CLASSIFICAZIONE

ART. 8 CEDU - DIRITTO ALLA RISERVATEZZA – CONSERVAZIONE DEI DATI DI COMUNICAZIONI VIA INTERNET – DECRIPTAZIONE DI MESSAGGISTICA END TO END – ACCESSO DELLE AUTORITA' SU BASE GENERALIZZATA E SENZA ADEGUATE GARANZIE – VIOLAZIONE DELL'ART. 8.

PRONUNCIA SEGNALATA

Corte E.D.U., 13 febbraio 2024, caso *Podchasov c. Russia*, n. 33696/19

RIFERIMENTI NORMATIVI

CONVENZIONE EDU, artt. 8 e 13

RIFERIMENTI GIURISPRUDENZIALI

Yüksel Yalçınkaya c. Türkiye [GC], 26 settembre 2023; *Ekimdzhiev e altri c. Bulgaria*, 11 gennaio 2022; *Big Brother Watch e altri c. Regno Unito* [GC], 25 maggio 2021; *P.N. c. Germany*, 11 giugno 2020; *Breyer c. Germania*, 30 gennaio 2020; *Catt c. Regno Unito*, 24 gennaio 2019; *Roman Zakharov c. Russia*, [GC], 2015; *Uzun c. Germany*, CEDU 2010; *Delfi AS c. Estonia* [CG], CEDU 2015; *Centro per le risorse giuridiche per conto di Valentin Câmpeanu c. Romania* [GC], CEDU 2014; *K.U. c. Finlandia*, 2008; S*. e Marper c. Regno Unito* [GC], 2008;

ABSTRACT

Il ricorrente, utente dell'applicazione di messaggistica "Telegram", ha lamentato violazione dell'art. 8 e dell'art. 13 CEDU con riferimento alla normativa nazionale russa che ***impone al fornitore di servizi*** *e agli organizzatori di comunicazioni Internet di conservare i dati delle comunicazioni per tre anni e il loro contenuto fino a sei mesi e di comunicare alle forze dell'ordine e alle autorità di pubblica sicurezza i dati per la decrittazione dei messaggi conservati.*

La Corte ha ritenuto ***che il mantenimento di tutte le comunicazioni via Internet*** *degli utenti,* ***l'accesso diretto dei servizi di sicurezza ai dati memorizzati senza adeguate garanzie*** *contro gli abusi e* ***l'obbligo di decrittazione delle comunicazioni criptate, applicato a quelle criptate end-to-end, non può essere considerato necessario in una società democratica****.*

La Corte ha ravvisato una violazione dell'articolo 8 della Convenzione, poiché la normativa interna russa consente alle autorità pubbliche di accedere, su base generalizzata e senza garanzie sufficienti, al contenuto delle ***comunicazioni elettroniche come sopra conservate****; ha ritenuto, in particolare, che essa pregiudica l'essenza stessa del diritto al rispetto della vita privata*

e che lo Stato convenuto ha oltrepassato qualsiasi margine di apprezzamento accettabile al riguardo.

Infine, la Corte ha ritenuto non necessario esaminare la denunciata violazione dell'articolo 13 della Convenzione, per essere qualsiasi danno morale subito dal ricorrente soddisfatto con l'accertamento di una violazione.

IL CASO

Il caso riguarda **l'obbligo**, previsto dalla legge russa, per gli "**organizzatori di comunicazioni *on line***" **di conservare** tutti i dati per un anno e il contenuto di tutte le comunicazioni per sei mesi, nonché quello di esibire tali dati alle pubbliche autorità nelle circostanze specificate dalla legge, in uno con le informazioni necessarie per decifrare i messaggi elettronici, ove criptati.

In qualità di gestore *on line*, iscritto in apposito registro, la polizia federale russa ha chiesto nel 2017 a "***Telegram*"** di render note e inviare le informazioni tecniche per decrittare le comunicazioni di alcuni utenti *Telegram* per finalità di lotta al terrorismo (con invio di un indirizzo IP, di un numero di porta e dei dati relativi alle chiavi [di cifratura], necessari e sufficienti a decrittare una comunicazione) sulla base di **sei autorizzazioni** rilasciate da un tribunale. *Telegram Messenger* ha rifiutato di eseguire l'ordine di divulgazione, sostenendo che era tecnicamente impossibile farlo senza creare una *backdoor* che avrebbe indebolito il meccanismo di crittografia per tutti gli utenti, atteso che i sei utenti per i quali erano stati emessi gli ordini avevano attivato la funzione "*chat* segreta" e utilizzato la crittografia *end-to-end*. La società veniva multata dal tribunale distrettuale di Meshchanskiy di Mosca il 12 dicembre 2017 e, con sentenza del 13 aprile 2018, il tribunale distrettuale di Mosca Taganskiy disponeva il blocco dell'applicazione in Russia. Entrambe le sentenze venivano confermate in appello. Il ricorrente e altre trentaquattro persone impugnavano l'ordine di divulgazione dinanzi a un tribunale, sostenendo che la fornitura di chiavi di cifratura avrebbe permesso all'autorità di sicurezza la decrittazione delle comunicazioni di tutti gli utenti senza dover ottenere l'autorizzazione giudiziaria richiesta dalla legge russa, in violazione del diritto al rispetto della vita privata e della riservatezza delle comunicazioni. Il tribunale distrettuale di Meshchanskiy dichiarava inammissibile la denuncia, ritenendo che l'ordine di divulgazione contestato non incidesse sui diritti dei ricorrenti e la decisione era confermata dal tribunale di Mosca in appello; il ricorso per cassazione era dichiarato non ricevibile, per difetto di violazioni rilevanti del diritto sostanziale o procedurale incidenti sull'esito del procedimento e un ulteriore ricorso per cassazione era respinto dalla Corte suprema della Federazione russa. L'applicazione *Telegram Messenger* è ancora disponibile e funzionante in Russia.

LA VIOLAZIONE DELL'ART. 8 CEDU

a) Sull'esistenza dell'interferenza e sul suo ambito di applicazione

La Corte ha ripreso alcuni principi già affermati per ribadire che **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** ai sensi dell'articolo 8 CEDU, a prescindere dall'uso di tali informazioni, pur precisando che, nel valutare se le informazioni personali conservate dalle autorità riguardino uno dei vari aspetti della vita privata, deve tenersi in debito conto il contesto specifico in cui sono state registrate e conservate, la natura dei documenti, il modo in cui sono utilizzate e trattate e i risultati che possono essere ottenuti (con rinvio a *S. e Marper c. il Regno Unito* [GC], nn. 30562/04 e 30566/04, § 67, CEDU 2008).

Nella specie, ha ritenuto che **l'archiviazione da parte del gestore dei contenuti di tutte le comunicazioni del ricorrente e dei relativi dati avesse interferito con il suo diritto al rispetto della vita privata e della corrispondenza** (richiamando *Breyer c. Germania*, n. 50001/12, § 81, 30 gennaio 2020, e *Ekimdzhiev e altri c. Bulgaria*, n. 70078/12, §§ 372 e 373, 11 gennaio 2022), indipendentemente dal fatto che i dati siano stati poi consultati o meno dalle autorità. **Lo stoccaggio, anche se effettuato da privati, é imposto dalla legge, cosicché l'interferenza con il diritto fondamentale va attribuita allo Stato russo** (*Ekimdzhiev e altri* cit., §§ 372 e 375), riguardando non solo la memorizzazione dei dati, ma anche la possibilità per le autorità nazionali di accedervi (richiamando *Breyer*, § 61, e *Ekimdzhiev e altri*, § 376, entrambi citate).

L'impossibilità, poi, di sapere con certezza se l'accesso a quei dati da parte dell'autorità sia avvenuto o meno ha reso opportuno analizzare la questione se vi sia un'interferenza ai sensi dell'articolo 8 per il fatto dell'esistenza stessa di leggi che consentono alle autorità di accedervi.

La Corte ha, dunque, operato un rinvio ai principi già formulati a proposito della normativa russa sull'attività di sorveglianza segreta (vedi *Ekimdzhiev e altri*, cit., § 376) e, segnatamente al caso *Roman Zakharov c. Russia*, [GC], n. 47143/06, §§ 31-33 e 51, ECHR 2015: in quella sede, valutate la natura delle misure, la circostanza che esse riguardavano tutti gli utenti delle reti di comunicazione e la mancanza di rimedi efficaci a livello nazionale per contestarne l'applicazione, la Corte aveva già riconosciuto che ciò costituiva interferenza con la vita privata di un utente.

Proprio come nel caso di specie, in cui il governo ha ammesso che l'accesso alle comunicazioni *Internet* conservate e ai relativi dati di comunicazione è disciplinato dalla medesima legge presa in esame nel caso *Roman Zakharov* , **è la stessa esistenza della normativa a costituire un'ingerenza nell'esercizio dei diritti del ricorrente ai sensi dell'articolo 8**.

Per quanto attiene, poi, **all'obbligo di decrittazione, la Corte ha precisato che l'esame del caso è limitato alle comunicazioni *end-to-end* criptate** (cioè, quanto a *Telegram*, le "*chats*

segrete"), poiché non è stato formulato un motivo di ricorso inerente al sistema di crittografia utilizzato nelle "*chats cloud*". Il richiedente ha sostenuto essere tecnicamente impossibile fornire alle autorità chiavi di cifratura associate a utenti specifici, sicché, **per decrittare le comunicazioni *end to end* cifrate, è necessario forzare la tecnologia di crittografia utilizzata dall'applicazione con misure che non possono essere limitate a individui specifici, ma che colpirebbero tutti gli utenti indiscriminatamente** (argomentazione ripresa dagli argomenti della difesa *Telegram* nel procedimento interno), assunto che la Corte ha ritenuto provato, in mancanza di smentita da parte del governo.

In conclusione, **la Corte ha ritenuto che l'archiviazione delle comunicazioni Internet del ricorrente e dei relativi dati di comunicazione da parte di *Telegram*, il potenziale accesso delle autorità a tali dati e l'obbligo di *Telegram* di decifrarli ove criptati, ai sensi della legge sull'informazione e dei suoi regolamenti di attuazione, costituiscono un'interferenza con i diritti dell'articolo 8 del ricorrente** e poiché, nella specie, i dati personali sono conservati al fine di consentire alle autorità nazionali competenti di effettuare una sorveglianza segreta mirata delle comunicazioni via Internet, le relative questioni devono considerarsi, nella specie, strettamente connesse.

b) Sulla giustificazione della interferenza

b.1) Principi generali

Quanto a tale profilo, la Corte ha rilevato che, sebbene **il caso** riguardasse principalmente il problema della conservazione dei dati personali del ricorrente, esso **andava 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'articolo 8 nei limiti di ciò che è "necessario in una società democratica".**

Ha ribadito che **un'interferenza può essere giustificata** ai sensi dell'articolo 8 § 2 **solo in presenza di determinate condizioni (garanzie), vale a dire**: ove conforme alla legge; se persegua uno o più degli scopi legittimi a cui si riferisce l'articolo 8, § 2; se sia necessaria in una società democratica per raggiungere tale obiettivo, oltre che compatibile con lo Stato di diritto, cosicché la relativa normativa deve essere accessibile alla persona interessata e prevedibile quanto ai suoi effetti.

La necessità di tali garanzie, peraltro, è ancor più sentita allorché si tratti della protezione dei dati personali sottoposti a trattamento automatico e quando essi siano utilizzati a fini di polizia (con richiamo anche, sia pur nel contesto dell'intercettazione di massa delle comunicazioni, a *Big Brother Watch e altri c. Regno Unito* [GC], n. 58170/13, § 330), tenuto anche conto del fatto che la tecnologia è sempre più sofisticata (v. *Uzun c. Germany*, n.

35623/05, § 61, CEDU 2010 (estratti); *Catt c. Regno Unito*, n. 43514/15, §114, 24 gennaio 2019; *Gaughran c. Regno Unito*, n. 45245/15, §86, 13 febbraio 2020).

Quanto alla legge di previsione, in particolare, la Corte ha ricordato quanto sia importante la chiarezza e specificità delle norme quanto all'ambito di applicazione delle misure e alle garanzie minime riguardanti, tra l'altro, la durata, la conservazione, l'uso, l'accesso di terzi, le procedure per preservare l'integrità e la riservatezza dei dati e quelle per la loro distruzione, sì da fornire sufficienti garanzie contro il rischio di abuso e arbitrarietà (anche *P.N. c. Germany*, n. 74440/17, § 62, 11 giugno 2020). Pertanto, **il diritto nazionale dovrebbe 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.**

Ora, **nel caso della sorveglianza segreta**, **i rischi di arbitrarietà sono evidenti**, cosicché, per soddisfare il requisito della "prevedibilità", **la legge nazionale avrebbe dovuto contenere un'indicazione adeguata delle circostanze e delle condizioni di autorizzazione della autorità pubblica a farvi ricorso**. 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**. Inoltre, la riservatezza delle comunicazioni è elemento essenziale del diritto al rispetto della vita privata e della corrispondenza, come previsto dall'articolo 8, 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** (con richiamo a *K.U. c. Finlandia*, n. 2872/02, § 49, CEDU 2008, e *Delfi AS c. Estonia* [CG], n. 64569/09, § 149, CEDU 2015).

b.2) Applicazione dei principi al caso in esame

Nel caso all'esame, la Corte ha ritenuto di esaminare congiuntamente i temi della sussistenza di un motivo legittimo e quello della necessità dell'interferenza in una società democratica e, sul punto, ha ritenuto esistente una cornice legale (legge sull'informazione, codice di procedura penale, legge sulle attività di ricerca operativa) disciplinante la conservazione delle comunicazioni via Internet e l'accesso ai relativi dati da parte delle autorità. Al contempo, ha rilevato che la tecnologia ha notevolmente aumentato la quantità delle comunicazioni che attraversano Internet a livello globale e come si siano moltiplicate le minacce cui sono esposti gli Stati contraenti e i loro cittadini (il riferimento è al terrorismo globale, al traffico di droga e di esseri umani e allo

sfruttamento sessuale dei bambini), minacce che provengono da reti internazionali e da soggetti che hanno accesso a tecnologie sempre più sofisticate che consentono loro di comunicare senza essere scoperti, concludendo nel senso che **le disposizioni normative impugnate perseguono l'obiettivo legittimo di tutelare la sicurezza nazionale, prevenire il disordine e la criminalità e tutelare i diritti e le libertà altrui, dovendosi valutare se il diritto nazionale contenga anche garanzie adeguate ed efficaci per soddisfare i requisiti della "qualità della legge" e della "necessità in una società democratica**".

(a) Memorizzazione dei dati relativi alle comunicazioni via Internet

La Corte ha rilevato che un crescente volume di comunicazioni assume oggi forma digitale e che la normativa interna impone la conservazione automatica e continua dei contenuti di tutte le comunicazioni via Internet per la durata di sei mesi e dei relativi dati per la durata di un anno, per tutti i servizi di comunicazione Internet utilizzati per trasmettere comunicazioni vocali, testuali, visive, sonore, video o altre comunicazioni elettroniche; essa riguarda tutti gli utenti delle comunicazioni via Internet, senza la necessità che costoro siano ragionevolmente sospettati di esser coinvolti in attività criminali o che mettano a rischio la sicurezza nazionale e in assenza di altri motivi per ritenere che la conservazione dei dati possa contribuire alla lotta contro i crimini più gravi o alla protezione della sicurezza nazionale; inoltre, essa riguarda il contenuto di tutte le comunicazioni, di tutti i dati di comunicazione senza limiti territoriali, temporali o legati ai soggetti delle cui comunicazioni si discute. **Si tratta di un obbligo di conservazione estremamente ampio che determina, di conseguenza, un'interferenza eccezionalmente ampia e grave che impone una particolare attenzione quanto alla verifica del secondo requisito (se il diritto interno, cioè, offra garanzie adeguate e sufficienti contro gli abusi).**

(b) Potenziale accesso ai dati memorizzati ai fini della sorveglianza segreta mirata.

Su tale aspetto specifico, la Corte ha ribadito che **l'accesso ai dati nei singoli casi deve essere accompagnato, *mutatis mutandis*, dalle stesse garanzie previste per l'ipotesi della sorveglianza segreta**: nella specie, nonostante il governo abbia confermato la **necessità di un'autorizzazione da parte di un giudice**, la Corte ha rilevato che in Russia le autorità non sono tenute a esibire tale autorizzazione al fornitore del servizio prima di ottenere l'accesso alle comunicazioni di una persona, poiché il gestore è tenuto a installare apparecchiature che garantiscano alle autorità l'accesso diretto a distanza ai dati memorizzati. **Manca, nel sistema 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**. Come rilevato nel caso *Roman Zakharov*, a proposito delle intercettazioni di comunicazioni telefoniche mobili, **un sistema come quello russo (nel quale i servizi di sicurezza possono accedere**

alle comunicazioni e ai dati memorizzati su Internet senza un'autorizzazione giudiziaria preventiva) è particolarmente soggetto ad abusi e, come già osservato a proposito di quel diverso caso, la normativa russa non soddisfa il requisito della "qualità della legge", poiché non prevede garanzie adeguate ed efficaci contro l'arbitrarietà e il rischio di abusi, non contenendo "l'interferenza" nei limiti di quanto "necessario in una società democratica"; non sono definite con sufficiente chiarezza le situazioni nelle quali le autorità sono autorizzate a ricorrere a misure di sorveglianza segrete per individuare, prevenire e indagare su reati penali o proteggere i cittadini russi, la sicurezza militare, economica o ecologica; il procedimento di autorizzazione non è in grado di garantire che le misure di sorveglianza segrete siano ordinate solo quando "necessario in una società democratica"; **il controllo delle intercettazioni non è esercitato secondo i parametri necessari della indipendenza e competenza**; **i rimedi** apprestati sono **inefficaci,** poiché in nessun momento è prevista la notifica o un effettivo accesso ai relativi documenti. Secondo la Corte, non vi sono motivi per giungere a diversa conclusione nel caso all'esame, poiché **la normativa nazionale non prevede garanzie adeguate e sufficienti contro gli abusi relativamente all'accesso delle autorità alle comunicazioni via Internet e ai relativi dati conservati dal gestore.**

(c) Obbligo legale di decriptare le comunicazioni

Infine, per quanto riguarda **il trattamento dei dati criptati** (e il connesso tema dell'obbligo di esibizione alle autorità di sicurezza delle informazioni necessarie per la decrittazione), la Corte ha osservato come alcuni soggetti giuridici internazionali abbiano sostenuto che **la crittografia fornisce efficaci garanzie tecniche contro l'accesso illegale al contenuto delle comunicazioni** e viene largamente utilizzata come mezzo per proteggere il diritto al rispetto della vita privata e della corrispondenza *on line*, contribuendo – nell'era digitale – a garantire il godimento di diritti fondamentali, come la libertà di espressione, aiutando i cittadini e le imprese a difendersi dagli abusi delle tecnologie dell'informazione, come l'*hacking*, il furto di identità e dei dati personali, la frode e la divulgazione impropria di informazioni riservate. Di ciò deve tenersi conto nel valutare le misure che possano rendere la crittografia meno efficace, posto che, come già rilevato, per consentire la decrittazione delle comunicazioni protette da crittografia *end-to-end*, come le *chats* segrete di *Telegram*, sembra non si possa evitare un indebolimento del sistema per tutti gli utenti indiscriminatamente, anche per coloro che non rappresentano una minaccia ad un legittimo interesse del governo. Come affermato da molti esperti del settore, **l'indebolimento della crittografia mediante creazione di *backdoors* renderebbe 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.**

La Corte prende atto che la crittografia può essere utilizzata anche dai criminali e quindi interferire con indagini penali (operando un rinvio a *Yüksel Yalçınkaya c. Türkiye* [GC], n. 15669/20, § 312, 26 settembre 2023), ma rileva, a tal proposito, come siano state indicate "soluzioni alternative alla decrittazione senza indebolire i meccanismi di protezione, sia nella legislazione che attraverso la continua evoluzione tecnologica" (si vedano la dichiarazione comune di Europol e dell'Agenzia dell'Unione europea per la sicurezza informatica del 20 maggio 2016; il paragrafo 24 della Relazione sul diritto alla privacy nell'era digitale da parte dell'Alto Commissariato delle Nazioni Unite per i Diritti Umani, del 4 agosto 2022, A/HRC/51/17, ma anche la spiegazione fornita dai terzi intervenuti, cioè *European Information Society Institute* – EISI – e *Privacy International*, i cui contributi sul tema sono stati riportati ai §§ 47 e 48). E conclude nel senso che, **nel caso in esame, l'obbligo legale del gestore di decrittare le comunicazioni crittografate *end-to-end* ha comportato il rischio di indebolire il meccanismo di cifratura per tutti gli utenti e non è, pertanto, proporzionato agli obiettivi legittimi perseguiti.**

(d) Conclusioni

La Corte ha ritenuto che **la normativa impugnata che prevede il mantenimento delle comunicazioni via Internet di tutti gli utenti, l'accesso diretto dei servizi di sicurezza ai dati memorizzati senza adeguate garanzie contro gli abusi e l'obbligo di decrittare le comunicazioni cifrate, applicato alle comunicazioni *end-to-end*, non può essere considerato necessario in una società democratica**. Si è rilevata, quindi, la violazione dell'art. 8 CEDU, ritenendo non necessario pronunciarsi separatamente sulla ricevibilità e sul merito della denuncia ai sensi dell'articolo 13 della Convenzione (sotto il profilo del difetto di un ricorso interno effettivo), avuto riguardo ai fatti, alle osservazioni delle parti e alle proprie conclusioni ai sensi dell'articolo 8 (rinviando a *Centro per le risorse giuridiche per conto di Valentin Câmpeanu c. Romania* [GC], n. 47848/08, § 156, CEDU 2014 per respingere la domanda di condanna al danno non patrimoniale, l'accertamento della violazione costituendo di per sé sufficiente forma di risarcimento dello stesso.

Su tema collegato, le **Sezioni Unite**, con pronuncia del **29.2.2024**, della quale si è diffusa informazione provvisoria, hanno deciso, tra l'altro, che il trasferimento all'Autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'Autorità giudiziaria estera in un proprio procedimento penale, rientra nell'acquisizione di atti di un procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 7 disp. att. cod. proc. pen., 238, 270 cod. proc. pen. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE. Fatto salvo il vaglio di inutilizzabilità da parte del giudice.

APPENDICE

1. LA DISSENTING OPINION SULL'ART. 13 CEDU

1. Deve segnalarsi una ***dissenting opinion*** limitatamente alla denunciata violazione dell'art. 13 della Convenzione: il giudice Serghides, richiamando il parere già formulato in altri procedimenti, ha ribadito che la Corte ha il dovere di esaminare la domanda anche sotto tale profilo, altrimenti il diritto del ricorrente a un ricorso effettivo non godrebbe di tutela, secondo i principi di effettività e indivisibilità dei diritti e del diritto a un ricorso individuale; la violazione accertata è grave e il ricorso non può essere rigettato con frasi stereotipate come "*l'accertamento di una violazione costituisce di per sé una giusta soddisfazione di qualsiasi danno morale subito dal ricorrente*".

2. I PARERI DEI TERZI INTERVENUTI NEL GIUDIZIO

2. Vanno poi segnalati, per l'attualità del tema, **i pareri dei terzi intervenuti**.

A) Secondo **EISI** (*European Information Society Institute*) la crittografia *end-to-end* é un meccanismo di autodifesa contro ogni forma di controllo [per mezzo di una chiave "pubblica" qualsiasi messaggio ("testo in chiaro") viene tradotto in una combinazione apparentemente casuale di lettere, numeri o simboli ("testo cifrato"); solo i mittenti e i destinatari possono vedere il testo in chiaro, mentre gli estranei solo quello cifrato e la conversione in chiaro avviene sul dispositivo del ricevitore; inoltre, il gestore del servizio di messaggistica non ha mai accesso alla chiave privata o al messaggio originale in chiaro]. L'ordine di esibizione da parte della polizia federale ha colpito indiscriminatamente tutti gli utenti di *Telegram*, cosicché il suo rispetto imporrebbe a *Telegram* di memorizzare centralmente le chiavi "private", ma così facendo il gestore non potrebbe più fornire legalmente servizi crittografati *end-to-end* ai propri utenti. Ha illustrato quali sono le finalità legittime del sistema (garantire l'integrità e la sicurezza dei messaggi durante la trasmissione e offrire protezione alle persone vulnerabili, come giornalisti, *leaders* dell'opposizione o vittime di abusi informatici), osservando come **vi sia una forte connessione tra crittografia e diritti umani**, in particolare quelli di cui agli articoli 8 e 10 della Convenzione e come l'introduzione di *backdoors* nelle comunicazioni criptate comporti rischi per la sicurezza, esponendo la generalità degli utenti anche al rischio di esser fatti oggetto di attività criminali al fine di consentire indagini nei confronti di un ristretto numero di soggetti, considerata l'esistenza di alternative meno invasive e mirate alla lotta contro la criminalità e alla protezione della sicurezza nazionale, sebbene le stesse siano meno economiche per lo Stato e più difficili da utilizzare su larga scala.

B) ***Privacy International*** ha descritto il sistema *end-to-end*, rilevando che sia la crittografia che la decrittazione dei messaggi inviati e ricevuti si verificano sui dispositivi degli utenti, solo i destinatari (e nemmeno il fornitore del servizio) avendo accesso al contenuto del messaggio, poiché la chiave "privata" utilizzata per decifrare il messaggio da parte del destinatario è conservata sul dispositivo del destinatario e non è condivisa con altri; ha sostenuto che la normativa impugnata si pone in contrasto con l'obbligo di tutela della riservatezza e della privacy e con quello di garantire l'integrità dei sistemi di comunicazione, costringendo il gestore ad apportare modifiche radicali al *software* che indeboliscono il sistema di crittografia, attraverso la creazione di *backdoors* che, una volta individuate, potrebbero essere sfruttate anche da criminali.

C) Secondo una dichiarazione congiunta di **Europol** e dell'**Agenzia dell'Unione europea per la sicurezza informatica** (ENISA) del 20 maggio 2016, sull'indagine penale rispettosa della protezione dei dati nel XXI secolo, l'intercettazione di dati criptati potrebbe essere considerata proporzionale con riguardo a un sospettato determinato, laddove la violazione indiscriminata del sistema di crittografia potrebbe determinare danni collaterali. Secondo tale dichiarazione, è necessario porre l'attenzione sull'accesso indiscriminato ai dati. Dal momento che, ad un certo punto, la comunicazione criptata per essere utile deve essere decrittata, potrebbero impiegarsi **rimedi alternativi (operazioni sotto copertura, soggetti infiltrati in gruppi criminali, sequestro degli apparecchi e analisi forensi sul contenuto, intercettazioni durante l'utilizzo dei dispositivi da parte dei sospettati).** Tuttavia, ci sono casi nei quali non vi è altra alternativa se non la decrittazione. La progettazione e realizzazione dei sistemi di crittografia non sono perfette e la decrittazione è uno strumento sempre meno adatto ad essere utilizzato per finalità di contrasto alla criminalità. Di qui le proposte per utilizzare *backdoors* obbligatorie per indebolire la crittografia che, da un lato, darebbe agli investigatori l'accesso legale ai dati per perseguire gravi crimini o minacce terroristiche, dall'altro, aumenterebbe le possibilità di commettere abusi, consentendo agli stessi criminali di aggirare un sistema indebolito e fare uso delle conoscenze acquisite sulla crittografia per sviluppare nuove soluzioni senza impiego di *backdoor* o *key escrow*.

D) Il **Comitato europeo per la protezione dei dati** (*European data Protection Board* - EDPB) e il **Garante europeo della protezione dei dati** hanno adottato il **parere comune n. 4/2022** sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per prevenire e combattere gli abusi sessuali sui minori. In quella sede, si è affermato che le misure che consentono alle pubbliche autorità un accesso generalizzato al contenuto delle comunicazioni al fine di investigare tali crimini, hanno maggiori probabilità di incidere sull'essenza dei diritti garantiti dagli articoli 7 e 8 della Carta, esprimendo dubbi quanto all'efficienza delle misure di

blocco e ritenendo che **l'obbligo per i fornitori di servizi Internet di decrittare le comunicazioni *on line* al fine di bloccare quelle riguardanti materiale inerente ad abusi sessuali su minori sarebbe sproporzionato,** evidenziando come le tecnologie di crittografia contribuiscano in maniera importante al rispetto della vita privata e alla riservatezza delle comunicazioni, alla libertà di espressione, nonché alla crescita dell'economia digitale che fa affidamento sul livello di affidabilità e riservatezza che tali sistemi garantiscono. Suggeriscono la ricerca di altri metodi onde poter bilanciare il diritto dei consociati di disporre di canali sicuri e riservati per le loro comunicazioni con la lotta all'abuso di tali sistemi, evidenziando la necessità di affermare con chiarezza nella proposta di Regolamento che nulla possa essere interpretato come proibizione o indebolimento del sistema di crittografia. Imporre ai gestori di trattare i dati relativi alle comunicazioni elettroniche per scopi diversi dalla fornitura del servizio o imporre loro l'obbligo di inviare tali dati a terzi comporterebbe il rischio di avere un servizio di crittografia meno sicuro, minando la protezione di diritti fondamentali dei cittadini europei. Deve, quindi, essere adeguatamente considerato che le tecnologie (indicate nella relazione di valutazione d'impatto che accompagna la proposta) per aggirare la riservatezza garantita dalla crittografia *end-to-end* introdurrebbero lacune in materia di sicurezza. La soluzione contenuta nella "Proposta" di lasciare al fornitore interessato la scelta delle tecnologie da utilizzare per conformarsi agli ordini dell'autorità non dovrebbe essere intesa come un incoraggiamento o uno scoraggiamento dell'uso di una determinata tecnologia, ma resta il fatto che **alcuni ordini di controllo sono strutturalmente incompatibili con il sistema di crittografia *end-to-end* (che costituisce, allo stato, la miglior forma di protezione tecnologica per la riservatezza)** e ciò può diventare un forte disincentivo al suo impiego, con ricadute assai gravi sulla libertà di espressione e sul legittimo uso privato dei servizi di comunicazione elettronica.