mentre sono ancora utilizzati dai sospettati.

Ci sono casi, tuttavia, **in cui tali alternative non esistono e l'accesso ai contenuti nascosti può essere ottenuto solo tramite una forma di decrittazione**.

Dopo tale premessa è stato rilevato che, sebbene nessun meccanismo pratico di crittografia sia perfetto nella sua progettazione e implementazione, la decrittazione sembra essere sempre meno fattibile per scopi di applicazione della legge, portando a proposte per introdurre *backdoor* obbligatorie o deposito di chiavi per indebolire la crittografia. «Le soluzioni che indeboliscono intenzionalmente i meccanismi di protezione tecnica a sostegno delle forze dell'ordine indeboliranno intrinsecamente anche la protezione contro i criminali».

Quando l'accesso alle informazioni crittografate è fondamentale per la sicurezza e la giustizia, comunque, «**è necessario offrire soluzioni fattibili alla decrittazione senza**

indebolire i meccanismi di protezione», sia nella legislazione che attraverso la continua evoluzione tecnica. Per quest'ultimo, è fortemente consigliata la promozione di una **stretta collaborazione con i partner industriali**.

6. Il 28 luglio 2022 il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD) hanno adottato il parere congiunto 4/2022 sulla proposta di regolamento del Parlamento europeo e del Consiglio recante norme per prevenire e combattere la sessualità infantile abuso. In tale parere, è stato osservato, tra l'altro, che «**le tecnologie di crittografia contribuiscono in modo fondamentale al rispetto della vita privata** e della riservatezza delle comunicazioni, alla libertà di espressione nonché all'innovazione e alla crescita dell'economia digitale, che si basa sull'elevato livello di fiducia e la fiducia che tali tecnologie forniscono».

Nel contesto delle comunicazioni interpersonali, la crittografia *end-to-end* è uno **strumento fondamentale per garantire la riservatezza** delle comunicazioni elettroniche, poiché fornisce solide garanzie tecniche contro l'accesso al contenuto delle comunicazioni da parte di soggetti diversi, compreso il fornitore. Ciascuna delle tecniche per limitarne la portata, tra l'altro, esporrebbe a pericoli: la scansione lato client porterebbe a un accesso sostanziale e non mirato e all'elaborazione di contenuti non crittografati sui dispositivi dell'utente finale; la scansione lato server porterebbe al trattamento in massa di dati personali sui server dei fornitori.

7. Dopo l'ampia illustrazione delle fonti sovranazionali relative alle comunicazioni per mezzo di sistemi informatici che impiegano la crittografia, la Corte EDU ha ribadito che, come già affermato in una precedente decisione (Corte EDU (GC) 5 dicembre 2015, Rom an Zakharov c. Russia, ric. n. 47143/06), **l'archiviazione, da parte del gestore della piattaforma di messaggistica *on line*, delle comunicazioni via Internet e dei dati relativi alla vita privata di una persona costituisce in sé interferenza che contrasta con il diritto alla riservatezza tutelato dall'art. 8 CEDU**, a prescindere dall'uso successivo di tali informazioni e indipendentemente dal fatto che i dati siano stati poi consultati o meno dalle autorità.

La Corte, poi, ha rilevato che, sebbene il caso riguardi principalmente il problema della conservazione dei dati personali del ricorrente, esso va esaminato alla luce della propria **giurisprudenza in materia di sorveglianza segreta**, poiché le garanzie applicabili sono essenzialmente simili e dovrebbero garantire contro il rischio intrinseco di abuso, sì da mantenere l'interferenza con i diritti protetti dall'art. 8 Cedu nei limiti di ciò che è "*necessario in una società democratica*". Un'interferenza può essere giustificata solo se conforme alla legge, se persegua uno o più degli scopi legittimi a cui si riferisce l'art. 8, § 2; se sia necessaria in una società democratica per raggiungere tale obiettivo.

La necessità di tali garanzie, peraltro, è ancor più sentita allorché si tratti della protezione dei dati personali sottoposti a **trattamento automatico**, soprattutto quando essi siano utilizzati a fini di polizia, tenuto anche conto del fatto che la tecnologia è sempre più sofisticata.

La protezione offerta dall'art. 8 della Cedu, peraltro, verrebbe indebolita in modo inaccettabile se l'uso delle moderne tecnologie nel sistema di giustizia penale fosse consentito ad ogni costo e senza bilanciare attentamente i potenziali benefici dell'uso estensivo di tali tecnologie con importanti interessi della vita privata.

Il diritto nazionale, pertanto, **deve garantire che i dati conservati siano pertinenti rispetto alle finalità per cui sono conservati**; siano conservati in una forma che

consenta l'identificazione degli interessati per un periodo non superiore a quello necessario allo scopo per il quale sono memorizzati; **vi siano garanzie adeguate a scongiurare abusi**; la conservazione dei dati sia proporzionata allo scopo della raccolta e riguardi periodi di conservazione limitati.

Per soddisfare il requisito della "prevedibilità", inoltre, la legge nazionale deve contenere un'indicazione adeguata delle circostanze e delle condizioni di autorizzazione della autorità pubblica ad accedere ai dati conservati per eseguire misure di sorveglianza segreta. Inoltre, poiché l'utilizzo di tali misure, proprio perché segrete, non è controllabile dagli interessati o dalla collettività, sarebbe contrario allo stato di diritto che il potere discrezionale dell'esecutivo o del giudice fosse incondizionato, sicché devono essere previste in modo chiaro la portata della discrezionalità e le modalità del suo esercizio.

La riservatezza delle comunicazioni, comunque, **è contenuto essenziale del diritto al rispetto della vita privata e della corrispondenza**, come previsto dall'art. 8 Cedu, sicché va garantito agli utenti delle telecomunicazioni e dei servizi Internet il rispetto della privacy e della libertà di espressione, pur trattandosi di una garanzia non assoluta allorquando siano in gioco interessi collettivi come la prevenzione del disordine o della criminalità o la protezione dei diritti e delle libertà altrui.

8. Nel caso di specie, la Corte EDU ha ritenuto che **le misure consentite dalla legge russa**, consistenti nella conservazione di tutte le comunicazioni Internet di tutti gli utenti, nell'accesso diretto dei servizi di sicurezza ai dati archiviati senza adeguate garanzie contro gli abusi e nell'obbligo di decriptare le comunicazioni criptate, come applicato ai terminali comunicazioni crittografate end-to-end, **non possono essere considerate necessarie in una società democratica**.

In quanto questa normativa consente alle autorità pubbliche di avere accesso, in modo generalizzato e senza garanzie sufficienti, al contenuto delle comunicazioni elettroniche, **essa pregiudica l'essenza stessa del diritto al rispetto della vita privata previsto dall'art. 8 della Convenzione**. Lo Stato convenuto ha quindi oltrepassato qualsiasi margine di discrezionalità accettabile a questo riguardo.

9. In particolare, la Corte ha ritenuto che **le disposizioni impugnate perseguano gli scopi legittimi** di tutela della sicurezza nazionale, di prevenzione dei disordini e della criminalità e di tutela dei diritti e delle libertà altrui. Le capacità tecnologiche, difatti, hanno notevolmente aumentato il volume delle comunicazioni elettroniche; al contempo, si sono anche moltiplicate le minacce cui devono far fronte gli Stati contraenti e i loro cittadini che includono il terrorismo, il traffico di droga, la tratta di esseri umani e lo sfruttamento sessuale dei bambini.

La legge russa "sull'informazione", tuttavia, **non contiene garanzie adeguate ed efficaci per soddisfare i requisiti di "qualità del diritto" e di "necessità in una società democratica"**.

Essa impone **un obbligo di conservazione estremamente ampio** che determina, di conseguenza, un'interferenza eccezionalmente ampia e grave rispetto al diritto alla riservatezza.

L'archiviazione dei *traffic data* e delle *chat* non è infatti subordinata alla sussistenza di un ragionevole sospetto di un coinvolgimento degli utenti in attività criminali o che mettono in pericolo la sicurezza nazionale.

Al tempo stesso, l'acquisizione dei dati esterni e/o del contenuto delle conservazioni da parte delle autorità giudiziaria o di polizia non è subordinato a un controllo giurisdizionale, preventivo o successivo; **manca**, nel sistema normativo russo, una garanzia fondamentale contro gli abusi, vale a dire **l'obbligo di esibire al gestore l'autorizzazione giudiziale** prima di ottenere l'accesso ai dati conservati; non sono previsti rimedi adeguati a prevenire o contrastare possibili abusi.

L'obbligo legale del gestore di decrittare le comunicazioni crittografate *end-to-end*, infine, **comporta il rischio di indebolire il meccanismo di cifratura per tutti gli utenti** e non è, pertanto, proporzionato agli obiettivi legittimi perseguiti.

L'indebolimento della crittografia mediante creazione di *backdoors*, difatti, rende tecnicamente possibile una sorveglianza generale e indiscriminata delle comunicazioni elettroniche personali, di ciò potendo approfittare anche reti criminali, con conseguente, seria compromissione della sicurezza di tutte le comunicazioni elettroniche degli utenti, anche di quelli estranei al procedimento penale.

Osservazioni

1. *Telegram* è un'applicazione di messaggistica che può essere utilizzata su telefoni cellulari, tablet o computer. Il servizio è erogato, gratuitamente e senza fini di lucro, da *Telegram* LLC, una società con sede a Dubai fondata da un imprenditore russo.

Questa applicazione è utilizzata da milioni di persone in Russia e nel mondo.

Secondo il suo sito web ufficiale, *Telegram* non utilizza, come impostazione predefinita, la crittografia *end - to - end* (*client-client*), ma solo uno schema di crittografia *server-client*, ovvero è cifrata dal dispositivo fino ai server della società e viceversa. È possibile per l'utente passare alla crittografia *end – to - end* attivando la funzione "*chat segreta*" in luogo di quella base definita "*chat cloud*": in questo caso, nessun soggetto diverso da coloro che si scambiano i messaggi, può decifrarli, compresa la società che eroga il servizio. Sotto questo profilo ***Telegram* funziona diversamente da *WhatsApp* e da *Signal*,** applicazioni che offrono comunicazioni che sono sempre crittografate *end-to-end*, potendo essere lette o ascoltate solo dai destinatari previsti.

2. La Corte EDU, con la sentenza illustrata, ha affrontato **per la prima volta** il tema dell'uso della crittografia nelle comunicazioni tramite *software* di messaggistica istantanea, verificando la compatibilità con l'art. 8 delle Cedu delle misure volte a consentire l'accesso alle autorità statali alle informazioni trasmesse.

La Corte ha affermato che **le disposizioni giuridiche russe** che disciplinano gli obblighi degli "organizzatori di comunicazioni internet" e le misure di sorveglianza segreta, pur perseguendo scopi legittimi di tutela della sicurezza nazionale, di prevenzione della criminalità e di tutela dei diritti, non soddisfano il requisito di "qualità della legge", perché **non prevedono garanzie adeguate ed effettive contro l'arbitrarietà e il rischio di abusi**.

La normativa impugnata è stata cesurata perché:

- impone la conservazione dei dati delle comunicazioni e del contenuto delle stesse di tutti gli utenti in modo indifferenziato;
- permette l'accesso dei servizi di sicurezza ai dati archiviati senza adeguate garanzie contro gli abusi ed in particolare senza l'autorizzazione dell'autorità giudiziaria;
- permette un accesso generalizzato e non mirato a tutte le conversazioni degli utenti;
- impone alle società l'obbligo di decriptare le comunicazioni criptate.

Esse, quindi, sono incapaci di mantenere l'"*ingerenza*" nel diritto alla riservatezza in ciò che è "*necessario in una società democratica*" come prescritto dall'art. 8 Cedu.

3. Richiamando atti delle organizzazioni internazionali, la Corte EDU ha riconosciuto il rilievo della crittografia come strumento di tutela effettiva della riservatezza.

Questo è il primo aspetto di particolare interesse della decisione in esame.

Secondo la Corte, la crittografia è «un **fattore chiave per la privacy** e la sicurezza online ed è essenziale per salvaguardare i diritti, compresi i diritti alla libertà di opinione e di espressione, alla libertà di associazione e di riunione pacifica, alla sicurezza, alla salute e alla non discriminazione». Essa garantisce che le persone possano condividere liberamente le informazioni, senza timore che le loro informazioni possano diventare note ad altri, siano essi autorità statali o criminali informatici.

La crittografia, dunque, **è essenziale se si vuole che le persone si sentano sicure nello scambiare liberamente informazioni con altri** su esperienze, pensieri e identità, comprese informazioni sensibili sulla salute o finanziarie, conoscenze sull'identità di genere e sull'orientamento sessuale, espressione artistica e informazioni relative allo status di minoranza.

In Stati in cui esistono meccanismi di censura, la crittografia consente agli individui di mantenere **uno spazio per contenere, esprimere e scambiare opinioni con altri**.

Quanto affermato è stato avvalorato da un dato emblematico: nei conflitti armati, la messaggistica crittografata è indispensabile per garantire comunicazioni sicure tra i civili; nei due mesi successivi allo scoppio del conflitto armato in Ucraina, il 24 febbraio 2022, il numero di *download* in Ucraina dell'app di messaggistica crittografata *Signal* è aumentato di oltre il 1.000 % rispetto ai mesi precedenti (verosimilmente con un passaggio di utenti a scapito proprio di *Telegram*, per ovvie ragioni).

4. La Corte EDU, però, ha evidenziato come l'uso della crittografia ponga **un dilemma per i governi**, tenuti a ricercare l'equilibrio corretto tra la necessità di proteggere i cittadini, in special modo i più vulnerabili, da gravi crimini e minacce alla sicurezza e quella di non minare i diritti umani.

La Corte ha ammesso, infatti, che le comunicazioni crittografate possono essere utilizzate anche da criminali, complicando non poco le indagini penali che si fondano soprattutto su intercettazioni quando hanno ad oggetto gravi reati.

La sentenza in esame, allora, richiamando atti di organizzazioni sovranazionali, elenca le possibili **soluzioni alternative** che, senza incidere in modo definitivo sul sistema di decriptazione *end to end*, con la creazione di *backdoors*, e, dunque, senza indebolire i meccanismi di protezione della riservatezza, consentono una efficace attività investigativa.

Le soluzioni alternative sono in sostanza quelle contenute in una dichiarazione congiunta di Europol e dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) del 20 maggio 2016 sulle indagini penali legali che rispettano la protezione dei dati del 21° secolo.

Esse possono così essere sintetizzate:

- **operazioni sotto copertura,**

- **infiltrazione in gruppi criminali;**
- **accesso ai dispositivi di comunicazione oltre il punto di crittografia** (ad esempio mediante analisi forensi in tempo reale sui dispositivi sequestrati o mediante intercettazione legale su tali dispositivi mentre sono ancora utilizzati dai sospettati);
- metodi forensi che fanno uso dei metadati dei dispositivi (potrebbero non aiutare a intercettare il contenuto della comunicazione stessa, ma potrebbero fornire altri importanti indizi per l'investigatore).

La stessa Corte EDU, però, rinviando alla citata dichiarazione congiunta di Europol e dell'Agenzia dell'Unione europea per la sicurezza informatica, ha riconosciuto che «… **Ciononostante ci sono casi in cui tali alternative non esistono e l'accesso ai contenuti nascosti può essere ottenuto solo tramite una forma di decrittazione**» (cfr. par. 33 della sentenza).

Questo è il punto più delicato, che emerge quando, allo stato dell'evoluzione tecnologica, non è possibile «l'**accesso ai dispositivi di comunicazione oltre il punto di crittografia**».

In tale momento, «**è necessario offrire soluzioni fattibili alla decrittazione senza indebolire i meccanismi di protezione, sia nella legislazione che attraverso la continua evoluzione tecnica**».

In questa prospettiva «è fortemente consigliata la promozione di una stretta collaborazione con i partner industriali, nonché con la comunità di ricerca con esperienza in criptoanalisi per la violazione della crittografia, ove legalmente indicato».

L'obiettivo da perseguire è quello di trovare una soluzione che raggiunga un equilibrio ragionevole e praticabile tra i diritti individuali e la tutela degli interessi di sicurezza dei cittadini dell'UE.

5. Le soluzioni alternative citate nella sentenza, in particolare la captazione di comunicazioni oltre il punto di crittografia, invero, appaiono in astratto praticabili nel caso di impiego di sistemi di comunicazione criptati *end to end*, come *Telegram, WhatsApp, Signal*.

L'utilizzo di tali sistemi non sembra escludere, almeno in ipotesi, la possibilità di intercettazione di comunicazioni che si svolgono per mezzo di applicativi che si scaricano sui cellulari comuni.

In questi casi, infatti, è possibile procedere ad intercettazioni legali sui dispositivi dei sospettati prima che le conversazioni siano criptate oppure dopo che sono state decodificate, inoculando nel dispositivo, tramite la rete, un *trojan*. Si tratta di applicazioni residenti in dispositivi che sono connessi alla rete internet, che permettono comunicazioni con la rete GSM e che non impediscono la presenza di altre App.

Diversamente, invece, nel caso in cui le comunicazioni elettroniche avvengano tramite criptofonini.

Sono stati definiti **"criptofonini"** i telefoni cellulari che permettono lo scambio di dati crittografati con una cifratura a più livelli. Tali apparecchi sono costituiti da un *hardware* opportunamente modificato (in genere *Apple*, *Android* o *Black Berry*) e da un sistema operativo avente particolari requisiti di sicurezza, in quanto i servizi di localizzazione (GPS, *Bluetooth*, fotocamera, scheda SD e porta USB) sono disabilitati. Le chiamate rimangono attive solo in modalità *Voice over IP* (VoiP), utilizzando applicazioni che assicurano comunicazione cifrate (*Encrochat*, *Sky ECC, Anom, No1bc*, etc.) ed evitando l'uso della rete GSM.

La Corte di Giustizia, a seguito di rinvio pregiudiziale intervenuto nel corso di un procedimento penale tedesco, si è occupata dell'uso processuale delle chat tratte da **telefoni che usavano il programma *Encrochat***, una rete di comunicazione eliminata a seguito della complessa operazione di polizia congiunta tra Francia e Paesi Bassi che è stata descritta in precedenza.

In diversi procedimenti penali italiani e in altri Stati dell'Unione, inoltre, sono stati usate come prove le chat tratte da criptofonini che utilizzavano il **diverso applicativo *Sky Ecc***. Tale programma apparteneva a *Sky Global,* società fornitrice di servizi di comunicazione con sede a Vancouver, in Canada. Nel 2021 erano oltre 171.000 gli apparati registrati, principalmente in Europa, Nord America, diversi Paesi del Centro e Sud America – principalmente Colombia – e Medio Oriente.

Questi sistemi di comunicazione sono realizzati in modo da assicurare la **completa ermeticità dei telefoni cellullari** ed offrendo servizi come:

- utilizzo di sistemi di cifratura avanzata, sia dei dati memorizzati, sia del canale di comunicazione;
- volatilità dei messaggi con la possibilità, anche da parte di un terzo, di effettuare da remoto sul dispositivo l'autodistruzione del contenuto del messaggio, che comunque interviene dopo un certo lasso di tempo (per esempio dopo sette giorni dall'ultima accensione o impiego) ovvero in occasione del riavvio del sistema in alcune configurazioni o ancora dopo un certo lasso di tempo di disconnessione dalla rete telefonica o telematica;
- l'impiego di "*fake up*" per simulare un apparato ordinario e trarre in inganno l'operatore di polizia in caso di eventuale controllo del dispositivo;
- la possibilità di rilevare la presenza di *IMSI Catcher,* un dispositivo che si finge una cella di una rete mobile in grado di intercettare le comunicazioni tra il dispositivo e la rete, incluse chiamate vocali, messaggi di testo e dati internet e finanche di interrompere il servizio e di non ricevere i cosiddetti sms "silenti o occulti";
- la possibilità di prevedere l'impiego di codici di sblocco sia del sistema operativo di sia di ogni singola applicazione;
- la possibilità di impiegare schede straniere non intestate a soggetti giuridici.

Queste caratteristiche rendono l'apparecchio non penetrabile tramite *trojan*, non essendo possibile, pertanto, una "scansione lato cliente"

6. Quello dei criptofonini sembrerebbe proprio il caso in cui non esistono alternative all'accesso ai contenuti nascosti tramite una forma di decrittazione.

Per l'accesso da parte delle Forze dell'ordine alle comunicazioni che avvengono con tali apparecchi è stato necessario violare il server, **unico modo per poter procedere all'intercettazione dei dispositivi**. Si è trattato di una operazione complessa, realizzata grazie ad una cooperazione di polizia tra Stati membri dell'Unione, verosimilmente attuata con l'aiuto di partner industriali e l'impiego di programmi necessariamente sottoposti al segreto di Stato (perché altrimenti sarebbero pericolosi per tutti i sistemi di comunicazione *end to end* che sono necessari, come ha spiegato la sentenza della CEDU illustrata, per la tutela della riservatezza).

Nel caso delle comunicazioni che si svolgevano con l'applicativo Sky ECC, ad esempio, il giudice istruttore di Lille, in data 14 giugno 2019, ha emesso la prima «autorizzazione all'intercettazione di corrispondenza per via elettronica», autorizzando la collocazione di un dispositivo per «l'intercettazione, la registrazione e la trascrizione delle comunicazioni

effettuate mediante comunicazioni elettroniche» tra due server e delle «comunicazioni elettroniche in entrata e in uscita dal server principale». In questo modo, è stato captato il flusso telematico in transito tra due server di una società di *hosting* denominata OVH, uno dei quali di *backup*. A questo primo provvedimento hanno fatto seguito altre autorizzazioni e decreti di proroga di intercettazioni.

In particolare, dall'informativa sull'andamento delle indagini del "*Brigadiere di polizia*" al pubblico ministero del 18 luglio 2019, emerge che «un'analisi preliminare del flusso di rete ha rivelato elementi promettenti: parte del traffico di rete non è stato crittografato; alcune informazioni sono passate in chiaro; un'analisi sintetica dei primi pacchetti di rete intercettati ha consentito di risalire ai clienti delle email di conferma dell'attivazione dell'account SKY ECC compreso il numero IMEI, il numero seriale del telefono attivato, l'identificativo SK YECC, ecc.). Per vedere i messaggi degli utenti e i loro metadati passa in forma crittografata …».

Le indagini svolte in Francia, comunque, hanno permesso di svelare gradualmente il meccanismo di funzionamento dell'infrastruttura utilizzata per le comunicazioni man mano che gli investigatori penetravano in essa, appurando i complessi sistemi di crittografia adoperati negli scambi di flussi dati tra i criptofonini e i server utilizzati dalla società.

Nel prosieguo dell'attività investigativa, nel dicembre del 2020, è stato emesso un ulteriore provvedimento di autorizzazione, questa volta dal giudice istruttore di Parigi, con cui è stato impiantato un programma informatico ("*un dispositif de captation de données sur le lien externe du serveur*"), che, ancorché inserito sul server, è servito per cogliere la chiave di cifratura presente in ciascun apparecchio telefonico. A questo provvedimento, nel febbraio 2021, ha fatto seguito un altro provvedimento, sempre del giudice istruttore di Parigi, per l'installazione di un secondo "*dispositif de captation de données*".

Solo a questo punto, acquisite grazie alle intercettazioni le chiavi di cifratura che erano conservate nei *server* e recuperati a mezzo di *trojan* gli algoritmi di decodifica che erano riposti nei criptofonini, la polizia giudiziaria francese ha potuto decodificare i messaggi già registrati e apprendere il significato di quelli che intervenivano successivamente.

In seguito, il 9 marzo 2021, la polizia giudiziaria ha eseguito una operazione su base internazionale, così rendendo pubblica l'avvenuta violazione del sistema criptato, con l'accesso ai "*flussi di informazione di oltre 70.000 utenti*".

In questa data è stato eseguito il sequestro dei server della società OVH, su cui il provider del servizio Sky ECC conservava copia della cronologia delle conversazioni intrattenute. Di tali server è stata fatta copia forense ed il loro contenuto è stato decrittato, così creando un archivio di conversazioni "in chiaro".

La sintetica descrizione dell'operazione che ha riguardato *Sky Ecc*, comunque, dimostra chiaramente le conseguenze di una attività che riguardi il server usato per le comunicazioni: è stata svolta una intercettazione "massiva", che ha posto dubbi sul piano del rispetto dei diritti delle persone coinvolte, rispetto alla quale il recupero della proporzionalità dell'ingerenza sui diritti individuali è intervenuta nel momento della selezione del materiale utile come prova nel processo penale.

7. La complessità della ricerca del corretto bilanciamento tra i diritti confliggenti si coglie chiaramente da una risoluzione del Consiglio dell'Unione europea. Il 14 dicembre 2020, infatti, è stata adottata la **risoluzione sulla crittografia**, intitolata "*La sicurezza attraverso la crittografia e nonostante la crittografia*".

In tale atto è stato sottolineato il sostegno del Consiglio allo sviluppo, all'attuazione e all'utilizzo di una crittografia forte quale strumento necessario per tutelare i diritti fondamentali e la sicurezza digitale dei cittadini, dei governi, dell'industria e della società.

Il Consiglio, al tempo stesso, ha rilevato **la necessità di garantire che le autorità di contrasto e giudiziarie competenti siano in grado di esercitare i loro poteri**, online e offline, **per proteggere la società e i cittadini**, osservando che le autorità di contrasto e giudiziarie dipendono in misura crescente dall'accesso alle prove elettroniche per combattere efficacemente il terrorismo, la criminalità organizzata, gli abusi sessuali su minori e una serie di altre forme di ciber-criminalità e di reati favoriti dall'informatica. L'accesso alle comunicazioni elettroniche, pertanto, è essenziale per il successo delle attività di contrasto e della giustizia penale nel ciberspazio. Tuttavia, **ci sono casi in cui la crittografia rende estremamente difficile o praticamente impossibile l'accesso alle prove e la relativa analisi**. Ed allora «È di fondamentale importanza tutelare il carattere privato e la sicurezza delle comunicazioni attraverso la crittografia e, nel contempo, **preservare la possibilità per le autorità competenti nel settore della sicurezza e della giustizia penale di accedere legalmente ai dati pertinenti per scopi legittimi e chiaramente definiti,** nell'ambito della lotta contro le forme gravi di criminalità e/o la criminalità organizzata e il terrorismo, anche nel mondo digitale, e nel rispetto dello Stato di diritto».

È indispensabile intraprendere azioni per «rispettare attentamente **l'equilibrio tra tali interessi e i principi di necessità, proporzionalità e sussidiarietà**».

In questa prospettiva l'UE si sta adoperando per instaurare un dibattito attivo con l'industria del settore tecnologico, coinvolgendo in modo diretto la ricerca, il mondo accademico, l'industria, la società civile e altre parti interessate, al fine di trovare **il giusto equilibrio** tra la continuità dell'utilizzo di una tecnologia crittografica forte e la garanzia dei poteri delle autorità di contrasto e giudiziarie affinché possano operare alle stesse condizioni del mondo *offline*. Le potenziali soluzioni tecniche dovranno rispettare la vita privata e i diritti fondamentali e preservare il valore che il progresso tecnologico apporta alla società.